Amazon Elastic Compute Cloud

用户指南（适用于 Linux 实例）



Amazon Elastic Compute Cloud: 用户指南（适用于 Linux 实例）

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆或者贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是 Amazon EC2？ ... 1
Amazon EC2 的功能 ... 1
如何开始使用 Amazon EC2 ... 1
相关服务 ... 2
访问 Amazon EC2 ... 3
Amazon EC2 定价 ... 3
PCI DSS 合规性 ... 4
设置 ... 5
注册一个 Amazon Web Services 账户 ... 5
保护 IAM 用户 ... 5
创建密钥对 ... 5
创建安全组 ... 6
入门教程 ... 9
概览 ... 9
先决条件 ... 10
步骤 1：启动实例 ... 10
步骤 2：连接到您的实例 ... 11
步骤 3：清除您的实例 ... 11
后续步骤 ... 12
最佳实践 ... 13
教程 ... 15
在 Amazon Linux 2023 上安装 LAMP ... 15
步骤 1：准备 LAMP 服务器 ... 16
步骤 2：测试 LAMP 服务器 ... 18
步骤 3：确保数据库服务器的安全 ... 20
步骤 4：(可选) 安装 phpMyAdmin ... 20
问题排查 ... 23
相关主题 ... 23
在 Amazon Linux 2 上安装 LAMP ... 24
步骤 1：准备 LAMP 服务器 ... 24
步骤 2：测试 LAMP 服务器 ... 27
步骤 3：确保数据库服务器的安全 ... 28
步骤 4：(可选) 安装 phpMyAdmin ... 29
问题排查 ... 32
相关主题 ... 32
在 Amazon Linux AMI 上安装 LAMP ... 33
步骤 1：准备 LAMP 服务器 ... 33
步骤 2：测试 Lamp 服务器 ... 36
步骤 3：确保数据库服务器的安全 ... 37
步骤 4：(可选) 安装 phpMyAdmin ... 38
问题排查 ... 41
相关主题 ... 42
在 Amazon Linux 2023 上配置 SSL/TLS ... 42
先决条件 ... 43
步骤 1：在服务器上启用 TLS ... 43
步骤 2：获取 CA 签名的证书 ... 45
步骤 3：测试和强化安全配置 ... 49
问题排查 ... 51
证书自动化：在 Amazon Linux 2023 上将 Let's Encrypt 与 Certbot 结合使用 ... 52
在 Amazon Linux 2 上配置 SSL/TLS ... 55
先决条件 ... 56
步骤 1：在服务器上启用 TLS ... 43
步骤 2：获取 CA 签名的证书 ... 58
步骤 3：测试和强化安全配置 ... 62

问题排查 64
证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 65
使用 Amazon Linux AMI 配置 SSL/TLS 68
先决条件 69
步骤 1：在服务器上启用 TLS 69
步骤 2：获取 CA 签名的证书 70
步骤 3：测试和强化安全配置 75
问题排查 76
增加 Amazon EBS 卷的大小 77
第 1 步：启动一个带有附加卷的实例 77
第 2 步：使数据卷可供使用 80
第 3 步：增加数据卷的大小 81
第 4 步：扩展文件系统 83
第 5 步：清除 84
在 Amazon Linux 2023 上托管 WordPress 博客 85
先决条件 85
安装 WordPress 85
后续步骤 92
帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪 92
在Amazon Linux 2 上托管 WordPress 博客 93
先决条件 94
安装 WordPress 94
后续步骤 99
帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪 100
Amazon Machine Images 101
使用 AMI 101
创建您自己的 AMI 102
购买、共享和出售 AMI 102
注销您的 AMI 102
Amazon Linux 2 和 Amazon Linux AMI 103
AMI 类型 103
启动许可 103
根设备存储 103
虚拟化类型 106
启动模式 107
启动 实例 108
AMI 启动模式参数 110
实例类型启动模式 111
实例启动模式 111
操作系统启动模式 112
设置 AMI 启动模式 113
UEFI 变量 116
查找 Linux AMI 116
使用 Amazon EC2 控制台查找 Linux AMI 117
使用 Amazon CLI 查找 AMI 118
使用 Systems Manager 查找最新的 Amazon Linux AMI 118
使用 Systems Manager 参数查找 AMI 119
共享 AMI 121
经过验证的提供商 122
查找共享 AMI 122
将 AMI 设为公用 124
与特定 Amazon 账户共享 AMI 126
取消与您的账户共享 AMI 128
使用书签 129
共享 Linux AMI 指导原则 130
付费 AMI 133
出售您的 AMI 134

查找付费 AMI 134
购买付费 AMI 135
获取实例的产品代码 135
使用付费支持 136
付费和支持 AMI 的账单 136
管理您的 Amazon Web Services Marketplace 订阅 136
AMI 周期 137
创建 AMI 137
修改 AMI 172
复制 AMI 172
存储和还原 AMI 178
弃用 AMI 183
注销您的 AMI 188
从回收站恢复 AMI 193
自动化 EBS 支持的 AMI 生命周期 196
将加密与 EBS 支持的 AMI 结合使用 196
启动实例场景 197
映像复制场景 199
监控 AMI 事件 200
AMI 事件 201
创建 Amazon EventBridge 规则 203
了解 AMI 账单 204
AMI 账单字段 205
查找 AMI 账单信息 206
验证账单上的 AMI 费用 208
Amazon Linux 208
Amazon Linux 可用性 208
连接到 Amazon Linux 实例 209
识别 Amazon Linux 映像 209
Amazon 命令行工具 210
程序包存储库 211
Extras 库 (Amazon Linux 2) 213
Amazon Linux 2 支持的内核 213
访问源软件包以获取参考信息 214
cloud-init 215
订阅 Amazon Linux通知 216
在本地运行 Amazon Linux 2 218
内核实时修补 221
用户提供的内核 226
HVM AMIs (GRUB) 227
半虚拟化 AMIs (PV-GRUB) 227
配置 MATE 桌面连接 231
先决条件 232
配置 RDP 连接 232
AMI 限额 233
请求增加 AMI 的限额 234
实例 235
实例和 AMI 235
实例 236
AMI 237
实例类型 238
实例类型名称 238
可用实例类型 239
硬件规格 245
AMI 虚拟化类型 246
基于 Nitro 系统构建的实例 246
联网和存储功能 247

实例限制 252
通用型 252
计算优化 305
内存优化 322
存储优化 347
加速计算 358
查找 实例类型 396
获取建议 397
更改实例类型 399
实例购买选项 404
确定实例生命周期 405
按需型实例 406
Reserved Instances 408
计划实例 447
Spot Instances 448
Dedicated Hosts 504
Dedicated Instances 533
On-Demand Capacity Reservations 538
实例生命周期 570
实例启动 571
实例停止和启动（仅限 Amazon EBS 支持的实例） 571
实例休眠（仅限 Amazon EBS 支持的实例） 572
实例重启 572
实例指令引退 572
实例终止 572
重启、停止、休眠和终止之间的区别 573
启动 574
停止和启动 610
休眠 616
重启 631
停用 632
终止 634
恢复 640
连接 644
连接到您的实例 644
将实例连接到资源 673
配置实例 699
常见配置方案 699
管理软件 699
管理用户 705
处理器状态控制 707
输入/输出调度器 713
设置时间 714
优化 CPU 选项 721
更改主机名 744
设置动态 DNS 747
启动时运行命令 748
实例元数据和用户数据 754
Amazon EI 808
识别 实例 808
检查 实例身份文档 809
检查系统 UUID 809
检查系统虚拟机生成标识符 809
队列 814
EC2 Fleet 814
EC2 队列限制 815
可突增性能实例 815

EC2 队列请求类型 815
EC2 队列配置策略 832
使用 EC2 队列 853
Spot 队列 871
Spot 队列请求类型 871
Spot 实例集配置策略 871
使用 Spot 队列 892
Spot 队列的 CloudWatch 指标 912
Spot 队列的自动扩展 914
监控队列事件 920
EC2 队列 事件类型 920
Spot 队列事件类型 924
创建 EventBridge 规则 929
教程 935
教程：将 EC2 队列 与实例权重一起使用 936
教程：使用 EC2 队列 并将按需作为主容量 938
教程：使用目标容量预留启动按需实例 939
教程：将 Spot 实例集与实例权重一起使用 943
示例配置 945
EC2 队列 示例配置 945
Spot 队列示例配置 958
队列配额 970
请求增加目标容量配额 971
显示器 972
自动和手动监控 972
自动监控工具 973
手动监控工具 974
监控最佳实践 974
监控实例状态 974
实例状态检查 975
状态更改事件 979
计划的事件 981
使用 CloudWatch 监控您的实例 1000
启用详细监控 1001
列出可用的指标 1002
获取指标的统计数据 1012
绘制指标图形 1019
创建警报 1020
创建停止、终止、重启或恢复实例的警报 1021
使用 EventBridge 自动执行 1029
Amazon EC2 事件类型 1029
监控内存和磁盘指标 1030
使用 CloudWatch 代理收集指标 1030
已弃用：使用 CloudWatch 监控脚本收集指标 1030
使用 Amazon CloudTrail 记录 API 调用。 1037
CloudTrail 中的 Amazon EC2 和 Amazon EBS 信息 1037
了解 Amazon EC2 和 Amazon EBS 日志文件条目 1037
审核通过 EC2 Instance Connect 连接的用户 1038
联网 1040
区域和可用区 1040
区域 1041
可用区 1045
Local Zones 1048
Wavelength 区域 1050
Amazon Outposts 1052
实例 IP 寻址 1053
私有 IPv4 地址 1053

公有 IPv4 地址 1054
弹性 IP 地址 (IPv4) 1055
IPv6 地址 1055
使用实例的 IPv4 地址 1055
使用实例的 IPv6 地址 1057
多个 IP 地址 1059
EC2 实例主机名 1066
实例主机名类型 1067
EC2 主机名的类型 1067
查看资源名称和 IP 名称的位置 1068
如何决定是选择资源名称还是 IP 名称 1069
修改主机名类型和 DNS 主机名配置 1069
自带 IP 地址 1070
BYOIP 定义 1071
要求和配额 1071
载入先决条件 1072
载入 BYOIP 1077
使用地址范围 1079
验证 BYOIP 1080
分配前缀 1083
分配前缀的基础知识 1083
前缀的注意事项和限制 1084
使用前缀 1084
弹性 IP 地址 1094
弹性 IP 地址定价 1094
弹性 IP 地址基本信息 1094
使用弹性 IP 地址 1095
弹性 IP 地址限制 1104
网络接口 1104
网络接口基础知识 1105
网卡 1106
每种实例类型的每个网络接口的 IP 地址数 1107
使用网络接口 1129
配置网络接口的最佳实践 1136
网络接口方案 1138
请求者托管的网络接口 1140
网络带宽 1141
可用实例带宽 1141
监控实例带宽 1142
增强联网 1142
增强联网支持 1143
在实例上启用增强联网 1143
Elastic Network Adapter (ENA) 1143
ENA Express 1152
Intel 82599 VF 1158
操作系统优化 1164
网络性能指标 1164
对 ENA 进行问题排查 1169
置放群组 1177
置放群组策略 1177
置放群组规则和限制 1179
使用置放群组 1180
共享置放群组 1188
Amazon Outposts 上的置放群组 1191
网络 MTU 1192
巨型帧 (9001 MTU) 1192
路径 MTU 发现 1193

查看两个主机之间的路径 MTU 1193
在您的 Linux 实例上检查并设置 MTU 1194
问题排查 1194
Virtual Private Cloud 1194
您的默认 VPC 1195
创建额外的 VPC 1195
从您的实例访问互联网 1196
对您的实例进行 SSH 访问 1196
EC2-Classic 1196
检测支持的平台 1197
EC2-Classic 中提供的实例类型 1197
EC2-Classic 和 VPC 中的实例之间的区别 1198
在 EC2-Classic 与 VPC 之间共享和访问资源 1200
ClassicLink 1201
从 EC2-Classic 迁移到 VPC 1211
安全性 1219
基础设施安全性 1219
网络隔离 1219
物理主机上的隔离 1220
控制网络流量 1220
故障恢复能力 1220
数据保护 1221
Amazon EBS 数据安全 1221
静态加密 1222
传输中加密 1222
Identity and Access Management 1223
对您的实例的网络访问 1224
Amazon EC2 权限属性 1224
IAM 和 Amazon EC2 1224
IAM policy 1225
Amazon 托管策略 1276
IAM 角色 1277
网络访问 1287
密钥对 1289
创建密钥对 1290
标记公有密钥 1294
描述公有密钥 1296
删除公有密钥 1300
在实例上添加或删除公有密钥 1301
验证密钥 1302
安全组 1303
安全组规则 1304
连接跟踪 1306
默认和自定义安全组 1308
使用安全组 1309
针对不同使用案例的安全组规则 1315
Amazon PrivateLink 1319
创建接口 VPC 终端节点 1319
创建端点策略 1319
更新管理 1320
合规性验证 1320
存储 1322
Amazon EBS 1323
Amazon EBS 的功能 1324
EBS 卷 1324
EBS 快照 1368
Amazon Data Lifecycle Manager 1448

EBS 数据服务 1493
EBS 卷和 NVMe 1518
EBS 优化 1522
EBS 性能 1550
EBS CloudWatch 指标 1563
EBS EventBridge 事件 1569
实例存储 1579
实例存储生命周期 1580
实例存储卷 1581
添加实例存储卷 1592
SSD 实例存储卷 1596
实例存储交换卷 1597
优化磁盘性能 1599
文件存储 1600
Amazon S3 1600
Amazon EFS 1602
Amazon FSx 1603
实例卷限制 1607
Nitro 系统卷限制 1607
特定于 Linux 的卷限制 1607
带宽与容量 1607
根设备卷 1608
根设备存储概念 1608
按根设备类型选择 AMI 1609
确定实例的根设备类型 1610
将根卷更改为保留 1611
更改根卷的初始大小 1613
设备名称 1614
可用设备名称 1614
设备名称注意事项 1615
块设备映射 1615
块储存设备映射的概念 1615
AMI 块储存设备映射 1618
实例块储存设备映射 1620
撕裂写防护 1624
定价 1624
支持的块大小和块边界对齐 1624
要求 1624
检查撕裂写防护支持和配置 1625
配置您的软件堆栈以防止撕裂写 1626
资源和标签 1627
回收站 1627
如何工作？ 1627
支持的资源 1628
注意事项 1628
配额 1630
相关服务 1630
定价 1630
所需的 IAM 权限 1631
使用保留规则 1634
使用回收站中的资源 1643
监控回收站 1643
资源位置 1656
资源 ID 1656
列出并筛选您的资源 1657
控制台步骤 1657
CI 和 API 步骤 1661

全局视图（跨区域） 1663
标记资源 1664
有关标签的基本知识 1664
标记 资源 1665
标签限制 1668
标签和访问管理 1668
为资源添加标签以便于进行计费 1669
通过控制台使用标签 1669
通过命令行使用标签 1672
使用实例元数据中的实例标签 1675
使用 CloudFormation 为资源添加标签 1677
Service Quotas 1678
查看您的当前限制 1678
请求提高 1679
对使用端口 25 发送的电子邮件的限制 1680
问题排查 1681
排查启动问题 1681
设备名称无效 1681
超出实例限制 1682
实例容量不足 1682
当前不支持请求的配置。请查看文档以了解支持的配置。 1683
实例立即终止 1683
连接到您的实例 1684
连接问题的常见原因 1685
连接到您的实例时出错：连接超时 1686
Error: unable to load key ...(错误：无法加载密钥...) Expecting: ANY PRIVATE KEY(需要：任何私有密钥) 1689
错误：服务器无法识别用户密钥 1689
错误：权限被拒绝或 [实例] 端口 22 关闭了连接 1690
错误：未保护的私有密钥文件 1692
错误：私有密钥的格式必须以“-----BEGIN RSA PRIVATE KEY-----”开头，以“-----END RSA PRIVATE KEY-----”结尾 1693
错误：服务器拒绝我们的密钥或 没有支持的身份验证方法 1693
无法对实例执行 Ping 操作 1694
错误：服务器意外关闭了网络连接 1694
错误：EC2 Instance Connect 的主机密钥验证失败 1694
无法使用 EC2 Instance Connect 连接到 Ubuntu 实例 1696
我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ 1696
停止实例 1700
强制停止实例 1700
创建替代实例 1701
终止实例 1703
实例立即终止 1703
延迟的实例终止 1703
已终止实例仍然显示 1703
错误：此实例可能无法终止。修改其“disableApiTermination”实例属性 1703
自动启动或终止的实例 1703
故障状态检查 1704
查看状态检查信息 1704
检索系统日志 1705
诊断基于 Linux 的实例的系统日志错误 1705
内存不足：终止进程 1706
错误：mmu_update 失败 (内存管理更新失败) 1706
I/O 错误（块储存设备故障） 1707
I/O 错误：既不是本地磁盘也不是远程磁盘（破损的分布式块储存设备） 1708
request_module：runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) 1709
“严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配) 1710

“FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) 1710
ERROR：无效内核 (EC2 不兼容内核) 1711
fsck：尝试打开时没有找到此文件或目录... (未找到文件系统) 1712
挂载文件系统时出现一般性错误（挂载失败） 1714
VFS：无法在未知块上挂载根 fs (根文件系统不匹配) 1715
错误：无法确定根设备的主/次编号...（根文件系统/设备不匹配） 1716
XENBUS：设备没有驱动程序... 1717
... 没有检查时，已强制执行检查的工作日 (文件系统检查要求) 1718
fsck 卡在退出状态...（设备缺失） 1718
GRUB 提示 (grubdom>) 1719
提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。(硬编码的 MAC 地址)。 1721
无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误) 1722
XENBUS：连接设备时超时 (Xenbus 超时) 1723
排查无法访问的实例的问题 1723
实例重启 1723
实例控制台输出 1724
捕获无法访问的实例的屏幕截图 1724
主机发生故障时的实例恢复 1725
从错误的卷启动 1726
EC2Rescue for Linux 1727
安装 EC2Rescue for Linux 1727
（可选）验证 EC2Rescue for Linux 的签名 1728
使用 EC2Rescue for Linux 1730
开发 EC2Rescue 模块 1732
EC2 Serial Console 1736
配置对 EC2 Serial Console 的访问 1736
连接到 EC2 Serial Console 1742
终止 EC2 Serial Console 会话 1746
使用 EC2 Serial Console 对实例进行故障排查 1747
发送诊断中断 1752
支持的实例类型 1753
先决条件 1753
发送诊断中断 1755
相关信息 1756
文档历史记录 1757
之前年份的历史 1767

什么是 Amazon EC2？

Amazon Elastic Compute Cloud (Amazon EC2) 在 Amazon Web Services (Amazon) 云中提供可扩展的计算容量。使用 Amazon EC2 可避免前期的硬件投入，因此您能够快速开发和部署应用程序。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。Amazon EC2 可让您扩展或缩减以处理需求变化或使用高峰，从而减少预测流量的需求。

有关云计算的更多信息，请参阅何为“云计算”？

Amazon EC2 的功能

Amazon EC2 提供以下功能：

- 虚拟计算环境，也称为实例
- 实例的预配置模板，也称为 Amazon 系统映像 (AMI)，其中包含您的服务器需要的程序包（包括操作系统和其他软件）。
- 实例 CPU、内存、存储和网络容量的多种配置，也称为实例类型
- 使用密钥对的实例的安全登录信息（Amazon 存储公有密钥，您在安全位置存储私有密钥）
- 临时数据（停止、休眠或终止实例时会删除这些数据）的存储卷，也称为实例存储卷
- 使用 Amazon Elastic Block Store (Amazon EBS) 的数据的持久性存储卷，也称为 Amazon EBS 卷。
- 用于存储资源的多个物理位置，例如实例和 Amazon EBS 卷，也称为区域 和可用区
- 防火墙，让您可以指定协议、端口，以及能够使用安全组到达您的实例的源 IP 范围
- 用于动态云计算的静态 IPv4 地址，称为弹性 IP 地址
- 元数据，也称为标签，您可以创建元数据并分配给您的 Amazon EC2 资源
- 您可以创建的虚拟网络，这些网络与其余 Amazon 云在逻辑上隔离，并且您可以选择连接到您自己的网络，也称为 Virtual Private Cloud (VPC)。

有关 Amazon EC2 功能的更多信息，请参阅 Amazon EC2 产品页。

有关在 Amazon 上运行网站的更多信息，请参阅 Web 托管。

如何开始使用 Amazon EC2

首先，您应进行设置以使用 Amazon EC2。设置完毕后，您便基本上完成了 Amazon EC2 入门教程。如果需要有关 Amazon EC2 功能的更多信息，可阅读技术文档。

设置和运行

- 设置以使用 Amazon EC2 (p. 5)
- 教程：Amazon EC2 Linux 实例入门 (p. 9)

基础知识

- 实例和 AMI (p. 235)
- 区域和可用区 (p. 1040)

- 实例类型 (p. 238)
- 标签 (p. 1664)

网络和安全性

- 密钥对 (p. 1289)
- 安全组 (p. 1303)
- 弹性 IP 地址 (p. 1094)
- Virtual Private Cloud (p. 1194)

存储

- Amazon EBS (p. 1323)
- 实例存储 (p. 1579)

使用 Linux 实例

- Amazon Systems Manager 用户指南中的 Amazon Systems Manager Run Command
- 教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)
- 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)

对于 Amazon 是否适合您，如果有任何疑问，请联系 Amazon 销售。如果遇到有关 Amazon EC2 的技术问题，请使用 Amazon EC2 论坛。

相关服务

您可以直接使用 Amazon EC2 预配置 Amazon EC2 资源，例如示例和卷。您也可以使用其他 Amazon 服务预置 Amazon EC2 资源。有关更多信息，请参阅以下文档：

- Amazon EC2 Auto Scaling 用户指南
- Amazon CloudFormation 用户指南
- Amazon Elastic Beanstalk 开发人员指南
- Amazon OpsWorks 用户指南

要跨多个实例自动分配应用程序的传入流量，可使用 Elastic Load Balancing。有关更多信息，请参阅 Elastic Load Balancing 用户指南。

要获取云中托管的关系数据库，可使用 Amazon Relational Database Service (Amazon RDS) 启动数据库实例。尽管可以在 EC2 实例上设置数据库，但是 Amazon RDS 为您处理数据库管理任务提供了优势，例如修补软件、备份以及存储备份。有关更多信息，请参阅 Amazon Relational Database Service 开发人员指南。

为了更轻松地管理 EC2 实例的集群上的 Docker 容器，请使用 Amazon Elastic Container Service (Amazon ECS)。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南或适用于 Amazon Fargate 的 Amazon Elastic Container Service 用户指南。

要监控您的实例和 Amazon EBS 卷的基本统计数据，可使用 Amazon CloudWatch。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

要检测对 EC2 实例的潜在授权或恶意使用，请使用 Amazon GuardDuty。有关更多信息，请参阅 Amazon GuardDuty 用户指南。

访问 Amazon EC2

Amazon EC2 提供基于 Web 的用户界面，即 Amazon EC2 控制台。如果您已注册Amazon账户，可以通过登录 Amazon Web Services Management Console 并从控制台主页选择 EC2 来访问 Amazon EC2 控制台。

如果倾向于使用命令行界面，您可使用以下选项：

Amazon 命令行界面（CLI）

提供大量 Amazon 产品的相关命令，同时被 Windows、Mac 和 Linux 支持。要开始使用，请参阅 Amazon Command Line Interface 用户指南。有关 Amazon EC2 命令的更多信息，请参阅 Amazon CLI Command Reference 中的 ec2。

Amazon Tools for Windows PowerShell

为在 PowerShell 环境中编写脚本的用户提供大量 Amazon 产品的相关命令。要开始使用，请参阅 Amazon Tools for Windows PowerShell 用户指南。有关 Amazon EC2 的 cmdlet 的更多信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考。

Amazon EC2 支持使用 Amazon CloudFormation 创建资源。您可以在 JSON 或 YAML 中创建描述您的 Amazon 资源的模板，然后 Amazon CloudFormation 会为您预置和配置这些资源。您可以重复使用 CloudFormation 模板来多次预置相同的资源，无论是在同一地区和账户中，还是在多个地区和账户中。有关 Amazon EC2 的资源类型和属性的更多信息，请参阅 Amazon CloudFormation 用户指南中的 EC2 资源类型参考。

Amazon EC2 提供查询 API。这些请求属于 HTTP 或 HTTPS 请求，需要使用 HTTP 动词 GET 或 POST 以及一个名为 `Action` 的查询参数。有关 Amazon EC2 的 API 操作的更多信息，请参阅《Amazon EC2 API 参考》中的操作。

如果您倾向于使用特定语言的 API 而非通过 HTTP 或 HTTPS 提交请求来构建应用程序，Amazon 为软件开发人员提供了库文件、示例代码、教程和其他资源。这些库文件提供可自动执行任务的基本功能，例如以加密方式对请求签名、重试请求和处理错误响应，以便您可以更轻松地上手。有关更多信息，请参阅用于在 Amazon 上构建的工具 。

Amazon EC2 定价

Amazon EC2 为实例提供以下购买选项：

按需实例

您只需按秒支付使用实例的费用（最少 60 秒），无需长期订阅或支付预付款。

预留实例

可以通过承诺在 1 年或 3 年期限内提供特定的实例配置（包括实例类型和区域）来降低您的 Amazon EC2 成本。

竞价型实例

请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。

有关 Amazon EC2 的费用和价格的完整列表，请参阅 Amazon EC2 定价。

在计算预配置环境的成本时，请记住包括附带成本，例如 EBS 卷的快照存储。

若要查看您的账单，请转到 Amazon Billing and Cost Management 控制台中的账单和成本管理控制面板。您的账单中包含了提供您的账单详情的使用情况报告的链接。要了解有关 Amazon 账户账单的更多信息，请参阅 Amazon 账单和成本管理用户指南。

如果您有关于 Amazon 账单、账户和事件的问题，请联系 Amazon Support。

Trusted Advisor 可帮助您优化成本、安全性和您的 Amazon 环境性能，有关其概述，请参阅 Amazon Trusted Advisor。

PCI DSS 合规性

Amazon EC2 支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。有关 PCI DSS 的更多信息，包括如何请求 Amazon PCI Compliance Package 的副本，请参阅 PCI DSS 第 1 级。

设置以使用 Amazon EC2

完成本部分中的任务，以便为首次启动 Amazon EC2 实例进行设置：

1. 注册一个 Amazon Web Services 账户 (p. 5)
2. 保护 IAM 用户 (p. 5)
3. 创建密钥对 (p. 5)
4. 创建安全组 (p. 6)

完成后，您将准备好学习 Amazon EC2 入门 (p. 9)教程。

注册一个 Amazon Web Services 账户

如果您还没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

注册 Amazon Web Services 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

   当您注册 Amazon Web Services 账户 时，系统将会创建一个 Amazon Web Services 账户根用户。根用户有权访问该账户中的所有 Amazon Web Services和资源。作为安全最佳实践，请 为管理用户分配管理访问权限，并且只使用根用户执行 需要根用户访问权限的任务。

Amazon注册过程完成后，会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择 My Account (我的账户) 来查看当前的账户活动并管理您的账户。

保护 IAM 用户

注册 Amazon Web Services 账户 后，启用多重身份验证（MFA）保护您的管理用户。有关说明，请参阅 IAM 用户指南中的为 为 IAM 用户（控制台）启用虚拟 MFA 设备。

要授予其他用户访问您的 Amazon Web Services 账户 资源的权限，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅 IAM 用户指南中的以下主题：

- 在您的 Amazon Web Services 账户 中创建 IAM 用户
- 适用于 Amazon 资源的访问管理
- IAM 基于身份的策略示例

创建密钥对

Amazon 使用公有密钥密码术来保护实例的登录信息。Linux 实例没有密码；您可以使用密钥对安全地登录您的实例。在启动实例时指定密钥对的名称，然后在使用 SSH 登录时提供私有密钥，

如果您尚未创建密钥对，则可以通过 Amazon EC2 控制台自行创建。请注意，如果您计划在多个 Amazon Web Services 区域中启动实例，则需要在每个区域中创建密钥对。有关 区域的更多信息，请参阅区域和可用区 (p. 1040)。

创建密钥对

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Key Pairs (密钥对)。
3. 选择 Create key pair (创建密钥对)。
4. 对于 Name (名称)，为模板输入一个描述性名称。Amazon EC2 将公有密钥与您指定的密钥名称相关联。密钥名称最多可包含 255 个 ASCII 字符。它不能包含前导空格或尾随空格。
5. 对于 Key pair type（密钥对类型），选择 RSA 或者 ED25519。请注意，Windows 实例不支持 ED25519 密钥。
6. 对于 Private key file format（私有密钥文件格式），选择要保存私有密钥的格式。要以可与 OpenSSH 一起使用的格式保存私有密钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私有密钥，请选择 ppk。
7. 选择 Create key pair (创建密钥对)。
8. 您的浏览器会自动下载私有密钥文件。基本文件名是指定为密钥对名称的名称，文件扩展名由您选择的文件格式确定。将私有密钥文件保存在安全位置。

   Important

   这是您保存私有密钥文件的唯一机会。
9. 如果您计划在 macOS 或 Linux 计算机上使用 SSH 客户端连接到 Linux 实例，请使用以下命令设置私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 key-pair-name.pem
```

   如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅错误：未保护的私有密钥文件 (p. 1692)。

有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

创建安全组

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须在安全组中添加规则，以便能够使用 SSH 从您的 IP 地址连接到实例。您还可以添加允许来自任意位置的入站和出站 HTTP 和 HTTPS 访问的规则。

请注意，如果您计划在多个 Amazon Web Services 区域 中启动实例，则需要在每个区域中创建安全组。有关 区域的更多信息，请参阅区域和可用区 (p. 1040)。

先决条件

您需要使用本地计算机的公有 IPv4 地址。Amazon EC2 控制台中的安全组编辑器可以为您自动检测公有 IPv4 地址。此外，您可以在 Internet 浏览器中使用搜索短语“什么是我的 IP 地址”，或使用以下服务：检查 IP。如果您正通过 Internet 服务提供商 (ISP) 连接或者在不使用静态 IP 的情况下从防火墙后面连接，则您需要找出客户端计算机使用的 IP 地址范围。

您可以使用以下方法之一创建自定义安全组。

New console

创建具有最小特权的安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从顶部的导航栏中选择安全组的 Amazon Web Services 区域。安全组特定于某一区域，因此您应选择已创建密钥对的区域。
3. 在左侧导航窗格中，选择 Security Groups (安全组)。
4. 选择Create security group（创建安全组）。
5. 对于 Basic details (基本详细信息)，执行以下操作：
   a. 输入新安全组的名称和描述。使用一个容易记住的名称，例如，您的用户名称，后跟 _SG_，加区域名称。例如，me_SG_uswest2。
   b. 在 VPC 列表中，为区域选择您的默认 VPC。
6. 对于 Inbound rules (入站规则)，创建允许传输到您的实例的规则。例如，对于接受 HTTP 和 HTTPS 流量的 Web 服务器，请使用以下规则。有关更多示例，请参阅 针对不同使用案例的安全组规则 (p. 1315)。
   a. 选择 Add rule。对于 Type，选择 HTTP。对于 Source (源)，请选择 Anywhere (任何位置)。
   b. 选择 Add rule。对于 Type，选择 HTTPS。对于 Source (源)，请选择 Anywhere (任何位置)。
   c. 选择 Add rule (添加规则)。对于 Type (类型)，选择 SSH。对于 Source (源)，执行以下操作之一：
      - 选择 My IP (我的 IP)：自动添加本地计算机的公有 IPv4 地址。
      - 选择 Custom (自定义) 并使用 CIDR 表示法指定计算机的公有 IPv4 地址或网络。要采用 CIDR 表示法指定单个 IP 地址，请添加路由前缀 /32，例如 `203.0.113.25/32`。如果您的公司或路由器要分配同一范围内的地址，请指定整个范围，例如 `203.0.113.0/24`。

      Warning

      出于安全原因，请勿为具有 SSH 规则的 Source (源) 选择 Anywhere (任何地方)。这会允许从互联网上的所有 IP 地址访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。
7. 对于 Outbound rules (出站规则)，请保留允许所有出站流量的默认规则。
8. 选择Create security group（创建安全组）。

Old console

创建具有最小特权的安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Security Groups (安全组)。
3. 选择 Create Security Group。
4. 输入新安全组的名称和描述。使用一个容易记住的名称，例如，您的用户名称，后跟 _SG_，加区域名称。例如，me_SG_uswest2。
5. 在 VPC 列表中，为区域选择您的默认 VPC。
6. 在Inbound（入站）规则选项卡上，创建以下规则（为每个新规则选择添加规则）：
   - 从 Type 列表中选择 HTTP，确保 Source 设置为 Anywhere (`0.0.0.0/0`)。
   - 从 Type 列表中选择 HTTPS，确保 Source 设置为 Anywhere (`0.0.0.0/0`)。
   - 从 Type 列表中选择 SSH。在源框中，选择 My IP 以便使用本地计算机的公有 IPv4 地址自动填充该字段。或者，选择自定义并使用 CIDR 表示法指定计算机的公有 IPv4 地址或网络。要采用

CIDR 表示法指定单个 IP 地址，请添加路由前缀 /32，例如 203.0.113.25/32。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 203.0.113.0/24。

Warning

出于安全原因，请勿允许 SSH 从所有 IP 地址访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。

7. 在 Outbound (出站) 规则 选项卡上，请保留允许所有出站流量的默认规则。
8. 选择Create security group（创建安全组）。

Command line

创建具有最小特权的安全组

使用以下命令之一：

- create-security-group (Amazon CLI)
- New-EC2SecurityGroup (Amazon Tools for Windows PowerShell)

有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

教程：Amazon EC2 Linux 实例入门

利用本教程开始使用 Amazon Elastic Compute Cloud (Amazon EC2)。您将了解如何启动、连接到和使用 Linux 实例。实例是 Amazon 云中的虚拟服务器。您可以使用 Amazon EC2 来创建和配置在实例上运行的操作系统和应用程序。

注册Amazon后，您可以通过Amazon免费套餐开始使用 Amazon EC2。如果您在过去 12 个月内创建过 Amazon 账户，并且还没有超出 Amazon EC2 的免费套餐权益范围，则学完本教程不需要任何费用，因为我们会帮助您选择免费套餐权益范围内的选项。否则，您将从启动实例的那一刻开始承担标准的 Amazon EC2 使用费，直至终止实例 (本教程最后一项任务)，即使实例处于闲置状态也要计费。

相关教程

- 如果您希望启动 Windows 实例，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的以下教程：Amazon EC2 Windows 实例入门。
- 如果您希望使用命令行，请参阅 Amazon Command Line Interface 用户指南中的以下教程：通过 Amazon CLI 使用 Amazon EC2。

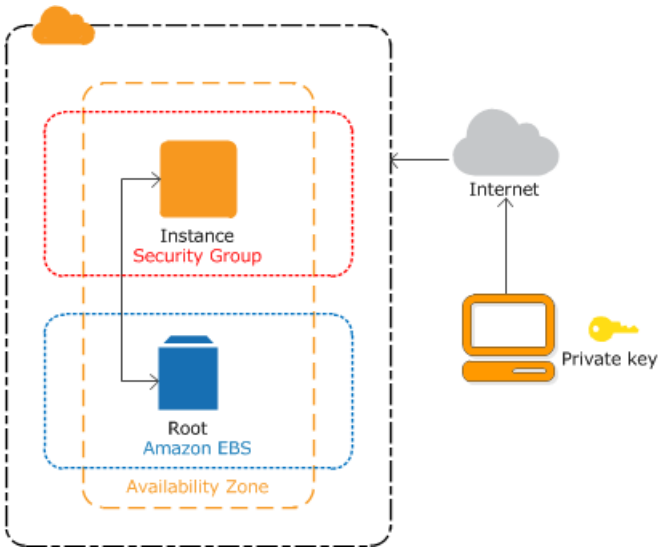
目录

- 概览 (p. 9)
- 先决条件 (p. 10)
- 步骤 1：启动实例 (p. 10)
- 步骤 2：连接到您的实例 (p. 11)
- 步骤 3：清除您的实例 (p. 11)
- 后续步骤 (p. 12)

概览

本教程中启动的实例为 Amazon EBS 支持的实例（即，根卷为 EBS 卷）。您可以指定在其中运行您的实例的可用区，也可以让 Amazon EC2 为您选择可用区。可用区是每个区域内的多个相互隔离的位置。您可以将可用区视为孤立的数据中心。

启动实例时，您可以通过指定密钥对（证明您的身份）和一个安全组（充当虚拟防火墙来控制入站和出站流量）来保护实例的安全。连接到您的实例时，您必须提供您在启动实例时指定的密钥对的私有密钥。



先决条件

开始之前，请确保您已完成 设置以使用 Amazon EC2 (p. 5) 中的步骤。

步骤 1：启动实例

您可以根据以下过程所述使用 Amazon Web Services Management Console 启动 Linux 实例。本教程旨在帮助您快速启动第一个实例，因此不会涵盖所有可能的选项。有关高级选项的信息，请参阅 使用新启动实例向导启动实例 (p. 575)。有关启动实例的其他方式的信息，请参阅启动实例 (p. 574)。

启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从 EC2 控制台控制面板中，在 Launch instance（启动实例）框中，选择 Launch instance（启动实例），然后从显示的选项中选择Launch instance（启动实例）。
3. 在 Name and tags（名称与标签）下，为 Name（名称）输入实例的描述性名称。
4. 在 Application and OS Images (Amazon Machine Image)（应用程序和操作系统映像 (Amazon Machine Image)）中，执行以下操作：

   a. 选择 Quick Start（快速启动），然后选择 Amazon Linux。这是适用于您的实例的操作系统 (OS)。

   b. 从 Amazon Machine Image (AMI) 中，选择 Amazon Linux 2 的 HVM 版本。请注意，这些 AMI 标记为 Free tier eligible（符合条件的免费套餐）。Amazon Machine Image (AMI) 是基本配置，用作您的实例的模板。
5. 在 Instance type（实例类型）下，从 Instance type（实例类型）列表中，您可以为您的实例选择硬件配置。选择 `t2.micro` 实例类型，这是默认情况下的选择。`t2.micro` 实例类型适用免费套餐。在 `t2.micro` 不可用的区域中，您可以使用免费套餐下的 `t3.micro` 实例。有关更多信息，请参阅 AmazonFree Tier（免费套餐）。
6. 在 Key pair (login)（密钥对（登录））下，对于 Key pair name（密钥对名称），选择在开始设置时创建的密钥对。

   Warning

   不要选择 Proceed without a key pair (Not recommended)（在没有密钥对的情况下继续（不推荐））。如果您启动的实例没有密钥对，就不能连接到该实例。

7. 在 Network settings（网络设置）旁边，选择 Edit（编辑）。对于 Security group name（安全组名称），您将看到向导为您创建并选择了安全组。使用以下步骤，您可以使用此安全组，或者也可以选择在设置时创建的安全组：

   a. 选择 Select existing security group（选择现有安全组）。

   b. 从 Common security groups（通用安全组）中，从现有安全组列表中选择您的安全组。

8. 对于您的实例的其他配置设置，保留默认选择。
9. 查看 Summary（摘要）面板中您的实例配置的摘要，当您准备好后，选择 Launch instance（启动实例）。
10. 确认页面会让您知道自己的实例已启动。选择 View all instances（查看所有实例）以关闭确认页面并返回控制台。
11. 在实例屏幕上，您可以查看启动状态。启动实例只需很短的时间。启动实例时，其初始状态为 `pending`。实例启动后，其状态变为 `running`，并且会收到一个公有 DNS 名称。（如果 Public IPv4 DNS（公有 IPv4 DNS）列已隐藏，请选择右上角的设置图标（  ），打开 Public IPv4 DNS（公有 IPv4 DNS），然后选择 Confirm（确认）。
12. 可能需要花几分钟时间，实例才能准备好让您连接到它。检查您的实例是否通过了状态检查；您可以在状态检查列中查看此信息。

步骤 2：连接到您的实例

有几种方法可以连接到您的 Linux 实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

Important

除非您在启动实例时使用具有 `.pem` 文件的密钥对以及允许从您计算机进行 SSH 访问的安全组，否则您无法连接到实例。如果您无法连接到实例，请参阅排查实例的连接问题。 (p. 1684)以获得帮助。

步骤 3：清除您的实例

在您完成为本教程创建的实例后，应通过终止该实例进行清除。如果在清除该实例前要对其执行更多操作，请参阅后续步骤 (p. 12)。

Important

终止实例可有效地删除实例；无法在终止实例后重新连接到实例。

如果您启动的实例不在 Amazon 免费套餐范围内，则该实例一旦变为 `shutting down` 或 `terminated` 状态，就会停止产生费用。为了在不产生费用的情况下保留实例以供将来使用，您可以立即停止该实例，然后在稍后再次启动它。有关更多信息，请参阅停止和启动您的实例 (p. 610)。

终止您的实例

1. 在导航窗格中，选择实例。在实例列表中选择实例。
2. 依次选择实例状态、终止实例。
3. 当系统提示您确认时，选择终止。

   Amazon EC2 关闭并终止您的实例。您的实例在终止之后，短时间内仍将在控制台上可见，然后该条目将自动删除。您不能自己从控制台显示中删除已终止的实例。

后续步骤

启动实例后，您可能想尝试以下的一些练习：

- 了解如何使用 Run Command 远程管理您的 EC2 实例。有关更多信息，请参阅 Amazon Systems Manager 用户指南中的 Amazon Systems Manager Run Command。
- 配置 CloudWatch 警报以在您的使用量超出免费套餐时向您发出通知。有关更多信息，请参阅 Amazon Billing 用户指南中的跟踪 Amazon 免费套餐使用情况。
- 添加 EBS 卷。有关更多信息，请参阅 创建 Amazon EBS 卷 (p. 1344) 和 将 Amazon EBS 卷挂载到实例 (p. 1347)。
- 安装 LAMP 堆栈。有关更多信息，请参阅教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)。

Amazon EC2 的最佳实践

为最大程度地利用 Amazon EC2 的优势，建议您执行以下最佳实践。

安全性

- 尽可能将身份联合验证与身份提供商和 IAM 角色结合使用，以管理对 Amazon 资源和 API 的访问权限。有关更多信息，请参阅 IAM 用户指南 中的创建 IAM policy。
- 为安全组实现最严格的规则。有关更多信息，请参阅安全组规则 (p. 1304)。
- 定期修补、更新和保护实例上的操作系统和应用程序。有关更新 Amazon Linux 2 或 Amazon Linux AMI 的更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的管理 Linux 实例上的软件。
- 使用 Amazon Inspector 可以自动发现并扫描 Amazon EC2 实例是否存在软件漏洞和意外网络暴露。有关更多信息，请参阅 Amazon Inspector 用户指南。
- 根据安全最佳实践和安全标准，使用 Amazon Security Hub 控件监控 Amazon EC2 资源。有关使用 Security Hub 的更多信息，请参阅《Amazon Security Hub 用户指南》中的 Amazon Elastic Compute Cloud 控件。

存储

- 了解根设备类型对数据持久性、备份和恢复的影响。有关更多信息，请参阅根设备存储 (p. 103)。
- 对操作系统与您的数据分别使用单独的 Amazon EBS 卷。确保含有您数据的卷可在实例终止后保留。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。
- 使用您的实例可用的实例存储来存储临时数据。请注意，当您停止、休眠或终止您的实例时，系统会删除存储在实例存储中的数据。如果将实例存储用于数据库存储，请确保您拥有一个具有重复因子的集群，从而确保容错。
- 对 EBS 卷和快照进行加密。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

资源管理

- 使用实例元数据和自定义资源标签跟踪并确定您的 Amazon 资源。有关更多信息，请参阅 实例元数据和用户数据 (p. 754) 和 标记 Amazon EC2 资源 (p. 1664)。
- 查看您的 Amazon EC2 的当前限制。需要时请提前计划请求提高限制。有关更多信息，请参阅Amazon EC2 Service Quotas (p. 1678)。
- 使用 Amazon Trusted Advisor 检查您的 Amazon 环境，然后在有可能节省开支、提高系统可用性和性能或弥补安全漏洞时为您提供建议。有关更多信息，请参阅 Amazon Web Services Support 用户指南中的 Amazon Trusted Advisor。

备份和恢复

- 使用 Amazon EBS 快照 (p. 1368)定期备份您的 EBS 卷，并从您的实例创建 Amazon Machine Image (AMI) (p. 101)，以便保存配置以作为启动未来实例的模板。有关有助于实现此使用案例的 Amazon 服务的更多信息，请参阅 Amazon Backup 和 Amazon Data Lifecycle Manager。
- 跨多个可用区部署应用程序的关键组件，并适当地复制数据。
- 设计您的应用程序，以便在实例重新启动时处理动态 IP 地址分配。有关更多信息，请参阅Amazon EC2 实例 IP 寻址 (p. 1053)。
- 监控和响应事件。有关更多信息，请参阅监控 Amazon EC2 (p. 972)。
- 确保您已准备好处理故障转移。对于基本解决方案，您可以手动将网络接口或弹性 IP 地址附加到替换实例。有关更多信息，请参阅弹性网络接口 (p. 1104)。对于自动解决方案，您可以使用 Amazon EC2 Auto Scaling。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。

- 定期测试恢复您的实例和 Amazon EBS 卷的过程，以确保成功还原数据和服务。

联网

- 对于 IPv4 和 IPv6，将应用程序的生存时间 (TTL) 值设置为 255。如果使用更小的值，则存在 TTL 在应用程序流量传输过程中过期的风险，从而导致实例发生可访问性问题。

运行 Linux 的 Amazon EC2 实例的相关教程

以下教程为您介绍了如何使用运行 Linux 的 EC2 实例执行常见任务。Amazon 提供了 Amazon Linux 2023、Amazon Linux 2 和 Amazon Linux AMI。有关更多信息，请参阅 Amazon Linux 2、Amazon Linux 2023 和 Amazon Linux AMI。有关视频教程，请参阅 Amazon 教学视频和实验室。

教程

- 教程：在 Amazon Linux 2023 上安装 LAMP Web 服务器 (p. 15)
- 教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)
- 教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器 (p. 33)
- 教程：在 Amazon Linux 2023 上配置 SSL/TLS (p. 42)
- 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)
- 教程：使用 Amazon Linux AMI 配置 SSL/TLS (p. 68)
- 教程：增加 EC2 实例上 Amazon EBS 卷的大小 (p. 77)
- 教程：在 Amazon Linux 2023 上托管 WordPress 博客 (p. 85)
- 教程：在上托管 WordPress 博客 Amazon Linux 2 (p. 93)

教程：在 Amazon Linux 2023 上安装 LAMP Web 服务器

通过以下步骤，您可以将带 PHP 和 MariaDB（一个由社区开发的 MySQL 分支）支持的 Apache Web 服务器（有时称为 LAMP Web 服务器或 LAMP 堆栈）安装到 Amazon Linux 2023 实例上。您可以使用此服务器来托管静态网站或部署能对数据库中的信息执行读写操作的动态 PHP 应用程序。

> **Important**
>
> 这些过程适用于 Amazon Linux 2023。如果您尝试在其他发行版（例如 Ubuntu 或红帽企业 Linux）上设置 LAMP Web 服务器，则本教程不适合。对于 Amazon Linux 2，请参阅教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)。对于 Amazon Linux AMI，请参阅 教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器 (p. 33)。对于 Ubuntu，请参阅以下 Ubuntu 社区文档：ApacheMySQLPHP。有关其他发布版本，请参阅特定于该版本的文档。

任务

- 步骤 1：准备 LAMP 服务器 (p. 16)
- 步骤 2：测试 LAMP 服务器 (p. 18)
- 步骤 3：确保数据库服务器的安全 (p. 20)
- 步骤 4：(可选) 安装 phpMyAdmin (p. 20)
- 问题排查 (p. 23)
- 相关主题 (p. 23)

步骤 1：准备 LAMP 服务器

先决条件

- 本教程假定您已经使用 Amazon Linux 2023 启动具有可从 Internet 访问的公有 DNS 名称的新实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。您还必须配置安全组，以便允许 SSH (端口 22)、HTTP (端口 80) 和 HTTPS (端口 443) 连接。有关这些先决条件的更多信息，请参阅 为您的 Linux 实例授权入站流量 (p. 1287)。
- 以下过程将安装 Amazon Linux 2023 上可用的最新 PHP 版本（当前为 7.4）。如果您计划使用本教程中所述的 PHP 应用程序之外的 PHP 应用程序，则应检查其与 7.4 的兼容性。

准备 LAMP 服务器

1. 连接到您的 实例 (p. 11)。
2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

   ```
   [ec2-user ~]$ sudo dnf update -y
   ```
3. 安装 Apache Web 服务器的最新版本，以及适用于 Amazon Linux 2023 的 PHP 程序包。

   ```
   [ec2-user ~]$ sudo dnf install -y httpd wget php-fpm php-mysqli php-json php php-devel
   ```
4. 安装 MariaDB 软件包。使用 dnf install 命令可同时安装多个软件包和所有相关依赖项。

   ```
   [ec2-user ~]$ sudo dnf install mariadb105-server
   ```

   您可以使用以下命令查看这些程序包的当前版本：

   ```
   [ec2-user ~]$ sudo dnf info package_name
   ```

   示例：

   ```
   [root@ip-172-31-25-170 ec2-user]# dnf info mariadb105
   Last metadata expiration check: 0:00:16 ago on Tue Feb 14 21:35:13 2023.
   Installed Packages
   Name         : mariadb105
   Epoch        : 3
   Version      : 10.5.16
   Release      : 1.amzn2023.0.6
   Architecture : x86_64
   Size         : 18 M
   Source       : mariadb105-10.5.16-1.amzn2023.0.6.src.rpm
   Repository   : @System
   From repo    : amazonlinux
   Summary      : A very fast and robust SQL database server
   URL          : http://mariadb.org
   License      : GPLv2 and LGPLv2
   Description  : MariaDB is a community developed fork from MySQL - a multi-user, multi-
   threaded
                : SQL database server. It is a client/server implementation consisting of
                : a server daemon (mariadbd) and many different client programs and
    libraries.
                : The base package contains the standard MariaDB/MySQL client programs and
   ```

```
            : utilities.
```

5. 启动 Apache Web 服务器。

```
[ec2-user ~]$ sudo systemctl start httpd
```

6. 使用 systemctl 命令配置 Apache Web 服务器，使其在每次系统启动时启动。

```
[ec2-user ~]$ sudo systemctl enable httpd
```

您可以通过运行以下命令验证 httpd 是否已启用：

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

7. 如果您尚未这样做，请添加安全规则以允许与您的实例的入站 HTTP (端口 80) 连接。默认情况下，启动期间将为您的实例创建 launch-wizard-*N* 安全组。如果您没有添加其他安全组规则，此组仅包含允许 SSH 连接的一条规则。

   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 在左侧的导航中，选择 Instances（实例），然后选择您的实例。
   c. 在安全选项卡上，查看入站规则。您应看到以下规则：

```
Port range   Protocol     Source
22           tcp          0.0.0.0/0
```

      Warning

      使用 0.0.0.0/0 可允许所有 IPv4 地址使用 SSH 访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产环境中，您仅授权特定 IP 地址或地址范围访问您的实例。

   d. 如果没有允许 HTTP（端口 80）连接的入站规则，则必须立即添加规则。选择安全组的链接。使用向安全组添加规则 (p. 1311) 中的过程，添加具有以下值的新入站安全规则：

      - Type：HTTP
      - Protocol：TCP
      - Port Range：80
      - Source：Custom

8. 测试您的 Web 服务器。在 Web 浏览器中，键入您的实例的公有 DNS 地址 (或公有 IP 地址)。如果 /var/www/html 中没有内容，您应该会看到 Apache 测试页面，该页面将显示消息 It works!（它工作正常！）。

   您可以使用 Amazon EC2 控制台获取实例的公有 DNS（选中 Public IPv4 DNS（公有 IPv4 DNS）列；如果此列处于隐藏状态，请选择首选项（齿轮状图标），并开启 Public IPv4 DNS（公有 IPv4 DNS）。

   验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

      Important

      如果您使用的不是 Amazon Linux，则还可能需要在实例上配置防火墙才能允许这些连接。有关如何配置防火墙的更多信息，请参阅适用于特定分配的文档。

   Apache 测试页面。

Apache httpd 提供的文件保存在名为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录为 /var/www/html，默认情况下归根用户所有。

要允许 ec2-user 账户操作此目录中的文件，必须修改其所有权和权限。有多种方式可以完成此任务。在本教程中，可将 ec2-user 添加到 apache 组，将 /var/www 目录的所有权授予 apache 组，并为该组指定写入权限。

设置文件权限

1. 将您的用户 (这里指 ec2-user) 添加到 apache。

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. 先退出再重新登录以选取新组，然后验证您的成员资格。

   a. 退出（使用 exit 命令或关闭终端窗口）：

```
[ec2-user ~]$ exit
```

   b. 要验证您是否为 apache 组的成员，请重新连接到实例，然后运行以下命令：

```
[ec2-user ~]$ groups
ec2-user adm wheel apache systemd-journal
```

3. 将 /var/www 及其内容的组所有权更改到 apache 组。

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. 要添加组写入权限以及设置未来子目录上的组 ID，请更改 /var/www 及其子目录的目录权限。

```
[ec2-user ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775
 {} \;
```

5. 要添加组写入权限，请递归地更改 /var/www 及其子目录的文件权限：

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

这样，ec2-user (和 apache 组的任何未来成员) 可以添加、删除和编辑 Apache 文档根目录中的文件，允许您添加内容，如静态网站或 PHP 应用程序。

保护您的 Web 服务器 (可选)

运行 HTTP 协议的 Web 服务器不为其发送或接收的数据提供传输安全。当您使用 Web 浏览器连接 HTTP 服务器时，对于您访问的 URL、您接收的网页内容以及您提交的任何 HTML 表的内容 (包括密码)，窃取者可在网络路径上的任何位置看到。保护您的 Web 服务器的最佳实践是安装 HTTPS (HTTP Secure) 支持，它将使用 SSL/TLS 加密保护您的数据。

有关在服务器上启用 HTTPS 的信息，请参阅 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。

步骤 2：测试 LAMP 服务器

如果服务器已安装并运行，且文件权限设置正确，则 ec2-user 账户应该能够在 /var/www/html 目录 (可从 Internet 访问) 中创建 PHP 文件。

测试您的 LAMP 服务器

1. 在 Apache 文档根目录中创建一个 PHP 文件。

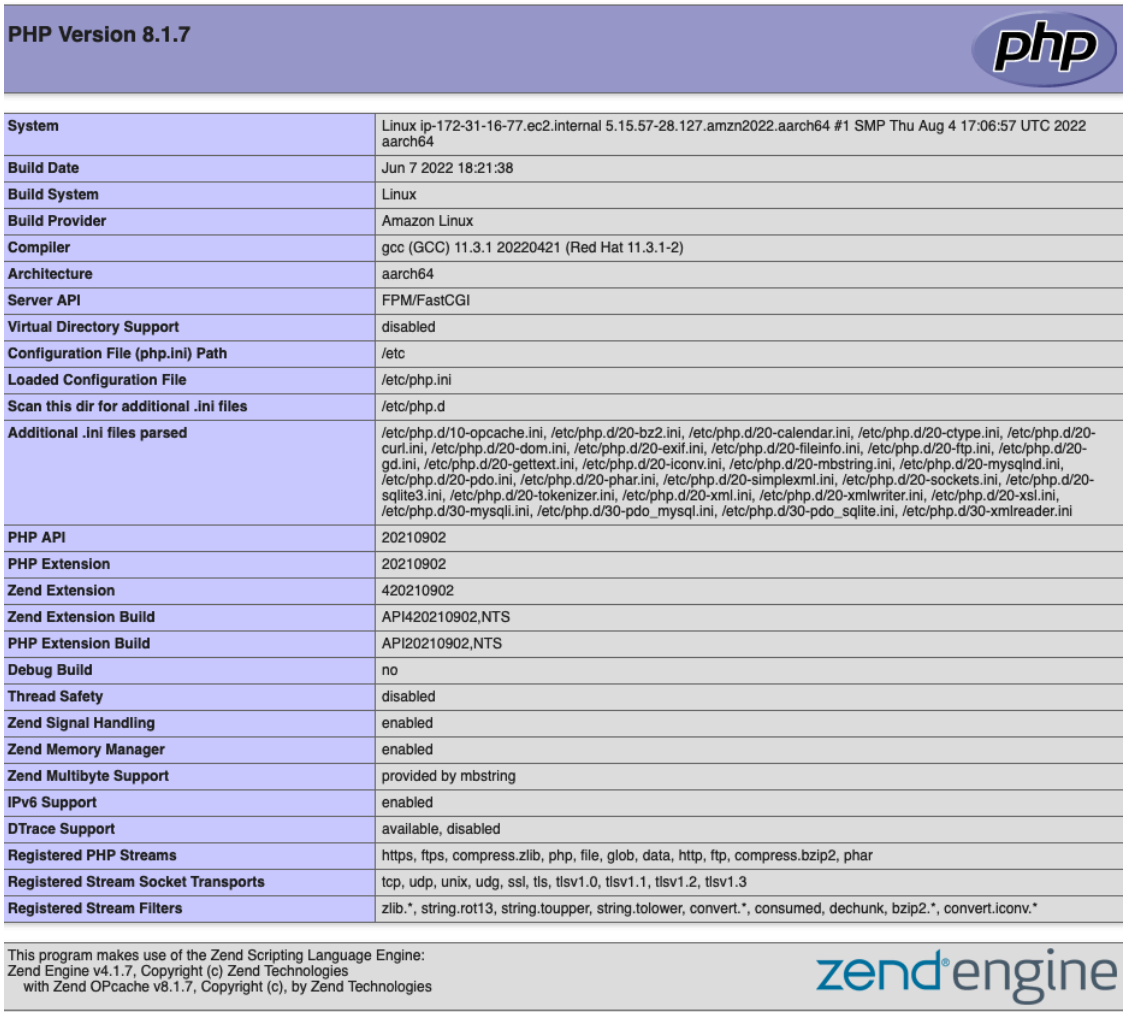
```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

尝试运行该命令时，如果出现“Permission denied (权限被拒绝)”错误，请尝试先注销，再重新登录，以获取您在 设置文件权限 (p. 18) 中配置的适当组权限。

2. 在 Web 浏览器中，键入您刚刚创建的文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。例如：

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该会看到 PHP 信息页面：



PHP Version 8.1.7

System	Linux ip-172-31-16-77.ec2.internal 5.15.57-28.127.amzn2022.aarch64 #1 SMP Thu Aug 4 17:06:57 UTC 2022 aarch64
Build Date	Jun 7 2022 18:21:38
Build System	Linux
Build Provider	Amazon Linux
Compiler	gcc (GCC) 11.3.1 20220421 (Red Hat 11.3.1-2)
Architecture	aarch64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS
PHP Extension Build	API20210902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.1.7, Copyright (c) Zend Technologies
with Zend OPcache v8.1.7, Copyright (c), by Zend Technologies

如果您未看到此页面，请验证上一步中是否已正确创建 /var/www/html/phpinfo.php 文件。您还可以使用以下命令验证已经安装了所有必需的程序包。

```
[ec2-user ~]$ sudo dnf list installed httpd mariadb-server php-mysqlnd
```

如果输出中未列出任何必需的程序包，请使用 sudo yum install ***package*** 命令安装它们。

3. 删除 phpinfo.php 文件。尽管此信息可能很有用，但出于安全考虑，不应将其传播到 Internet。

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

现在，您应该有了一个功能完善的 LAMP Web 服务器。如果您将内容添加到 Apache 文档根目录 (位于 `/var/www/html`)，您应该能够在您的实例的公有 DNS 地址中看到该内容。

步骤 3：确保数据库服务器的安全

MariaDB 服务器的默认安装提供有多种功能，这些功能对于测试和开发都很有帮助，但对于产品服务器，应禁用或删除这些功能。mysql_secure_installation 命令可引导您设置根密码并删除安装中的不安全功能。即使您不打算使用 MariaDB 服务器，我们也建议执行此步骤。

保护 MariaDB 服务器

1. 启动 MariaDB 服务器。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

2. 运行 mysql_secure_installation。

```
[ec2-user ~]$ sudo mysql_secure_installation
```

   a. 在提示时，键入根账户的密码。

      i. 键入当前根密码。默认情况下，根账户没有设置密码。按 Enter。

      ii. 键入 **Y** 设置密码，然后键入两次安全密码。有关创建安全密码的更多信息，请访问 https://identitysafe.norton.com/password-generator/。确保将此密码存储在安全位置。

      设置 MariaDB 根密码仅是保护数据库的最基本措施。在您构建或安装数据库驱动的应用程序时，您通常可以为该应用程序创建数据库服务用户，并避免使用根账户执行除数据库管理以外的操作。

   b. 键入 **Y** 删除匿名用户账户。

   c. 键入 **Y** 禁用远程根登录。

   d. 键入 **Y** 删除测试数据库。

   e. 键入 **Y** 重新加载权限表并保存您的更改。

3. (可选) 如果您不打算立即使用 MariaDB 服务器，请停止它。您可以在需要时再次重新启动。

```
[ec2-user ~]$ sudo systemctl stop mariadb
```

4. (可选) 如果您希望每次启动时 MariaDB 服务器都启动，请键入以下命令。

```
[ec2-user ~]$ sudo systemctl enable mariadb
```

步骤 4：(可选) 安装 phpMyAdmin

phpMyAdmin 是一种基于 Web 的数据库管理工具，可用于在 EC2 实例上查看和编辑 MySQL 数据库。按照下述步骤操作，在您的 Amazon Linux 实例上安装和配置 `phpMyAdmin`。

Important

除非您在 Apache 中启用了 SSL/TLS，否则我们不建议您使用 `phpMyAdmin` 访问 LAMP 服务器；如果您使用 phpMyAdmin，您的数据库管理员密码和其他数据将无法安全地通过 Internet 传输。有关开发人员提供的安全建议，请参阅保护 phpMyAdmin 安装。有关在 EC2 实例上保护 Web 服务器的一般信息，请参阅 教程：在 Amazon Linux 2023 上配置 SSL/TLS (p. 42)。

安装 phpMyAdmin

1. 安装所需的依赖项。

```
[ec2-user ~]$ sudo dnf install php-mbstring php-xml -y
```

2. 重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

3. 重启 php-fpm.

```
[ec2-user ~]$ sudo systemctl restart php-fpm
```

4. 导航到位于 /var/www/html 的 Apache 文档根。

```
[ec2-user ~]$ cd /var/www/html
```

5. 从 https://www.phpmyadmin.net/downloads 选择最新 phpMyAdmin 发行版的源软件包。要将文件直接下载到您的实例，请复制链接并将其粘贴到 wget 命令，如本示例中所述：

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. 使用以下命令创建 phpMyAdmin 文件夹并将程序包提取到其中。

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. 删除 *phpMyAdmin-latest-all-languages.tar.gz* tarball。

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (可选) 如果 MySQL 服务器未运行，请立即启动它。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

9. 在 Web 浏览器中，键入 phpMyAdmin 安装的 URL。此 URL 是实例的公有 DNS 地址 (或公有 IP 地址)，后接正斜杠和您安装目录的名称。例如：

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

您应该会看到 phpMyAdmin 登录页面：



10. 使用您先前创建的 `root` 用户名和 MySQL 根密码登录到 phpMyAdmin 安装。

    您的安装仍需进行配置，然后才能投入使用。我们建议您首先手动创建配置文件，如下所示：

    a. 要从最小的配置文件开始，请使用您常用的文本编辑器创建一个新文件，然后将 `config.sample.inc.php` 的内容复制到该文件中。
    b. 在包含 `config.inc.php` 的 phpMyAdmin 目录中将文件保存为 `index.php`。
    c. 有关任何其他设置，请参阅 phpMyAdmin 安装说明的使用设置脚本部分中的文件后创建说明。

有关使用 phpMyAdmin 的信息，请参阅 phpMyAdmin 用户指南。

问题排查

本部分提供了解决在设置新 LAMP 服务器时可能遇到的常见问题的建议。

我无法使用 Web 浏览器连接到我的服务器

执行以下检查以查看您的 Apache Web 服务器是否正在运行且可以访问。

- Web 服务器正在运行吗？

  您可以通过运行以下命令验证 httpd 是否已启用：

  ```
  [ec2-user ~]$ sudo systemctl is-enabled httpd
  ```

  如果 httpd 进程未运行，请重复准备 LAMP 服务器 (p. 16)中描述的步骤。
- 防火墙是否配置正确？

  验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

我无法使用 HTTPS 连接到我的服务器

执行以下检查以查看 Apache Web 服务器是否配置为支持 HTTPS。

- Web 服务器配置是否正确？

  安装 Apache 后，服务器将针对 HTTP 流量进行配置。要支持 HTTPS，请在服务器上启用 TLS 并安装 SSL 证书。有关信息，请参阅 教程：在 Amazon Linux 2023 上配置 SSL/TLS (p. 42)。
- 防火墙是否配置正确？

  验证实例的安全组是否包含允许端口 443 上的 HTTPS 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

相关主题

有关将文件传输到您的实例或在 Web 服务器上安装 WordPress 博客的更多信息，请参阅以下文档：

- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 666)
- 使用 SCP 客户端将文件传输到 Linux 实例 (p. 651)
- 教程：在 Amazon Linux 2023 上托管 WordPress 博客 (p. 85)

有关本教程中使用的命令和软件的更多信息，请参阅以下网页：

- Apache Web 服务器：http://httpd.apache.org/
- MariaDB 数据库服务器：https://mariadb.org/
- PHP 编程语言：http://php.net/
- chmod 命令：https://en.wikipedia.org/wiki/Chmod

- chown 命令：https://en.wikipedia.org/wiki/Chown

有关注册 Web 服务器域名或将现有域名转移到此主机的更多信息，请参阅 Amazon Route 53 开发人员指南中的创建域和子域并将其迁移到 Amazon Route 53。

教程：在 Amazon Linux 2 上安装 LAMP Web 服务器

通过以下步骤，您可以将带 PHP 和 MariaDB（一个由社区开发的 MySQL 分支）支持的 Apache Web 服务器（有时称为 LAMP Web 服务器或 LAMP 堆栈）安装到您的 Amazon Linux 2 实例上。您可以使用此服务器来托管静态网站或部署能对数据库中的信息执行读写操作的动态 PHP 应用程序。

> **Important**
>
> 如果您尝试在其他发行版（例如 Ubuntu 或红帽企业 Linux）上设置 LAMP Web 服务器，则本教程不适合。对于 Amazon Linux AMI，请参阅 教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器 (p. 33)。对于 Ubuntu，请参阅以下 Ubuntu 社区文档：ApacheMySQLPHP。有关其他发布版本，请参阅特定于该版本的文档。

选项：使用 Automation 完成本教程

要使用 Amazon Systems Manager Automation 而不是以下任务完成本教程，请运行 AmazonDocs-InstallALAMPServer-AL2 Automation 文档。

任务

- 步骤 1：准备 LAMP 服务器 (p. 24)
- 步骤 2：测试 LAMP 服务器 (p. 27)
- 步骤 3：确保数据库服务器的安全 (p. 28)
- 步骤 4：(可选) 安装 phpMyAdmin (p. 29)
- 问题排查 (p. 32)
- 相关主题 (p. 32)

步骤 1：准备 LAMP 服务器

先决条件

- 本教程假定您已经使用 Amazon Linux 2 启动具有可从 Internet 访问的公有 DNS 名称的新实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。您还必须配置安全组，以便允许 SSH (端口 22)、HTTP (端口 80) 和 HTTPS (端口 443) 连接。有关这些先决条件的更多信息，请参阅 为您的 Linux 实例授权入站流量 (p. 1287)。
- 以下过程将安装 Amazon Linux 2 上可用的最新 PHP 版本（当前为 PHP 7.2）。如果您计划使用本教程中所述的 PHP 应用程序之外的 PHP 应用程序，则应检查其与 PHP 7.2 的兼容性。

> **Note**
>
> 请注意，此安装软件包使用 Mariadb (lamp-mariadb10.2-php7.2) 进行捆绑。此后，php7.2 中的许多漏洞已通过 Amazon 修补逆向移植，但是，您的特定安全软件可能仍会标记此版本的 PHP。确保经常执行系统更新。您可以选择安装新版本的 PHP，但是您需要单独安装 MariaDB。

准备 LAMP 服务器

1. 连接到您的 实例 (p. 11)。
2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. 安装 lamp-mariadb10.2-php7.2 和 php7.2 Amazon LinuxExtras 存储库，以获取适用于 Amazon Linux 2 的 LAMP MariaDB 和 PHP 程序包的最新版本。

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
   ```

   如果您收到指示 sudo: amazon-linux-extras: command not found 的错误，则表示您的实例未与 Amazon Linux 2 AMI 一起启动（也许您可以改用 Amazon Linux AMI）。您可以使用以下命令查看 Amazon Linux 的版本。

   ```
   cat /etc/system-release
   ```

   要在 Amazon Linux AMI 上设置 LAMP Web 服务器，请参阅教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器 (p. 33)。
4. 您的实例处于最新状态后，便可以安装 Apache Web 服务器、MariaDB 和 PHP 软件包。

   使用 yum install 命令可同时安装多个软件包和所有相关依赖项。

   ```
   [ec2-user ~]$ sudo yum install -y httpd mariadb-server
   ```

   您可以使用以下命令查看这些程序包的当前版本：

   ```
   yum info package_name
   ```

5. 启动 Apache Web 服务器。

   ```
   [ec2-user ~]$ sudo systemctl start httpd
   ```

6. 使用 systemctl 命令配置 Apache Web 服务器，使其在每次系统启动时启动。

   ```
   [ec2-user ~]$ sudo systemctl enable httpd
   ```

   您可以通过运行以下命令验证 httpd 是否已启用：

   ```
   [ec2-user ~]$ sudo systemctl is-enabled httpd
   ```

7. 如果您尚未这样做，请添加安全规则以允许与您的实例的入站 HTTP (端口 80) 连接。默认情况下，初始化期间将为您的实例设置 launch-wizard-*N* 安全组。此组包含一条允许 SSH 连接的规则。

   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 选择 Instances 并选择您的实例。
   c. 在安全选项卡上，查看入站规则。您应看到以下规则：

   ```
   Port range   Protocol     Source
   ```

```
22              tcp             0.0.0.0/0
```

Warning

使用 0.0.0.0/0 可允许所有 IPv4 地址使用 SSH 访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产环境中，您仅授权特定 IP 地址或地址范围访问您的实例。

d. 选择安全组的链接。使用 向安全组添加规则 (p. 1311) 中的过程，添加具有以下值的新入站安全规则：

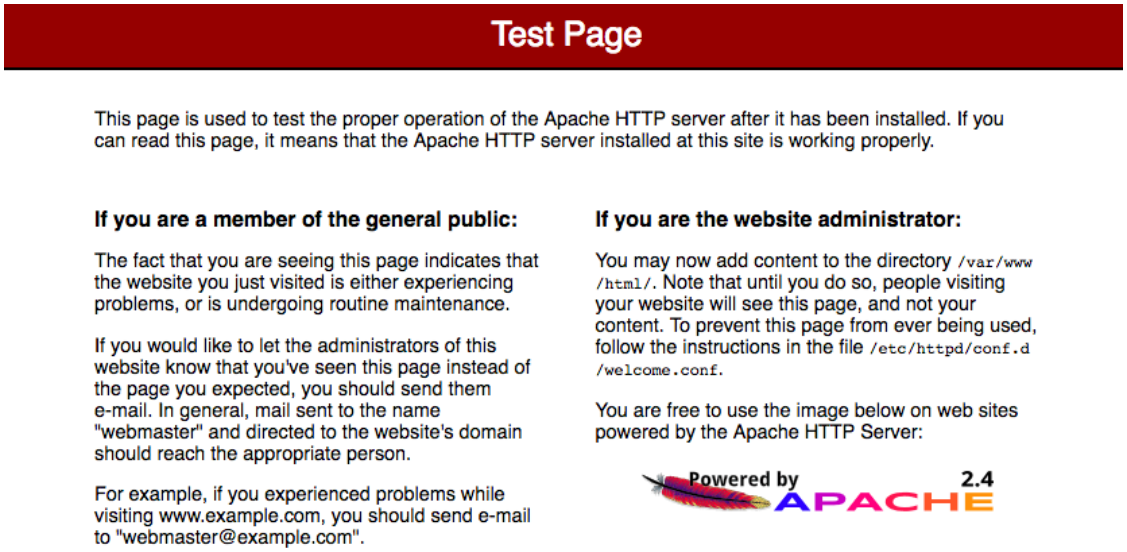
- Type：HTTP
- Protocol：TCP
- Port Range：80
- Source：Custom

8. 测试您的 Web 服务器。在 Web 浏览器中，键入您的实例的公有 DNS 地址 (或公有 IP 地址)。如果 /var/www/html 中没有内容，您应该会看到 Apache 测试页面。您可以使用 Amazon EC2 控制台获取实例的公有 DNS（选中 Public DNS (公有 DNS) 列；如果此列处于隐藏状态，请选择 Show/Hide Columns (显示/隐藏列)（齿轮状图标）并选择 Public DNS (公有 DNS)）。

   验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

   Important

   如果您使用的不是 Amazon Linux，则还可能需要在实例上配置防火墙才能允许这些连接。有关如何配置防火墙的更多信息，请参阅适用于特定分配的文档。



Apache httpd 提供的文件保存在名为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录为 /var/www/html，默认情况下归根用户所有。

要允许 ec2-user 账户操作此目录中的文件，必须修改其所有权和权限。有多种方式可以完成此任务。在本教程中，可将 ec2-user 添加到 apache 组，将 /var/www 目录的所有权授予 apache 组，并为该组指定写入权限。

设置文件权限

1. 将您的用户 (这里指 ec2-user) 添加到 apache。

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. 先退出再重新登录以选取新组，然后验证您的成员资格。

   a. 退出（使用 exit 命令或关闭终端窗口）：

   ```
   [ec2-user ~]$ exit
   ```

   b. 要验证您是否为 apache 组的成员，请重新连接到实例，然后运行以下命令：

   ```
   [ec2-user ~]$ groups
   ec2-user adm wheel apache systemd-journal
   ```

3. 将 /var/www 及其内容的组所有权更改到 apache 组。

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. 要添加组写入权限以及设置未来子目录上的组 ID，请更改 /var/www 及其子目录的目录权限。

```
[ec2-user ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775
 {} \;
```

5. 要添加组写入权限，请递归地更改 /var/www 及其子目录的文件权限：

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

这样，ec2-user (和 apache 组的任何未来成员) 可以添加、删除和编辑 Apache 文档根目录中的文件，允许您添加内容，如静态网站或 PHP 应用程序。

保护您的 Web 服务器 (可选)

运行 HTTP 协议的 Web 服务器不为其发送或接收的数据提供传输安全。当您使用 Web 浏览器连接 HTTP 服务器时，对于您访问的 URL、您接收的网页内容以及您提交的任何 HTML 表的内容 (包括密码)，窃取者可在网络路径上的任何位置看到。保护您的 Web 服务器的最佳实践是安装 HTTPS (HTTP Secure) 支持，它将使用 SSL/TLS 加密保护您的数据。

有关在服务器上启用 HTTPS 的信息，请参阅 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。

步骤 2：测试 LAMP 服务器

如果服务器已安装并运行，且文件权限设置正确，则 ec2-user 账户应该能够在 /var/www/html 目录 (可从 Internet 访问) 中创建 PHP 文件。

测试您的 LAMP 服务器

1. 在 Apache 文档根目录中创建一个 PHP 文件。

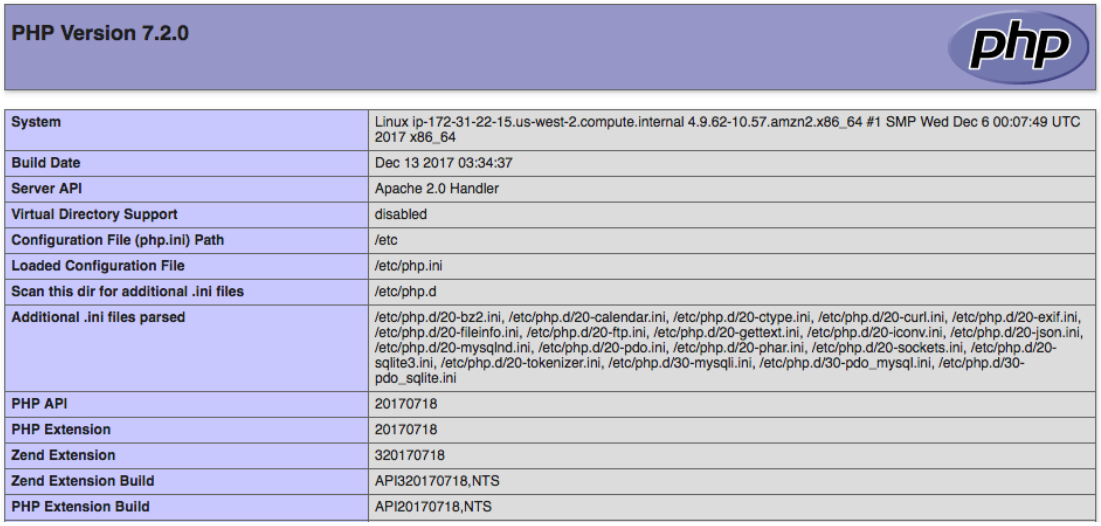
```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

   尝试运行该命令时，如果出现“Permission denied (权限被拒绝)”错误，请尝试先注销，再重新登录，以获取您在 设置文件权限 (p. 27) 中配置的适当组权限。

2. 在 Web 浏览器中，键入您刚刚创建的文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。例如：

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该会看到 PHP 信息页面：



PHP Version 7.2.0

System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64 #1 SMP Wed Dec 6 00:07:49 UTC 2017 x86_64
Build Date	Dec 13 2017 03:34:37
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

如果您未看到此页面，请验证上一步中是否已正确创建 `/var/www/html/phpinfo.php` 文件。您还可以使用以下命令验证已经安装了所有必需的程序包。

```
[ec2-user ~]$ sudo yum list installed httpd mariadb-server php-mysqlnd
```

如果输出中未列出任何必需的程序包，请使用 sudo yum install ***package*** 命令安装它们。另请验证在 `php7.2` 命令的输出中启用了 `lamp-mariadb10.2-php7.2` 和 amazon-linux-extras Extras。

3. 删除 `phpinfo.php` 文件。尽管此信息可能很有用，但出于安全考虑，不应将其传播到 Internet。

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

现在，您应该有了一个功能完善的 LAMP Web 服务器。如果您将内容添加到 Apache 文档根目录 (位于 `/var/www/html`)，您应该能够在您的实例的公有 DNS 地址中看到该内容。

步骤 3：确保数据库服务器的安全

MariaDB 服务器的默认安装提供有多种功能，这些功能对于测试和开发都很有帮助，但对于产品服务器，应禁用或删除这些功能。mysql_secure_installation 命令可引导您设置根密码并删除安装中的不安全功能。即使您不打算使用 MariaDB 服务器，我们也建议执行此步骤。

保护 MariaDB 服务器

1. 启动 MariaDB 服务器。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

2. 运行 mysql_secure_installation。

```
[ec2-user ~]$ sudo mysql_secure_installation
```

a. 在提示时，键入根账户的密码。

   i. 键入当前根密码。默认情况下，根账户没有设置密码。按 Enter。

   ii. 键入 **Y** 设置密码，然后键入两次安全密码。有关创建安全密码的更多信息，请访问 https://identitysafe.norton.com/password-generator/。确保将此密码存储在安全位置。

   设置 MariaDB 根密码仅是保护数据库的最基本措施。在您构建或安装数据库驱动的应用程序时，您通常可以为该应用程序创建数据库服务用户，并避免使用根账户执行除数据库管理以外的操作。

b. 键入 **Y** 删除匿名用户账户。

c. 键入 **Y** 禁用远程根登录。

d. 键入 **Y** 删除测试数据库。

e. 键入 **Y** 重新加载权限表并保存您的更改。

3. (可选) 如果您不打算立即使用 MariaDB 服务器，请停止它。您可以在需要时再次重新启动。

```
[ec2-user ~]$ sudo systemctl stop mariadb
```

4. (可选) 如果您希望每次启动时 MariaDB 服务器都启动，请键入以下命令。

```
[ec2-user ~]$ sudo systemctl enable mariadb
```

步骤 4：(可选) 安装 phpMyAdmin

phpMyAdmin 是一种基于 Web 的数据库管理工具，可用于在 EC2 实例上查看和编辑 MySQL 数据库。按照下述步骤操作，在您的 Amazon Linux 实例上安装和配置 phpMyAdmin。

> **Important**
>
> 除非您在 Apache 中启用了 SSL/TLS，否则我们不建议您使用 phpMyAdmin 访问 LAMP 服务器；如果您使用 phpMyAdmin，您的数据库管理员密码和其他数据将无法安全地通过 Internet 传输。有关开发人员提供的安全建议，请参阅保护 phpMyAdmin 安装。有关在 EC2 实例上保护 Web 服务器的一般信息，请参阅 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。

安装 phpMyAdmin

1. 安装所需的依赖项。

```
[ec2-user ~]$ sudo yum install php-mbstring php-xml -y
```

2. 重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

3. 重启 php-fpm.

```
[ec2-user ~]$ sudo systemctl restart php-fpm
```

4. 导航到位于 /var/www/html 的 Apache 文档根。

```
[ec2-user ~]$ cd /var/www/html
```

5. 从 https://www.phpmyadmin.net/downloads 选择最新 phpMyAdmin 发行版的源软件包。要将文件直接下载到您的实例，请复制链接并将其粘贴到 wget 命令，如本示例中所述：

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. 使用以下命令创建 phpMyAdmin 文件夹并将程序包提取到其中。

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. 删除 *phpMyAdmin-latest-all-languages.tar.gz* tarball。

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (可选) 如果 MySQL 服务器未运行，请立即启动它。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

9. 在 Web 浏览器中，键入 phpMyAdmin 安装的 URL。此 URL 是实例的公有 DNS 地址 (或公有 IP 地址)，后接正斜杠和您安装目录的名称。例如：

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

您应该会看到 phpMyAdmin 登录页面：



10. 使用您先前创建的 `root` 用户名和 MySQL 根密码登录到 phpMyAdmin 安装。

    您的安装仍需进行配置，然后才能投入使用。我们建议您首先手动创建配置文件，如下所示：

    a. 要从最小的配置文件开始，请使用您常用的文本编辑器创建一个新文件，然后将 `config.sample.inc.php` 的内容复制到该文件中。
    b. 在包含 `config.inc.php` 的 phpMyAdmin 目录中将文件保存为 `index.php`。
    c. 有关任何其他设置，请参阅 phpMyAdmin 安装说明的使用设置脚本部分中的文件后创建说明。

有关使用 phpMyAdmin 的信息，请参阅 phpMyAdmin 用户指南。

问题排查

本部分提供了解决在设置新 LAMP 服务器时可能遇到的常见问题的建议。

我无法使用 Web 浏览器连接到我的服务器

执行以下检查以查看您的 Apache Web 服务器是否正在运行且可以访问。

- Web 服务器正在运行吗？

  您可以通过运行以下命令验证 httpd 是否已启用：

  ```
  [ec2-user ~]$ sudo systemctl is-enabled httpd
  ```

  如果 httpd 进程未运行，请重复准备 LAMP 服务器 (p. 25)中描述的步骤。
- 防火墙是否配置正确？

  验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

我无法使用 HTTPS 连接到我的服务器

执行以下检查以查看 Apache Web 服务器是否配置为支持 HTTPS。

- Web 服务器配置是否正确？

  安装 Apache 后，服务器将针对 HTTP 流量进行配置。要支持 HTTPS，请在服务器上启用 TLS 并安装 SSL 证书。有关信息，请参阅 教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。
- 防火墙是否配置正确？

  验证实例的安全组是否包含允许端口 443 上的 HTTPS 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

相关主题

有关将文件传输到您的实例或在 Web 服务器上安装 WordPress 博客的更多信息，请参阅以下文档：

- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 666)
- 使用 SCP 客户端将文件传输到 Linux 实例 (p. 651)
- 教程：在上托管 WordPress 博客 Amazon Linux 2 (p. 93)

有关本教程中使用的命令和软件的更多信息，请参阅以下网页：

- Apache Web 服务器：http://httpd.apache.org/
- MariaDB 数据库服务器：https://mariadb.org/
- PHP 编程语言：http://php.net/
- chmod 命令：https://en.wikipedia.org/wiki/Chmod

- chown 命令：https://en.wikipedia.org/wiki/Chown

有关注册 Web 服务器域名或将现有域名转移到此主机的更多信息，请参阅 Amazon Route 53 开发人员指南中的创建域和子域并将其迁移到 Amazon Route 53。

教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器

通过以下步骤，您可以将支持 PHP 和 MySQL 的 Apache Web 服务器 (有时称为 LAMP Web 服务器或 LAMP 堆栈) 安装到您的 Amazon Linux 实例上。您可以使用此服务器来托管静态网站或部署能对数据库中的信息执行读写操作的动态 PHP 应用程序。

> **Important**
>
> 如果您尝试在其他发行版（例如 Ubuntu 或红帽企业 Linux）上设置 LAMP Web 服务器，则本教程不适合。对于 Amazon Linux 2，请参阅教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)。对于 Ubuntu，请参阅以下 Ubuntu 社区文档：ApacheMySQLPHP。有关其他发布版本，请参阅特定于该版本的文档。

选项：使用 Automation 完成本教程

要使用 Amazon Systems Manager Automation 而不是以下任务完成本教程，请运行 AmazonDocs-InstallALAMPServer-AL Automation 文档。

任务

- 步骤 1：准备 LAMP 服务器 (p. 33)
- 步骤 2：测试 Lamp 服务器 (p. 36)
- 步骤 3：确保数据库服务器的安全 (p. 37)
- 步骤 4：(可选) 安装 phpMyAdmin (p. 38)
- 问题排查 (p. 41)
- 相关主题 (p. 42)

步骤 1：准备 LAMP 服务器

先决条件

本教程假定您已经使用 Amazon Linux AMI 启动具有可从 Internet 访问的公有 DNS 名称的新实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。您还必须配置安全组，以便允许 SSH (端口 22)、HTTP (端口 80) 和 HTTPS (端口 443) 连接。有关这些先决条件的更多信息，请参阅 为您的 Linux 实例授权入站流量 (p. 1287)。

使用 Amazon Linux AMI 安装和启动 LAMP Web 服务器

1. 连接到您的 实例 (p. 11)。
2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. 您的实例处于最新状态后，便可以安装 Apache Web 服务器、MySQL 和 PHP 软件包。

   Important

   一些应用程序可能与以下建议的软件环境不兼容。在安装这些软件包之前，请检查您的 LAMP 应用程序是否与其兼容。如果出现问题，您可能需要安装替代环境。有关更多信息，请参阅 我想在我的服务器上运行的应用程序软件与所安装的 PHP 版本或其他软件不兼容 (p. 41)

   使用 yum install 命令可同时安装多个软件包和所有相关依赖项。

   ```
   [ec2-user ~]$ sudo yum install -y httpd24 php72 mysql57-server php72-mysqlnd
   ```

   如果您收到错误 No package *package-name* available，则表示您的实例未使用 Amazon Linux AMI 启动（可能您使用的是 Amazon Linux 2）。您可以使用以下命令查看 Amazon Linux 的版本。

   ```
   cat /etc/system-release
   ```

4. 启动 Apache Web 服务器。

   ```
   [ec2-user ~]$ sudo service httpd start
   Starting httpd:                                            [  OK  ]
   ```

5. 使用 chkconfig 命令配置 Apache Web 服务器，使其在每次系统启动时启动。

   ```
   [ec2-user ~]$ sudo chkconfig httpd on
   ```

   当您成功地使用 chkconfig 命令启用服务时，该命令不提供任何确认消息。

   您可以通过运行以下命令验证 httpd 是否已启用：

   ```
   [ec2-user ~]$ chkconfig --list httpd
   httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
   ```

   在这里，httpd 是处于运行级别 2、3、4 和 5 的 on（这是您希望看到的）。

6. 如果您尚未这样做，请添加安全规则以允许与您的实例的入站 HTTP (端口 80) 连接。默认情况下，初始化期间将为您的实例设置 launch-wizard-*N* 安全组。此组包含一条允许 SSH 连接的规则。

   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 选择 Instances 并选择您的实例。
   c. 在安全选项卡上，查看入站规则。您应看到以下规则：

      ```
      Port range   Protocol     Source
      22           tcp          0.0.0.0/0
      ```

      Warning

      使用 0.0.0.0/0 可允许所有 IPv4 地址使用 SSH 访问您的实例。这在测试环境中可以接受一小段时间，但是在生产环境中并不安全。在生产环境中，您仅授权特定 IP 地址或地址范围访问您的实例。

   d. 选择安全组的链接。使用 向安全组添加规则 (p. 1311) 中的过程，添加具有以下值的新入站安全规则：

      - Type：HTTP
      - Protocol：TCP
      - Port Range：80

- Source：Custom

7. 测试您的 Web 服务器。在 Web 浏览器中，键入您的实例的公有 DNS 地址 (或公有 IP 地址)。可以使用 Amazon EC2 控制台获取实例的公有 DNS 地址。如果 /var/www/html 中没有内容，您应该会看到 Apache 测试页面。将内容添加到文档根目录后，您的内容将显示在您的实例的公有 DNS 地址中，而不显示在本测试页面。

   验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

   如果您使用的不是 Amazon Linux，则还可能需要在实例上配置防火墙才能允许这些连接。有关如何配置防火墙的更多信息，请参阅适用于特定分配的文档。

Apache httpd 提供的文件保存在名为 Apache 文档根目录的目录中。Amazon Linux Apache 文档根目录为 /var/www/html，默认情况下归根用户所有。

```
[ec2-user ~]$ ls -l /var/www
total 16
drwxr-xr-x 2 root root 4096 Jul 12 01:00 cgi-bin
drwxr-xr-x 3 root root 4096 Aug  7 00:02 error
drwxr-xr-x 2 root root 4096 Jan  6  2012 html
drwxr-xr-x 3 root root 4096 Aug  7 00:02 icons
drwxr-xr-x 2 root root 4096 Aug  7 21:17 noindex
```

要允许 ec2-user 账户操作此目录中的文件，必须修改其所有权和权限。有多种方式可以完成此任务。在本教程中，可将 ec2-user 添加到 apache 组，将 /var/www 目录的所有权授予 apache 组，并为该组指定写入权限。

设置文件权限

1. 将您的用户 (这里指 ec2-user) 添加到 apache。

   ```
   [ec2-user ~]$ sudo usermod -a -G apache ec2-user
   ```

2. 先退出再重新登录以选取新组，然后验证您的成员资格。

   a. 退出（使用 exit 命令或关闭终端窗口）：

      ```
      [ec2-user ~]$ exit
      ```

   b. 要验证您是否为 apache 组的成员，请重新连接到实例，然后运行以下命令：

      ```
      [ec2-user ~]$ groups
      ec2-user wheel apache
      ```

3. 将 /var/www 及其内容的组所有权更改到 apache 组。

   ```
   [ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
   ```

4. 要添加组写入权限以及设置未来子目录上的组 ID，请更改 /var/www 及其子目录的目录权限。

   ```
   [ec2-user ~]$ sudo chmod 2775 /var/www
   [ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
   ```

5. 要添加组写入权限，请递归地更改 /var/www 及其子目录的文件权限：

   ```
   [ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
   ```

这样，ec2-user (和 apache 组的任何未来成员) 可以添加、删除和编辑 Apache 文档根目录中的文件，允许您添加内容，如静态网站或 PHP 应用程序。

(可选) 保护您的 Web 服务器

运行 HTTP 协议的 Web 服务器不为其发送或接收的数据提供传输安全。当您使用 Web 浏览器连接 HTTP 服务器时，对于您访问的 URL、您接收的网页内容以及您提交的任何 HTML 表的内容 (包括密码)，窃取者可在网络路径上的任何位置看到。保护您的 Web 服务器的最佳实践是安装 HTTPS (HTTP Secure) 支持，它将使用 SSL/TLS 加密保护您的数据。

有关在服务器上启用 HTTPS 的信息，请参阅 教程：使用 Amazon Linux AMI 配置 SSL/TLS (p. 68)。

步骤 2：测试 Lamp 服务器

如果服务器已安装并运行，且文件权限设置正确，则 ec2-user 账户应该能够在 /var/www/html 目录 (可从 Internet 访问) 中创建 PHP 文件。

测试您的 LAMP Web 服务器

1. 在 Apache 文档根目录中创建一个 PHP 文件。

   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   尝试运行该命令时，如果出现“Permission denied (权限被拒绝)”错误，请尝试先注销，再重新登录，以获取您在 步骤 1：准备 LAMP 服务器 (p. 33) 中配置的适当组权限。

2. 在 Web 浏览器中，键入您刚刚创建的文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。例如：

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   您应该会看到 PHP 信息页面：

   PHP Version 7.2.0

System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64 #1 SMP Wed Dec 6 00:07:49 UTC 2017 x86_64
Build Date	Dec 13 2017 03:34:37
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

   如果您未看到此页面，请验证上一步中是否已正确创建 /var/www/html/phpinfo.php 文件。您还可以使用以下命令验证已经安装了所有必需的程序包。第二列中的程序包版本不需要与此示例输出匹配。

   ```
   [ec2-user ~]$ sudo yum list installed httpd24 php72 mysql57-server php72-mysqlnd
   Loaded plugins: priorities, update-motd, upgrade-helper
   ```

```
Installed Packages
httpd24.x86_64                          2.4.25-1.68.amzn1                   @amzn-
updates
mysql56-server.x86_64                   5.6.35-1.23.amzn1                   @amzn-
updates
php70.x86_64                            7.0.14-1.20.amzn1                   @amzn-
updates
php70-mysqlnd.x86_64                    7.0.14-1.20.amzn1                   @amzn-
updates
```

如果输出中未列出任何必需的程序包，请使用 sudo yum install ***package*** 命令安装它们。

3. 删除 phpinfo.php 文件。尽管此信息可能很有用，但出于安全考虑，不应将其传播到 Internet。

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

步骤 3：确保数据库服务器的安全

MySQL 服务器的默认安装提供有多种功能，这些功能对于测试和开发都很有帮助，但对于产品服务器，应禁用或删除这些功能。mysql_secure_installation 命令可引导您设置根密码并删除安装中的不安全功能。即使您不打算使用 MySQL 服务器，我们也建议执行此步骤。

确保数据库服务器的安全

1. 启动 MySQL 服务器。

```
[ec2-user ~]$ sudo service mysqld start
Initializing MySQL database:
...

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
...

Starting mysqld:                                           [  OK  ]
```

2. 运行 mysql_secure_installation。

```
[ec2-user ~]$ sudo mysql_secure_installation
```

   a. 在提示时，键入根账户的密码。

      i. 键入当前根密码。默认情况下，根账户没有设置密码。按 Enter。

      ii. 键入 **Y** 设置密码，然后键入两次安全密码。有关创建安全密码的更多信息，请访问 https://identitysafe.norton.com/password-generator/。确保将此密码存储在安全位置。

      设置 MySQL 根密码仅是保护数据库的最基本措施。在您构建或安装数据库驱动的应用程序时，您通常可以为该应用程序创建数据库服务用户，并避免使用根账户执行除数据库管理以外的操作。

   b. 键入 **Y** 删除匿名用户账户。

   c. 键入 **Y** 禁用远程根登录。

   d. 键入 **Y** 删除测试数据库。

   e. 键入 **Y** 重新加载权限表并保存您的更改。

3. (可选) 如果您不打算立即使用 MySQL 服务器，请停止它。您可以在需要时再次重新启动。

```
[ec2-user ~]$ sudo service mysqld stop
```

```
Stopping mysqld:                                           [  OK  ]
```

4. (可选) 如果您希望每次启动时 MySQL 服务器都启动，请键入以下命令。

```
[ec2-user ~]$ sudo chkconfig mysqld on
```

现在，您应该有了一个功能完善的 LAMP Web 服务器。如果您将内容添加到 Apache 文档根目录 (位于 `/var/www/html`)，您应该能够在您的实例的公有 DNS 地址中看到该内容。

步骤 4：(可选) 安装 phpMyAdmin

安装 phpMyAdmin

phpMyAdmin 是一种基于 Web 的数据库管理工具，可用于在 EC2 实例上查看和编辑 MySQL 数据库。按照下述步骤操作，在您的 Amazon Linux 实例上安装和配置 phpMyAdmin。

> **Important**
>
> 除非您在 Apache 中启用了 SSL/TLS，否则我们不建议您使用 phpMyAdmin 访问 LAMP 服务器；如果您使用 phpMyAdmin，您的数据库管理员密码和其他数据将无法安全地通过 Internet 传输。有关开发人员提供的安全建议，请参阅保护 phpMyAdmin 安装。

> **Note**
>
> Amazon Linux 包管理系统当前不支持 PHP 7 环境中的 phpMyAdmin 自动安装。本教程介绍如何手动安装 phpMyAdmin。

1. 使用 SSH 登录您的 EC2 实例。
2. 安装所需的依赖项。

```
[ec2-user ~]$ sudo yum install php72-mbstring.x86_64 -y
```

3. 重启 Apache。

```
[ec2-user ~]$ sudo service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
```

4. 导航到位于 `/var/www/html` 的 Apache 文档根。

```
[ec2-user ~]$ cd /var/www/html
[ec2-user html]$
```

5. 从 https://www.phpmyadmin.net/downloads 选择最新 phpMyAdmin 发行版的源软件包。要将文件直接下载到您的实例，请复制链接并将其粘贴到 wget 命令，如本示例中所述：

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. 使用以下命令创建 phpMyAdmin 文件夹并将程序包提取到其中。

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. 删除 *phpMyAdmin-latest-all-languages.tar.gz* tarball。

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (可选) 如果 MySQL 服务器未运行，请立即启动它。

```
[ec2-user ~]$ sudo service mysqld start
Starting mysqld:                                           [  OK  ]
```

9. 在 Web 浏览器中，键入 phpMyAdmin 安装的 URL。此 URL 是实例的公有 DNS 地址 (或公有 IP 地址)，后接正斜杠和您安装目录的名称。例如：

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

您应该会看到 phpMyAdmin 登录页面：



10. 使用您先前创建的 `root` 用户名和 MySQL 根密码登录到 phpMyAdmin 安装。

    您的安装仍需进行配置，然后才能投入使用。要配置 phpMyAdmin，您可以手动创建配置文件、使用设置控制台或者结合这两种方法。

    有关使用 phpMyAdmin 的信息，请参阅 phpMyAdmin 用户指南。

问题排查

本部分提供了解决在设置新 LAMP 服务器时可能遇到的常见问题的建议。

我无法使用 Web 浏览器连接到我的服务器。

执行以下检查以查看您的 Apache Web 服务器是否正在运行且可以访问。

- Web 服务器正在运行吗？

  您可以通过运行以下命令验证 httpd 是否已启用：

```
[ec2-user ~]$ chkconfig --list httpd
httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

  在这里，httpd 是处于运行级别 2、3、4 和 5 的 on（这是您希望看到的）。

  如果 httpd 进程未运行，请重复步骤 1：准备 LAMP 服务器 (p. 33)中描述的步骤。
- 防火墙是否配置正确？

  验证实例的安全组是否包含允许端口 80 上的 HTTP 流量的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

我想在我的服务器上运行的应用程序软件与所安装的 PHP 版本或其他软件不兼容

本教程建议安装最新版本的 Apache HTTP Server、PHP 和 MySQL。在安装其他 LAMP 应用程序之前，请检查其要求以确认它们与已安装的环境兼容。如果不支持最新版本的 PHP，则可以 (并且完全安全) 降级到较旧的受支持配置。您还可以并行安装 PHP 的多个版本，至少可以解决部分兼容性问题。有关如何从安装的多个版本 PHP 中选择其一配置为首选项的信息，请参阅 Amazon Linux AMI 2016.09 发行说明。

如何降级

本教程的以前版本经过良好测试，需要以下核心 LAMP 程序包：

- httpd24
- php56
- mysql55-server
- php56-mysqlnd

如果您已按照本教程开头的建议安装了最新的软件包，您必须首先卸载如下这些软件包和其他依赖项：

```
[ec2-user ~]$ sudo yum remove -y httpd24 php72 mysql57-server php72-mysqlnd perl-DBD-
MySQL57
```

其次，安装替代环境：

```
[ec2-user ~]$ sudo yum install -y  httpd24 php56 mysql55-server php56-mysqlnd
```

如果您以后决定升级到建议的环境，您必须先删除自定义软件包和依赖项：

```
[ec2-user ~]$ sudo yum remove -y  httpd24 php56 mysql55-server php56-mysqlnd perl-DBD-
MySQL56
```

现在，您可以如前所述安装最新版的软件包。

相关主题

有关将文件传输到您的实例或在 Web 服务器上安装 WordPress 博客的更多信息，请参阅以下文档：

- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 666)
- 使用 SCP 客户端将文件传输到 Linux 实例 (p. 651)
- 教程：在上托管 WordPress 博客 Amazon Linux 2 (p. 93)

有关本教程中使用的命令和软件的更多信息，请参阅以下网页：

- Apache Web 服务器：http://httpd.apache.org/
- MySQL 数据库服务器：http://www.mysql.com/
- PHP 编程语言：http://php.net/
- chmod 命令：https://en.wikipedia.org/wiki/Chmod
- chown 命令：https://en.wikipedia.org/wiki/Chown

有关注册 Web 服务器域名或将现有域名转移到此主机的更多信息，请参阅 Amazon Route 53 开发人员指南中的创建域和子域并将其迁移到 Amazon Route 53。

教程：在 Amazon Linux 2023 上配置 SSL/TLS

安全套接字层/传输层安全性 (SSL/TLS) 可在 Web 服务器和 Web 客户端之间创建一个加密通道，以防止数据在传输过程中被窃听。本教程介绍如何在具有 Amazon Linux 2023 和 Apache Web 服务器的 EC2 实例上手动添加对 SSL/TLS 的支持。本教程假定您未使用负载均衡器。如果您正在使用 Elastic Load Balancing，则可以选择使用来自 Amazon Certificate Manager 的证书在负载均衡器上配置 SSL 卸载。

由于历史原因，Web 加密通常简称为 SSL。虽然 Web 浏览器仍支持 SSL，但使用其下一代协议 TLS 更不易受攻击。默认情况下，Amazon Linux 2023 将禁用所有版本的 SSL 的服务器端支持。安全标准机构认为 TLS 1.0 不安全。TLS 1.0 和 TLS 1.1 已于 2021 年 3 月正式弃用。本教程仅包含有关启用 TLS 1.2 的指导。TLS 1.3 于 2018 年定版，只需支持和启用底层 TLS 库（本教程中为 OpenSSL）即可在 Amazon Linux 2 中使用。客户端必须在 2023 年 6 月 28 日之前支持 TLS 1.2 或更高版本。有关更新的加密标准的更多信息，请参阅 RFC 7568 和 RFC 8446。

在本教程中，将现代 Web 加密简称为 TLS。

> **Important**
>
> 这些过程适用于 Amazon Linux 2023。如果您尝试设置运行不同分配的 EC2 实例，或者运行旧版本 Amazon Linux 的实例，则本教程中的一些过程可能不适合。对于 Amazon Linux 2，请参阅教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。对于 Ubuntu，请参阅以下 Ubuntu 社区文档：Open SSL on Ubuntu。有关 Red Hat Enterprise Linux 的信息，请参阅以下：设置 Apache HTTP Web 服务器。有关其他发布版本，请参阅特定于该版本的文档。

> **Note**
>
> 或者，您还可以使用适用于 Amazon Nitro Enclaves 的 Amazon Certificate Manager (ACM)，这是一个 Enclave 应用程序，可使您通过 Amazon Nitro Enclaves 将公有和私有 SSL/TLS 证书与在 Amazon EC2 实例上运行的 Web 应用程序和服务器一起使用。Nitro Enclaves 是一项 Amazon EC2 功能，可以创建隔离的计算环境以保护和安全地处理高度敏感的数据，例如 SSL/TLS 证书和私有密钥。

适用于 Nitro Enclaves 的 ACM 与运行在 Amazon EC2 Linux 实例上的 nginx 结合使用，以创建私有密钥、分发证书和私有密钥以及管理证书续订。
要使用适用于 Nitro Enclaves 的 ACM，必须使用启用了 Enclave 的 Linux 实例。
有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？和适用于 Nitro Enclaves 的 Amazon Certificate Manager。

目录

- 先决条件 (p. 43)
- 步骤 1：在服务器上启用 TLS (p. 43)
- 步骤 2：获取 CA 签名的证书 (p. 45)
- 步骤 3：测试和强化安全配置 (p. 49)
- 问题排查 (p. 51)
- 证书自动化：在 Amazon Linux 2023 上将 Let's Encrypt 与 Certbot 结合使用 (p. 52)

先决条件

在开始本教程之前，请完成以下步骤：

- 启动由 EBS 支持的 Amazon Linux 2023 实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。
- 配置安全组以允许您的实例接受以下 TCP 端口上的连接：
  - SSH (端口 22)
  - HTTP (端口 80)
  - HTTPS (端口 443)

  有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
- 安装 Apache Web 服务器。有关分步说明，请参阅教程：在 Amazon Linux 2023 上安装 LAMP Web 服务器 (p. 15)。仅需要 httpd 包及其依赖项，因此可以忽略涉及 PHP 和 MariaDB 的说明。
- 要识别和验证网站，TLS 公有密钥基础设施 (PKI) 依赖于域名系统 (DNS)。要使用 EC2 实例托管公共网站，您需要为 Web 服务器注册一个域名，或者将现有域名转让给您的 Amazon EC2 主机。可通过很多第三方域注册和 DNS 托管服务来执行此操作，也可以使用 Amazon Route 53 执行此操作。

步骤 1：在服务器上启用 TLS

此过程将指导您完成在 Amazon Linux 2023 上使用自签名数字证书设置 TLS 的过程。

Note

自签名证书对于测试是可接受的，但对于生产不是。如果您将自签名证书公开到 Internet，您网站的访客将会看到安全警告。

在服务器上启用 TLS

1. 连接到您的实例 (p. 11)并确认 Apache 正在运行。

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

如果返回的值不是“启用”，则启动 Apache 并将它设置为每次随系统一起启动。

```
[ec2-user ~]$ sudo systemctl start httpd && sudo systemctl enable httpd
```

2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   Note

   -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

```
[ec2-user ~]$ sudo dnf install openssl mod_ssl
```

3. 输入以下命令后，系统将向您显示提示框，您可以在其中输入有关站点的信息。

```
[ec2-user ~]$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/
pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/certs/apache-selfsigned.crt
```

   这会在 /etc/pki/tls/certs/ 目录中生成一个新文件 localhost.crt。指定的文件名与 /etc/httpd/conf.d/ssl.conf 中的 SSLCertificateFile 指令指定的默认值匹配。

   您的实例现在具有以下文件，可使用这些文件配置安全服务器并创建证书以进行测试：

   - /etc/httpd/conf.d/ssl.conf

     mod_ssl 的配置文件。它包含一些指令 以指示 Apache 在何处查找以下信息：加密密钥和证书、要允许的 TLS 协议版本以及要接受的加密密码。这将是您的本地证书文件：

   - /etc/pki/tls/certs/localhost.crt

   该文件包含自签名证书以及证书的私有密钥。Apache 要求证书和密钥采用 PEM 格式，其中包含 Base64 编码的 ASCII 字符，并用“BEGIN”和“END”行框起来，如以下简短示例所示。

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLjOOCI8u1PTcGmAah5kEitCEc0wzmNeo
BCl0wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMZoT
...
56tE7THvH7vOEf4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs
27hDzPDinrquSEvoZIggkDMlh2irTiipJ/GhkvTpoQlv0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U6O4FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo
4QQvAqOa8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3DlK44D9dlU3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----END CERTIFICATE-----
```

   文件名和扩展名只是为了提供便利，对功能没有影响。例如，只要 ssl.conf 文件中的相关指令使用相同的名称，您就可以将证书命名为 cert.crt、cert.pem 或任何其他文件名。

   Note

   在使用您自己的自定义文件替换默认 TLS 文件时，请确保它们采用 PEM 格式。

4. 重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

Note

确保 TCP 端口 443 在您的 EC2 实例上是可访问的，如之前所述。

5. 现在，您的 Apache Web 服务器应通过端口 443 支持 HTTPS (安全 HTTP)。通过将您的 EC2 实例的 IP 地址或完全限定域名与前缀 **https://** 一起输入浏览器 URL 栏中来对其进行测试。

   由于您正在使用自签名的不可信主机证书连接到站点，因此您的浏览器可能会显示一系列安全警告。忽视这些警告并继续连接站点。

   如果默认 Apache 测试页面打开，这意味着您已成功在服务器上配置 TLS。在浏览器和服务器之间传输的所有数据现在都已加密。

   Note

   为了防止站点访问者遇到警告屏幕，您必须获取一个可信 CA 签名证书，该证书不仅进行加密，而且还公开验证您是否为站点拥有者。

步骤 2：获取 CA 签名的证书

您可以使用以下过程获取 CA 签名证书：

- 从私有密钥生成证书签名请求 (CSR)
- 将 CSR 提交给证书颁发机构 (CA)
- 获取签名的主机证书
- 配置 Apache 以使用证书

从加密角度看，自签名 TLS X.509 主机证书与 CA 签名证书完全相同。二者之间的区别在于社交层面，而非数学层面。CA 承诺，在向申请者颁发证书之前，至少验证域的所有权。每个 Web 浏览器均包含一个 CA 的列表，浏览器供应商信任这些 CA 来执行此操作。X.509 证书主要包含一个与您的私有服务器密钥对应的公有密钥和一个以加密方式与该公有密钥关联的 CA 的签名。当浏览器通过 HTTPS 连接到 Web 服务器时，服务器将提供证书以便浏览器检查其可信 CA 的列表。如果签署人位于列表上，或可通过由其他可信签署人组成的一系列信任访问，则浏览器将与服务器协商一个快速加密数据通道并加载页面。

由于验证请求需要投入人力，证书通常会产生费用，因此应货比三家。一些 CA 免费提供基础级别证书。其中最值得注意的 CA 是 Let's Encrypt 项目，该项目还支持证书创建和续订过程的自动化。有关将 Let's Encrypt 用作 CA 的更多信息，请参阅证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 (p. 65)。

如果您打算提供商业级服务，Amazon Certificate Manager 是一个不错的选择。

主机证书的基础是密钥。从 2019 年开始，政府和行业群体建议 RSA 密钥使用 2048 位的最小密钥（模数）大小，旨在将文档一直保护到 2030 年。Amazon Linux 2023 中的 OpenSSL 生成的默认模数大小为 2048 位，适用于 CA 签名证书。在以下过程中，为需要自定义密钥的人员提供了一个可选步骤，例如，具有较大模数或使用不同加密算法的步骤。

Important

除非您拥有注册并托管的 DNS 域，否则，有关获取 CA 签名主机证书的这些说明不适用。

获取 CA 签名的证书

1. 连接到您的实例 (p. 11)并导航到 /etc/pki/tls/private/。这是存储 TLS 的服务器私有密钥的目录。如果您希望使用现有的主机密钥生成 CSR，请跳到步骤 3。

2. (可选) 生成新的私有密钥。下面是一些密钥配置示例。任何生成的密钥都可用于您的 Web 服务器，但它们实施安全的程度和类型有所不同。

   - 示例 1：创建默认 RSA 主机密钥。生成的文件 **custom.key** 是一个 2048 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key
     ```

   - 示例 2：创建具有更大模数的更严格的 RSA 密钥。生成的文件 **custom.key** 是一个 4096 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
     ```

   - 示例 3：创建具有密码保护的 4096 位加密的 RSA 密钥。生成的文件 **custom.key** 是一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

     Important

     对密钥进行加密可增强安全性，但由于加密的密钥需要密码，因此依赖于加密密钥的服务无法自动启动。每当您使用此密钥时，都必须通过 SSH 连接提供密码（在上一示例中为“abcde12345”）。

     ```
     [ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key
      4096
     ```

   - 示例 4：使用非 RSA 密码创建密钥。RSA 加密可能相对较慢，因为其公有密钥的大小基于两个大素数的乘积。不过，可以为 TLS 创建使用非 RSA 密码的密钥。在交付同等级别的安全性时，基于椭圆曲线的数学运算的密钥更小，计算起来更快。

     ```
     [ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
     ```

     结果为一个使用 prime256v1（OpenSSL 支持的“命名曲线”）的 256 位椭圆曲线私有密钥。根据 NIST，其加密强度略高于 2048 位 RSA 密钥。

     Note

     并非所有 CA 对基于椭圆曲线的密钥的支持级别与对 RSA 密钥的支持级别相同。

   请确保新的私有密钥具有高度限制的所有权和权限 (所有者=根、组=根、仅面向所有者的读取/写入权限)。命令将如以下示例所示。

   ```
   [ec2-user ~]$ sudo chown root:root custom.key
   [ec2-user ~]$ sudo chmod 600 custom.key
   [ec2-user ~]$ ls -al custom.key
   ```

   上述命令生成以下结果。

   ```
   -rw------- root root custom.key
   ```

   在创建并配置满意的密钥后，可以创建 CSR。

3. 使用您首选的密钥创建 CSR。下面的示例使用了 **custom.key**。

   ```
   [ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
   ```

   OpenSSL 将打开一个对话框，并提示您输入下表中显示的信息。对于基本的经域验证的主机证书来说，除 Common Name 以外的所有字段都是可选字段。

名称	描述	示例
国家/地区名称	代表国家/地区的两个字母 ISO 缩写。	US (=美国)
州或省名称	组织所在州或省的名称。此名称不可使用缩写。	Washington
所在地名称	您的组织所在的位置，例如城市。	Seattle
组织名称	组织的法定全称。请勿缩写组织名称。	Example Corporation
组织部门名称	额外的组织信息 (如果有)。	示例部门
公用名	此值必须与您希望用户输入浏览器中的 Web 地址完全匹配。通常，这表示以主机名称为前缀的域名或采用 **www.example.com** 格式的别名。在使用自签名证书且无 DNS 解析的测试中，公用名可能只包含主机名。CA 还提供费用更高的证书，这些证书接受通配符名称（例如 ***.example.com**）。	www.example.com
电子邮件地址	服务器管理员的电子邮件地址。	someone@example.com

最后，OpenSSL 将提示您输入可选的质询密码。此密码仅适用于 CSR 和您与 CA 之间的事务，因此请遵循 CA 提供的有关此密码以及其他可选字段、可选公司名的建议。CSR 质询密码不会影响服务器操作。

生成的文件 **csr.pem** 包含您的公有密钥、您的公有密钥的数字签名以及您输入的元数据。

4. 将 CSR 提交给 CA。这通常包括在文本编辑器中打开 CSR 文件并将内容复制到 Web 表格中。此时，您可能需要提供一个或多个主题备用名称 (SAN) 以放置到证书上。如果 **www.example.com** 是公用名，则 **example.com** 将是一个很好的 SAN，反之亦然。您网站的访客如果输入这两个名称的任何一个，便可看到一个没有错误的连接。如果您的 CA Web 表格允许该连接，请在 SAN 列表中包含公用名。一些 CA 会自动包含公用名。

   在您的请求获得批准后，您将收到一个由 CA 签署的新主机证书。此外，系统可能会指示您下载中间证书文件，该文件包含完成 CA 的信任链所需的其他证书。

   Note

   您的 CA 可能会针对各种用途发送多种格式的文件。在本教程中，您应只使用 PEM 格式的证书文件，此格式通常会（但不总是）标有 `.pem` 或 `.crt` 文件扩展名。如果您不确定要使用哪个文件，请使用文本编辑器打开这些文件，并查找一个包含一个或多个以下面的行开始的块的文件。

   ```
   - - - - -BEGIN CERTIFICATE - - - - -
   ```

   该文件还应以下面的行结束。

   ```
   - - - -END CERTIFICATE - - - - -
   ```

   您还可以在命令行上测试文件，如下所示。

   ```
   [ec2-user certs]$ openssl x509 -in certificate.crt -text
   ```

   验证这些行是否显示在文件中。请勿使用结尾为 `.p7b`、`.p7c` 或类似文件扩展名的文件。

5. 将新的 CA 签名证书和任何中间证书放在 /etc/pki/tls/certs 目录中。

   Note

   可通过多种方法将新证书上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 /etc/pki/tls/certs 目录内部，检查文件所有权、组和权限设置是否与高度限制的 Amazon Linux 2023 默认权限（所有者根权限、组根权限、仅面向所有者的读取/写入权限）匹配。以下示例显示了要使用的命令。

   ```
   [ec2-user certs]$ sudo chown root:root custom.crt
   [ec2-user certs]$ sudo chmod 600 custom.crt
   [ec2-user certs]$ ls -al custom.crt
   ```

   这些命令应生成以下结果。

   ```
   -rw------- root root custom.crt
   ```

   中间证书文件的权限并不严格 (所有者=根、组=根、所有者可以写入、组可以读取、任何人均可读取)。以下示例显示了要使用的命令。

   ```
   [ec2-user certs]$ sudo chown root:root intermediate.crt
   [ec2-user certs]$ sudo chmod 644 intermediate.crt
   [ec2-user certs]$ ls -al intermediate.crt
   ```

   这些命令应生成以下结果。

   ```
   -rw-r--r-- root root intermediate.crt
   ```

6. 将用于创建 CSR 的私有密钥放在 /etc/pki/tls/private/ 目录中。

   Note

   可通过多种方法将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 /etc/pki/tls/private 目录内部，使用以下命令验证文件所有权、组和权限设置是否与高度限制的 Amazon Linux 2023 默认权限（拥有者根权限、组根权限、仅面向拥有者的读取/写入权限）匹配。

   ```
   [ec2-user private]$ sudo chown root:root custom.key
   [ec2-user private]$ sudo chmod 600 custom.key
   [ec2-user private]$ ls -al custom.key
   ```

   这些命令应生成以下结果。

   ```
   -rw------- root root custom.key
   ```

7. 编辑 /etc/httpd/conf.d/ssl.conf 以反映您的新证书和密钥文件。

   a. 在 Apache 的 SSLCertificateFile 指令中提供 CA 签名主机证书的路径和文件名：

```
SSLCertificateFile /etc/pki/tls/certs/custom.crt
```

b. 如果您收到一个中间证书文件（此示例中为 `intermediate.crt`），请使用 Apache 的 `SSLCACertificateFile` 指令提供其路径和文件名：

```
SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
```

> **Note**
>
> 一些 CA 将主机证书和中间证书合并到单个文件中，从而不再需要使用 `SSLCACertificateFile` 指令。请查询您的 CA 提供的说明。

c. 在 Apache 的 `SSLCertificateKeyFile` 指令中提供私有密钥的路径和文件名（在该示例中为 `custom.key`）：

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

8. 保存 `/etc/httpd/conf.d/ssl.conf` 并重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

9. 通过在浏览器 URL 栏中输入带有 `https://` 前缀的域名来测试您的服务器。您的浏览器应通过 HTTPS 加载测试页面而不会产生错误。

步骤 3：测试和强化安全配置

在 TLS 可操作且公开发布后，应测试其实际安全性。使用在线服务（例如 Qualys SSL Labs，该服务可对您的安全设置执行免费的全面分析）可轻松执行此操作。根据结果，您可以决定通过控制接受的协议、首选的密码和排除的密码来强化默认安全配置。有关更多信息，请参阅 Qualys 如何用公式表示其分数。

> **Important**
>
> 实际测试对服务器的安全性非常重要。少量配置错误可能导致严重的安全漏洞和数据丢失。由于建议的安全实践会不断变化以响应调查和新兴威胁，因此定期安全审核对于良好的服务器管理来说是必不可少的。

在 Qualys SSL Labs 站点上，使用 **`www.example.com`** 格式输入服务器的完全限定域名。约两分钟后，您将收到您站点的评级 (从 A 到 F) 和结果的详细信息。下表总结了具有与 Amazon Linux 2023 上默认 Apache 配置相同的设置以及默认 Certbot 证书的域报告。

总评	B
证书	100%
协议支持	95%
密钥交换	70%
密码强度	90%

虽然概述信息显示配置基本正确，但详细报告标记了几个潜在的问题（在此处按严重性顺序列出）：

✗ 支持某些旧浏览器使用 RC4 密码。密码是加密算法的数学核心。RC4 是一种用于加密 TLS 数据流的快速密码，已知这种密码存在一些严重缺点。除非您有充分理由支持旧版浏览器，否则，应禁用该密码。

✗ 支持旧 TLS 版本。该配置支持 TLS 1.0（已弃用）和 TLS 1.1（即将弃用）。从 2018 年开始，仅建议使用 TLS 1.2。

✗ 不完全支持向前保密性。向前保密性是一种算法功能，它使用从私有密钥派生的临时会话密钥进行加密。这意味着，在实践中，攻击者无法解密 HTTPS 数据，即使他们拥有 Web 服务器的长期私有密钥。

纠正 TLS 配置并供将来使用

1. 在文本编辑器中打开 `/etc/httpd/conf.d/ssl.conf` 配置文件，并在以下行的开头输入“#”以注释掉该行。

```
#SSLProtocol all -SSLv3
```

2. 添加以下指令：

```
#SSLProtocol all -SSLv3
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

该指令显式禁用 SSL 版本 2 和 3 以及 TLS 版本 1.0 和 1.1。现在，服务器拒绝接受与使用 TLS 1.2 以外的任何协议的客户端之间的加密连接。指令中的冗长文字更清楚地向人类读者阐述为服务器配置的用途。

> **Note**
>
> 以此方式禁用 TLS 1.0 和 1.1 版可阻止一小部分过时的 Web 浏览器访问您的网站。

修改允许的密码列表

1. 在 `/etc/httpd/conf.d/ssl.conf` 配置文件中，找到包含 **`SSLCipherSuite`** 指令的部分，并通过在现有行的开头输入“#”来注释掉该行。

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

2. 指定显式的密码套件，并指定密码顺序以优先使用向前保密性并避免不安全的密码。此处使用的 `SSLCipherSuite` 指令基于 Mozilla SSL 配置生成器的输出，该生成器根据服务器上运行的特定软件定制 TLS 配置。（有关更多信息，请参阅 Mozilla 的有用资源安全性/服务器端 TLS。）首先，通过使用以下命令的输出确定 Apache 和 OpenSSL 版本。

```
[ec2-user ~]$ yum list installed | grep httpd

[ec2-user ~]$ yum list installed | grep openssl
```

例如，如果返回的信息是 Apache 2.4.34 和 OpenSSL 1.0.2，我们将其输入到生成器中。如果您选择“现代”兼容性模型，这将创建一条 `SSLCipherSuite` 指令，虽然该指令积极实施安全性，但仍适用于大多数浏览器。如果您的软件不支持现代配置，则可以更新软件或改为选择“中间”配置。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-
AES128-SHA256
```

选定的密码名称中包含 ECDHE，它是 Elliptic Curve Diffie-Hellman Ephemeral 的缩写。术语 ephemeral 表示向前保密性。副作用是，这些密码不支持 RC4。

建议您使用密码的明确列表，而不是依赖于内容不可见的默认值或简短指令。

将生成的指令复制到 /etc/httpd/conf.d/ssl.conf 中。

Note

此处为方便阅读将指令显示为几行，但在复制到 /etc/httpd/conf.d/ssl.conf 时，该指令必须位于一行中，并且密码名称之间只有一个冒号（无空格）。

3. 最后，通过删除以下行开头的“#”来取消对该行的注释。

```
#SSLHonorCipherOrder on
```

该指令强制服务器优先使用排名较高的密码，包括（在该示例中）支持向前保密性的密码。启用此指令后，服务器会在回滚到允许的安全性较低的密码之前尝试建立高度安全的连接。

在完成这两个过程后，将更改保存到 /etc/httpd/conf.d/ssl.conf 并重新启动 Apache。

如果在 Qualys SSL Labs 上再次测试域，将会看到已修复 RC4 漏洞和其他警告，并且摘要如下所示。

总评	A
证书	100%
协议支持	100%
密钥交换	90%
密码强度	90%

在每次更新 OpenSSL 时，将引入新的密码并删除对旧密码的支持。使 EC2 Amazon Linux 2023 实例保持最新，关注来自 OpenSSL 的安全公告，并留意技术出版物中对新安全漏洞的报告。

问题排查

- 除非我输入密码，否则我的 Apache Web 服务器不会启动

  如果您安装了受密码保护的加密的私有服务器密钥，这是预期行为。

  您可以从密钥中删除加密和密码要求。假设在默认目录中具有一个称为 custom.key 的加密的私有 RSA 密钥，并且此密钥上的密码是 **abcde12345**，则对 EC2 实例运行以下命令可生成此密钥的未加密版本。

```
[ec2-user ~]$ cd /etc/pki/tls/private/
[ec2-user private]$ sudo cp custom.key custom.key.bak
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out
 custom.key.nocrypt
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key
[ec2-user private]$ sudo chown root:root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ sudo systemctl restart httpd
```

  Apache 现在启动时应该不会提示您提供密码。

- 我在运行 sudo dnf install -y mod_ssl 时收到了错误。

  在为 SSL 安装所需的程序包时，您可能会看到与以下内容类似的错误。

```
Error: httpd24-tools conflicts with httpd-tools-2.2.34-1.16.amzn1.x86_64
```

```
Error: httpd24 conflicts with httpd-2.2.34-1.16.amzn1.x86_64
```

这通常意味着 EC2 实例没有运行 Amazon Linux 2023。本教程仅支持从官方 Amazon Linux 2023 AMI 新创建的实例。

证书自动化：在 Amazon Linux 2023 上将 Let's Encrypt 与 Certbot 结合使用

Warning

"Let's Encrypt"交叉签名 DST 根 CA X3 证书已在 2021 年 9 月 30 日过期。在 CentOS/RHEL7 和 Amazon Linux 上使用 OpenSSL 1.0.x 时，这会导致 Let's Encrypt 连接失败。补救步骤可以参见此处，或者您可以遵照 OpenSSL 博客页面上提供的人工解决方法之一。

Important

除非您拥有注册并托管的 DNS 域，否则，有关获取 Let's Encrypt 主机证书的这些说明不适用。这些说明不适用于 Amazon 分配的公有 DNS 主机名。

Let's Encrypt 证书颁发机构是电子前沿基金会 (EFF) 致力于对整个 Internet 进行加密的核心所在。按照该目标，Let's Encrypt 主机证书被设计为用最小的人工干预来进行创建、验证、安装和维护。证书管理的自动化方面由在 Web 服务器上运行的软件代理执行。在安装并配置代理后，它与 Let's Encrypt 安全地通信并在 Apache 和密钥管理系统上执行管理任务。本教程使用免费的 Certbot 代理，因为它允许您提供自定义的加密密钥作为您证书的基础，或允许代理自身根据其默认值创建密钥。您也可以将 Certbot 配置为定期续订您的证书，无需人工交互，如自动化 Certbot (p. 54)中所述。有关更多信息，请参阅 Certbot 用户指南和手册页。

尽管 Certbot 不受 Amazon Linux 2023 官方支持，但可供下载并且能够在安装时正常运行。建议您执行以下备份来保护数据并避免造成不便：

- 在开始之前，请为您的 Amazon EBS 根卷制作快照。这使您能够还原 EC2 实例的原始状态。有关创建 EBS 快照的信息，请参阅创建 Amazon EBS 快照 (p. 1372)。
- 以下过程要求您编辑您的 `httpd.conf` 文件，该文件控制 Apache 的操作。Certbot 对此配置文件和其他配置文件进行其自动化更改。创建整个 `/etc/httpd` 目录的备份副本，以便您在需要时还原该目录。

准备安装

在安装 Certbot 之前，请完成以下过程。

1. 下载 Extra Packages for Enterprise Linux (EPEL) 7 存储库程序包。需要这些程序包才能提供 Certbot 所需的依赖项。

   a. 导航到您的主目录 (`/home/ec2-user`)。使用以下命令下载并安装这些软件包。

   ```
   [ec2-user ~]$ sudo dnf install -y python3 augeas-libs pip
   ```

   b. 在计算机上的命令行上执行以下指令以设置 Python 虚拟环境。

   ```
   sudo python3 -m venv /opt/certbot/
   ```

   c. 安装 pip 的最新版本。

   ```
   [ec2-user ~]$ sudo /opt/certbot/bin/pip install --upgrade pip
   ```

   安装 certbot。

```
[ec2-user ~]$ sudo /opt/certbot/bin/pip install certbot
```

添加一个符号链接。

```
[ec2-user ~]$ sudo ln -s /opt/certbot/bin/certbot /usr/bin/certbot
```

2. 您需要在下一步之前停止 http。

```
sudo systemctl stop httpd
```

如果您无法停止 Web 服务器，或者您也可以使用以下命令。

```
[ec2-user ~]$ sudo certbot certonly --webroot
```

运行 Certbot。

此过程基于有关在 Fedora 和 RHEL 7 上安装 Certbot 的 EFF 文档。其中介绍 Certbot 的默认使用，即根据 2048 位 RSA 密钥生成证书。

1. 运行 Certbot。

```
[ec2-user ~]$ sudo certbot certonly --standalone
```

2. 在提示符“Enter email address (used for urgent renewal and security notices)”处，输入联系人地址并按 Enter。
3. 在提示符处，同意 Let's Encrypt 服务条款。输入“A”并按 Enter 以继续。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A
```

4. 完成授权以使 EFF 将您加入发送名单中，输入“Y”或“N”并按 Enter。
5. Certbot 显示您在 VirtualHost 数据块中提供的公用名和主题替代名称 (SAN)。

```
Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: example.com
2: www.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
```

将输入保留空白并按 Enter。

6. Certbot 在创建证书和配置 Apache 时将显示以下输出。然后，它提示您有关将 HTTP 查询重定向到 HTTPS 的事项。

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for example.com
```

```
http-01 challenge for www.example.com
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/httpd/conf/httpd-le-ssl.conf
Deploying Certificate for example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf
Enabling site /etc/httpd/conf/httpd-le-ssl.conf by adding Include to root configuration
Deploying Certificate for www.example.com to VirtualHost /etc/httpd/conf/httpd-le-
ssl.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```

要允许访客通过未加密的 HTTP 连接到服务器，请输入“1”。若要仅接受通过 HTTPS 的加密连接，请输入“2”。按 Enter 提交您的选择。

7. Certbot 完成 Apache 的配置并报告成功和其他信息。

```
Congratulations! You have successfully enabled https://example.com and
https://www.example.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=example.com
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/certbot.oneeyedman.net/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/certbot.oneeyedman.net/privkey.pem
   Your cert will expire on 2019-08-01. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
```

8. 在完成安装后，测试并优化您服务器的安全性，如步骤 3：测试和强化安全配置 (p. 49)中所述。

配置自动证书续订

Certbot 被设计成服务器系统的一个不可见的防错部分。默认情况下，它会生成具有短暂的 90 天到期时间的主机证书。如果您还未将系统配置为自动调用命令，则必须在到期之前手动重新运行 certbot 命令。此过程介绍如何通过设置 cron 作业来实现 Certbot 自动化。

自动化 Certbot

1. 使用 sudo，在文本编辑器（例如 vim 或 nano）中打开 `/etc/crontab` 文件。或者，请使用 sudo crontab -e。
2. 添加类似于下文的行并保存文件。

```
39      1,13    *       *       *       root    certbot renew --no-self-upgrade
```

这是每个组件的说明：

`39 1,13 * * *`

排定一个在每天 01:39 和 13:39 运行的命令。所选的值是随机的，但 Certbot 开发人员建议每天运行该命令至少两次。这将确保立即撤销并替换任何发现已损坏的证书。

`root`

该命令使用根权限运行。

`certbot renew --no-self-upgrade`

将要运行的命令。renew 子命令会使 Certbot 检查任何先前获取的证书并续订即将到期的证书。`--no-self-upgrade` 标记可防止 Certbot 在没有您干预的情况下自行升级。

3. 重启 cron 守护程序。

```
[ec2-user ~]$ sudo systemctl restart crond
```

教程：在 Amazon Linux 2 上配置 SSL/TLS

安全套接字层/传输层安全性 (SSL/TLS) 可在 Web 服务器和 Web 客户端之间创建一个加密通道，以防止数据在传输过程中被窃听。本教程介绍如何在具有 Amazon Linux 2 和 Apache Web 服务器的 EC2 实例上手动添加对 SSL/TLS 的支持。本教程假定您未使用负载均衡器。如果您正在使用 Elastic Load Balancing，则可以选择使用来自 Amazon Certificate Manager 的证书在负载均衡器上配置 SSL 卸载。

由于历史原因，Web 加密通常简称为 SSL。虽然 Web 浏览器仍支持 SSL，但使用其下一代协议 TLS 更不易受攻击。默认情况下，Amazon Linux 2 将禁用所有版本的 SSL 的服务器端支持。安全标准机构认为 TLS 1.0 不安全。TLS 1.0 和 TLS 1.1 已于 2021 年 3 月正式弃用。本教程仅包含有关启用 TLS 1.2 的指导。TLS 1.3 于 2018 年定版，只需支持和启用底层 TLS 库（本教程中为 OpenSSL）即可在 Amazon Linux 2 中使用。客户端必须在 2023 年 6 月 28 日之前支持 TLS 1.2 或更高版本。有关更新的加密标准的更多信息，请参阅 RFC 7568 和 RFC 8446。

在本教程中，将现代 Web 加密简称为 TLS。

Important

这些过程适用于 Amazon Linux 2。我们还假定您从新的 Amazon EC2 实例开始。如果您尝试设置运行不同分配的 EC2 实例，或者运行旧版本 Amazon Linux 2 的实例，则本教程中的一些过程可能不适合。对于 Amazon Linux AMI，请参阅 教程：使用 Amazon Linux AMI 配置 SSL/TLS (p. 68)。对于 Ubuntu，请参阅以下社区文档：Open SSL on Ubuntu。有关 Red Hat Enterprise Linux 的信息，请参阅以下：设置 Apache HTTP Web 服务器。有关其他发布版本，请参阅特定于该版本的文档。

Note

或者，您还可以使用适用于 Amazon Nitro Enclaves 的 Amazon Certificate Manager (ACM)，这是一个 Enclave 应用程序，可使您通过 Amazon Nitro Enclaves 将公有和私有 SSL/TLS 证书与在 Amazon EC2 实例上运行的 Web 应用程序和服务器一起使用。Nitro Enclaves 是一项 Amazon EC2 功能，可以创建隔离的计算环境以保护和安全地处理高度敏感的数据，例如 SSL/TLS 证书和私有密钥。
适用于 Nitro Enclaves 的 ACM 与运行在 Amazon EC2 Linux 实例上的 nginx 结合使用，以创建私有密钥、分发证书和私有密钥以及管理证书续订。
要使用适用于 Nitro Enclaves 的 ACM，必须使用启用了 Enclave 的 Linux 实例。
有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？和适用于 Nitro Enclaves 的 Amazon Certificate Manager。

目录

- 先决条件 (p. 56)
- 步骤 1：在服务器上启用 TLS (p. 43)
- 步骤 2：获取 CA 签名的证书 (p. 58)
- 步骤 3：测试和强化安全配置 (p. 62)
- 问题排查 (p. 64)
- 证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 (p. 65)

先决条件

在开始本教程之前，请完成以下步骤：

- 启动 EBS 支持的 Amazon Linux 2 实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。
- 配置安全组以允许您的实例接受以下 TCP 端口上的连接：
  - SSH (端口 22)
  - HTTP (端口 80)
  - HTTPS (端口 443)

  有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
- 安装 Apache Web 服务器。有关分步说明，请参阅教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)。仅需要 httpd 包及其依赖项，因此可以忽略涉及 PHP 和 MariaDB 的说明。
- 要识别和验证网站，TLS 公有密钥基础设施 (PKI) 依赖于域名系统 (DNS)。要使用 EC2 实例托管公共网站，您需要为 Web 服务器注册一个域名，或者将现有域名转让给您的 Amazon EC2 主机。可通过很多第三方域注册和 DNS 托管服务来执行此操作，也可以使用 Amazon Route 53 执行此操作。

步骤 1：在服务器上启用 TLS

选项：使用 Automation 完成本教程

要使用 Amazon Systems Manager Automation 而不是以下任务完成本教程，请运行 Automation 文档。

该过程指导您完成在 Amazon Linux 2 上使用自签名数字证书设置 TLS 的过程。

> **Note**
>
> 自签名证书对于测试是可接受的，但对于生产不是。如果您将自签名证书公开到 Internet，您网站的访客将会看到安全警告。

在服务器上启用 TLS

1. 连接到您的实例 (p. 11)并确认 Apache 正在运行。

   ```
   [ec2-user ~]$ sudo systemctl is-enabled httpd
   ```

   如果返回的值不是“启用”，则启动 Apache 并将它设置为每次随系统一起启动。

   ```
   [ec2-user ~]$ sudo systemctl start httpd && sudo systemctl enable httpd
   ```

2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   > **Note**
   >
   > -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

```
[ec2-user ~]$ sudo yum update -y
```

3. 现在，您的实例是最新的，请安装 Apache 模块 mod_ssl 以添加 TLS 支持。

```
[ec2-user ~]$ sudo yum install -y mod_ssl
```

您的实例现在具有以下文件，可使用这些文件配置安全服务器并创建证书以进行测试：

- /etc/httpd/conf.d/ssl.conf

  mod_ssl 的配置文件。它包含一些指令 以指示 Apache 在何处查找以下信息：加密密钥和证书、要允许的 TLS 协议版本以及要接受的加密密码。

- /etc/pki/tls/certs/make-dummy-cert

  用于为服务器主机生成自签名 X.509 证书和私有密钥的脚本。要测试是否正确设置 Apache 以使用 TLS，该证书是非常有用的。由于不提供身份证明，因此，不应在生产环境中使用该证书。如果在生产环境中使用该证书，则将在 Web 浏览器中触发警告。

4. 运行脚本以生成自签名虚拟证书和密钥以进行测试。

```
[ec2-user ~]$ cd /etc/pki/tls/certs
sudo ./make-dummy-cert localhost.crt
```

这会在 /etc/pki/tls/certs/ 目录中生成一个新文件 localhost.crt。指定的文件名与 /etc/httpd/conf.d/ssl.conf 中的 SSLCertificateFile 指令指定的默认值匹配。

该文件包含自签名证书以及证书的私有密钥。Apache 要求证书和密钥采用 PEM 格式，其中包含 Base64 编码的 ASCII 字符，并用“BEGIN”和“END”行框起来，如以下简短示例所示。

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLjOOCI8u1PTcGmAah5kEitCEc0wzmNeo
BCl0wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMZoT
...
56tE7THvH7vOEf4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs
27hDzPDinrquSEvoZIggkDMlh2irTiipJ/GhkvTpoQlv0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U6O4FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo
4QQvAqOa8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb211U3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb211T3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb211T3JnYW5pemF0aW9uYWxV
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3DlK44D9dlU3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----END CERTIFICATE-----
```

文件名和扩展名只是为了提供便利，对功能没有影响。例如，只要 ssl.conf 文件中的相关指令使用相同的名称，您就可以将证书命名为 cert.crt、cert.pem 或任何其他文件名。

> **Note**
>
> 在使用您自己的自定义文件替换默认 TLS 文件时，请确保它们采用 PEM 格式。

5. 使用您常用的文本编辑器（如 vim 或 nano）以根用户身份打开 `/etc/httpd/conf.d/ssl.conf` 文件并注释掉以下行，因为自签名虚拟证书也包含密钥。如果在完成下一步之前没有注释掉该行，Apache 服务将无法启动。

```
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

6. 重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

   Note

   确保 TCP 端口 443 在您的 EC2 实例上是可访问的，如之前所述。

7. 现在，您的 Apache Web 服务器应通过端口 443 支持 HTTPS (安全 HTTP)。通过将您的 EC2 实例的 IP 地址或完全限定域名与前缀 **`https://`** 一起输入浏览器 URL 栏中来对其进行测试。

   由于您正在使用自签名的不可信主机证书连接到站点，因此您的浏览器可能会显示一系列安全警告。忽视这些警告并继续连接站点。

   如果默认 Apache 测试页面打开，这意味着您已成功在服务器上配置 TLS。在浏览器和服务器之间传输的所有数据现在都已加密。

   Note

   为了防止站点访问者遇到警告屏幕，您必须获取一个可信 CA 签名证书，该证书不仅进行加密，而且还公开验证您是否为站点拥有者。

步骤 2：获取 CA 签名的证书

您可以使用以下过程获取 CA 签名证书：

- 从私有密钥生成证书签名请求 (CSR)
- 将 CSR 提交给证书颁发机构 (CA)
- 获取签名的主机证书
- 配置 Apache 以使用证书

从加密角度看，自签名 TLS X.509 主机证书与 CA 签名证书完全相同。二者之间的区别在于社交层面，而非数学层面。CA 承诺，在向申请者颁发证书之前，至少验证域的所有权。每个 Web 浏览器均包含一个 CA 的列表，浏览器供应商信任这些 CA 来执行此操作。X.509 证书主要包含一个与您的私有服务器密钥对应的公有密钥和一个以加密方式与该公有密钥关联的 CA 的签名。当浏览器通过 HTTPS 连接到 Web 服务器时，服务器将提供证书以便浏览器检查其可信 CA 的列表。如果签署人位于列表上，或可通过由其他可信签署人组成的一系列信任访问，则浏览器将与服务器协商一个快速加密数据通道并加载页面。

由于验证请求需要投入人力，证书通常会产生费用，因此应货比三家。一些 CA 免费提供基础级别证书。其中最值得注意的 CA 是 Let's Encrypt 项目，该项目还支持证书创建和续订过程的自动化。有关将 Let's Encrypt 用作 CA 的更多信息，请参阅证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 (p. 65)。

如果您打算提供商业级服务，Amazon Certificate Manager 是一个不错的选择。

主机证书的基础是密钥。从 2019 年开始，政府和行业群体建议 RSA 密钥使用 2048 位的最小密钥（模数）大小，旨在将文档一直保护到 2030 年。Amazon Linux 2 中的 OpenSSL 生成的默认模数大小为 2048 位，这适用于 CA 签名证书。在以下过程中，为需要自定义密钥的人员提供了一个可选步骤，例如，具有较大模数或使用不同加密算法的步骤。

Important

除非您拥有注册并托管的 DNS 域，否则，有关获取 CA 签名主机证书的这些说明不适用。

获取 CA 签名的证书

1. 连接到您的实例 (p. 11)并导航到 /etc/pki/tls/private/。这是存储 TLS 的服务器私有密钥的目录。如果您希望使用现有的主机密钥生成 CSR，请跳到步骤 3。
2. (可选) 生成新的私有密钥。下面是一些密钥配置示例。任何生成的密钥都可用于您的 Web 服务器，但它们实施安全的程度和类型有所不同。

   - 示例 1：创建默认 RSA 主机密钥。生成的文件 **custom.key** 是一个 2048 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key
     ```

   - 示例 2：创建具有更大模数的更严格的 RSA 密钥。生成的文件 **custom.key** 是一个 4096 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
     ```

   - 示例 3：创建具有密码保护的 4096 位加密的 RSA 密钥。生成的文件 **custom.key** 是一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

     Important

     对密钥进行加密可增强安全性，但由于加密的密钥需要密码，因此依赖于加密密钥的服务无法自动启动。每当您使用此密钥时，都必须通过 SSH 连接提供密码（在上一示例中为“abcde12345”）。

     ```
     [ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key
      4096
     ```

   - 示例 4：使用非 RSA 密码创建密钥。RSA 加密可能相对较慢，因为其公有密钥的大小基于两个大素数的乘积。不过，可以为 TLS 创建使用非 RSA 密码的密钥。在交付同等级别的安全性时，基于椭圆曲线的数学运算的密钥更小，计算起来更快。

     ```
     [ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
     ```

     结果为一个使用 prime256v1（OpenSSL 支持的“命名曲线”）的 256 位椭圆曲线私有密钥。根据 NIST，其加密强度略高于 2048 位 RSA 密钥。

     Note

     并非所有 CA 对基于椭圆曲线的密钥的支持级别与对 RSA 密钥的支持级别相同。

请确保新的私有密钥具有高度限制的所有权和权限 (所有者=根、组=根、仅面向所有者的读取/写入权限)。命令将如以下示例所示。

```
[ec2-user ~]$ sudo chown root:root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

上述命令生成以下结果。

```
-rw------- root root custom.key
```

在创建并配置满意的密钥后，可以创建 CSR。

3. 使用您首选的密钥创建 CSR。下面的示例使用了 **custom.key**。

```
[ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
```

OpenSSL 将打开一个对话框，并提示您输入下表中显示的信息。对于基本的经域验证的主机证书来说，除 Common Name 以外的所有字段都是可选字段。

名称	描述	示例
国家/地区名称	代表国家/地区的两个字母 ISO 缩写。	US (=美国)
州或省名称	组织所在州或省的名称。此名称不可使用缩写。	Washington
所在地名称	您的组织所在的位置，例如城市。	Seattle
组织名称	组织的法定全称。请勿缩写组织名称。	Example Corporation
组织部门名称	额外的组织信息 (如果有)。	示例部门
公用名	此值必须与您希望用户输入浏览器中的 Web 地址完全匹配。通常，这表示以主机名称为前缀的域名或采用 **www.example.com** 格式的别名。在使用自签名证书且无 DNS 解析的测试中，公用名可能只包含主机名。CA 还提供费用更高的证书，这些证书接受通配符名称（例如 ***.example.com**）。	www.example.com
电子邮件地址	服务器管理员的电子邮件地址。	someone@example.com

最后，OpenSSL 将提示您输入可选的质询密码。此密码仅适用于 CSR 和您与 CA 之间的事务，因此请遵循 CA 提供的有关此密码以及其他可选字段、可选公司名的建议。CSR 质询密码不会影响服务器操作。

生成的文件 **csr.pem** 包含您的公有密钥、您的公有密钥的数字签名以及您输入的元数据。

4. 将 CSR 提交给 CA。这通常包括在文本编辑器中打开 CSR 文件并将内容复制到 Web 表格中。此时，您可能需要提供一个或多个主题备用名称 (SAN) 以放置到证书上。如果 **www.example.com** 是公用名，则 **example.com** 将是一个很好的 SAN，反之亦然。您网站的访客如果输入这两个名称的任何一个，便可看到一个没有错误的连接。如果您的 CA Web 表格允许该连接，请在 SAN 列表中包含公用名。一些 CA 会自动包含公用名。

   在您的请求获得批准后，您将收到一个由 CA 签署的新主机证书。此外，系统可能会指示您下载中间证书文件，该文件包含完成 CA 的信任链所需的其他证书。

   Note

   您的 CA 可能会针对各种用途发送多种格式的文件。在本教程中，您应只使用 PEM 格式的证书文件，此格式通常会（但不总是）标有 `.pem` 或 `.crt` 文件扩展名。如果您不确定要使用哪个文件，请使用文本编辑器打开这些文件，并查找一个包含一个或多个以下面的行开始的块的文件。

   ```
   - - - - -BEGIN CERTIFICATE - - - - -
   ```

   该文件还应以下面的行结束。

```
- - - -END CERTIFICATE - - - - -
```

您还可以在命令行上测试文件，如下所示。

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

验证这些行是否显示在文件中。请勿使用结尾为 .p7b、.p7c 或类似文件扩展名的文件。

5. 将新的 CA 签名证书和任何中间证书放在 /etc/pki/tls/certs 目录中。

   Note

   可通过多种方法将新证书上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 /etc/pki/tls/certs 目录内部，检查文件所有权、组和权限设置是否与高度限制的 Amazon Linux 2 默认权限（所有者根权限、组根权限、仅面向所有者的读取/写入权限）匹配。以下示例显示了要使用的命令。

   ```
   [ec2-user certs]$ sudo chown root:root custom.crt
   [ec2-user certs]$ sudo chmod 600 custom.crt
   [ec2-user certs]$ ls -al custom.crt
   ```

   这些命令应生成以下结果。

   ```
   -rw------- root root custom.crt
   ```

   中间证书文件的权限并不严格 (所有者=根、组=根、所有者可以写入、组可以读取、任何人均可读取)。以下示例显示了要使用的命令。

   ```
   [ec2-user certs]$ sudo chown root:root intermediate.crt
   [ec2-user certs]$ sudo chmod 644 intermediate.crt
   [ec2-user certs]$ ls -al intermediate.crt
   ```

   这些命令应生成以下结果。

   ```
   -rw-r--r-- root root intermediate.crt
   ```

6. 将用于创建 CSR 的私有密钥放在 /etc/pki/tls/private/ 目录中。

   Note

   可通过多种方法将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 /etc/pki/tls/private 目录内部，使用以下命令验证文件所有权、组和权限设置是否与高度限制的 Amazon Linux 2 默认权限（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。

   ```
   [ec2-user private]$ sudo chown root:root custom.key
   [ec2-user private]$ sudo chmod 600 custom.key
   ```

```
[ec2-user private]$ ls -al custom.key
```

这些命令应生成以下结果。

```
-rw------- root root custom.key
```

7. 编辑 /etc/httpd/conf.d/ssl.conf 以反映您的新证书和密钥文件。

   a. 在 Apache 的 SSLCertificateFile 指令中提供 CA 签名主机证书的路径和文件名：

   ```
   SSLCertificateFile /etc/pki/tls/certs/custom.crt
   ```

   b. 如果您收到一个中间证书文件（此示例中为 intermediate.crt），请使用 Apache 的 SSLCACertificateFile 指令提供其路径和文件名：

   ```
   SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
   ```

   > **Note**
   >
   > 一些 CA 将主机证书和中间证书合并到单个文件中，从而不再需要使用 SSLCACertificateFile 指令。请查询您的 CA 提供的说明。

   c. 在 Apache 的 SSLCertificateKeyFile 指令中提供私有密钥的路径和文件名（在该示例中为 custom.key）：

   ```
   SSLCertificateKeyFile /etc/pki/tls/private/custom.key
   ```

8. 保存 /etc/httpd/conf.d/ssl.conf 并重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

9. 通过在浏览器 URL 栏中输入带有 https:// 前缀的域名来测试您的服务器。您的浏览器应通过 HTTPS 加载测试页面而不会产生错误。

步骤 3：测试和强化安全配置

在 TLS 可操作且公开发布后，应测试其实际安全性。使用在线服务（例如 Qualys SSL Labs，该服务可对您的安全设置执行免费的全面分析）可轻松执行此操作。根据结果，您可以决定通过控制接受的协议、首选的密码和排除的密码来强化默认安全配置。有关更多信息，请参阅 Qualys 如何用公式表示其分数。

> **Important**
>
> 实际测试对服务器的安全性非常重要。少量配置错误可能导致严重的安全漏洞和数据丢失。由于建议的安全实践会不断变化以响应调查和新兴威胁，因此定期安全审核对于良好的服务器管理来说是必不可少的。

在 Qualys SSL Labs 站点上，使用 **www.example.com** 格式输入服务器的完全限定域名。约两分钟后，您将收到您站点的评级 (从 A 到 F) 和结果的详细信息。下表总结了具有与 Amazon Linux 2 上的默认 Apache 配置相同的设置以及默认 Certbot 证书的域的报告。

总评	B
证书	100%
协议支持	95%
密钥交换	70%

密码强度	90%

虽然概述信息显示配置基本正确，但详细报告标记了几个潜在的问题（在此处按严重性顺序列出）：

✗ 支持某些旧浏览器使用 RC4 密码。密码是加密算法的数学核心。RC4 是一种用于加密 TLS 数据流的快速密码，已知这种密码存在一些严重缺点。除非您有充分理由支持旧版浏览器，否则，应禁用该密码。

✗ 支持旧 TLS 版本。该配置支持 TLS 1.0（已弃用）和 TLS 1.1（即将弃用）。从 2018 年开始，仅建议使用 TLS 1.2。

✗ 不完全支持向前保密性。向前保密性是一种算法功能，它使用从私有密钥派生的临时会话密钥进行加密。这意味着，在实践中，攻击者无法解密 HTTPS 数据，即使他们拥有 Web 服务器的长期私有密钥。

纠正 TLS 配置并供将来使用

1. 在文本编辑器中打开 `/etc/httpd/conf.d/ssl.conf` 配置文件，并在以下行的开头输入“#”以注释掉该行。

```
#SSLProtocol all -SSLv3
```

2. 添加以下指令：

```
#SSLProtocol all -SSLv3
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

该指令显式禁用 SSL 版本 2 和 3 以及 TLS 版本 1.0 和 1.1。现在，服务器拒绝接受与使用 TLS 1.2 以外的任何协议的客户端之间的加密连接。指令中的冗长文字更清楚地向人类读者阐述为服务器配置的用途。

> **Note**
>
> 以此方式禁用 TLS 1.0 和 1.1 版可阻止一小部分过时的 Web 浏览器访问您的网站。

修改允许的密码列表

1. 在 `/etc/httpd/conf.d/ssl.conf` 配置文件中，找到包含 **`SSLCipherSuite`** 指令的部分，并通过在现有行的开头输入“#”来注释掉该行。

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

2. 指定显式的密码套件，并指定密码顺序以优先使用向前保密性并避免不安全的密码。此处使用的 `SSLCipherSuite` 指令基于 Mozilla SSL 配置生成器的输出，该生成器根据服务器上运行的特定软件定制 TLS 配置。（有关更多信息，请参阅 Mozilla 的有用资源安全性/服务器端 TLS。）首先，通过使用以下命令的输出确定 Apache 和 OpenSSL 版本。

```
[ec2-user ~]$ yum list installed | grep httpd

[ec2-user ~]$ yum list installed | grep openssl
```

例如，如果返回的信息是 Apache 2.4.34 和 OpenSSL 1.0.2，我们将其输入到生成器中。如果您选择“现代”兼容性模型，这将创建一条 `SSLCipherSuite` 指令，虽然该指令积极实施安全性，但仍适用于大多数浏览器。如果您的软件不支持现代配置，则可以更新软件或改为选择“中间”配置。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:
```

```
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-
AES128-SHA256
```

选定的密码名称中包含 ECDHE，它是 Elliptic Curve Diffie-Hellman Ephemeral 的缩写。术语 ephemeral 表示向前保密性。副作用是，这些密码不支持 RC4。

建议您使用密码的明确列表，而不是依赖于内容不可见的默认值或简短指令。

将生成的指令复制到 `/etc/httpd/conf.d/ssl.conf` 中。

Note

此处为方便阅读将指令显示为几行，但在复制到 `/etc/httpd/conf.d/ssl.conf` 时，该指令必须位于一行中，并且密码名称之间只有一个冒号（无空格）。

3. 最后，通过删除以下行开头的“#”来取消对该行的注释。

```
#SSLHonorCipherOrder on
```

该指令强制服务器优先使用排名较高的密码，包括（在该示例中）支持向前保密性的密码。启用此指令后，服务器会在回滚到允许的安全性较低的密码之前尝试建立高度安全的连接。

在完成这两个过程后，将更改保存到 `/etc/httpd/conf.d/ssl.conf` 并重新启动 Apache。

如果在 Qualys SSL Labs 上再次测试域，将会看到已修复 RC4 漏洞和其他警告，并且摘要如下所示。

总评	A
证书	100%
协议支持	100%
密钥交换	90%
密码强度	90%

在每次更新 OpenSSL 时，将引入新的密码并删除对旧密码的支持。使 EC2 Amazon Linux 2 实例保持最新，关注来自 OpenSSL 的安全公告，并留意技术出版物中对新安全漏洞的报告。

问题排查

- 除非我输入密码，否则我的 Apache Web 服务器不会启动

  如果您安装了受密码保护的加密的私有服务器密钥，这是预期行为。

  您可以从密钥中删除加密和密码要求。假设在默认目录中具有一个称为 `custom.key` 的加密的私有 RSA 密钥，并且此密钥上的密码是 **abcde12345**，则对 EC2 实例运行以下命令可生成此密钥的未加密版本。

```
[ec2-user ~]$ cd /etc/pki/tls/private/
[ec2-user private]$ sudo cp custom.key custom.key.bak
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out
 custom.key.nocrypt
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key
[ec2-user private]$ sudo chown root:root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ sudo systemctl restart httpd
```

Apache 现在启动时应该不会提示您提供密码。

- 我在运行 sudo yum install -y mod_ssl 时收到了错误。

  在为 SSL 安装所需的程序包时，您可能会看到与以下内容类似的错误。

  ```
  Error: httpd24-tools conflicts with httpd-tools-2.2.34-1.16.amzn1.x86_64
  Error: httpd24 conflicts with httpd-2.2.34-1.16.amzn1.x86_64
  ```

  这通常意味着您的 EC2 实例没有运行 Amazon Linux 2。本教程仅支持从官方 Amazon Linux 2 AMI 新创建的实例。

证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用

> **Warning**
>
> “Let's Encrypt”交叉签名 DST 根 CA X3 证书已在 2021 年 9 月 30 日过期。在 CentOS/RHEL7 和 Amazon Linux 上使用 OpenSSL 1.0.x 时，这会导致 Let's Encrypt 连接失败。补救步骤可以参见此处，或者您可以遵照 OpenSSL 博客页面上提供的人工解决方法之一。
>
> **Important**
>
> 除非您拥有注册并托管的 DNS 域，否则，有关获取 Let's Encrypt 主机证书的这些说明不适用。这些说明不适用于 Amazon 分配的公有 DNS 主机名。

Let's Encrypt 证书颁发机构是电子前沿基金会 (EFF) 致力于对整个 Internet 进行加密的核心所在。按照该目标，Let's Encrypt 主机证书被设计为用最小的人工干预来进行创建、验证、安装和维护。证书管理的自动化方面由在 Web 服务器上运行的软件代理执行。在安装并配置代理后，它与 Let's Encrypt 安全地通信并在 Apache 和密钥管理系统上执行管理任务。本教程使用免费的 Certbot 代理，因为它允许您提供自定义的加密密钥作为您证书的基础，或允许代理自身根据其默认值创建密钥。您也可以将 Certbot 配置为定期续订您的证书，无需人工交互，如自动化 Certbot (p. 67)中所述。有关更多信息，请参阅 Certbot 用户指南和手册页。

虽然 Certbot 不受 Amazon Linux 2 官方支持，但可供下载并在安装时正常工作。建议您执行以下备份来保护数据并避免造成不便：

- 在开始之前，请为您的 Amazon EBS 根卷制作快照。这使您能够还原 EC2 实例的原始状态。有关创建 EBS 快照的信息，请参阅创建 Amazon EBS 快照 (p. 1372)。
- 以下过程要求您编辑您的 `httpd.conf` 文件，该文件控制 Apache 的操作。Certbot 对此配置文件和其他配置文件进行其自动化更改。创建整个 `/etc/httpd` 目录的备份副本，以便您在需要时还原该目录。

准备安装

在安装 Certbot 之前，请执行以下操作。

1. 编辑主要 Apache 配置文件 `/etc/httpd/conf/httpd.conf`。找到“`Listen 80`”指令并在后面添加以下行，将示例域名替换为实际公用名和主题替代名称 (SAN)。

   ```
   <VirtualHost *:80>
       DocumentRoot "/var/www/html"
       ServerName "example.com"
       ServerAlias "www.example.com"
   </VirtualHost>
   ```

2. 保存并关闭 文件。
3. 重启 Apache。

```
[ec2-user ~]$ sudo systemctl restart httpd
```

安装并运行 Certbot

此过程基于有关在 Fedora 和 RHEL 7 上安装 Certbot 的 EFF 文档。其中介绍 Certbot 的默认使用，即根据 2048 位 RSA 密钥生成证书。

1. 安装 Amazon Extras repo for epel。

```
[ec2-user ~]$ sudo amazon-linux-extras install epel -y
```

2. 使用以下命令安装 Certbot 包和依赖项。

```
[ec2-user ~]$ sudo yum install -y certbot python2-certbot-apache
```

3. 运行 Certbot。

```
[ec2-user ~]$ sudo certbot
```

4. 在提示符“Enter email address (used for urgent renewal and security notices)”处，输入联系人地址并按 Enter。
5. 在提示符处，同意 Let's Encrypt 服务条款。输入“A”并按 Enter 以继续。

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(A)gree/(C)ancel: A
```

6. 完成授权以使 EFF 将您加入发送名单中，输入“Y”或“N”并按 Enter。
7. Certbot 显示您在 VirtualHost 数据块中提供的公用名和主题替代名称 (SAN)。

```
Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: example.com
2: www.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
```

将输入保留空白并按 Enter。

8. Certbot 在创建证书和配置 Apache 时将显示以下输出。然后，它提示您有关将 HTTP 查询重定向到 HTTPS 的事项。

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for example.com
http-01 challenge for www.example.com
Waiting for verification...
Cleaning up challenges
```

```
Created an SSL vhost at /etc/httpd/conf/httpd-le-ssl.conf
Deploying Certificate for example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf
Enabling site /etc/httpd/conf/httpd-le-ssl.conf by adding Include to root configuration
Deploying Certificate for www.example.com to VirtualHost /etc/httpd/conf/httpd-le-
ssl.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```

要允许访客通过未加密的 HTTP 连接到服务器，请输入“1”。若要仅接受通过 HTTPS 的加密连接，请输入“2”。按 Enter 提交您的选择。

9. Certbot 完成 Apache 的配置并报告成功和其他信息。

```
Congratulations! You have successfully enabled https://example.com and
https://www.example.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=example.com
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/certbot.oneeyedman.net/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/certbot.oneeyedman.net/privkey.pem
   Your cert will expire on 2019-08-01. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
```

10. 在完成安装后，测试并优化您服务器的安全性，如步骤 3：测试和强化安全配置 (p. 62)中所述。

配置自动证书续订

Certbot 被设计成服务器系统的一个不可见的防错部分。默认情况下，它会生成具有短暂的 90 天到期时间的主机证书。如果您还未将系统配置为自动调用命令，则必须在到期之前手动重新运行 certbot 命令。此过程介绍如何通过设置 cron 作业来实现 Certbot 自动化。

自动化 Certbot

1. 使用 sudo，在文本编辑器（例如 vim 或 nano）中打开 `/etc/crontab` 文件。或者，请使用 sudo crontab -e。
2. 添加类似于下文的行并保存文件。

```
39      1,13    *       *       *       root    certbot renew --no-self-upgrade
```

这是每个组件的说明：

`39 1,13 * * *`

排定一个在每天 01:39 和 13:39 运行的命令。所选的值是随机的，但 Certbot 开发人员建议每天运行该命令至少两次。这将确保立即撤销并替换任何发现已损坏的证书。

`root`

该命令使用根权限运行。

`certbot renew --no-self-upgrade`

将要运行的命令。renew 子命令会使 Certbot 检查任何先前获取的证书并续订即将到期的证书。`--no-self-upgrade` 标记可防止 Certbot 在没有您干预的情况下自行升级。

3. 重启 cron 守护程序。

```
[ec2-user ~]$ sudo systemctl restart crond
```

教程：使用 Amazon Linux AMI 配置 SSL/TLS

安全套接字层/传输层安全性 (SSL/TLS) 可在 Web 服务器和 Web 客户端之间创建一个加密通道，以防止数据在传输过程中被窃听。本教程介绍如何在具有 Amazon Linux AMI 和 Apache Web 服务器的 EC2 实例上手动添加对 SSL/TLS 的支持。本教程假定您未使用负载均衡器。如果您正在使用 Elastic Load Balancing，则可以选择使用来自 Amazon Certificate Manager 的证书在负载均衡器上配置 SSL 卸载。

由于历史原因，Web 加密通常简称为 SSL。虽然 Web 浏览器仍支持 SSL，但使用其下一代协议 TLS 更不易受攻击。默认情况下，Amazon Linux AMI 将禁用所有版本的 SSL 的服务器端支持。安全标准机构认为 TLS 1.0 不安全。TLS 1.0 和 TLS 1.1 已于 2021 年 3 月正式弃用。本教程仅包含有关启用 TLS 1.2 的指导。TLS 1.3 于 2018 年定版，只需支持和启用底层 TLS 库（本教程中为 OpenSSL）即可在 Amazon Linux 2 中使用。客户端必须在 2023 年 6 月 28 日之前支持 TLS 1.2 或更高版本。有关更新的加密标准的更多信息，请参阅 RFC 7568 和 RFC 8446。

在本教程中，将现代 Web 加密简称为 TLS。

Important

这些过程适用于 Amazon Linux AMI。如果您尝试具有其他分配的实例上设置 LAMP Web 服务器，则本教程中的一些过程可能不适合您。对于 Amazon Linux 2，请参阅教程：在 Amazon Linux 2 上配置 SSL/TLS (p. 55)。对于 Ubuntu，请参阅以下社区文档：Open SSL on Ubuntu。有关 Red Hat Enterprise Linux 的信息，请参阅以下：设置 Apache HTTP Web 服务器。有关其他发布版本，请参阅特定于该版本的文档。

Note

或者，您还可以使用适用于 Amazon Nitro Enclaves 的 Amazon Certificate Manager (ACM)，这是一个 Enclave 应用程序，可使您通过 Amazon Nitro Enclaves 将公有和私有 SSL/TLS 证书与在 Amazon EC2 实例上运行的 Web 应用程序和服务器一起使用。Nitro Enclaves 是一项 Amazon EC2 功能，可以创建隔离的计算环境以保护和安全地处理高度敏感的数据，例如 SSL/TLS 证书和私有密钥。
适用于 Nitro Enclaves 的 ACM 与运行在 Amazon EC2 Linux 实例上的 nginx 结合使用，以创建私有密钥、分发证书和私有密钥以及管理证书续订。
要使用适用于 Nitro Enclaves 的 ACM，必须使用启用了 Enclave 的 Linux 实例。
有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？和适用于 Nitro Enclaves 的 Amazon Certificate Manager。

目录

- 先决条件 (p. 69)
- 步骤 1：在服务器上启用 TLS (p. 69)

- 步骤 2：获取 CA 签名的证书 (p. 70)
- 步骤 3：测试和强化安全配置 (p. 75)
- 问题排查 (p. 76)

先决条件

在开始本教程之前，请完成以下步骤：

- 使用 Amazon Linux AMI 启动 EBS 支持的实例。有关更多信息，请参阅步骤 1：启动实例 (p. 10)。
- 配置安全组以允许您的实例接受以下 TCP 端口上的连接：
  - SSH (端口 22)
  - HTTP (端口 80)
  - HTTPS (端口 443)

  有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
- 安装 Apache Web 服务器。有关分步说明，请参阅教程：在 Amazon Linux 上安装 LAMP Web 服务器 (p. 33)。仅需要 http24 包及其依赖项；可以忽略涉及 PHP 和 MySQL 的说明。
- 为了识别和验证网站，TLS 公有密钥基础设施 (PKI) 依赖于域名系统 (DNS)。要使用 EC2 实例托管公共网站，您需要为 Web 服务器注册一个域名，或者将现有域名转让给您的 Amazon EC2 主机。可通过很多第三方域注册和 DNS 托管服务来执行此操作，也可以使用 Amazon Route 53 执行此操作。

步骤 1：在服务器上启用 TLS

选项：使用 Automation 完成本教程

要使用 Amazon Systems Manager 而不是以下任务完成本教程，请运行 Automation 文档。

该过程指导您完成在 Amazon Linux 上使用自签名数字证书设置 TLS 的过程。

> **Note**
>
> 自签名证书对于测试是可接受的，但对于生产不是。如果您将自签名证书公开到 Internet，则您网站的访客将收到安全警告。

在服务器上启用 TLS

1. 连接到您的实例 (p. 11)并确认 Apache 正在运行。

   ```
   [ec2-user ~]$ sudo service httpd status
   ```

   如有必要，启动 Apache。

   ```
   [ec2-user ~]$ sudo service httpd start
   ```

2. 为确保您的所有软件包都处于最新状态，请对您的实例执行快速软件更新。此过程可能需要几分钟的时间，但必须确保您拥有最新的安全更新和缺陷修复。

   > **Note**
   >
   > -y 选项安装更新时不提示确认。如果您希望在安装前检查更新，则可以忽略该选项。

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. 现在，您的实例是最新的，请安装 Apache 模块 mod_ssl 以添加 TLS 支持：

```
[ec2-user ~]$ sudo yum install -y mod24_ssl
```

您的实例现在具有以下文件，可使用这些文件配置安全服务器并创建证书以进行测试：

`/etc/httpd/conf.d/ssl.conf`

mod_ssl 的配置文件。它包含一些“指令”以指示 Apache 在何处查找以下信息：加密密钥和证书、要允许的 TLS 协议版本以及要接受的加密密码。

`/etc/pki/tls/private/localhost.key`

针对 Amazon EC2 主机的自动生成的 2048 位 RSA 私有密钥。在安装期间，OpenSSL 已使用此密钥生成自签名主机证书，您也可使用此密钥生成证书签名请求 (CSR) 以提交给证书颁发机构 (CA)。

`/etc/pki/tls/certs/localhost.crt`

针对服务器主机的自动生成的自签名 X.509 证书。要测试是否正确设置 Apache 以使用 TLS，该证书是非常有用的。

`.key` 和 `.crt` 文件均为 PEM 格式，其中包含采用 Base64 编码的 ASCII 字符，并用“BEGIN”和“END”行框起来，如下面的简短证书示例所示：

```
-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----END CERTIFICATE-----
```

文件名和扩展名只是为了提供便利，对功能没有影响；只要 `cert.crt` 文件中的相关指令使用相同的名称，您可以将证书命名为 `cert.pem`、`ssl.conf` 或任何其他文件名。

Note

在使用您自己的自定义文件替换默认 TLS 文件时，请确保它们采用 PEM 格式。

4. 重启 Apache。

```
[ec2-user ~]$ sudo service httpd restart
```

5. 现在，您的 Apache Web 服务器应通过端口 443 支持 HTTPS (安全 HTTP)。通过将您的 EC2 实例的 IP 地址或完全限定域名与前缀 **`https://`** 一起键入浏览器 URL 栏中来对其进行测试。由于您正在使用自签名的不可信主机证书连接到站点，因此您的浏览器可能会显示一系列安全警告。

   忽视这些警告并继续连接站点。如果默认 Apache 测试页面打开，这意味着您已成功在服务器上配置 TLS。在浏览器和服务器之间传输的所有数据现在都被安全地加密了。

   为了防止站点访问者遇到警告屏幕，您需要获取一个证书，该证书不仅用于加密，而且还用于公开验证您的站点所有者身份。

步骤 2：获取 CA 签名的证书

您可以使用以下过程获取 CA 签名证书：

- 从私有密钥生成证书签名请求 (CSR)
- 将 CSR 提交给证书颁发机构 (CA)
- 获取签名的主机证书
- 配置 Apache 以使用证书

从加密角度看，自签名 TLS X.509 主机证书与 CA 签名证书完全相同。二者之间的区别在于社交层面，而非数学层面；CA 承诺，在向申请者颁发证书之前，至少验证域的所有权。每个 Web 浏览器均包含一个 CA 的列表，浏览器供应商信任这些 CA 来执行此操作。X.509 证书主要包含一个与您的私有服务器密钥对应的公有密钥和一个以加密方式与该公有密钥关联的 CA 的签名。当浏览器通过 HTTPS 连接到 Web 服务器时，服务器将提供证书以便浏览器检查其可信 CA 的列表。如果签署人位于列表上，或可通过由其他可信签署人组成的一系列信任访问，则浏览器将与服务器协商一个快速加密数据通道并加载页面。

由于验证请求需要投入人力，证书通常会产生费用，因此应货比三家。一些 CA 免费提供基础级别证书。其中最值得注意的 CA 是 Let's Encrypt 项目，该项目还支持证书创建和续订过程的自动化。有关将 Let's Encrypt 用作 CA 的更多信息，请参阅证书自动化：在 Amazon Linux 2 上将 Let's Encrypt 与 Certbot 结合使用 (p. 65)。

如果您打算提供商业级服务，Amazon Certificate Manager 是一个不错的选择。

主机证书的基础是密钥。自 2017 年起，政府和行业群体建议对 RSA 密钥使用 2048 位的最小密钥 (模数) 大小，旨在保护文档直到 2030 年。OpenSSL 在 Amazon Linux 中生成的默认系数大小为 2048 位，意味着现有的自动生成的密钥适用于 CA 签名的证书。下面介绍了适合需要自定义密钥的人员的替代过程，例如，具有较大系数或使用不同加密方法的过程。

除非您拥有注册并托管的 DNS 域，否则，有关获取 CA 签名主机证书的这些说明不适用。

获取 CA 签名的证书

1. 连接到您的实例 (p. 11)并导航到 /etc/pki/tls/private/。这是存储适用于 TLS 的服务器私有密钥的目录。如果您希望使用现有主机密钥来生成 CSR，请跳至步骤 3。
2. (可选) 生成新的私有密钥。下面是一些密钥配置示例。任何生成的密钥都将用于 Web 服务器，但它们实施安全的方式和程度有所不同。

   - 示例 1：创建默认 RSA 主机密钥。生成的文件 **custom.key** 是一个 2048 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key
     ```

   - 示例 2：创建具有更大模数的更严格的 RSA 密钥。生成的文件 **custom.key** 是一个 4096 位 RSA 私有密钥。

     ```
     [ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
     ```

   - 示例 3：创建具有密码保护的 4096 位加密的 RSA 密钥。生成的文件 **custom.key** 是一个已使用 AES-128 密码加密的 4096 位 RSA 私有密钥。

     Important

     对密钥进行加密可增强安全性，但由于加密的密钥需要密码，因此依赖于加密密钥的服务无法自动启动。每当您使用此密钥时，都必须通过 SSH 连接提供密码（在上一示例中为“abcde12345”）。

     ```
     [ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key
      4096
     ```

   - 示例 4：使用非 RSA 密码创建密钥。RSA 加密可能相对较慢，因为其公有密钥的大小基于两个大素数的乘积。不过，可以为 TLS 创建使用非 RSA 密码的密钥。在交付同等级别的安全性时，基于椭圆曲线的数学运算的密钥更小，计算起来更快。

```
[ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
```

结果为一个使用 prime256v1（OpenSSL 支持的“命名曲线”）的 256 位椭圆曲线私有密钥。根据 NIST，其加密强度略高于 2048 位 RSA 密钥。

Note

并非所有 CA 对基于椭圆曲线的密钥的支持级别与对 RSA 密钥的支持级别相同。

请确保新的私有密钥具有高度限制的所有权和权限 (所有者=根、组=根、仅面向所有者的读取/写入权限)。命令如下：

```
[ec2-user ~]$ sudo chown root.root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

上述命令应生成以下结果：

```
-rw------- root root custom.key
```

在创建并配置满意的密钥后，可以创建 CSR。

3. 使用您的首选密钥创建 CSR；下面的示例将使用 **custom.key**：

```
[ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
```

OpenSSL 将打开一个对话框，并提示您输入下表中显示的信息。对于基本的经域验证的主机证书来说，除 Common Name 以外的所有字段都是可选字段。

名称	描述	示例
国家/地区名称	代表国家/地区的两个字母 ISO 缩写。	US (=美国)
州或省名称	组织所在州或省的名称。此名称不可使用缩写。	Washington
所在地名称	您的组织所在的位置，例如城市。	Seattle
组织名称	组织的法定全称。请勿缩写组织名称。	Example Corporation
组织部门名称	额外的组织信息 (如果有)。	示例部门
公用名	此值必须与您希望用户键入浏览器中的 Web 地址完全匹配。通常，这表示以主机名称为前缀的域名或采用 **www.example.com** 格式的别名。在使用自签名证书且无 DNS 解析的测试中，公用名可能只包含主机名。CA 还提供费用更高的证书，这些证书接受通配符名称（例如 ***.example.com**）。	www.example.com
电子邮件地址	服务器管理员的电子邮件地址。	someone@example.com

最后，OpenSSL 将提示您输入可选的质询密码。此密码仅适用于 CSR 和您与 CA 之间的事务，因此请遵循 CA 提供的有关此密码以及其他可选字段、可选公司名的建议。CSR 质询密码不会影响服务器操作。

生成的文件 **csr.pem** 包含您的公有密钥、您的公有密钥的数字签名以及您输入的元数据。

4. 将 CSR 提交给 CA。这通常包括在文本编辑器中打开 CSR 文件并将内容复制到 Web 表格中。此时，您可能需要提供一个或多个主题备用名称 (SAN) 以放置到证书上。如果 **www.example.com** 是公用名，则 **example.com** 将是一个很好的 SAN，反之亦然。您网站的访客如果键入这两个名称的任何一个，便可看到一个没有错误的连接。如果您的 CA Web 表格允许该连接，请在 SAN 列表中包含公用名。一些 CA 会自动包含公用名。

   在您的请求获得批准后，您将收到一个由 CA 签署的新主机证书。此外，系统可能会指示您下载中间证书文件，该文件包含完成 CA 的信任链所需的其他证书。

   Note

   您的 CA 可能会针对各种不同用途，发送多种格式的文件。对于本教程，您应该只使用 PEM 格式的证书文件，此格式通常会 (但不总会) 标有 `.pem` 或 `.crt` 扩展名。如果您不确定要使用哪个文件，请用文本编辑器打开这些文件，并查找包含一个或多个具有以下开头的块的文件：

   ```
   - - - - -BEGIN CERTIFICATE - - - - -
   ```

   该文件还应具有以下结尾：

   ```
   - - - -END CERTIFICATE - - - - -
   ```

   您还可以如下所示在命令行上测试文件：

   ```
   [ec2-user certs]$ openssl x509 -in certificate.crt -text
   ```

   验证这些行是否显示在文件中。请勿使用结尾为 `.p7b`、`.p7c` 或类似文件扩展名的文件。

5. 将新的 CA 签名证书和任何中间证书放在 `/etc/pki/tls/certs` 目录中。

   Note

   可通过多种方法将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在本地计算机和 EC2 实例上打开一个文本编辑器（例如，vi、nano 或记事本），然后在这两者之间复制并粘贴文件内容。在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 `/etc/pki/tls/certs` 目录内部，使用以下命令验证文件所有权、组和权限设置是否与高度限制的 Amazon Linux 默认权限（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。

   ```
   [ec2-user certs]$ sudo chown root.root custom.crt
   [ec2-user certs]$ sudo chmod 600 custom.crt
   [ec2-user certs]$ ls -al custom.crt
   ```

   上述命令应生成以下结果：

   ```
   -rw------- root root custom.crt
   ```

   中间证书文件的权限并不严格 (所有者=根、组=根、所有者可以写入、组可以读取、任何人均可读取)。命令如下：

   ```
   [ec2-user certs]$ sudo chown root.root intermediate.crt
   [ec2-user certs]$ sudo chmod 644 intermediate.crt
   [ec2-user certs]$ ls -al intermediate.crt
   ```

上述命令应生成以下结果：

```
-rw-r--r-- root root intermediate.crt
```

6. 如果您使用自定义密钥创建您的 CSR 和由此生成的主机证书，请从 /etc/pki/tls/private/ 目录中删除或重命名旧密钥，然后在该目录中安装新密钥。

   Note

   有多种方法可以将自定义密钥上传到 EC2 实例，但最直接、最有益的方法是在本地计算机及 EC2 实例上各打开一个文本编辑器（如 vi、nano、记事本等），然后在这两者之间复制并粘贴文件内容。当在 EC2 实例上执行这些操作时，您需要根 [sudo] 权限。这样，一旦有任何权限或路径问题，您可以立即看到。但请小心操作，不要在复制内容时添加任何多余的行或以任何方式更改内容。

   从 /etc/pki/tls/private 目录内部，检查文件所有权、组和权限设置是否与高度限制的 Amazon Linux 默认权限（拥有者=根用户、组=根、仅面向拥有者的读取/写入权限）匹配。命令如下：

   ```
   [ec2-user private]$ sudo chown root.root custom.key
   [ec2-user private]$ sudo chmod 600 custom.key
   [ec2-user private]$ ls -al custom.key
   ```

   上述命令应生成以下结果：

   ```
   -rw------- root root custom.key
   ```

7. 编辑 /etc/httpd/conf.d/ssl.conf 以反映您的新证书和密钥文件。

   a. 在 Apache 的 SSLCertificateFile 指令中提供 CA 签名主机证书的路径和文件名：

      ```
      SSLCertificateFile /etc/pki/tls/certs/custom.crt
      ```

   b. 如果您收到一个中间证书文件（此示例中为 intermediate.crt），请使用 Apache 的 SSLCACertificateFile 指令提供其路径和文件名：

      ```
      SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
      ```

      Note

      一些 CA 将主机证书和中间证书组合到一个文件中，便不再需要此指令了。请查询您的 CA 提供的说明。

   c. 在 Apache 的 SSLCertificateKeyFile 指令中提供私有密钥的路径和文件名：

      ```
      SSLCertificateKeyFile /etc/pki/tls/private/custom.key
      ```

8. 保存 /etc/httpd/conf.d/ssl.conf 并重启 Apache。

   ```
   [ec2-user ~]$ sudo service httpd restart
   ```

9. 通过在浏览器 URL 栏中输入带有 https:// 前缀的域名来测试您的服务器。您的浏览器应通过 HTTPS 加载测试页面而不会产生错误。

步骤 3：测试和强化安全配置

在 TLS 可操作且公开发布后，应测试其实际安全性。使用在线服务（例如 Qualys SSL Labs，该服务可对您的安全设置执行免费的全面分析）可轻松执行此操作。根据结果，您可以决定通过控制接受的协议、首选的密码和排除的密码来强化默认安全配置。有关更多信息，请参阅 Qualys 如何用公式表示其分数。

> **Important**
>
> 实际测试对服务器的安全性非常重要。少量配置错误可能导致严重的安全漏洞和数据丢失。由于建议的安全实践会不断变化以响应调查和新兴威胁，因此定期安全审核对于良好的服务器管理来说是必不可少的。

在 Qualys SSL Labs 站点上，用 **www.example.com** 格式键入服务器的完全限定域名。约两分钟后，您将收到您站点的评级 (从 A 到 F) 和结果的详细信息。虽然概述信息显示配置基本正确，但详细报告标记了几个潜在的问题。例如：

✗ 支持某些旧浏览器使用 RC4 密码。密码是加密算法的数学核心。RC4 是一种用于加密 TLS 数据流的快速密码，已知这种密码存在一些严重缺点。除非您有充分理由支持旧版浏览器，否则，应禁用该密码。

✗ 支持旧 TLS 版本。该配置支持 TLS 1.0（已弃用）和 TLS 1.1（即将弃用）。从 2018 年开始，仅建议使用 TLS 1.2。

纠正 TLS 配置

1. 在文本编辑器中打开 /etc/httpd/conf.d/ssl.conf 配置文件，并在以下每个行的开头键入“#”来注释掉这些行：

```
#SSLProtocol all -SSLv3
#SSLProxyProtocol all -SSLv3
```

2. 添加以下指令：

```
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
SSLProxyProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

这些指令显式禁用 SSL 版本 2 和 3，以及 TLS 版本 1.0 和 1.1。现在，服务器拒绝接受与使用 TLS 1.2 以外的任何协议的客户端之间的加密连接。指令中冗长的文字可更清楚地告知人类读者服务器的作用。

> **Note**
>
> 以此方式禁用 TLS 1.0 和 1.1 版可阻止一小部分过时的 Web 浏览器访问您的网站。

修改允许的密码列表

1. 打开配置文件 /etc/httpd/conf.d/ssl.conf，找到包含用于配置 **SSLCipherSuite** 和 **SSLProxyCipherSuite** 的已注释掉的示例的部分。

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
#SSLProxyCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

保留它们不变，并在它们下面添加以下指令：

> **Note**
>
> 此处为方便阅读将指令显示为几行，但这两个指令必须各在一行上且密码名称之间不能有空格。

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES:!aNULL:!
eNULL:!EXPORT:!DES:
!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA

SSLProxyCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-
ECDSA-CHACHA20-POLY1305:
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES:!aNULL:!
eNULL:!EXPORT:!DES:
!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
```

这些密码是 OpenSSL 中更长的受支持密码列表的子集。根据以下标准选择这些密码并对其进行排序：

- 对向前保密性的支持
- Strength
- Speed
- 具体密码位于密码系列之前
- 允许的密码位于拒绝的密码之前

高级密码的名称中具有 ECDHE（表示 Elliptic Curve Diffie-Hellman Ephemeral）；ephemeral 表示向前保密性。此外，RC4 现在位于禁止的密码中的结尾处。

建议您使用密码的明确列表，而不依赖于内容不可见的默认值或简短指令。此处显示的密码列表只是很多可能的列表之一；例如，您可能希望优化列表以加快速度而不是向前保密性。

如果您预计需要支持较旧的客户端，则可以允许 DES-CBC3-SHA 密码套件。

对 OpenSSL 的每次更新将引入新密码并弃用旧密码。使 EC2 Amazon Linux 实例保持最新，关注来自 OpenSSL 的安全公告，并留意技术出版物中对新安全漏洞的报告。

2. 通过删除“#”取消对以下行的注释：

```
#SSLHonorCipherOrder on
```

该命令强制服务器优先选择高级密码，包括 (在此示例中) 支持向前保密性的密码。启用此指令后，服务器会在回滚到允许的安全性较低的密码之前尝试建立高度安全的连接。

3. 重启 Apache。如果您在 Qualys SSL Labs 上再次测试域，应会发现 RC4 漏洞已修复。

问题排查

- 除非我输入密码，否则我的 Apache Web 服务器不会启动

  如果您安装了受密码保护的加密的私有服务器密钥，这是预期行为。

  您可以从密钥中删除加密和密码要求。假设在默认目录中具有一个称为 `custom.key` 的加密的私有 RSA 密钥，并且此密钥上的密码是 **`abcde12345`**，则对 EC2 实例运行以下命令可生成此密钥的未加密版本。

```
[ec2-user ~]$ cd /etc/pki/tls/private/
[ec2-user private]$ sudo cp custom.key custom.key.bak
```

```
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out
 custom.key.nocrypt
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key
[ec2-user private]$ sudo chown root.root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ sudo service httpd restart
```

Apache 现在启动时应该不会提示您提供密码。

教程：增加 EC2 实例上 Amazon EBS 卷的大小

本教程将演示如何使用 EC2 启动实例向导启动 Amazon EC2 实例并添加 Amazon Elastic Block Store（Amazon EBS）卷。添加的卷必须使用文件系统格式化并完成挂载后才能使用。假设在使用此配置六个月后，您添加的卷已满。本教程演示如何将添加的卷大小增加一倍，以及如何扩展文件系统。

本教程使用一个 Amazon EC2 T3 实例，这是一种基于 Nitro 系统 的低成本通用实例类型。

在完成本教程中的步骤时，请注意以下几点：

- 两个卷 – 启动 Amazon EC2 实例后，您将有两个卷：一个根卷和一个附加卷。为了区分这些卷，在本教程中，附加卷将称为数据卷。
- 数据卷可用性 – 要使数据卷可用，您需要格式化并挂载数据卷。
- 文件系统 – 要利用增加大小后的数据卷，您需要扩展文件系统。

完成教程所需的时间

1 小时

成本

您在完成本教程过程中创建的 Amazon 资源可能会产生费用。只要您的 Amazon Web Services 账户创建后未满 12 个月，并且您根据 Free Tier 的要求配置了资源，则您可以在 Free Tier 下使用 Amazon EC2。完成本教程后，您可以删除不需要的任何资源。有关删除不需要的资源的步骤，请参阅 第 5 步：清除不需要的资源 (p. 84)

完成教程的步骤

- 第 1 步：启动一个带有附加 EBS 卷的 EC2 实例 (p. 77)
- 第 2 步：使数据卷可供使用 (p. 80)
- 第 3 步：增加数据卷的大小 (p. 81)
- 第 4 步：扩展文件系统 (p. 83)
- 第 5 步：清除不需要的资源 (p. 84)

第 1 步：启动一个带有附加 EBS 卷的 EC2 实例

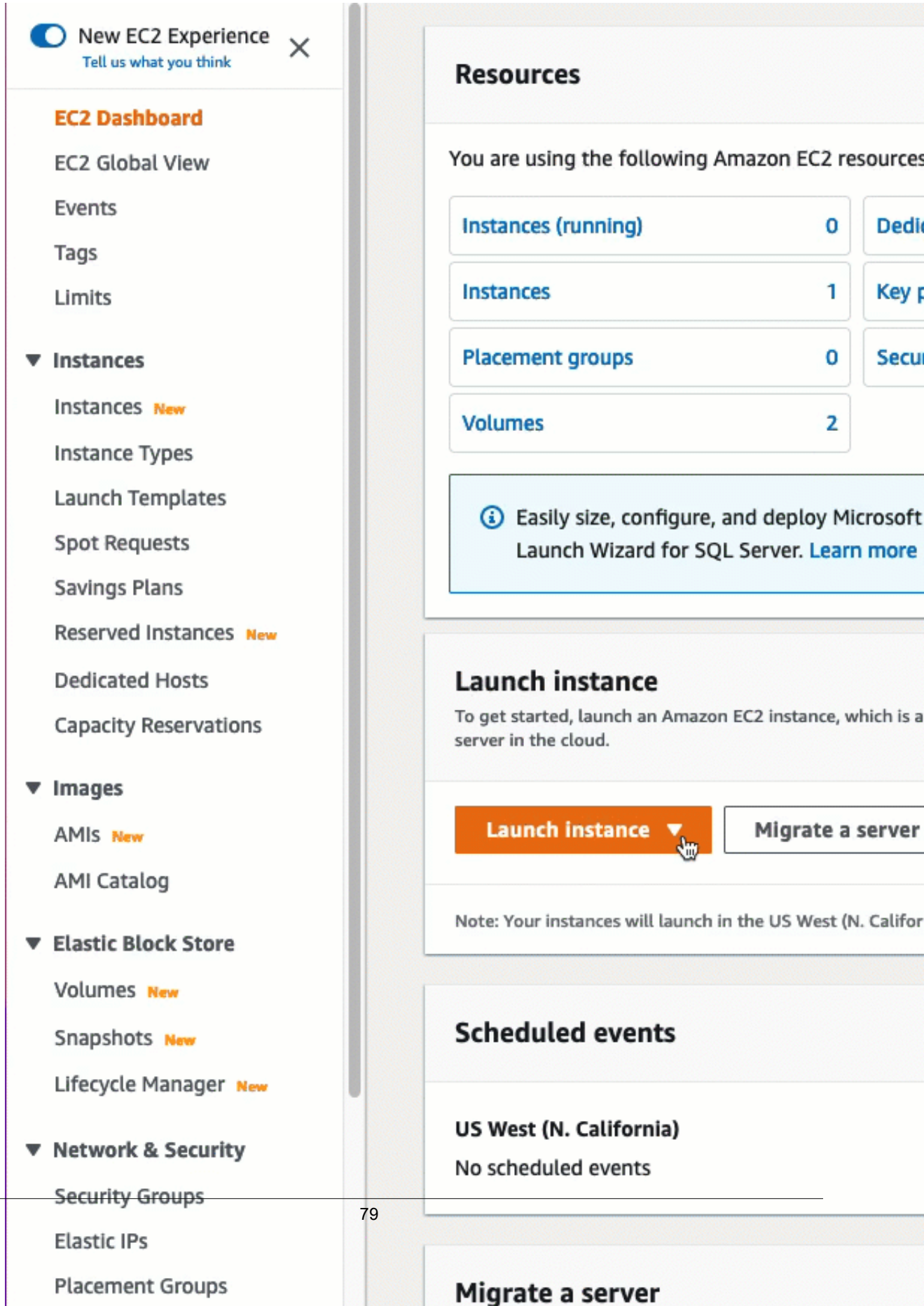
要启动实例，请选择一个 Amazon Web Services 区域、一个操作系统（OS）、一个 Amazon 机器映像（AMI）、一个实例类型，然后使用一个密钥对安全地连接到您的实例、设置网络并配置存储。启动实例时，您可以选择一个描述性名称以便于标识实例。在这一步中，您将启动一个叫做 `tutorial-volumes` 的实例。

> **Note**
>
> 本教程使用 Amazon Linux 2 AMI，这可能不适用于使用其他 Linux 发行版的其他自定义 AMI。

有关 Amazon Linux 2 AMI 的更多信息，请参阅 Amazon Linux 2 和 Amazon Linux AMI。

您可以观看动画：启动带有附加 EBS 卷的 EC2 实例，观看演示了如何启动带有 EBS 卷的 EC2 实例的动画。对于书面步骤，请查看随后的过程。

观看动画：启动带有附加 EBS 卷的 EC2 实例



启动 EC2 实例

1. 登录 Amazon Web Services Management Console，打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 EC2 Dashboard（EC2 控制面板）上，选择 Launch instance（启动实例）。
3. 在 Name and tags（名称和标签）下，对于 Name（名称），输入 **tutorial-volumes**。
4. 在 Application and OS Images（应用程序和操作系统镜像）下，选择 Quick Start（快速入门），并验证以下默认值：
   a. 实例的操作系统已选择为 Amazon Linux。
   b. 在 Amazon Machine Image (AMI) [Amazon 机器映像（AMI）]下，已选中 Amazon Linux 2 AMI。
5. 在 Instance type（实例类型）下，选择 `t3.micro`。
6. 在 Key pair (login) [密钥对（登录）]下，选择您的密钥对。
7. 在 Network settings（网络设置）下，请确保已选中 Allow SSH traffic（允许 SSH 流量）复选框。这将允许您使用 SSH 连接到您的实例。

   Warning

   出于安全原因，对于 Source（源），请勿选择 Anywhere（任何地方）。这将允许从互联网上的所有 IP 地址访问您的实例。在本教程中使用此设置是可接受的，但如果在生产环境中使用，则不太安全。
8. 在 Configure storage（配置存储）下，选择 Add new volume（添加新卷）。确保添加的 EBS volume（EBS 卷）大小为 8 GB，类型为 gp3。
   - 要确保在实例终止时删除数据卷，请选择 Advanced（高级）。在 Volume 2 (Custom) [卷 2（自定义）]下，选择 Delete on termination（终止时删除），然后选择 Yes（是）。
9. 在 Summary（摘要）面板中，选择 Launch instance（启动实例）。
10. 选择 View all instances（查看所有实例）以关闭确认页面并返回 Amazon EC2 控制台。

有关启动实例的更多信息，请参阅 使用新启动实例向导启动实例。

第 2 步：使数据卷可供使用

在第 1 步 (p. 77)中启动的 Amazon EC2 实例具有两个 EBS 卷：一个是根设备，另一个是附加存储设备（数据卷）。按照以下过程使数据卷可供使用。在本教程中，您将使用 XFS 文件系统。

Note

本教程中使用的实例类型（`t3.micro`）是基于 Nitro 系统构建的，这会将 EBS 卷公开为 NVMe 块设备。

有关使卷可供使用的更多信息，请参阅 在 Linux 上使 Amazon EBS 卷可供使用。

格式化并挂载数据卷

1. 在 Amazon EC2 控制台的导航窗格中，选择 Instances（实例），然后选择 **tutorial-volumes**。
2. 要连接到您的实例，请选择 Connect（连接），确保选中 EC2 Instance Connect，然后选择 Connect（连接）。
3. 在终端窗口中，使用以下命令查看可用磁盘设备及其挂载点。lsblk 的输出移除了完整设备路径中的 `/dev/` 前缀。

```
[ec2-user ~]$ sudo lsblk -f
```

以下示例输出显示有两个设备挂载到实例：根设备 /dev/nvme0n1 和数据卷 /dev/nvme1n1。在此例中，您可以在 FSTYPE 列下看到数据卷没有文件系统。

```
[ec2-user@                ~]$ sudo lsblk -f
NAME          FSTYPE LABEL UUID                                 MOUNTPOINT
nvme1n1
nvme0n1
├─nvme0n1p1   xfs    /     111667cd-96f8-41ba-bb2d-7c558ae6ad71 /
└─nvme0n1p128
```

4. 要创建文件系统，请使用以下命令和数据卷名称（/dev/nvme1n1）。

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/nvme1n1
```

5. 要创建数据卷的挂载点目录，请使用以下命令。挂载点是卷在文件系统树中的位置，以及您在安装卷之后读写文件的位置。下面的示例创建一个名为 /data 的目录。

```
[ec2-user ~]$ sudo mkdir /data
```

6. 要在刚刚创建的目录中挂载数据卷，请使用以下命令以及数据卷名称（/dev/nvme1n1）和挂载点目录名称（/data）。

```
[ec2-user ~]$ sudo mount /dev/nvme1n1 /data
```

7. 重启实例后，挂载点不会自动保存。要在重启后自动挂载数据卷，请参阅 重启后自动挂载附加的卷。
8. 要验证您是否已格式化并挂载了数据卷，请再次运行以下命令。

```
[ec2-user ~]$ lsblk -f
```

下面的示例输出显示，数据卷 /dev/nvme1n1 具有 XFS 文件系统，挂载在 /data 挂载点。

```
[ec2-user@                ~]$ lsblk -f
NAME          FSTYPE LABEL UUID                                 MOUNTPOINT
nvme1n1       xfs          db1a8fd8-ef7a-4143-b550-fa05e0135bac /data
nvme0n1
├─nvme0n1p1   xfs    /     111667cd-96f8-41ba-bb2d-7c558ae6ad71 /
└─nvme0n1p128
```

第 3 步：增加数据卷的大小

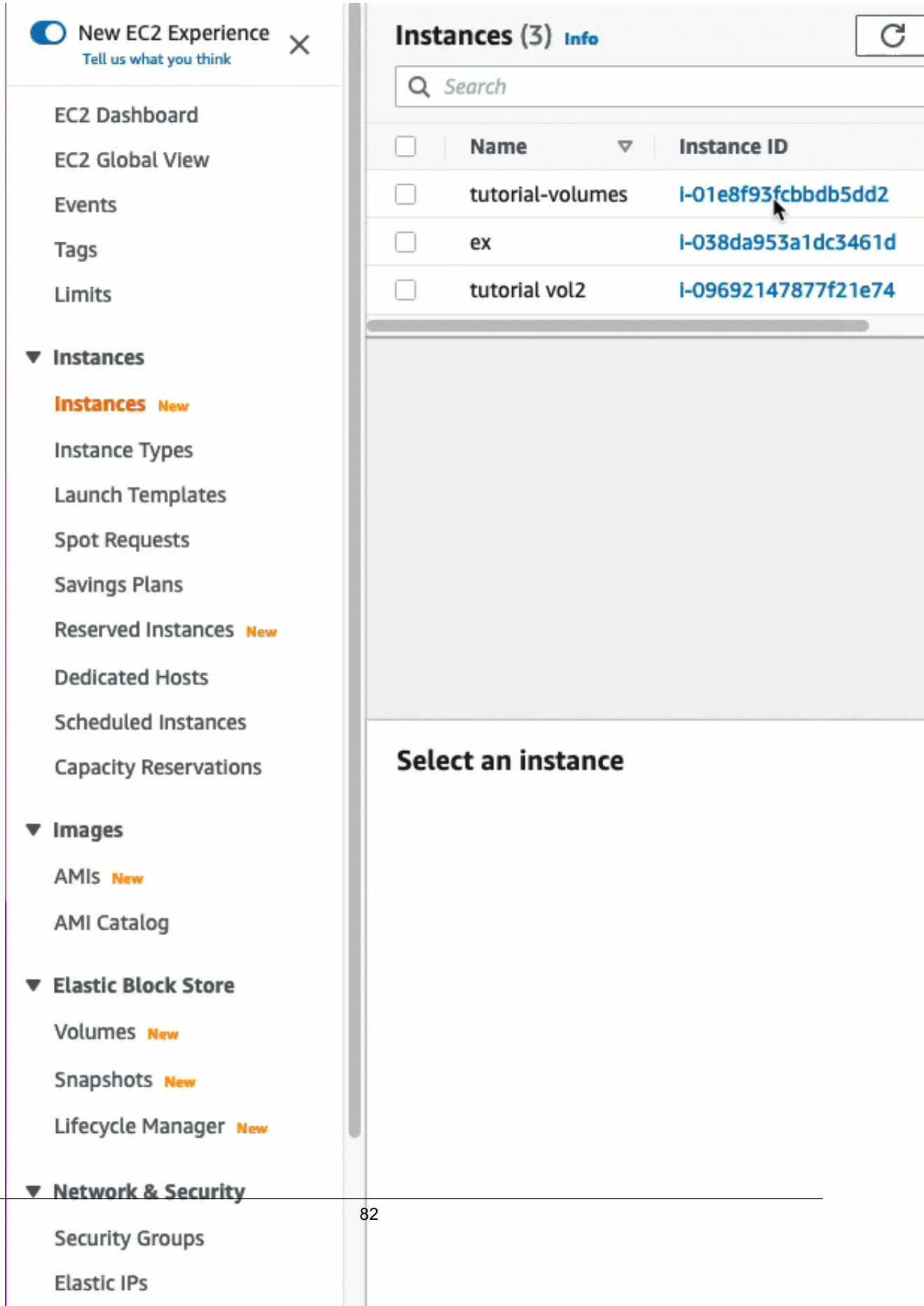
假设在使用上述配置六个月后，您用完了数据卷上的存储空间。您决定将数据卷的大小增加一倍。为此，您首先要创建一个快照，然后增加数据卷的大小。创建快照时，使用一个描述来标识该快照。在本教程中，您创建了一个名为 tutorial-volumes-backup 的快照。

Note

在修改 EBS 卷时，它将依次经过以下状态：modifying、optimizing 和 completed。请记住，在卷进入 optimizing 状态之前，您将无法扩展文件系统。

您可以展开观看动画：增加数据卷的大小，以观看动画演示如何创建快照并增加数据卷大小的动画。对于书面步骤，请查看随后的过程。

观看动画：增加数据卷的大小



增加数据卷的大小

1. 关闭 EC2 Instance Connect 的浏览器窗口，返回 Amazon EC2 控制台。
2. 如果需要回滚更改，请创建数据卷的快照。
   a. 在 Amazon EC2 控制台的导航窗格中，选择 Instances（实例），然后选择 **tutorial-volumes**。
   b. 在 Storage（存储）选项卡的 Block devices（块设备）下，选择该数据卷的 Volume ID（卷 ID）。
   c. 在 Volumes（卷）详细信息页面上，选择 Actions（操作），然后选择 Create snapshot（创建快照）。
   d. 在 Description（描述）下，输入 **tutorial-volumes-backup**。
   e. 选择 Create snapshot (创建快照)。
3. 要增加数据卷大小，请在导航窗格中选择 Instances（实例），然后选择 **tutorial-volumes**。
4. 在 Storage（存储）选项卡下，选择数据卷的 Volume ID（卷 ID）。
5. 选中您的 Volume ID（卷 ID）对应的复选框，选择 Actions（操作），然后选择 Modify volume（修改卷）。
6. Modify Volume（修改卷）屏幕会显示卷 ID 和卷的当前配置，包括类型、大小、每秒进行读写操作的次数（IOPS）和吞吐量。在本教程中，您会将数据卷的大小增加一倍。
   a. 对于 Volume type（卷类型），请勿更改任何值。
   b. 对于 Size（大小），更改为 16GB。
   c. 对于 IOPS，请勿更改任何值。
   d. 对于 Throughput（吞吐量），请勿更改任何值。
7. 选择 Modify（修改），然后在系统提示您确认时再次选择 Modify（修改）。卷修改开始后，您需要支付新卷配置的费用。有关定价信息，请参阅 Amazon EBS 定价。

   Note

   您必须等待至少六个小时并确保卷处于 `in-use` 或 `available` 状态，然后才能再次修改该卷。

第 4 步：扩展文件系统

数据卷进入 `optimizing` 状态后，您可以使用特定于文件系统的命令将文件系统扩展到更大的新大小。

有关扩展文件系统的更多信息，请参阅 在调整卷大小后扩展 Linux 文件系统。

扩展文件系统

1. 在 Amazon EC2 控制台中的 EC2 控制面板上，选择 Instances（实例），然后选择 **tutorial-volumes**。
2. 要连接到您的实例，请选择 Connect（连接），确保选中 EC2 Instance Connect，然后选择 Connect（连接）。
3. 在终端窗口中，使用以下命令获取文件系统的大小。

```
[ec2-user ~]$ df -hT
```

下面的示例输出显示数据卷 `/dev/nvme1n1` 的文件系统大小为 8GB。在前面的过程中，您将数据卷大小增加到 16GB。现在，您需要扩展文件系统以利用增加的存储空间。

```
[ec2-user@:                ]$ df -hT
Filesystem     Type      Size  Used Avail Use% Mounted on
devtmpfs       devtmpfs  462M     0  462M   0% /dev
tmpfs          tmpfs     471M     0  471M   0% /dev/shm
tmpfs          tmpfs     471M  412K  470M   1% /run
tmpfs          tmpfs     471M     0  471M   0% /sys/fs/cgroup
/dev/nvme0n1p1 xfs       8.0G  1.6G  6.5G  20% /
/dev/nvme1n1   xfs       8.0G   41M  8.0G   1% /data
tmpfs          tmpfs      95M     0   95M   0% /run/user/1000
```

4. 使用以下命令扩展挂载在 /data 挂载点的 XFS 文件系统。

```
[ec2-user ~]$ sudo xfs_growfs -d /data
```

5. 再次使用以下命令验证文件系统是否已成功扩展。

```
[ec2-user ~]$ df -hT
```

下面的示例输出显示 /dev/nvme1n1 的文件系统大小与数据卷的大小相同。

```
[ec2-user@:                ]$ df -hT
Filesystem     Type      Size  Used Avail Use% Mounted on
devtmpfs       devtmpfs  462M     0  462M   0% /dev
tmpfs          tmpfs     471M     0  471M   0% /dev/shm
tmpfs          tmpfs     471M  468K  470M   1% /run
tmpfs          tmpfs     471M     0  471M   0% /sys/fs/cgroup
/dev/nvme0n1p1 xfs       8.0G  1.6G  6.5G  20% /
/dev/nvme1n1   xfs        16G   50M   16G   1% /data
tmpfs          tmpfs      95M     0   95M   0% /run/user/1000
tmpfs          tmpfs      95M     0   95M   0% /run/user/0
```

第 5 步：清除不需要的资源

在以下步骤中，您将清除您在本教程中创建的资源。删除不再使用的资源是一个很好的习惯。通过删除资源，该资源也将停止产生费用。

> Note
>
> 已删除、终止或释放的资源将无法恢复。

终止实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选中 **tutorial-volumes** 对应的复选框。
4. 选择 Instance state（实例状态），然后选择 Terminate instance（终止实例）。
5. 当系统提示您确认时，选择终止。

如何删除快照

1. 在导航窗格中的 Elastic Block Store 下，选择 Snapshots。
2. 选中 **tutorial-volumes-backup** 对应的复选框。
3. 在 Actions（操作）下，选择 Delete snapshot（删除快照）。
4. 当系统提示进行确认时，选择 Delete（删除）。

教程：在 Amazon Linux 2023 上托管 WordPress 博客

以下步骤将帮助您在 Amazon Linux 2023 实例上安装、配置和保护 WordPress 博客。本教程是很好的 Amazon EC2 入门教程，因为您可以完全控制托管您 WordPress 博客的 Web 服务器，这对传统的托管服务来说并不是一个典型的方案。

您负责更新软件包并为您的服务器维护安全补丁。对于不需要与 Web 服务器配置直接交互的更自动化 WordPress 安装来说，Amazon CloudFormation 服务还会提供可让您快速入门的 WordPress 模板。有关更多信息，请参阅Amazon CloudFormation 用户指南中的入门。如果您更喜欢将您的 WordPress 博客托管在 Windows 实例上，请参阅 Amazon EC2 Windows 实例用户指南中的在您的 Amazon EC2 Windows 实例上部署 WordPress 博客。如果您需要带分离数据库的高可用性解决方案，请参阅Amazon Elastic Beanstalk 开发人员指南中的部署高可用性 WordPress 网站。

> **Important**
>
> 这些过程适用于 Amazon Linux 2023。对于 Amazon Linux 2，请参阅教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)。有关其他发布版本的信息，请参阅特定于该版本的文档。本教程中的很多步骤对 Ubuntu 实例并不适用。有关在 Ubuntu 实例上安装 WordPress 的帮助，请参阅 Ubuntu 文档中的 WordPress。您还可以使用 CodeDeploy 在 Amazon Linux、macOS 或 Unix 系统上完成此任务。

主题

- 先决条件 (p. 85)
- 安装 WordPress (p. 85)
- 后续步骤 (p. 92)
- 帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪 (p. 92)

先决条件

强烈建议您将弹性 IP 地址 (EIP) 与您正用于托管 WordPress 博客的实例关联。这将防止您的实例的公有 DNS 地址更改和中断您的安装。如果您有一个域名且打算将其用于您的博客，则可更新该域名的 DNS 记录，使其指向您的 EIP 地址 (如需帮助，请联系您的域名注册商)。您可以免费将一个 EIP 地址与正在运行的实例相关联。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。本 教程：在 Amazon Linux 2023 上安装 LAMP Web 服务器 (p. 15) 教程还介绍了配置安全组以允许 HTTP 和 HTTPS 流量的步骤，以及用于确保为 Web 服务器正确设置文件权限的几个步骤。有关添加规则到您安全组的信息，请参阅 向安全组添加规则 (p. 1311)。

如果您的博客还没有域名，则可使用 Route 53 注册一个域名并将您的实例的 EIP 地址与您的域名相关联。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的使用 Amazon Route 53 注册域名。

安装 WordPress

连接到您的实例 (p. 11)，然后下载 WordPress 安装软件包。

1. 使用以下命令下载并安装这些软件包。

```
dnf install wget php-mysqlnd httpd php-fpm php-mysqli mariadb105-server php-json php
 php-devel -y
```

2. 您可能会发现显示一条与输出中措辞类似的警告（版本可能随着时间变化）：

```
WARNING:
```

```
  A newer release of "Amazon Linux" is available.

  Available Versions:

dnf update --releasever=2023.0.20230202

    Release notes:
     https://aws.amazon.com

  Version 2023.0.20230204:
    Run the following command to update to 2023.0.20230204:

      dnf update --releasever=2023.0.20230204 ... etc
```

建议最好尽量让操作系统保持最新版本，但您可能需要迭代每个版本以确保环境中不存在冲突。如果步骤 1 中提及的软件包安装失败，则可能需要更新到所列出的某个较新版本，然后重试。

3. 使用 wget 命令下载最新的 WordPress 安装包。以下命令始终会下载最新版本。

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

4. 解压并解档安装包。安装文件夹解压到名为 `wordpress` 的文件夹。

```
[ec2-user ~]$ tar -xzf latest.tar.gz
```

为安装 WordPress 创建数据库用户和数据库

安装 WordPress 需要存储信息，例如数据库中的博客文章和用户评论。此过程帮助您创建自己的博客数据库，并创建一个有权读取该数据库的信息并将信息保存到该数据库的用户。

1. 启动数据库和 Web 服务器。

```
[ec2-user ~]$ sudo systemctl start mariadb httpd
```

2. 以 `root` 用户身份登录数据库服务器。在系统提示时输入您的数据库 `root` 密码，它可能与您的 `root` 系统密码不同；如果您尚未给您的数据库服务器加密，它甚至可能是空的。

   如果您尚未给您的数据库服务器加密，则必须执行这项操作。有关更多信息，请参阅 保护 MariaDB 服务器 (p. 28)（Amazon Linux 2023）或 确保数据库服务器的安全 (p. 37)（Amazon Linux 2023 AMI）。

```
[ec2-user ~]$ mysql -u root -p
```

3. 为您的 MySQL 数据库创建用户和密码。安装 WordPress 的过程将使用这些值与您的 MySQL 数据库通信。输入以下命令，以替换唯一的用户名和密码。

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

   确保为您的用户创建强密码。请勿在您的密码中使用单引号字符 (')，因为这将中断前面的命令。有关创建安全密码的更多信息，请转至 http://www.pctools.com/guides/password/。请勿重复使用现有密码，并确保将密码保存在安全的位置。

4. 创建数据库。为数据库提供一个有意义的描述性名称，例如 `wordpress-db`。

   Note

   以下命令中数据库名称两边的标点符号称为反引号。在标准键盘上，反引号 (`) 键通常位于 Tab 键的上方。并不总是需要反引号，但是它们允许您在数据库名称中使用其他的非法字符，例如连字符。

```
CREATE DATABASE `wordpress-db`;
```

5. 对您之前创建的 WordPress 用户授予您数据库的完全访问权限。

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. 刷新数据库权限以接受您的所有更改。

```
FLUSH PRIVILEGES;
```

7. 退出 mysql 客户端。

```
exit
```

创建和编辑 wp-config.php 文件

WordPress 安装文件夹包含名为 wp-config-sample.php 的示例配置文件。在本步骤中，您将复制此文件并进行编辑以适合您的具体配置。

1. 将 wp-config-sample.php 文件复制为一个名为 wp-config.php 的文件。这样做会创建新的配置文件并将原先的示例配置文件原样保留作为备份。

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. 用您喜欢的文本编辑器（例如 nano 或 vim）编辑 wp-config.php 文件并输入适用于您的安装的值。如果没有常用的文本编辑器，nano 比较适合初学者使用。

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

   a. 查找定义 DB_NAME 的行并将 database_name_here 更改为您在 Step 4 (p. 86) 的 为安装 WordPress 创建数据库用户和数据库 (p. 86) 中创建的数据库名称。

```
define('DB_NAME', 'wordpress-db');
```

   b. 查找定义 DB_USER 的行并将 username_here 更改为您在 Step 3 (p. 86) 的 为安装 WordPress 创建数据库用户和数据库 (p. 86) 中创建的数据库用户。

```
define('DB_USER', 'wordpress-user');
```

   c. 查找定义 DB_PASSWORD 的行并将 password_here 更改为您在 Step 3 (p. 86) 的 为安装 WordPress 创建数据库用户和数据库 (p. 86) 中创建的强密码。

```
define('DB_PASSWORD', 'your_strong_password');
```

   d. 查找名为 Authentication Unique Keys and Salts 的一节。这些 KEY 和 SALT 值为 WordPress 用户存储在其本地计算机上的浏览器 Cookie 提供了加密层。总而言之，添加长的随机值将使您的站点更安全。访问 https://api.wordpress.org/secret-key/1.1/salt/ 随机生成一组密钥值，您可以将这些密钥值复制并粘贴到 wp-config.php 文件中。要粘贴文本到 PuTTY 终端，请将光标放在您要粘贴文本的地方，并在 PuTTY 终端内部右键单击鼠标。

   有关安全密钥的更多信息，请转至 https://wordpress.org/support/article/editing-wp-config-php/#security-keys。

Note

以下值仅用作示例；请勿使用以下值进行安装。

```
define('AUTH_KEY',         ' #U$$+[RXN8:b^-L 0(WU_+ c+WFkI~c]o]-bHw+)/
Aj[wTwSiZ<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY',  'Zsz._P=l/|y.Lq)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?6OP
$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$DpB4Hj[JK:?{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%_-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
define('LOGGED_IN_SALT',   ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|e(76miC
+&W&+^0P/');
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

e. 保存 文件并退出文本编辑器。

将 WordPress 文件安装到 Apache 文档根目录下

- 现在，您已解压了安装文件夹、创建了 MySQL 数据库和用户并自定义了 WordPress 配置文件，那么也就准备好将您的安装文件复制到 Web 服务器文档根目录，以便可以运行安装脚本完成安装。这些文件的位置取决于您是希望 WordPress 博客位于 Web 服务器的实际根目录 (例如，*my.public.dns.amazonaws.com*) 还是位于根目录下的某个子目录或文件夹 (例如，*my.public.dns.amazonaws.com/blog*) 中。
  - 如果希望 WordPress 在文档根目录下运行，请复制 wordpress 安装目录的内容 (但不包括目录本身)，如下所示：

    ```
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/
    ```

  - 如果希望 WordPress 在文档根目录下的其他目录中运行，请先创建该目录，然后将文件复制到其中。在此示例中，WordPress 将从目录 `blog` 运行：

    ```
    [ec2-user ~]$ mkdir /var/www/html/blog
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
    ```

Important

出于安全原因，如果您不打算立即进入到下一个过程，请立即停止 Apache Web 服务器 (`httpd`)。将安装文件移动到 Apache 文档根目录下后，WordPress 安装脚本将不受保护，如果 Apache Web 服务器运行，攻击者可能会获得访问您博客的权限。要终止 Apache Web 服务器，请输入命令 sudo service httpd stop。如果您即将继续到下一个步骤，则不需要终止 Apache Web 服务器。

允许 WordPress 使用 permalink

WordPress permalink 需要使用 Apache `.htaccess` 文件才能正常工作，但默认情况下这些文件在 Amazon Linux 上处于禁用状态。使用此过程可允许 Apache 文档根目录中的所有覆盖。

1. 使用您常用的文本编辑器（如 `httpd.conf` 或 nano）打开 vim 文件。如果没有常用的文本编辑器，nano 比较适合初学者使用。

```
[ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
```

2. 找到以 <Directory "/var/www/html"> 开头的部分。

```
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>
```

3. 在以上部分中将 AllowOverride None 行改为读取 AllowOverride *All*。

   Note

   此文件中有多个 AllowOverride 行；请确保更改 <Directory "/var/www/html"> 部分中的行。

```
AllowOverride All
```

4. 保存 文件并退出文本编辑器。

在 Amazon Linux 2023 上安装 PHP 图形绘图库

PHP 的 GD 库允许您修改图像。如果您需要裁剪博客的标题图像，请安装此库。您安装的 phpMyAdmin 版本可能需要此库的特定最低版本（例如 8.1 版）。

使用以下命令在 Amazon Linux 2023 上安装 PHP 图形绘图库。例如，如果您在安装 LAMP 堆栈的过程中从源安装了 php8.1，则此命令将安装 8.1 版的 PHP 图形绘图库。

```
[ec2-user ~]$ sudo dnf install php-gd
```

要验证安装的版本，请使用以下命令：

```
[ec2-user ~]$ sudo dnf list installed | grep php-gd
```

下面是示例输出：

```
php-gd.x86_64                    8.1.30-1.amzn2             @amazonlinux
```

在 Amazon Linux AMI 上安装 PHP 图形绘图库

PHP 的 GD 库允许您修改图像。如果您需要裁剪博客的标题图像，请安装此库。您安装的 phpMyAdmin 版本可能需要此库的特定最低版本（例如 8.1 版）。

要验证哪些版本可用，请使用以下命令：

```
[ec2-user ~]$ dnf list | grep php
```

以下是 PHP 图形绘图库（8.1 版）的输出中的示例行：

```
php8.1.aarch64                                                 8.1.7-1.amzn2023.0.1
                  @amazonlinux
php8.1-cli.aarch64                                             8.1.7-1.amzn2023.0.1
                  @amazonlinux
php8.1-common.aarch64                                          8.1.7-1.amzn2023.0.1
                  @amazonlinux
php8.1-devel.aarch64                                           8.1.7-1.amzn2023.0.1
                  @amazonlinux
php8.1-fpm.aarch64                                             8.1.7-1.amzn2023.0.1
                  @amazonlinux
php8.1-gd.aarch64                                              8.1.7-1.amzn2023.0.1
                  @amazonlinux
```

使用以下命令在 Amazon Linux AMI 上安装特定版本的 PHP 图形绘图库（例如 php 8.1 版）：

```
[ec2-user ~]$ sudo dnf install -y php8.1-gd
```

修复 Apache Web 服务器的文件权限

WordPress 中的某些可用功能要求具有对 Apache 文档根目录的写入权限 (例如通过“Administration (管理)”屏幕上传媒体)。如果您尚未进行此操作，请应用以下组成员关系和权限 (在 LAMP Web 服务器教程 (p. 15)中有更为详细的描述)。

1. 将 /var/www 及其内容的文件所有权授予 apache 用户。

   ```
   [ec2-user ~]$ sudo chown -R apache /var/www
   ```

2. 将 /var/www 及其内容的组所有权授予 apache 组。

   ```
   [ec2-user ~]$ sudo chgrp -R apache /var/www
   ```

3. 更改 /var/www 及其子目录的目录权限，以添加组写入权限及设置未来子目录上的组 ID。

   ```
   [ec2-user ~]$ sudo chmod 2775 /var/www
   [ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
   ```

4. 递归地更改 /var/www 及其子目录的文件权限。

   ```
   [ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
   ```

Note

如果您还打算将 WordPress 用作 FTP 服务器，则需要在这里将 Group（组）设置为更宽松的值。请查看建议的 steps and security settings in WordPress（WordPress 中的步骤和安全设置）来完成这一操作。

5. 重启 Apache Web 服务器，让新组和权限生效。
   - Amazon Linux 2023

```
[ec2-user ~]$ sudo systemctl restart httpd
```

   -

使用 Amazon Linux 2023 运行 WordPress 安装脚本

您已准备好安装 WordPress。您使用的命令取决于操作系统。此过程中的命令适用于 Amazon Linux 2023。在此步骤之后的步骤中使用 Amazon Linux 2023 AMI。

1. 使用 systemctl 命令确保 `httpd` 和数据库服务在每次系统启动时启动。

```
[ec2-user ~]$ sudo systemctl enable httpd && sudo systemctl enable mariadb
```

2. 验证数据库服务器是否正在运行。

```
[ec2-user ~]$ sudo systemctl status mariadb
```

   如果数据库服务未运行，请启动。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

3. 验证您的 Apache Web 服务器 (`httpd`) 正在运行。

```
[ec2-user ~]$ sudo systemctl status httpd
```

   如果 `httpd` 服务未运行，请启动。

```
[ec2-user ~]$ sudo systemctl start httpd
```

4. 在 Web 浏览器中，键入您 WordPress 博客的 URL（您实例的公有 DNS 地址，或者该地址后跟 `blog` 文件夹）。您应该可以看到 WordPress 安装脚本。提供 WordPress 安装所需的信息。选择安装 WordPress 完成安装。有关更多信息，请参阅 WordPress 网站上的步骤 5：运行安装脚本。

使用 Amazon Linux 2023 AMI 运行 WordPress 安装脚本

1. 使用 chkconfig 命令确保 `httpd` 和数据库服务在每次系统启动时启动。

```
[ec2-user ~]$ sudo chkconfig httpd on && sudo chkconfig mysqld on
```

2. 验证数据库服务器是否正在运行。

```
[ec2-user ~]$ sudo service mysqld status
```

   如果数据库服务未运行，请启动。

```
[ec2-user ~]$ sudo service mysqld start
```

3. 验证您的 Apache Web 服务器 (httpd) 正在运行。

```
[ec2-user ~]$ sudo service httpd status
```

如果 httpd 服务未运行，请启动。

```
[ec2-user ~]$ sudo service httpd start
```

4. 在 Web 浏览器中，键入您 WordPress 博客的 URL（您实例的公有 DNS 地址，或者该地址后跟 blog 文件夹）。您应该可以看到 WordPress 安装脚本。提供 WordPress 安装所需的信息。选择安装 WordPress 完成安装。有关更多信息，请参阅 WordPress 网站上的步骤 5：运行安装脚本。

后续步骤

在测试您的 WordPress 博客后，请考虑更新其配置。

使用自定义域名

如果您有一个与您的 EC2 实例的 EIP 地址关联的域名，则可将您的博客配置为使用该域名而不是 EC2 公有 DNS 地址。有关更多信息，请参阅 WordPress 网站上的更改网站 URL。

配置您的博客

您可以将您的博客配置为使用不同的主题和插件，从而向您的读者提供更具个性化的体验。但是，有时安装过程可能事与愿违，从而导致您丢失您的整个博客。强烈建议您在尝试安装任何主题或插件之前，为您的实例创建一个备份 Amazon Machine Image (AMI)，以便在安装过程中出现任何问题时，您还可以还原您的博客。有关更多信息，请参阅创建您自己的 AMI (p. 102)。

增加容量

如果您的 WordPress 博客变得受关注并且您需要更多计算能力或存储，请考虑以下步骤：

- 对实例扩展存储空间。有关更多信息，请参阅Amazon EBS 弹性卷 (p. 1493)。
- 将您的 MySQL 数据库移动到 Amazon RDS 以利用服务的轻松扩展功能。

提高互联网流量的网络性能

如果希望您的博客吸引世界各地用户的流量，请考虑 Amazon Global Accelerator。Global Accelerator 通过改善用户客户端设备与 Amazon 上运行的 WordPress 应用程序之间的互联网流量性能，帮助您降低延迟。Global Accelerator 使用 Amazon 全球网络将流量定向到距离客户端最近的 Amazon 区域中正常运行的应用程序终端节点。

了解有关 WordPress 的更多信息

有关 WordPress 的信息，请参阅 http://codex.wordpress.org/ 上的 WordPress Codex 帮助文档。有关对安装进行故障排除的更多信息，请转至 https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems。有关如何使您的 WordPress 博客更安全的信息，请转至 https://wordpress.org/support/article/hardening-wordpress/。有关如何使您的 WordPress 博客保持最新的信息，请转至 https://wordpress.org/support/article/updating-wordpress/。

帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪

已使用您的 EC2 实例的公有 DNS 地址自动配置您的 WordPress 安装。如果您停止并重启实例，公有 DNS 地址将发生更改 (除非它与弹性 IP 地址相关联)，并且您的博客将不会再运行，因为您的博客引用了不再存在

的地址 (或已分配给另一个 EC2 实例的地址) 上的资源。https://wordpress.org/support/article/changing-the-site-url/ 中概括了有关该问题的更多详细说明和几个可能的解决方案。

如果您的 WordPress 安装发生了此问题，您可以使用以下过程恢复您的博客，该过程使用了适用于 WordPress 的 wp-cli 命令行界面。

使用 wp-cli 更改您的 WordPress 站点 URL

1. 使用 SSH 连接到您的 EC2 实例。
2. 请记下您的实例的旧站点 URL 和新站点 URL。安装了 WordPress 之后，旧站点 URL 可能是您的 EC2 实例的公有 DNS 名称。新站点 URL 是您的 EC2 实例的当前公有 DNS 名称。如果您不确定旧站点 URL 是什么，则可通过以下命令使用 curl 来查找它。

   ```
   [ec2-user ~]$ curl localhost | grep wp-content
   ```

   您应该会在输出中看到对您的旧公有 DNS 名称的引用，如下所示 (旧站点 URL 用红色表示)：

   ```
   <script type='text/javascript' src='http://ec2-52-8-139-223.us-
   west-1.compute.amazonaws.com/wp-content/themes/twentyfifteen/js/functions.js?
   ver=20150330'></script>
   ```

3. 使用以下命令下载 wp-cli。

   ```
   [ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-
   cli.phar
   ```

4. 使用以下命令在 WordPress 安装中搜索并替换旧站点 URL。替换您的 EC2 实例的旧站点 URL 和新站点 URL 和到您的 WordPress 安装的路径 (通常为 `/var/www/html` 或 `/var/www/html/blog`)。

   ```
   [ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/
   path/to/wordpress/installation --skip-columns=guid
   ```

5. 在 Web 浏览器中，输入您的 WordPress 博客的新站点 URL 以验证站点是否再次正常运行。否则，请参阅 https://wordpress.org/support/article/changing-the-site-url/ 和 https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems 以了解更多信息。

教程：在上托管 WordPress 博客 Amazon Linux 2

以下步骤将帮助您在 Amazon Linux 2 实例上安装、配置和保护 WordPress 博客。本教程是很好的 Amazon EC2 入门教程，因为您可以完全控制托管您 WordPress 博客的 Web 服务器，这对传统的托管服务来说并不是一个典型的方案。

您负责更新软件包并为您的服务器维护安全补丁。对于不需要与 Web 服务器配置直接交互的更自动化 WordPress 安装来说，Amazon CloudFormation 服务还会提供可让您快速入门的 WordPress 模板。有关更多信息，请参阅Amazon CloudFormation 用户指南中的入门。如果您更喜欢将您的 WordPress 博客托管在 Windows 实例上，请参阅 Amazon EC2 Windows 实例用户指南中的在您的 Amazon EC2 Windows 实例上部署 WordPress 博客。如果您需要带分离数据库的高可用性解决方案，请参阅Amazon Elastic Beanstalk 开发人员指南中的部署高可用性 WordPress 网站。

> **Important**
>
> 这些过程适用于 Amazon Linux 2。有关其他发布版本的更多信息，请参阅其具体文档。本教程中的很多步骤对 Ubuntu 实例并不适用。有关在 Ubuntu 实例上安装 WordPress 的帮助，请参阅 Ubuntu 文档中的 WordPress。您还可以使用 CodeDeploy 在 Amazon Linux、macOS 或 Unix 系统上完成此任务。

主题

- 先决条件 (p. 94)
- 安装 WordPress (p. 94)
- 后续步骤 (p. 99)
- 帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪 (p. 100)

先决条件

此教程假设您已遵照教程：在 Amazon Linux AMI 上安装 LAMP Web 服务器 (p. 33)（适用于 Amazon Linux 2 的 教程：在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)）中的所有步骤启动了一个 Amazon Linux 2 实例，其中包含支持 PHP 和数据库（MySQL 或 MariaDB）的功能正常的 Web 服务器。本教程还介绍了配置安全组以允许 HTTP 和 HTTPS 流量的步骤，以及用于确保为 Web 服务器正确设置文件权限的几个步骤。有关添加规则到您安全组的信息，请参阅 向安全组添加规则 (p. 1311)。

强烈建议您将弹性 IP 地址 (EIP) 与您正用于托管 WordPress 博客的实例关联。这将防止您的实例的公有 DNS 地址更改和中断您的安装。如果您有一个域名且打算将其用于您的博客，则可更新该域名的 DNS 记录，使其指向您的 EIP 地址 (如需帮助，请联系您的域名注册商)。您可以免费将一个 EIP 地址与正在运行的实例相关联。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

如果您的博客还没有域名，则可使用 Route 53 注册一个域名并将您的实例的 EIP 地址与您的域名相关联。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的使用 Amazon Route 53 注册域名。

安装 WordPress

选项：使用 Automation 完成本教程

要使用 Amazon Systems Manager Automation 而不是以下任务完成本教程，请运行 Automation 文档。

连接到您的实例，然后下载 WordPress 安装软件包。

下载并解压 WordPress 安装包

1. 使用 wget 命令下载最新的 WordPress 安装包。以下命令始终会下载最新版本。

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

2. 解压并解档安装包。安装文件夹解压到名为 `wordpress` 的文件夹。

```
[ec2-user ~]$ tar -xzf latest.tar.gz
```

为安装 WordPress 创建数据库用户和数据库

安装 WordPress 需要存储信息，例如数据库中的博客文章和用户评论。此过程帮助您创建自己的博客数据库，并创建一个有权读取该数据库的信息并将信息保存到该数据库的用户。

1. 启动数据库服务器。
   -
```
[ec2-user ~]$ sudo systemctl start mariadb
```
2. 以 `root` 用户身份登录数据库服务器。在系统提示时输入您的数据库 `root` 密码，它可能与您的 `root` 系统密码不同；如果您尚未给您的数据库服务器加密，它甚至可能是空的。

   如果您尚未给您的数据库服务器加密，则必须执行这项操作。有关更多信息，请参阅 保护 MariaDB 服务器 (p. 28)（Amazon Linux 2）。

```
[ec2-user ~]$ mysql -u root -p
```

3. 为您的 MySQL 数据库创建用户和密码。安装 WordPress 的过程将使用这些值与您的 MySQL 数据库通信。输入以下命令，以替换唯一的用户名和密码。

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

确保为您的用户创建强密码。请勿在您的密码中使用单引号字符 (')，因为这将中断前面的命令。有关创建安全密码的更多信息，请转至 http://www.pctools.com/guides/password/。请勿重复使用现有密码，并确保将密码保存在安全的位置。

4. 创建数据库。为数据库提供一个有意义的描述性名称，例如 wordpress-db。

   Note

   以下命令中数据库名称两边的标点符号称为反引号。在标准键盘上，反引号 (`) 键通常位于 Tab 键的上方。并不总是需要反引号，但是它们允许您在数据库名称中使用其他的非法字符，例如连字符。

```
CREATE DATABASE `wordpress-db`;
```

5. 对您之前创建的 WordPress 用户授予您数据库的完全访问权限。

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. 刷新数据库权限以接受您的所有更改。

```
FLUSH PRIVILEGES;
```

7. 退出 mysql 客户端。

```
exit
```

创建和编辑 wp-config.php 文件

WordPress 安装文件夹包含名为 wp-config-sample.php 的示例配置文件。在本步骤中，您将复制此文件并进行编辑以适合您的具体配置。

1. 将 wp-config-sample.php 文件复制为一个名为 wp-config.php 的文件。这样做会创建新的配置文件并将原先的示例配置文件原样保留作为备份。

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. 用您喜欢的文本编辑器（例如 nano 或 vim）编辑 wp-config.php 文件并输入适用于您的安装的值。如果没有常用的文本编辑器，nano 比较适合初学者使用。

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

   a. 查找定义 DB_NAME 的行并将 database_name_here 更改为您在 Step 4 (p. 95) 的 为安装 WordPress 创建数据库用户和数据库 (p. 94) 中创建的数据库名称。

```
define('DB_NAME', 'wordpress-db');
```

   b. 查找定义 DB_USER 的行并将 username_here 更改为您在 Step 3 (p. 95) 的 为安装 WordPress 创建数据库用户和数据库 (p. 94) 中创建的数据库用户。

```
define('DB_USER', 'wordpress-user');
```

c. 查找定义 DB_PASSWORD 的行并将 password_here 更改为您在 Step 3 (p. 95) 的 为安装 WordPress 创建数据库用户和数据库 (p. 94) 中创建的强密码。

```
define('DB_PASSWORD', 'your_strong_password');
```

d. 查找名为 Authentication Unique Keys and Salts 的一节。这些 KEY 和 SALT 值为 WordPress 用户存储在其本地计算机上的浏览器 Cookie 提供了加密层。总而言之，添加长的随机值将使您的站点更安全。访问 https://api.wordpress.org/secret-key/1.1/salt/ 随机生成一组密钥值，您可以将这些密钥值复制并粘贴到 wp-config.php 文件中。要粘贴文本到 PuTTY 终端，请将光标放在您要粘贴文本的地方，并在 PuTTY 终端内部右键单击鼠标。

有关安全密钥的更多信息，请转至 https://wordpress.org/support/article/editing-wp-config-php/#security-keys。

Note

以下值仅用作示例；请勿使用以下值进行安装。

```
define('AUTH_KEY',         ' #U$$+[RXN8:b^-L 0(WU_+ c+WFkI~c]o]-bHw+)/
Aj[wTwSiZ<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY',  'Zsz._P=l/|y.Lq)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?6OP
$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$DpB4Hj[JK:?{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%_-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
define('LOGGED_IN_SALT',   ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|e(76miC
+&W&+^0P/');
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

e. 保存 文件并退出文本编辑器。

将 WordPress 文件安装到 Apache 文档根目录下

- 现在，您已解压了安装文件夹、创建了 MySQL 数据库和用户并自定义了 WordPress 配置文件，那么也就准备好将您的安装文件复制到 Web 服务器文档根目录，以便可以运行安装脚本完成安装。这些文件的位置取决于您是希望 WordPress 博客位于 Web 服务器的实际根目录 (例如，*my.public.dns.amazonaws.com*) 还是位于根目录下的某个子目录或文件夹 (例如，*my.public.dns.amazonaws.com/blog*) 中。
  - 如果希望 WordPress 在文档根目录下运行，请复制 wordpress 安装目录的内容 (但不包括目录本身)，如下所示：

    ```
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/
    ```

  - 如果希望 WordPress 在文档根目录下的其他目录中运行，请先创建该目录，然后将文件复制到其中。在此示例中，WordPress 将从目录 blog 运行：

    ```
    [ec2-user ~]$ mkdir /var/www/html/blog
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
    ```

Important

出于安全原因，如果您不打算立即进入到下一个过程，请立即停止 Apache Web 服务器 (httpd)。将安装文件移动到 Apache 文档根目录下后，WordPress 安装脚本将不受保护，如果 Apache Web 服务器运行，攻击者可能会获得访问您博客的权限。要终止 Apache Web 服务器，请输入命令 sudo systemctl stop httpd。如果您即将继续到下一个步骤，则不需要终止 Apache Web 服务器。

允许 WordPress 使用 permalink

WordPress permalink 需要使用 Apache `.htaccess` 文件才能正常工作，但默认情况下这些文件在 Amazon Linux 上处于禁用状态。使用此过程可允许 Apache 文档根目录中的所有覆盖。

1. 使用您常用的文本编辑器（如 `httpd.conf` 或 nano）打开 vim 文件。如果没有常用的文本编辑器，nano 比较适合初学者使用。

```
[ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
```

2. 找到以 `<Directory "/var/www/html">` 开头的部分。

```
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks

    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None

    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>
```

3. 在以上部分中将 `AllowOverride None` 行改为读取 `AllowOverride All`。

   Note

   此文件中有多个 `AllowOverride` 行；请确保更改 `<Directory "/var/www/html">` 部分中的行。

```
AllowOverride All
```

4. 保存 文件并退出文本编辑器。

在 Amazon Linux 2 上安装 PHP 图形绘图库

PHP 的 GD 库允许您修改图像。如果您需要裁剪博客的标题图像，请安装此库。您安装的 phpMyAdmin 版本可能需要此库的特定最低版本（例如 7.2 版）。

使用以下命令在 Amazon Linux 2 上安装 PHP 图形绘图库。例如，如果您在安装 LAMP 堆栈的过程中从 amazon-linux-extras 安装了 php7.2，则此命令将安装 7.2 版的 PHP 图形绘图库。

```
[ec2-user ~]$ sudo yum install php-gd
```

要验证最新版本，请使用以下命令：

```
[ec2-user ~]$ php80-php-gd.x86_64                    8.0.17-1.el7.remi
 remi
```

下面是示例输出：

```
php-gd.x86_64                  7.2.30-1.amzn2           @amzn2extra-php7.2
```

修复 Apache Web 服务器的文件权限

WordPress 中的某些可用功能要求具有对 Apache 文档根目录的写入权限 (例如通过“Administration (管理)”屏幕上传媒体)。如果您尚未进行此操作，请应用以下组成员关系和权限 (在 LAMP Web 服务器教程 (p. 33)中有更为详细的描述)。

1. 将 /var/www 及其内容的文件所有权授予 apache 用户。

   ```
   [ec2-user ~]$ sudo chown -R apache /var/www
   ```

2. 将 /var/www 及其内容的组所有权授予 apache 组。

   ```
   [ec2-user ~]$ sudo chgrp -R apache /var/www
   ```

3. 更改 /var/www 及其子目录的目录权限，以添加组写入权限及设置未来子目录上的组 ID。

   ```
   [ec2-user ~]$ sudo chmod 2775 /var/www
   [ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
   ```

4. 递归地更改 /var/www 及其子目录的文件权限。

   ```
   [ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
   ```

   Note

   如果您还打算将 WordPress 用作 FTP 服务器，则需要在这里将 Group（组）设置为更宽松的值。请查看建议的 steps and security settings in WordPress（WordPress 中的步骤和安全设置）来完成这一操作。

5. 重启 Apache Web 服务器，让新组和权限生效。

   - ```
     [ec2-user ~]$ sudo systemctl restart httpd
     ```

使用 Amazon Linux 2 运行 WordPress 安装脚本

您已准备好安装 WordPress。您使用的命令取决于操作系统。此过程中的命令适用于 Amazon Linux 2。

1. 使用 systemctl 命令确保 httpd 和数据库服务在每次系统启动时启动。
     ```

```
[ec2-user ~]$ sudo systemctl enable httpd && sudo systemctl enable mariadb
```

2. 验证数据库服务器是否正在运行。

```
[ec2-user ~]$ sudo systemctl status mariadb
```

如果数据库服务未运行，请启动。

```
[ec2-user ~]$ sudo systemctl start mariadb
```

3. 验证您的 Apache Web 服务器 (httpd) 正在运行。

```
[ec2-user ~]$ sudo systemctl status httpd
```

如果 httpd 服务未运行，请启动。

```
[ec2-user ~]$ sudo systemctl start httpd
```

4. 在 Web 浏览器中，键入您 WordPress 博客的 URL（您实例的公有 DNS 地址，或者该地址后跟 blog 文件夹）。您应该可以看到 WordPress 安装脚本。提供 WordPress 安装所需的信息。选择安装 WordPress 完成安装。有关更多信息，请参阅 WordPress 网站上的步骤 5：运行安装脚本。

后续步骤

在测试您的 WordPress 博客后，请考虑更新其配置。

使用自定义域名

如果您有一个与您的 EC2 实例的 EIP 地址关联的域名，则可将您的博客配置为使用该域名而不是 EC2 公有 DNS 地址。有关更多信息，请参阅 WordPress 网站上的更改网站 URL。

配置您的博客

您可以将您的博客配置为使用不同的主题和插件，从而向您的读者提供更具个性化的体验。但是，有时安装过程可能事与愿违，从而导致您丢失您的整个博客。强烈建议您在尝试安装任何主题或插件之前，为您的实例创建一个备份 Amazon Machine Image (AMI)，以便在安装过程中出现任何问题时，您还可以还原您的博客。有关更多信息，请参阅创建您自己的 AMI (p. 102)。

增加容量

如果您的 WordPress 博客变得受关注并且您需要更多计算能力或存储，请考虑以下步骤：

- 对实例扩展存储空间。有关更多信息，请参阅Amazon EBS 弹性卷 (p. 1493)。
- 将您的 MySQL 数据库移动到 Amazon RDS 以利用服务的轻松扩展功能。

提高互联网流量的网络性能

如果希望您的博客吸引世界各地用户的流量，请考虑 Amazon Global Accelerator。Global Accelerator 通过改善用户客户端设备与 Amazon 上运行的 WordPress 应用程序之间的互联网流量性能，帮助您降低延迟。Global Accelerator 使用 Amazon 全球网络将流量定向到距离客户端最近的 Amazon 区域中正常运行的应用程序终端节点。

了解有关 WordPress 的更多信息

有关 WordPress 的信息，请参阅 http://codex.wordpress.org/ 上的 WordPress Codex 帮助文档。有关对安装进行故障排除的更多信息，请转至 https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems。有关如何使您的 WordPress 博客更安全的信息，请转至 https://wordpress.org/support/article/hardening-wordpress/。有关如何使您的 WordPress 博客保持最新的信息，请转至 https://wordpress.org/support/article/updating-wordpress/。

帮助！我的公有 DNS 名称发生更改导致我的博客瘫痪

已使用您的 EC2 实例的公有 DNS 地址自动配置您的 WordPress 安装。如果您停止并重启实例，公有 DNS 地址将发生更改 (除非它与弹性 IP 地址相关联)，并且您的博客将不会再运行，因为您的博客引用了不再存在的地址 (或已分配给另一个 EC2 实例的地址) 上的资源。https://wordpress.org/support/article/changing-the-site-url/ 中概括了有关该问题的更多详细说明和几个可能的解决方案。

如果您的 WordPress 安装发生了此问题，您可以使用以下过程恢复您的博客，该过程使用了适用于 WordPress 的 wp-cli 命令行界面。

使用 wp-cli 更改您的 WordPress 站点 URL

1. 使用 SSH 连接到您的 EC2 实例。
2. 请记下您的实例的旧站点 URL 和新站点 URL。安装了 WordPress 之后，旧站点 URL 可能是您的 EC2 实例的公有 DNS 名称。新站点 URL 是您的 EC2 实例的当前公有 DNS 名称。如果您不确定旧站点 URL 是什么，则可通过以下命令使用 curl 来查找它。

   ```
   [ec2-user ~]$ curl localhost | grep wp-content
   ```

   您应该会在输出中看到对您的旧公有 DNS 名称的引用，如下所示 (旧站点 URL 用红色表示)：

   ```
   <script type='text/javascript' src='http://ec2-52-8-139-223.us-
   west-1.compute.amazonaws.com/wp-content/themes/twentyfifteen/js/functions.js?
   ver=20150330'></script>
   ```

3. 使用以下命令下载 wp-cli。

   ```
   [ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-
   cli.phar
   ```

4. 使用以下命令在 WordPress 安装中搜索并替换旧站点 URL。替换您的 EC2 实例的旧站点 URL 和新站点 URL 和到您的 WordPress 安装的路径 (通常为 /var/www/html 或 /var/www/html/blog)。

   ```
   [ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/
   path/to/wordpress/installation --skip-columns=guid
   ```

5. 在 Web 浏览器中，输入您的 WordPress 博客的新站点 URL 以验证站点是否再次正常运行。否则，请参阅 https://wordpress.org/support/article/changing-the-site-url/ 和 https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems 以了解更多信息。

Amazon Machine Images (AMI)

Amazon Machine Image（AMI）是由 Amazon 提供的支持和维护映像，后者提供启动实例所需的信息。在启动实例时，您必须指定 (AMI)。在需要具有相同配置的多个实例时，您可以从单个 AMI 启动多个实例。在需要不同的配置的实例时，您可以使用其他 AMI 启动实例。

AMI 包括以下内容：

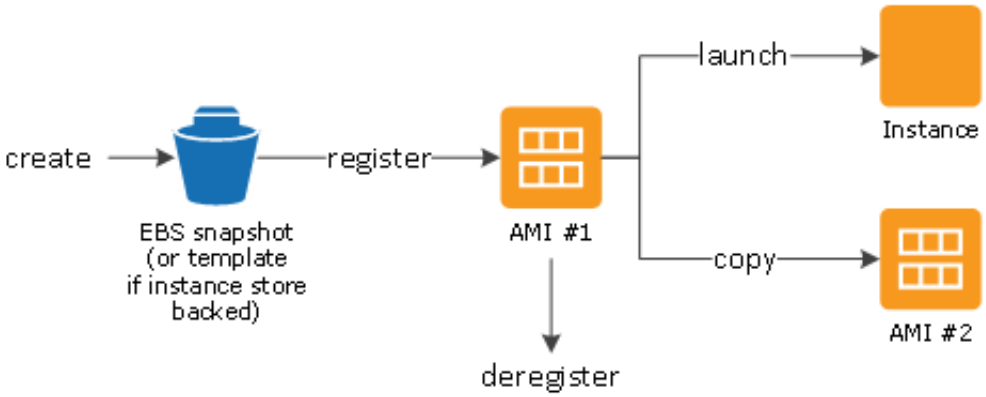
- 一个或多个 Amazon Elastic Block Store (Amazon EBS) 快照；对于由实例存储支持的 AMI，包括一个用于实例（例如，操作系统、应用程序服务器和应用程序）根卷的模板。
- 控制可以使用 AMI 启动实例的 Amazon 账户的启动许可。
- 数据块设备映射，指定在实例启动时要附加到实例的卷。

Amazon Machine Image（AMI）主题

- 使用 AMI (p. 101)
- 创建您自己的 AMI (p. 102)
- 购买、共享和出售 AMI (p. 102)
- 注销您的 AMI (p. 102)
- Amazon Linux 2 和 Amazon Linux AMI (p. 103)
- AMI 类型 (p. 103)
- Linux AMI 虚拟化类型 (p. 106)
- 启动模式 (p. 107)
- 查找 Linux AMI (p. 116)
- 共享 AMI (p. 121)
- 付费 AMI (p. 133)
- AMI 周期 (p. 137)
- 将加密与 EBS 支持的 AMI 结合使用 (p. 196)
- 使用 Amazon EventBridge 监控 AMI 事件 (p. 200)
- 了解 AMI 账单信息 (p. 204)
- Amazon Linux (p. 208)
- 用户提供的内核 (p. 226)
- 配置 Amazon Linux 2 MATE 桌面连接 (p. 231)
- AMI 限额 (p. 233)

使用 AMI

下图总结了 AMI 生命周期。创建并注册一个 AMI 之后，您可以将其用于启动新实例。(如果 AMI 拥有者向您授予启动许可，则您也可以从 AMI 启动实例。) 您可以在同一 Amazon 区域中复制 AMI，也可以将 AMI 复制到其他 Amazon 区域。不再需要某个 AMI 时，可以将其注销。



您可以搜索符合您的实例条件的 AMI。您可以搜索 Amazon 提供的 AMI 或社区提供的 AMI。有关更多信息，请参阅AMI 类型 (p. 103)和查找 Linux AMI (p. 116)。

从 AMI 启动实例后，您可以连接到该实例。连接到某个实例之后，您可以像使用任何其他服务器那样使用该实例。有关启动、连接和使用实例的信息，请参阅 教程：Amazon EC2 Linux 实例入门 (p. 9)。

创建您自己的 AMI

您可以从现有的 AMI 中启动实例、自定义该实例（例如，在此实例上安装软件 (p. 703)），然后将此更新后的配置另存为自定义 AMI。从该新自定义 AMI 启动的实例包括您在创建 AMI 时设置的自定义项。

实例的根存储设备确定创建 AMI 所遵循的过程。实例的根卷是 Amazon Elastic Block Store (Amazon EBS) 卷或实例存储卷。有关根设备卷的更多信息，请参阅Amazon EC2 实例根设备卷 (p. 1608)。

- 要创建一个 Amazon EBS-backed AMI，请参阅创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。
- 要创建由实例存储支持的 AMI，请参阅创建由实例存储支持的 Linux AMI (p. 142)。

您可以为 AMI 分配自定义标签，以帮助您对 AMI 进行分类和管理。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

购买、共享和出售 AMI

创建 AMI 之后，您可以将其设为私有，这样只有您才能使用它，也可以与指定的 Amazon 账户列表进行共享。您还可以选择公开您的自定义 AMI，以供社区使用。如果遵循一些简单的指导，为公共使用构建安全、可靠、可用的 AMI 的过程可以很简单。有关如何创建和使用共享 AMI 的信息，请参阅共享 AMI (p. 121)。

您可以从第三方购买 AMI，包括具有 Red Hat 等组织的服务合同的 AMI。您还可以创建 AMI 并将其出售给其他 Amazon EC2 用户。有关购买或出售 AMI 的更多信息，请参阅付费 AMI (p. 133)。

注销您的 AMI

使用完 AMI 之后，可以注销它。注销 AMI 之后，便无法将其用于启动新实例。从 AMI 启动的现有实例不受影响。有关更多信息，请参阅注销您的 AMI (p. 188)。

Amazon Linux 2 和 Amazon Linux AMI

Amazon Linux 2 和 Amazon Linux AMI 是 Amazon 提供、支持和维护的 Linux 映像。以下是一些 Amazon Linux 2 和 Amazon Linux AMI 功能：

- 稳定、安全和高性能的执行环境，适用于 Amazon EC2 上运行的应用程序。
- 对于 Amazon EC2 用户没有额外费用。
- 对多个版本的 MySQL、PostgreSQL、Python、Ruby、Tomcat 及许多常见软件包的存储库访问权限。
- 定期更新以包括最新组件，这些更新也可在 yum 存储库中使用，适用于安装在运行中的实例上。
- 包括可与 Amazon 服务轻松集成的软件包，如 Amazon CLI、Amazon EC2 API 和 AMI 工具、适用于 Python 的 Boto 库以及 Elastic Load Balancing 工具。

有关更多信息，请参阅Amazon Linux (p. 208)。

AMI 类型

可以基于以下特性选择要使用的 AMI：

- 区域 (请参阅区域和可用区 (p. 1040))
- 操作系统
- 架构 (32 位或 64 位)
- 启动许可 (p. 103)
- 根设备存储 (p. 103)

启动许可

AMI 的拥有者通过指定启动许可来确定其可用性。启动许可分为以下类别。

启动权限	描述
公有	拥有者向所有 Amazon 账户授予启动许可。
显式	拥有者向特定Amazon账户、企业或企业部门 (OU) 授予启动许可。
隐式	拥有者拥有 AMI 的隐式启动许可。

Amazon 和 Amazon EC2 社区提供了大量的公用 AMI。有关更多信息，请参阅共享 AMI (p. 121)。开发人员可以为其 AMI 收费。有关更多信息，请参阅付费 AMI (p. 133)。

根设备存储

所有 AMI 均可归类为由 Amazon EBS 支持或由实例存储支持。

- Amazon EBS-backed AMI – 从 AMI 启动的实例的根设备是从 Amazon EBS 快照创建的 Amazon Elastic Block Store (Amazon EBS) 卷。
- Amazon 实例存储支持的 AMI – 从 AMI 启动的实例的根设备是根据一个存储在 Amazon S3 中的模板创建而来的实例存储卷。

有关更多信息，请参阅Amazon EC2 实例根设备卷 (p. 1608)。

下表总结了使用两种类型的 AMI 时的重要区别。

特征	Amazon EBS-backed AMI	由 Amazon 实例存储支持的 AMI
实例的启动时间	通常不到 1 分钟	通常不到 5 分钟
根设备的大小限制	64 TiB**	10 GiB
根设备卷	EBS 卷	实例存储卷
数据持久性	默认情况下，实例终止时将删除根卷。* 默认情况下，在实例终止后，任何其他 EBS 卷上的数据仍然存在。	任意实例存储卷上的数据仅在实例的生命周期内保留。
修改	实例停止后，实例类型、内核、RAM 磁盘和用户数据仍可更改。	实例存在期间，实例属性是稳定不变的。
收费	您需要为实例使用、EBS 卷使用以及将 AMI 存储为 EBS 快照付费。	您需要为实例使用以及在 Amazon S3 中存储 AMI 付费。
AMI 创建/捆绑	使用单一命令/调用	需要安装和使用 AMI 工具
停止状态	可以处于停止状态。即使实例停止未运行，根卷也会保留在 Amazon EBS 中	不可置于停止状态；实例正在运行或已终止

* 默认情况下，EBS 根卷的 `DeleteOnTermination` 标志设置为 `true`。有关如何更改此标志以便卷在终止之后保留的信息，请参阅将根卷更改为保留 (p. 1611)。

** 仅支持 `io2` EBS Block Express。有关更多信息，请参阅io2 Block Express 卷 (p. 1334)。

确定 AMI 的根设备类型

New console

使用控制台确定 AMI 的根设备类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMI，然后选择 AMI。
3. 在 Details（详细信息）选项卡中检查 Root Device Type（根设备类型）的值，如下所示：
   - `ebs` – 这是由 EBS 支持的 AMI。
   - `instance store` – 这是由实例存储支持的 AMI。

Old console

使用控制台确定 AMI 的根设备类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMI，然后选择 AMI。
3. 在 Details（详细信息）选项卡中检查 Root Device Type（根设备类型）的值，如下所示：
   - `ebs` – 这是由 EBS 支持的 AMI。
   - `instance store` – 这是由实例存储支持的 AMI。

使用命令行确定 AMI 的根设备类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-images (Amazon CLI)
- Get-EC2Image (Amazon Tools for Windows PowerShell)

停止状态

您可以停止具有根设备的 EBS 卷的实例，但不能停止具有根设备实例存储卷的实例。

停止操作会导致实例停止运行 (它的状态会由 `running` 变成 `stopping` 再到 `stopped`)。停止的实例保留在 Amazon EBS 中，这样就可重新启动。停止与终止不同；您无法重新启动一个已终止的实例。因为具有实例存储卷作为根设备的实例无法停止，所以它们要么正在运行要么已终止。有关实例停止可能会发生情况及您可以执行哪些操作的更多信息，请参阅 停止和启动您的实例 (p. 610)。

默认数据存储和持久性

具有实例存储卷作为根设备的实例自动具有可用的实例存储（根卷包含根分区，并且您可以存储其它数据）。您可以通过附加一个或多个 EBS 卷向您的实例添加持久性存储。如果实例出故障或终止，实例存储卷上的所有数据均会删除。有关更多信息，请参阅实例存储生命周期 (p. 1580)。

具有 Amazon EBS 作为根设备的实例自动附加 EBS 卷。该卷像其他卷一样显示在您的卷列表中。对于大多数实例类型，具有 EBS 卷作为根设备的实例在默认情况下不具有实例存储卷。您可以使用块储存设备映射添加实例存储卷或连接 EBS 卷。有关更多信息，请参阅块设备映射 (p. 1615)。

启动时间

从 Amazon EBS-backed AMI 启动的实例比从实例存储支持的 AMI 启动的实例启动得快。当您从实例存储支持的 AMI 启动实例时，必须先从 Amazon S3 中检索所有部件才能使用该实例。使用 Amazon EBS-backed AMI 时，仅需从快照中检索启动实例所需的分段，然后即可使用该实例。但是，使用 EBS 卷作为根设备的实例在从快照中检索剩余分段并加载到卷中的这一小段时间内会运行地较为缓慢。当您停止和重新启动实例时，实例可快速启动，因为实例状态已存储在 EBS 卷中。

AMI 创建

要创建由实例存储支持的 Linux AMI，您必须使用 Amazon EC2 AMI 工具在您的实例上创建来自实例的 AMI。

AMI 创建对于由 Amazon EBS 支持的 AMI 来说要容易得多。`CreateImage` API 操作创建 Amazon EBS-backed AMI 并为其注册。Amazon Web Services Management Console中还有一个按钮能让您从正在运行的实例中创建 AMI。有关更多信息，请参阅创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。

如何向您收费

如果您使用由实例存储提供支持的 AMI，您需要为实例使用和在 Amazon S3 中存储 AMI 付费。如果您使用由 Amazon EBS 支持的 AMI，您需要为实例使用、EBS 卷的存储和使用、以 EBS 快照形式存储 AMI 付费。

如果您使用由 Amazon EC2 实例存储支持的 AMI，当您每次自定义以及新建一个 AMI 时，所有分段都存储在每个 AMI 的 Amazon S3 中。因此，每个自定义 AMI 的存储占用空间都是 AMI 的完整大小。对于 Amazon EBS-backed AMI，当您每次自定义以及新建 AMI 时，将仅存储更改内容。因此，您之后自定义的 AMI 的存储占用空间比首次自定义的 AMI 要小得多，从而降低 AMI 存储费用。

当由具有 EBS 卷作为根设备的实例停止后，您无需再为实例使用付费；但是，您仍需为卷存储付费。一旦您启动实例时，我们便会收取最低一分钟的使用费用。一分钟之后，我们仅按您使用的秒数收费。例如，如果您运行一个实例 20 秒后停止实例，我们将按一整分钟收取费用。如果您运行一个实例 3 分 40 秒，我们将收

取 3 分 40 秒的使用费用。我们将对您的实例保持运行状态的每秒钟收取费用，最低一分钟，即使实例处于闲置状态并且您没有连接到它也是如此。

Linux AMI 虚拟化类型

Linux Amazon 系统映像使用两种虚拟化类型之一：半虚拟化 (PV) 或硬件虚拟机 (HVM)。半虚拟化和 HVM AMI 之间的主要区别在于它们的启动方式，以及它们能否使用特定硬件扩展 (CPU、网络和存储) 实现更好的性能。

为获得最佳性能，建议您在启动您的实例时使用最新一代的实例类型和 HVM AMI。有关当前一代实例类型的更多信息，请参阅 Amazon EC2 实例类型。如果您正在使用上一代实例类型并且想升级，请参阅升级路径。

下表比较 HVM 和 PV AMI。

	全虚拟化	PV
描述	硬件虚拟机 AMI 配有一组完全虚拟化的硬件，通过执行映像根块储存设备的主启动记录来启动。通过此虚拟化类型可以直接在虚拟机上运行操作系统而不进行任何修改 (如同它在裸机硬件上运行一样)。Amazon EC2 主机系统可模拟向客户机提供的部分或所有底层硬件。	半虚拟化 AMIs 使用名为 PV-GRUB 的特殊启动加载程序启动，该加载程序开始启动周期，然后对映像链式加载 `menu.lst` 文件中指定的内核。半虚拟来宾可以在没有明确支持虚拟化的主机硬件上运行。以往，半虚拟化来宾在许多情况下的性能优于 HVM 来宾，但是由于硬件虚拟机虚拟化的功能增强以及 HVM AMI 可使用半虚拟化驱动程序，情况发生了改变。有关 PV-GRUB 及其在 Amazon EC2 中的使用情况的更多信息，请参阅 用户提供的内核 (p. 226)。
支持硬件扩展	是。与半虚拟化客户机不同，硬件虚拟机客户机可以利用硬件扩展快速访问主机系统上的底层硬件。有关 Amazon EC2 中可用的 CPU 虚拟化扩展的更多信息，请参阅 Intel 网站上的英特尔虚拟化技术。硬件虚拟机 AMI 需要利用增强联网和 GPU 处理。要将指令传递给专用网络和 GPU 设备，操作系统需要能够访问本机硬件平台；HVM 虚拟化提供这种访问。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)和Linux 加速计算实例 (p. 358)。	否，它们无法利用特殊的硬件扩展，例如增强网络或 GPU 处理。
支持的实例类型	当前一代的所有实例类型都支持 HVM AMI。	以下上一代实例类型支持 PV AMI：C1、C3、HS1、M1、M3、M2 和 T1。最新一代实例类型不支持 PV AMI。
支持的区域	所有区域都支持 HVM 实例。	亚太区域（东京）、亚太区域（新加坡）、亚太区域（悉尼）、欧洲（法兰克福）、欧

	全虚拟化	PV
		洲（爱尔兰）、南美洲（圣保罗）、US East (N. Virginia)、美国西部（加利福尼亚北部）和美国西部（俄勒冈）
如何查找	使用控制台或 describe-images 命令验证 AMI 的虚拟化类型是否已设置为 hvm。	使用控制台或 describe-images 命令验证 AMI 的虚拟化类型是否已设置为 paravirtual。

硬件虚拟机上的半虚拟化

以往，半虚拟化客户机在存储和网络操作方面的性能要优于硬件虚拟机客户机，因为它们可以对 I/O 使用特殊驱动程序，从而避免模拟网络和磁盘硬件的开销，而硬件虚拟机客户机必须将这些指令转换为模拟的硬件。现在，半虚拟化驱动程序可用于硬件虚拟机客户机，因此无法移植到半虚拟化环境中运行的操作系统仍可以通过它们获得存储和网络 I/O 方面的性能优势。借助这些硬件虚拟机驱动程序上的半虚拟化，硬件虚拟机客户机可以获得与半虚拟化客户机相同甚至更佳的性能。

启动模式

电脑启动时，它运行的第一个软件负责初始化平台并为操作系统执行特定于平台的操作提供界面。

在 Amazon EC2 中，支持启动模式软件的两种变体包括：统一可扩展固件接口（UEFI）和传统 BIOS。

AMI 上可能的启动模式参数

AMI 可以具有以下任一启动模式参数值：uefi、legacy-bios 或 uefi-preferred。AMI 启动模式参数是可选项。对于不带启动模式参数的 AMI，从这些 AMI 启动的实例将使用实例类型的默认启动模式值。

AMI 启动模式参数的用途

AMI 启动模式参数向 Amazon EC2 发出信号，指明启动实例时要使用哪种启动模式。当启动模式参数设置为 uefi 时，EC2 将尝试在 UEFI 上启动实例。如果操作系统未配置为支持 UEFI，则实例启动可能失败。

UEFI Preferred 启动模式参数

您可以使用 uefi-preferred 启动模式参数创建同时支持 UEFI 和传统 BIOS 的 AMI。当启动模式参数设置为 uefi-preferred 并且实例类型支持 UEFI 时，实例会在 UEFI 上启动。如果实例类型不支持 UEFI，实例会在传统 BIOS 上启动。

> **Warning**
>
> UEFI 安全启动等部分功能仅适用于在 UEFI 上启动的实例。将 uefi-preferred AMI 启动模式参数与不支持 UEFI 的实例类型结合使用时，实例将以传统 BIOS 启动，并禁用 UEFI 相关功能。如果您依赖于 UEFI 相关功能的可用性，请将 AMI 启动模式参数设置为 uefi。

实例类型的默认启动模式

- Graviton 实例类型：UEFI
- Intel 和 AMD 实例类型：传统 BIOS

UEFI 上运行 Intel 和 AMD 实例类型

Most Intel and AMD instance types 可以在 UEFI 和旧式 BIOS 上运行。要使用 UEFI，必须选择启动模式参数设置为 uefi 或 uefi-preferred 的 AMI，而且 AMI 中包含的操作系统必须配置为支持 UEFI。

启动模式主题

- 启动 实例 (p. 108)
- 确定 AMI 的启动模式参数 (p. 110)
- 确定实例类型支持的启动模式 (p. 111)
- 确定实例的启动模式 (p. 111)
- 确定操作系统的启动模式 (p. 112)
- 设置 AMI 的启动模式 (p. 113)
- UEFI 变量 (p. 116)

启动 实例

您可以在 UEFI 或传统 BIOS 启动模式下启动实例。

主题

- 限制 (p. 108)
- 注意事项 (p. 108)
- 在 UEFI 上启动实例的要求 (p. 109)

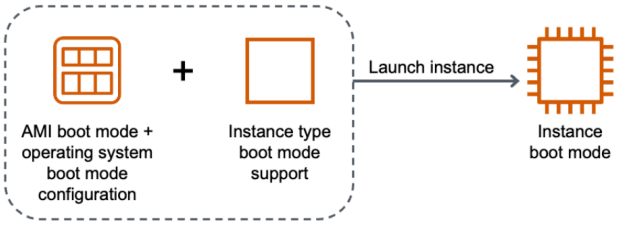
限制

在 Local Zones、Wavelength Zones 中，或者使用 Amazon Outposts 的情况下，不支持 UEFI 启动。

注意事项

启动实例时请注意以下事项：

- 实例的启动模式由 AMI 的配置、其中包含的操作系统和实例类型决定，如下图所示：



下表显示，实例的启动模式（由生成的实例启动模式列表示）由 AMI 的启动模式参数（第 1 列）、AMI 中包含的操作系统的启动模式配置（第 2 列）和实例类型的启动模式支持（第 3 列）共同决定。

AMI 启动模式参数	操作系统启动模式配置	实例类型启动模式支持	生成的实例启动模式
UEFI	UEFI	UEFI	UEFI
传统 BIOS	传统 BIOS	传统 BIOS	传统 BIOS
UEFI Preferred	UEFI	UEFI	UEFI
UEFI Preferred	UEFI	UEFI 和传统 BIOS	UEFI
UEFI Preferred	传统 BIOS	传统 BIOS	传统 BIOS
UEFI Preferred	传统 BIOS	UEFI 和传统 BIOS	传统 BIOS

AMI 启动模式参数	操作系统启动模式配置	实例类型启动模式支持	生成的实例启动模式
未指定启动模式 – ARM	UEFI	UEFI	UEFI
未指定启动模式 – x86	传统 BIOS	UEFI 和传统 BIOS	传统 BIOS

- 默认启动模式：
  - Graviton 实例类型：UEFI
  - Intel 和 AMD 实例类型：传统 BIOS
- 除了传统 BIOS 外，支持 UEFI 的 Intel 和 AMD 实例类型：
  - 所有基于 Amazon Nitro System 构建的实例，下列实例除外：裸机实例、DL1、G4ad、P4、u-3tb1、u-6tb1、u-9tb1、u-12tb1 和 VT1

查看特定区域中支持 UEFI 的可用实例类型

可用的实例类型因 Amazon Web Services 区域 而异。要查看某个区域中支持 UEFI 的可用实例类型，请使用带 `--region` 参数的 describe-instance-types 命令。如果省略 `--region` 参数，则会在请求中使用默认区域。包括 `--filters` 参数以将结果范围限定为支持 UEFI 的实例类型，并包括 `--query` 参数以将输出范围限定为 `InstanceType` 的值。

```
aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --query
 "InstanceTypes[*].[InstanceType]" --output text | sort
```

输出示例

```
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

要查看支持 UEFI 安全启动并在特定区域中保留非易失性变量的可用实例类型

目前，裸机实例不支持 UEFI 安全启动和非易失性变量。使用上述示例所述的 describe-instance-types 命令，但通过包含 `Name=hypervisor,Values=nitro` 筛选条件筛选出裸机实例。

```
aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=hypervisor,Values=nitro --query "InstanceTypes[*].[InstanceType]" --output text |
 sort
```

在 UEFI 上启动实例的要求

要在 UEFI 启动模式下启动实例，必须选择支持 UEFI 的实例类型，然后为 UEFI 配置 AMI 和操作系统，如下所示：

实例类型

启动实例时，必须选择支持 UEFI 的实例类型。有关更多信息，请参阅确定实例类型支持的启动模式 (p. 111)。

AMI

启动实例时，必须选择为 UEFI 配置的 AMI。AMI 必须按如下方式进行配置：

- 操作系统 – AMI 中包含的操作系统必须配置为使用 UEFI；否则，实例启动将失败。有关更多信息，请参阅确定操作系统的启动模式 (p. 112)。
- AMI 启动模式参数 – AMI 的启动模式参数必须设置为 `uefi` 或 `uefi-preferred`。有关更多信息，请参阅确定 AMI 的启动模式参数 (p. 110)。

Amazon 仅为基于 Graviton 的实例类型提供配置为支持的 UEFI 的 Linux AMI。要在其他 UEFI 实例类型上使用 Linux，必须配置 AMI (p. 113)。

有关受支持的 Windows AMI，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的 在 UEFI 上启动实例的要求。

确定 AMI 的启动模式参数

AMI 启动模式参数是可选项。AMI 可以具有以下任一启动模式参数值：`uefi`、`legacy-bios` 或 `uefi-preferred`。

某些 AMI 没有启动模式参数。如果 AMI 没有启动模式参数，从 AMI 启动的实例将使用实例类型的默认值，在 Graviton 上使用 `uefi`，并在 Intel 和 AMD 实例类型上使用 `legacy-bios`。

确定 AMI 的启动模式参数（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMI，然后选择 AMI。
3. 在详细信息选项卡上，检查启动模式字段。

在启动实例时确定 AMI 的启动模式参数（控制台）

使用启动实例向导启动实例时，请在选择 AMI 的步骤中检查启动模式字段。有关更多信息，请参阅应用程序和操作系统镜像 (Amazon Machine Image) (p. 577)。

确定 AMI 的启动模式参数 (Amazon CLI)

使用 describe-images 命令确定 AMI 的启动模式。

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890
```

输出中的 BootMode 字段表示 AMI 的启动模式。值 `uefi` 表示 AMI 支持 UEFI。值 `uefi-preferred` 表示 AMI 同时支持 UEFI 和传统 BIOS。

预期输出

```
{
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm",
            "BootMode": "uefi"
        }
```

```
    ]
}
```

确定实例类型支持的启动模式

您可以使用 Amazon CLI 确定实例类型支持的启动模式。

确定实例类型支持的启动模式

使用 describe-instance-types 命令确定实例类型支持的启动模式。通过包含 `--query` 参数，您可以筛选输出。在此示例中，将筛选输出以仅返回支持的引导模式。

以下示例显示 `m5.2xlarge` 支持 UEFI 和传统 BIOS 启动模式。

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --query
 "InstanceTypes[*].SupportedBootModes"
```

预期输出

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

以下示例显示 `t2.xlarge` 仅支持传统 BIOS。

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --query
 "InstanceTypes[*].SupportedBootModes"
```

预期输出

```
[
    [
        "legacy-bios"
    ]
]
```

确定实例的启动模式

实例的启动模式会在 Amazon EC2 控制台中的启动模式字段中，通过 Amazon CLI 中的 `currentInstanceBootMode` 参数显示。

启动实例时，其启动模式参数的值由启动该实例所用的 AMI 的启动模式参数的值决定，如下所示：

- 启动模式参数为 `uefi` 的 AMI 会创建 `currentInstanceBootMode` 参数为 `uefi` 的实例。
- 启动模式参数为 `legacy-bios` 的 AMI 会创建 `currentInstanceBootMode` 参数为 `legacy-bios` 的实例。
- 如果实例类型支持 UEFI，则启动模式参数为 `uefi-preferred` 的 AMI 会创建 `currentInstanceBootMode` 参数为 `uefi` 的实例；否则将创建 `currentInstanceBootMode` 参数为 `legacy-bios` 的实例。
- 没有启动模式参数值的 AMI 会创建参数值为 `currentInstanceBootMode` 的实例，该值取决于 AMI 架构是 ARM 还是 x86，以及实例类型支持哪种启动模式。Graviton 实例类型上的默认启动模式为 `uefi`，而 Intel 和 AMD 实例类型上的默认启动模式为 `legacy-bios`。

确定实例的启动模式（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在详细信息选项卡上，检查启动模式字段。

确定实例的启动模式 (Amazon CLI)

使用 describe-instances 命令确定实例的启动模式。您还可以确定用于创建实例的 AMI 的启动模式。

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
```

在输出中，以下参数对启动模式进行了描述：

- BootMode – 用于创建实例的 AMI 的启动模式。
- CurrentInstanceBootMode – 用于在启动时启动实例的启动模式。

预期输出

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                   "BootMode": "uefi",
                   "CurrentInstanceBootMode": "uefi"
                }
            ],
            "OwnerId": "1234567890",
            "ReservationId": "r-1234567890abcdef0"
        }
    ]
}
```

确定操作系统的启动模式

AMI 的启动模式指导 Amazon EC2 使用哪种启动模式来启动实例。要查看实例的操作系统是否配置为 UEFI，需要通过 SSH 连接到实例。

要确定实例操作系统的启动模式

1. 使用 SSH 连接到 Linux 实例 (p. 649)。
2. 要查看操作系统的启动模式，请尝试以下任一操作：

   - 运行以下命令。

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     在 UEFI 启动模式下启动的实例的预期输出

```
BootCurrent: 0001
Timeout: 0 seconds
BootOrder: 0000,0001
Boot0000* UiApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
```

- 运行以下命令以验证 /sys/firmware/efi 目录是否存在。仅当实例使用 UEFI 启动时，此目录才会存在。如果此目录不存在，该命令将返回 Legacy BIOS Boot Detected。

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo "Legacy
 BIOS Boot Detected"
```

在 UEFI 启动模式下启动的实例的预期输出

```
UEFI Boot Detected
```

在传统 BIOS 启动模式下启动的实例的预期输出

```
Legacy BIOS Boot Detected
```

- 运行以下命令以验证 EFI 是否出现在 dmesg 输出中。

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

在 UEFI 启动模式下启动的实例的预期输出

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

设置 AMI 的启动模式

使用 register-image 命令创建 AMI 时，可将 AMI 的启动模式设置为 uefi、legacy-bios 或 uefi-preferred。

当 AMI 启动模式设置为 uefi-preferred 时，实例将按如下方式启动：

- 对于同时支持 UEFI 和传统 BIOS 的实例类型（例如 m5.large），实例通过 UEFI 启动。
- 对于仅支持传统 BIOS 的实例类型（例如 m4.large），实例通过传统 BIOS 启动。

> **Note**
>
> 如果将 AMI 启动模式设置为 uefi-preferred，则操作系统必须支持同时启动 UEFI 和传统 BIOS 的功能。

> **Warning**
>
> UEFI 安全启动等部分功能仅适用于在 UEFI 上启动的实例。将 uefi-preferred AMI 启动模式参数与不支持 UEFI 的实例类型结合使用时，实例将以传统 BIOS 启动，并禁用 UEFI 相关功能。如果您依赖于 UEFI 相关功能的可用性，请将 AMI 启动模式参数设置为 uefi。

要将现有的基于传统 BIOS 的实例转换为 UEFI，或将现有的基于 UEFI 的实例转换为传统 BIOS，需要执行以下步骤：首先，修改实例的卷和操作系统以支持选定的启动模式。然后，创建该卷的快照。最后，使用 register-image 以通过快照创建 AMI。

您无法使用 create-image 命令设置 AMI 的启动模式。使用 create-image，AMI 可以继承用于创建 AMI 的 EC2 实例的启动模式。例如，如果从传统 BIOS 上运行的 EC2 实例创建 AMI，则 AMI 启动模式将配置为 `legacy-bios`。如果从通过 AMI（启动模式设置为 `uefi-preferred`）启动的 EC2 实例创建 AMI，则所创建 AMI 的启动模式也将设置为 `uefi-preferred`。

Warning

设置 AMI 启动模式参数不会自动将操作系统配置为指定的启动模式。在继续执行这些步骤之前，必须首先对实例的卷和操作系统进行适当的修改，以支持通过选定的启动模式启动；否则，生成的 AMI 将无法使用。所需的修改是特定于操作系统的。有关更多信息，请参阅操作系统的手册。

设置 AMI 的启动模式 (Amazon CLI)

1. 对实例的卷和操作系统进行适当的修改，以支持通过选定的启动模式启动。所需的修改是特定于操作系统的。有关更多信息，请参阅操作系统的手册。

   Note

   如果不执行此步骤，AMI 将无法使用。

2. 要查找实例的卷 ID，请使用 describe-instances 命令。您将在下一步中创建此卷的快照。

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
```

预期输出

```
...
            "BlockDeviceMappings": [
                        {
                            "DeviceName": "/dev/sda1",
                            "Ebs": {
                                "AttachTime": "",
                                "DeleteOnTermination": true,
                                "Status": "attached",
                                "VolumeId": "vol-1234567890abcdef0"
                            }
                        }
                        ...
```

3. 要创建卷的快照，请使用 create-snapshot 命令。使用上一步中的卷 ID。

```
aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
description "add text"
```

预期输出

```
{
 "Description": "add text",
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. 请注意上一步输出中的快照 ID。

5. 等到快照创建状态为 completed 后，继续执行下一步。要查询快照的状态，请使用 describe-snapshots 命令。

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

输出示例

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. 要创建新的 AMI，请使用 register-image 命令。使用您在前面步骤中记下的快照 ID。

   - 要将启动模式设置为 UEFI，请将 --boot-mode 参数添加到命令中并将 uefi 指定为值。

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

   - 要将启动模式设置为 uefi-preferred，请将 --boot-mode 参数添加到命令中并将 uefi-preferred 指定为值。

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

预期输出

```
{
"ImageId": "ami-new_ami_123"
}
```

7. 要验证新创建的 AMI 是否具有您在上一步中指定的启动模式，请使用 describe-images 命令。

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

预期输出

```
{
  "Images": [
   {
   "Architecture": "x86_64",
   "CreationDate": "2021-01-06T14:31:04.000Z",
   "ImageId": "ami-new_ami_123",
   "ImageLocation": "",
   ...
   "BootMode": "uefi"
   }
   ]
}
```

8. 使用新创建的 AMI 启动新实例。

   如果 AMI 启动模式为 `uefi` 或 `legacy-bios`，则从此 AMI 创建的实例所具有的启动模式与 AMI 相同。如果 AMI 启动模式为 `uefi-preferred`，则在实例类型支持 UEFI 的情况下，实例将通过 UEFI 启动；否则，实例将通过传统 BIOS 启动。有关更多信息，请参阅注意事项 (p. 108)。
9. 要验证新实例是否具有预期的启动模式，请使用 describe-instances 命令。

UEFI 变量

当您启动实例且其启动模式设置为 UEFI 时，将为变量创建键值存储。UEFI 和实例操作系统可以使用该键值存储来存储 UEFI 变量。

启动加载程序和操作系统使用 UEFI 变量来配置早期系统启动。它们允许操作系统管理启动过程的某些设置（例如启动顺序）或管理 UEFI 安全启动的密钥。

> Warning
>
> 您只能从实例内访问 UEFI 变量。任何可以连接到实例的人以及可能在实例上运行的任何软件都可以读取变量。您绝不应将敏感数据（例如密码或个人身份信息）存储在 UEFI 变量存储中。

UEFI 变量持久性

- 对于在 2022 年 5 月 10 日或之前启动的实例，UEFI 变量会在重启或停止时擦除。
- 对于在 2022 年 5 月 11 日或之后启动的实例，标记为非易失性的 UEFI 变量将在重启和停止/启动时保留。
- 裸机实例不会在实例停止/启动操作中保留 UEFI 非易失性变量。

查找 Linux AMI

启动实例之前，必须选择要从中启动实例的 AMI，然后才能启动实例。选择 AMI 时，对于要启动的实例，可能需要考虑以下要求：

- 区域
- 操作系统
- 架构：32 位 (`i386`)、64 位 (`x86_64`) 或 64 位 ARM (`arm64`)

- 根设备类型：Amazon EBS 或实例存储
- 提供商 (例如，Amazon Web Services)
- 其他软件（例如，SQL Server）

如果您要查找 Windows AMI，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的查找 Windows AMI。

如果您要查找 Ubuntu AMI，请参阅他们的 EC2 AMI 定位器。

如果您要查找 RedHat AMI，请参阅 RHEL 知识库文章。

查找 Linux AMI 主题

- 使用 Amazon EC2 控制台查找 Linux AMI (p. 117)
- 使用 Amazon CLI 查找 AMI (p. 118)
- 使用 Systems Manager 查找最新的 Amazon Linux AMI (p. 118)
- 使用 Systems Manager 参数查找 AMI (p. 119)

使用 Amazon EC2 控制台查找 Linux AMI

您可以使用 Amazon EC2 控制台查找 Linux AMI。您可以在使用启动实例向导启动实例时从 AMI 列表中进行选择，也可以使用 Images（映像）页面在所有可用的 AMI 中进行搜索。AMI ID 在每个 Amazon 区域中都是唯一的。

使用启动实例向导查找 Linux AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 从控制台控制面板中，选择启动实例。
4. （新控制台）在 Application and OS Images (Amazon Machine Image)（应用程序和操作系统映像 (Amazon Machine Image)）下，选择 Quick Start（快速启动），选择适用于实例的操作系统 (OS)，然后在 Amazon Machine Image (AMI) 中，从列表中选择一个常用的 AMI。如果您没有看到想要使用的 AMI，请选择 Browser more AMIs（浏览更多 AMI）以浏览完整的 AMI 目录。有关更多信息，请参阅应用程序和操作系统镜像 (Amazon Machine Image) (p. 577)。

   （旧控制台）在 Quick Start（快速启动）选项卡上，从列表中选择一个常用的 AMI。如果您没有看到要使用的 AMI，请选择 My AMIs（我的 AMI）、Amazon Web Services Marketplace 或 Community AMIs（社群 AMI）选项卡来查找其他 AMI。有关更多信息，请参阅步骤 1：选择 Amazon Machine Image (AMI) (p. 584)。

使用 AMI 页面查找 Linux AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 在导航窗格中，选择 AMIs。
4. （可选）使用筛选条件和搜索选项，将显示的 AMI 列表范围限定为仅能查看符合您的标准的 AMI。例如，要列出 Amazon 提供的所有 Linux AMI，请选择 Public images（公有映像）。然后使用搜索选项进一步缩小显示的 AMI 列表的范围。

   （新控制台）选择 Search（搜索）栏，然后从菜单中选择 Owner alias（拥有者别名），然后选择 = 运算符，最后选择值 amazon。再次选择 Search（搜索）栏以选择 Platform（平台），然后选择 = 运算符，然后从提供的列表中选择操作系统。

（旧控制台）选择 Search（搜索）栏，然后从菜单中选择 Owner（拥有者），然后选择值 Amazon images（Amazon 映像）。再次选择 Search（搜索）栏以选择 Platform（平台），然后从提供的列表中选择操作系统。

5. （可选）选择 Preferences（首选项）图标（新控制台）或 Show/Hide Columns（显示/隐藏列）图标（旧控制台）可选择要显示的镜像属性，例如根设备类型。或者，可以从列表中选择 AMI，然后在 Details（详细信息）选项卡中查看其属性。
6. 选择 AMI 之前，请确认它是由实例存储支持还是由 Amazon EBS 支持并了解此差异的影响，这十分重要。有关更多信息，请参阅根设备存储 (p. 103)。
7. 要从此 AMI 启动实例，请选择该实例，然后选择 Launch instance from image（从镜像启动实例）（新控制台）或 Launch（启动）（旧控制台）。有关使用控制台启动实例的更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。如果您没有准备好立即启动实例，请记下 AMI ID 以供将来使用。

使用 Amazon CLI 查找 AMI

您可以使用适用于 Amazon EC2 的 Amazon CLI 命令，以仅列出符合您要求的 Linux AMI。找到符合您要求的 AMI 之后，记录其 ID，以便用它来启动实例。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的启动实例。

describe-images 命令支持筛选参数。例如，使用 `--owners` 参数显示由 Amazon 拥有的公用 AMI。

```
aws ec2 describe-images --owners self amazon
```

您可以将以下筛选条件添加到上一个命令以便仅显示 Amazon EBS 支持的 AMI。

```
--filters "Name=root-device-type,Values=ebs"
```

Important

在 describe-images 命令中省略 `--owners` 标记将返回您拥有启动权限的所有映像，无论所有权如何。

使用 Systems Manager 查找最新的 Amazon Linux AMI

Amazon EC2 为 Amazon 维护的公用 AMI 提供了 Amazon Systems Manager 公用参数，您可以在启动实例时使用这些参数。例如，EC2 提供的参数 `/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2` 在所有区域中均可用，并且始终指向给定区域中 Amazon Linux 2 AMI 的最新版本。

在以下路径中提供 Amazon EC2 AMI 公有参数：

`/aws/service/ami-amazon-linux-latest`

您可以通过运行以下 Amazon CLI 命令查看当前 Amazon 区域中所有 Linux AMI 的列表。

```
aws ssm get-parameters-by-path --path /aws/service/ami-amazon-linux-latest --query
 "Parameters[].Name"
```

使用公有参数启动实例

以下示例通过 EC2 提供的公有参数，使用最新 Amazon Linux 2 AMI 启动 `m5.xlarge` 实例。

要在命令中指定参数，请使用以下语法：`resolve:ssm:`*`public-parameter`*，其中 `resolve:ssm` 是标准前缀，`public-parameter` 是公有参数的路径和名称。

在本示例中，不包括 `--count` 和 `--security-group` 参数。对于 `--count`，默认为 1。如有默认 VPC 和默认安全组，则将使用它们。

```
aws ec2 run-instances
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2
    --instance-type m5.xlarge
    --key-name MyKeyPair
```

有关详细信息，请参阅 Amazon Systems Manager 用户指南中的使用公共参数和使用 Amazon Systems Manager Parameter Store 查询最新的 Amazon Linux AMI ID。

使用 Systems Manager 参数查找 AMI

在控制台中使用 EC2 启动实例向导启动实例时，您可以从列表中选择 AMI，也可以选择指向 AMI ID 的 Amazon Systems Manager 参数。如果您使用自动化代码启动实例，则可以指定 Systems Manager 参数而不是 AMI ID。

Systems Manager 参数是客户定义的键/值对，您可以在 Systems Manager Parameter Store 中创建该键/值对。Parameter Store 提供了一个中央存储来对应用程序配置值进行外部化。有关更多信息，请参阅 Amazon Systems Manager 用户指南中的 Amazon Systems Manager Parameter Store。

创建指向 AMI ID 的参数时，请确保将数据类型指定为 `aws:ec2:image`。指定此数据类型可确保在创建或修改参数时，将参数值作为 AMI ID 进行验证。有关更多信息，请参阅 Amazon Systems Manager 用户指南中对 Amazon Machine Image ID 的原生参数支持。

Systems Manager 参数主题

- 使用案例 (p. 119)
- 权限 (p. 120)
- 限制 (p. 120)
- 使用 Systems Manager 参数启动实例 (p. 120)

使用案例

当您使用 Systems Manager 参数指向 AMI ID 时，您的用户在启动实例时可以更轻松地选择正确的 AMI。Systems Manager 参数还可以简化自动化代码的维护。

用户使用更简单

如果您需要使用特定 AMI 启动实例并且该 AMI 定期更新，我们建议您要求用户选择 Systems Manager 参数来查找 AMI。要求用户选择 Systems Manager 参数可确保使用最新的 AMI 启动实例。

例如，您的组织中可能会每个月创建一个新版本的 AMI，其中具有最新操作系统和应用程序修补程序。同时，您要求用户使用最新版本的 AMI 启动实例。为确保用户使用最新版本，您可以创建指向正确 AMI ID 的 Systems Manager 参数（例如 `golden-ami`）。每次创建新版本的 AMI 时，您需要更新参数中的 AMI ID 值，以使其始终指向最新 AMI。您的用户不需要了解对 AMI 的定期更新，因为他们每次都会继续选择相同的 Systems Manager 参数。为您的 AMI 使用 Systems Manager 参数可让他们更轻松地选择正确的 AMI 来启动实例。

简化自动化代码维护

如果您使用自动化代码启动实例，则可以指定 Systems Manager 参数而不是 AMI ID。如果创建了新版本的 AMI，您可以更改参数中的 AMI ID 值，以使其指向最新 AMI。每次创建新版本的 AMI 时，都不需要修改引用该参数的自动化代码。这样做简化了自动化的维护，有助于降低部署成本。

> **Note**
>
> 当您更改 Systems Manager 参数指向的 AMI ID 时，正在运行的实例不受影响。

权限

如果在启动实例向导中使用指向 AMI ID 的 Systems Manager 参数，则必须将 `ssm:DescribeParameters` 和 `ssm:GetParameters` 添加到 IAM policy 中。`ssm:DescribeParameters` 会授予用户查看和选择 Systems Manager 参数的权限。`ssm:GetParameters` 则会授予 IAM 用户检索 Systems Manager 参数值的权限。您还可以限制对特定 Systems Manager 参数的访问权限。有关更多信息，请参阅使用 EC2 启动实例向导 (p. 1269)。

限制

AMI 和 Systems Manager 参数特定于区域。要跨区域使用相同的 Systems Manager 参数名称，请在各个区域中创建具有相同名称的 Systems Manager 参数（例如，`golden-ami`）。在每个区域中，将 Systems Manager 参数指向该区域的 AMI。

使用 Systems Manager 参数启动实例

您可以使用控制台或 Amazon CLI 启动实例。您可以指定指向 AMI ID 的 Amazon Systems Manager 参数，而不是指定 AMI ID。

New console

使用 Systems Manager 参数查找 Linux AMI（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 从控制台控制面板中，选择启动实例。
4. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统镜像（Amazon 机器映像）] 下，选择 Browse more AMIs（浏览其他 AMI）。
5. 选择搜索栏右侧的箭头按钮，然后选择 Search by Systems Manager parameter（按 Systems Manager 参数搜索）。
6. 对于 Systems Manager 参数 (Systems Manager 参数)，请选择一个参数。相应的 AMI ID 将显示在 Currently resolves to（当前解析为）下方。
7. 选择搜索。与 AMI ID 匹配的 AMI 将显示在列表中。
8. 从列表中选择 AMI，然后选择选择。

有关使用启动实例向导启动实例的更多信息，请参阅 使用新启动实例向导启动实例 (p. 575)。

Old console

使用 Systems Manager 参数查找 Linux AMI（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 从控制台控制面板中，选择启动实例。
4. 选择 Search by Systems Manager parameter (按 Systems Manager 参数搜索)（位于右上角）。
5. 对于 Systems Manager 参数 (Systems Manager 参数)，请选择一个参数。相应的 AMI ID 将显示在 Currently resolves to (当前解析为) 的旁边。
6. 选择搜索。与 AMI ID 匹配的 AMI 将显示在列表中。
7. 从列表中选择 AMI，然后选择选择。

有关使用启动实例向导从 AMI 启动实例的更多信息，请参阅 步骤 1：选择 Amazon Machine Image (AMI) (p. 584)。

使用 Amazon Systems Manager 参数而不是 AMI ID 启动实例 (Amazon CLI)

以下示例使用 Systems Manager 参数 `golden-ami` 启动 `m5.xlarge` 实例。该参数指向 AMI ID。

要在命令中指定参数，请使用以下语法：`resolve:ssm:`*`parameter-name`*，其中 `resolve:ssm` 是标准前缀，`parameter-name` 是唯一参数名称。请注意，参数名称区分大小写。只有在参数是层次结构的一部分时，参数名称才需要使用反斜杠，例如，`/amis/production/golden-ami`。如果参数不是层次结构的一部分，您可以省略反斜杠。

在本示例中，不包括 `--count` 和 `--security-group` 参数。对于 `--count`，默认为 1。如有默认 VPC 和默认安全组，则将使用它们。

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

使用特定版本的 Amazon Systems Manager 参数启动实例 (Amazon CLI)

Systems Manager 参数具有版本支持。参数的每个迭代将分配一个唯一的版本号。您可以按照 `resolve:ssm:`*`parameter-name`*`:`*`version`* 的格式引用参数的版本，其中 `version` 是唯一版本号。默认情况下，未指定版本时将使用参数的最新版本。

以下示例使用参数的版本 2。

在本示例中，不包括 `--count` 和 `--security-group` 参数。对于 `--count`，默认值为 1。如果您有默认的 VPC 和默认安全组，则将使用它们。

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
    --instance-type m5.xlarge
    ...
```

使用 Amazon 提供的公有参数启动实例

Amazon EC2 为 Amazon 提供的公用 AMI 提供 Systems Manager 公用参数。例如，公有参数 /aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2 在所有区域中都可用，并且始终指向该区域中 Amazon Linux 2 AMI 的最新版本。

```
aws ec2 run-instances
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2
    --instance-type m5.xlarge
    ...
```

共享 AMI

共享 AMI 是开发人员创建并可供其他人员使用的 AMI。要开始使用 Amazon EC2，最简单的方法之一是使用共享 AMI，您可以从中获得所需的组件，然后添加自定义内容。您还可以创建自己的 AMI 并与他人共享。

使用共享 AMI 需自行承担风险。Amazon 不保证其他 Amazon EC2 用户共享的 AMI 的完整性或安全性。因此，您应该像处理其他您可能会考虑在自己的数据中心部署的外来代码一样处理共享 AMI，对其执行适当的功能调查。我们建议您从可靠来源获取 AMI。

经过验证的提供商

在 Amazon EC2 控制台中，将 Amazon 或经过验证的 Amazon 合作伙伴拥有的公有 AMI 标记为经过验证的提供商。

您也可以使用 describe-images Amazon CLI 命令标识来自经过验证的提供商的公共 AMI。Amazon 或经过验证的合作伙伴拥有的公共映像具有一个别名拥有者，`amazon` 或 `aws-marketplace`。在 CLI 输出中，将为 `ImageOwnerAlias` 显示这些值。其他用户不能对其 AMI 使用别名。这使您可以轻松查找来自 Amazon 或经过验证的合作伙伴的 AMI。

要成为经过验证的提供商，您必须在 Amazon Web Services Marketplace 上注册成为卖方。在注册后，您可以在 Amazon Web Services Marketplace 上列出您的 AMI。有关更多信息，请参阅《Amazon Web Services Marketplace 卖方指南》中的以卖方身份开始使用和基于 AMI 的产品。

共享 AMI 主题

- 查找共享 AMI (p. 122)
- 将 AMI 设为公用 (p. 124)
- 与特定 Amazon 账户共享 AMI (p. 126)
- 取消与您的 Amazon Web Services 账户 共享 AMI (p. 128)
- 使用书签 (p. 129)
- 共享 Linux AMI 指导原则 (p. 130)

如果您正在寻找有关其他主题的信息

- 有关创建 AMI 的信息，请参阅 创建实例存储支持的 Linux AMI 或创建 Amazon EBS 支持的 Linux AMI。
- 有关在 Amazon Web Services Marketplace 中构建、交付和维护应用程序的信息，请参阅 Amazon Web Services Marketplace 文档。

查找共享 AMI

可以使用 Amazon EC2 控制台或命令行查找共享 AMI。

AMI 是一种区域性资源。在搜索共享 AMI（公有或私有）时，必须在共享此 AMI 的同一区域中进行搜索。要使 AMI 能够在其他区域使用，请将该 AMI 复制到该区域，然后进行共享。有关更多信息，请参阅复制 AMI (p. 172)。

主题

- 查找共享 AMI（控制台） (p. 122)
- 查找共享 AMI (Amazon CLI) (p. 123)
- 使用共享 AMI (p. 124)

查找共享 AMI（控制台）

使用控制台查找共享的私有 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 在第一个筛选条件中，选择 Private images。将列出已与您共享的所有 AMI。要细化您的搜索，可选择 Search（搜索）栏并使用菜单中提供的筛选条件选项。

使用控制台查找共享的公用 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 在第一个筛选条件中，选择 Public images。要细化您的搜索，可选择 Search（搜索）字段，并使用菜单中提供的筛选条件选项。

使用控制台查找 Amazon 的共享公共 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 在第一个筛选条件中，选择 Public images。
4. 选择 Search（搜索）字段，然后从显示的菜单选项中选择 Owner alias（所有者别名），再选择 =，然后选择 amazon 以仅显示 Amazon 的公共映像。

使用控制台查找来自经过验证的提供商的共享公共 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMI Catalog（AMI 目录）。
3. 选择社区 AMI。
4. Verified provider（经过验证的提供商）标签表示来自 Amazon 或经过验证的合作伙伴的 AMI。

查找共享 AMI (Amazon CLI)

使用 describe-images 命令 (Amazon CLI) 可以列出 AMI。可以将该列表范围确定为所需的 AMI 类型，如以下示例所示。

示例：列出所有公用 AMI

以下命令将列出所有公用 AMI，包括您拥有的所有公用 AMI。

```
aws ec2 describe-images --executable-users all
```

示例：使用显式启动许可列出 AMI

以下命令列出您对其拥有显式启动许可的 AMI。此列表不包括您拥有的任何 AMI。

```
aws ec2 describe-images --executable-users self
```

示例：列出经过验证的提供商拥有的 AMI

以下命令将列出经过验证的提供商拥有的 AMI。经过验证的提供商（Amazon 或经过验证的合作伙伴）拥有的公共 AMI 具有一个别名拥有者，它将在账户字段中显示为 `amazon` 或 `aws-marketplace`。这可帮助您轻松查找来自经过验证的提供商的 AMI。其他用户不能对其 AMI 使用别名。

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

示例：列出账户拥有的 AMI

以下命令列出指定 Amazon Web Services 账户 拥有的 AMI。

```
aws ec2 describe-images --owners 123456789012
```

示例：使用筛选条件确定 AMI 的范围

要减少显示的 AMI 数量，请使用筛选条件只列出您感兴趣的 AMI 类型。例如，使用以下筛选条件可以只显示 EBS 支持的 AMI。

```
--filters "Name=root-device-type,Values=ebs"
```

使用共享 AMI

使用共享 AMI 之前，应执行以下步骤以确认没有预安装凭证允许第三方对您的实例进行不希望的访问，并且没有可能将敏感数据传输给第三方的预配置远程登录。查看 AMI 使用的 Linux 发行版的文档以了解有关提高系统安全性的信息。

为了确保您不会在无意中丢失对您的实例的访问，我们建议您启动两个 SSH 会话并将第二个会话保持为打开状态，直到您删除了无法识别的凭证并确认您仍可以使用 SSH 登录您的实例。

1. 标识并禁用任何未经授权的公有 SSH 密钥。该文件中的唯一密钥应是您用于启动 AMI 的密钥。以下命令查找 `authorized_keys` 文件：

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. 对根用户禁用基于密码的身份验证。打开 `sshd_configPermitRootLogin` 文件并编辑 行，如下所示：

   ```
   PermitRootLogin without-password
   ```

   或者，您可以禁用以根用户身份登录实例的功能：

   ```
   PermitRootLogin No
   ```

   重启 sshd 服务。
3. 检查是否有任何其他用户能够登录您的实例。具有超级用户权限的用户尤为危险。删除或锁定任何未知账户的密码。
4. 检查打开的端口以确认您未在使用和运行侦听传入连接的网络服务。
5. 要防止预配置的远程登录，应删除现有配置文件并重启 `rsyslog` 服务。例如：

   ```
   [ec2-user ~]$ sudo rm /etc/rsyslog.conf
   [ec2-user ~]$ sudo service rsyslog restart
   ```

6. 确认所有 cron 任务是合法的。

如果您发现了认为存在安全风险的公用 AMI，请联系 Amazon 安全团队。有关更多信息，请参阅 Amazon 安全中心。

将 AMI 设为公用

您能与其他 Amazon Web Services 账户 共享您的 AMI。要允许所有 Amazon Web Services 账户 使用 AMI 启动实例，请将该 AMI 设为公共。要仅允许特定账户使用 AMI 启动实例，请参阅 与特定 Amazon 账户共享 AMI (p. 126)。

公用 AMI 主题

- 注意事项 (p. 125)
- 与所有 Amazon 账户共享 AMI（控制台） (p. 125)
- 与所有 Amazon Web Services 账户（Amazon CLI）共享 AMI (p. 126)

注意事项

在将 AMI 设为公用之前，请考虑以下事项。

- 所有权 – 若要将 AMI 设为公有，您的 Amazon Web Services 账户 必须拥有 AMI。
- 有些 AMI 无法设为公共 – 如果您的 AMI 包含以下组件之一，则无法将其设为公共（但您可以将 AMI 与特定 Amazon Web Services 账户 账户共享 (p. 126)）：
  - 加密卷
  - 加密卷的快照
  - 产品代码
- 避免泄露敏感数据 – 要避免在共享 AMI 时泄露敏感数据，请阅读 共享 Linux AMI 指导原则 (p. 130) 中的安全注意事项并遵循建议的操作。
- 区域 – AMI 是一种区域性资源。当您共享 AMI 时，则它只能在您共享该 AMI 的区域使用。要使 AMI 能够在其他区域使用，请将该 AMI 复制到该区域并进行共享。有关更多信息，请参阅复制 AMI (p. 172)。
- 使用 – 当您共享 AMI 时，用户只能从该 AMI 启动实例。他们无法删除、共享或修改实例。但是，在他们使用您的 AMI 启动实例后，他们可以从其启动的实例创建 AMI。
- 自动弃用 – 默认情况下，所有公有 AMI 的弃用日期均设置为自 AMI 创建日期起 2 年。您可以将弃用日期设置为早于两年。要取消弃用日期，或将弃用移至未来某一日期，您必须通过仅将 AMI 与特定 Amazon Web Services 账户 共享 (p. 126)来将其设为私有。
- 账单 – 当其他 Amazon Web Services 账户 使用您的 AMI 启动实例时，您无需付费。使用 AMI 启动实例的账户将为它们启动的实例付费。

与所有 Amazon 账户共享 AMI（控制台）

将 AMI 设置为公有后，当您使用控制台在相同区域启动实例时，Community AMIs (社区 AMI) 中会出现该 AMI。请注意，将某个 AMI 设置为公用之后，可能需要一点时间 Community AMIs 中才会显示该 AMI。在将 AMI 设为私有后，也可能需要一点时间才能将它从 Community AMIs（社群 AMI）中删除。

New console

使用控制台共享公用 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 从列表中选择您的 AMI，然后选择 Actions（操作）、Edit AMI permissions（编辑 AMI 权限）。
4. 选择 Public（公有），然后选择 Save changes（保存更改）。

Old console

使用控制台共享公用 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 从列表中选择您的 AMI，然后选择 Actions、Modify Image Permissions。
4. 选择 Public（公有），然后选择 Save（保存）。

与所有 Amazon Web Services 账户（Amazon CLI）共享 AMI

每个 AMI 都有一个 `launchPermission` 属性，用于控制允许哪些 Amazon Web Services 账户（包括拥有者账户在内）使用该 AMI 启动实例。通过修改 AMI 的 `launchPermission` 属性，可以将该 AMI 设为公共（这会向所有 Amazon Web Services 账户 授予启动权限），或仅将其与您指定的 Amazon Web Services 账户 共享。

可以在具有 AMI 启动许可的账户的列表中添加或删除账户 ID。要将 AMI 设为公有，请指定 `all` 组。公用和显式启动许可都可以指定。

将 AMI 设为公用

1. 使用 modify-image-attribute 命令可以将 `all` 组添加到指定 AMI 的 `launchPermission` 列表中，如下所示。

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. 要验证 AMI 的启动权限，请使用 describe-image-attribute 命令。

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. （可选）要再次将 AMI 设为私有，请从其启动许可中删除 `all` 组。请注意，AMI 的拥有者始终具有启动许可，因此不受该命令影响。

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

与特定 Amazon 账户共享 AMI

您可以在不将 AMI 设为公共的情况下，与特定 Amazon Web Services 账户 共享 AMI。您需要的只是 Amazon Web Services 账户 ID。

注意事项

在与特定 Amazon Web Services 账户 共享 AMI 时，请考虑以下事项。

- 所有权 – 若要共享 AMI，您的 Amazon Web Services 账户 必须拥有 AMI。
- 共享限制 - 有关某一区域内可以共享 AMI 的最大实体数量，请参阅 Amazon EC2 服务限额。
- 标签 – 您无法共享用户定义的标签（附加到 AMI 的标签）。共享 AMI 时，与其共享 AMI 的任何 Amazon Web Services 账户 均无法使用用户定义的标签。
- 加密和密钥 – 您可以共享由未加密和加密快照支持的 AMI。
  - 加密快照必须使用 KMS 密钥加密。您无法共享由使用默认 Amazon 托管式密钥加密的快照支持的 AMI。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。
  - 如果您共享由加密快照支持的 AMI，则必须允许 Amazon Web Services 账户 使用用于加密快照的 KMS 密钥。。
- 区域 – AMI 是一种区域性资源。如果您共享 AMI，则它只能在该区域使用。要使 AMI 能够在其他区域使用，请将该 AMI 复制到该区域并进行共享。有关更多信息，请参阅复制 AMI (p. 172)。

- 使用 – 当您共享 AMI 时，用户只能从该 AMI 启动实例。他们无法删除、共享或修改实例。但是，在他们使用您的 AMI 启动实例后，他们可以从其实例创建 AMI。
- 复制共享 AMI – 如果另一个账户中的用户想复制共享 AMI，则必须向他们授予对支持 AMI 的存储的读取权限。有关更多信息，请参阅跨账户复制 (p. 177)。
- 账单 – 当其他 Amazon Web Services 账户 使用您的 AMI 启动实例时，您无需付费。使用 AMI 启动实例的账户将为它们启动的实例付费。

共享 AMI（控制台）

New console

使用控制台授予显式启动许可

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 在列表中选择您的 AMI，然后选择 Actions（操作）、Modify AMI Permissions（修改 AMI 权限）。
4. 选择 Private (私有)。
5. 在 Shared accounts（共享账户）下，选择 Add account ID（添加账户 ID）。
6. 对于 Amazon Web Services 账户 ID，输入要与其共享 AMI 的 Amazon Web Services 账户 ID，然后选择 Share AMI（共享 AMI）。

   要与多账户共享此 AMI，请重复此步骤 5 和 6，直至您添加完所需全部账户 ID。

   Note

   您不需要为了共享 AMI 而共享 AMI 引用的 Amazon EBS 快照。只需共享 AMI 本身；系统自动为实例提供访问所引用 Amazon EBS 快照的权限以便启动。不过，您确实需要共享用于对 AMI 引用的快照加密的所有 KMS 密钥。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。
7. 完成后，选择 Save changes（保存更改）。
8. （可选）要查看您已与其共享 AMI 的 Amazon Web Services 账户 ID，请在列表中选择该 AMI，然后选择 Permissions（权限）选项卡。要查找与您共享的 AMI，请参阅查找共享 AMI (p. 122)。

Old console

使用控制台授予显式启动许可

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 在列表中选择您的 AMI，然后选择 Actions、Modify Image Permissions。
4. 在 Amazon 账号字段中指定您想与其共享 AMI 的用户的 Amazon Web Services 账户 ID，然后选择添加权限。

   要与多个用户共享此 AMI，请重复此步骤，直至您添加完所需全部用户。

   Note

   您不需要为了共享 AMI 而共享 AMI 引用的 Amazon EBS 快照。只需共享 AMI 本身；系统自动为实例提供访问所引用 Amazon EBS 快照的权限以便启动。不过，您确实需要共享用于对 AMI 引用的快照加密的所有 KMS 密钥。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。
5. 完成后选择 Save (保存)。

6. （可选）要查看您已与其共享 AMI 的 Amazon Web Services 账户 ID，请在列表中选择该 AMI，然后选择 Permissions（权限）选项卡。要查找与您共享的 AMI，请参阅查找共享 AMI (p. 122)。

共享 AMI (Amazon CLI)

使用 modify-image-attribute 命令（Amazon CLI）共享 AMI，如以下示例所示。

要授予显式启动许可

以下命令向指定 Amazon Web Services 账户 授予指定 AMI 的启动权限。

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=123456789012}]"
```

Note

您不需要为了共享 AMI 而共享 AMI 引用的 Amazon EBS 快照。只需共享 AMI 本身；系统自动为实例提供访问所引用 Amazon EBS 快照的权限以便启动。不过，您确实需要共享用于对 AMI 引用的快照加密的所有 KMS 密钥。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

要删除账户的启动许可

以下命令从指定 Amazon Web Services 账户 中移除指定 AMI 的启动权限。

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=123456789012}]"
```

要删除所有的启动许可

以下命令从指定 AMI 中删除所有公用和显式启动许可。请注意，AMI 的拥有者始终具有启动许可，因此不受该命令影响。

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

取消与您的 Amazon Web Services 账户 共享 AMI

通过将账户添加到 AMI 的启动权限，可以 与特定 Amazon Web Services 账户 共享 (p. 126) 亚马逊云机器镜像（AMI）。如果已与您的 Amazon Web Services 账户 共享 AMI，而您不想再与您的账户共享该 AMI，则可以将您的账户从 AMI 的启动权限中移除。您可以通过运行 `cancel-image-launch-permission` Amazon CLI 命令进行这项操作。在运行此命令时，将从指定 AMI 的启动权限中移除您的 Amazon Web Services 账户。

例如，您可以取消与您的账户共享 AMI，以降低使用已与您共享的未使用或已弃用的 AMI 启动实例的可能性。当您取消与您的账户共享 AMI 时，它将不再出现在 EC2 控制台的任何 AMI 列表中，也不会出现在 describe-images 的输出中。

主题

- 限制 (p. 129)
- 取消与您的账户共享 AMI (p. 129)
- 查找与账户共享的 AMI (p. 129)

限制

- 您可将您的账户从仅与 Amazon Web Services 账户 共享的 AMI 的启动权限中移除。
- 您不能从 AMI 的启动权限中永久移除您的账户。AMI 拥有者可以再次与您的账户共享 AMI。
- AMI 是一种区域性资源。在运行 `cancel-image-launch-permission` 时，必须指定 AMI 所在的区域。可在命令中指定区域，或者使用 AWS_DEFAULT_REGION 环境变量。
- 只有 Amazon CLI 和 SDK 支持从 AMI 的启动权限中移除您的账户。EC2 控制台目前不支持此操作。

取消与您的账户共享 AMI

> **Note**
>
> 在您取消与您的账户共享 AMI 后，您将无法撤消该操作。要重新获得对 AMI 的访问权限，AMI 拥有者必须将其与您的账户共享。

取消与您的 Amazon Web Services 账户 共享 AMI

使用 cancel-image-launch-permission 命令并指定 AMI ID。

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

预期输出

```
{
    "Return": true
}
```

查找与账户共享的 AMI

若要查找与 Amazon Web Services 账户 共享的 AMI，请参阅 查找共享 AMI (p. 122)。

使用书签

如果您创建了公共 AMI，或与其他 Amazon Web Services 账户 共享了 AMI，您可以创建一个书签来允许用户访问您的 AMI 并允许他们立即在自己的账户中启动一个实例。这是共享 AMI 引用的一种简单方法，借助这种方法，用户无需花时间来查找您的 AMI 即可使用。

请注意，您的 AMI 必须为公用，否则必须与您要向其发送书签的用户共享它。

为您的 AMI 创建书签

1. 键入一个带有以下信息的 URL，其中 region 表示您的 AMI 驻留的区域：

   ```
   https://console.aws.amazon.com/ec2/v2/home?
   region=region#LaunchInstanceWizard:ami=ami_id
   ```

   例如，此 URL 从美国东部（弗吉尼亚州北部）us-east-1 区域内的 ami-0abcdef1234567890 AMI 启动实例：

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=us-
   east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
   ```

2. 将链接分发给那些想要使用您的 AMI 的用户。
3. 要使用书签，请选择链接或将其复制并粘贴到您的浏览器中。启动向导打开，同时 AMI 已被选定。

共享 Linux AMI 指导原则

使用以下指南可缩小攻击面并提高您创建的 AMI 的可靠性。

> **Important**
>
> 任何安全指南都不是详尽无遗的。请仔细构建您的共享 AMI，并花时间考虑可能导致暴露敏感数据的位置。

目录

- 在使用 AMI 工具之前对其进行更新 (p. 130)
- 对根用户禁用基于密码的远程登录 (p. 130)
- 禁用本地根访问 (p. 131)
- 删除 SSH 主机密钥对 (p. 131)
- 安装公有密钥凭证 (p. 132)
- 禁用 sshd DNS 检查（可选） (p. 133)
- 保护自己 (p. 133)

如果为 Amazon Web Services Marketplace 构建 AMI，请参阅 Amazon Web Services Marketplace 卖家指南中的构建 AMI 的最佳实践，以了解指导原则、策略和最佳实践。

有关安全共享 AMI 的更多信息，请参阅以下文章：

- How To Share and Use Public AMIs in A Secure Manner
- Public AMI Publishing: Hardening and Clean-up Requirements

在使用 AMI 工具之前对其进行更新

对于实例存储支持的 AMI，建议您的 AMI 先下载和更新 Amazon EC2 AMI 创建工具，然后再使用这些工具。这可确保基于您的共享 AMI 的新 AMI 拥有最新的 AMI 工具。

对于 Amazon Linux 2，安装 `aws-amitools-ec2` 软件包，并使用以下命令将 AMI 工具添加到 PATH。对于 Amazon Linux AMI，默认情况下已安装 `aws-amitools-ec2` 程序包。

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin > /
etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

使用以下命令升级 AMI 工具：

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

对于其他发行版，请确保您拥有最新的 AMI 工具。

对根用户禁用基于密码的远程登录

为公用 AMI 使用固定的根密码是一种很快为人知晓的安全风险。甚至于用户在第一次登录后更改密码都会给可能的滥用以可乘之机。

要解决此问题，请对根用户禁用基于密码的远程登录。

对根用户禁用基于密码的远程登录

1. 用文字编辑器打开 /etc/ssh/sshd_config 文件并查找以下行：

```
#PermitRootLogin yes
```

2. 将行更改为：

```
PermitRootLogin without-password
```

若您的发行版不同或您未运行 OpenSSH，此配置文件的位置可能也会不同。若情况如此，请咨询相关文档。

禁用本地根访问

在使用共享 AMI 时，最佳做法是禁用直接根登录。为此，请登录到您正在运行的实例并发出以下命令：

```
[ec2-user ~]$ sudo passwd -l root
```

Note

该命令不影响 sudo 的使用。

删除 SSH 主机密钥对

如果您计划共享源自公用 AMI 的 AMI，请删除 /etc/ssh 中的现有 SSH 主机密钥对。这会促使 SSH 在有人使用您的 AMI 启动实例时生成新的独特 SSH 密钥对，从而提高安全性并降低“中间人”攻击可能性。

删除系统上存在的以下所有密钥文件。

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

您可以使用以下命令安全地删除所有这些文件。

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

Warning

安全删除实用工具（例如 **shred**）可能不会删除存储介质中某个文件的所有副本。文件的隐藏副本可能是由日志文件系统 (包括 Amazon Linux 默认 ext4)、快照、备份、RAID 和临时缓存创建的。有关更多信息，请参阅 **shred** 文档。

Important

如果您忘记从您的公用 AMI 中删除现有 SSH 主机密钥对，我们的例行审核过程会通知您和所有运行您的 AMI 实例的客户存在潜在安全风险。短暂的宽限期过后，我们会将 AMI 标记为私有。

安装公有密钥凭证

配置 AMI 以防止使用密码进行登录后，您必须确保用户能用另一种机制登录。

Amazon EC2 允许用户在启动实例时指定公用–私有密钥对名称。向 `RunInstances` API 调用提供有效的密钥对名称后（或通过命令行 API 工具），公用密钥（Amazon EC2 在至 `CreateKeyPair` 或 `ImportKeyPair` 的调用后在服务器上保留的密钥对的部分)通过针对实例元数据的 HTTP 查询供实例使用。

要通过 SSH 登录，您的 AMI 必须在启动时检索密钥值并将该值附加到 `/root/.ssh/authorized_keys` (或 AMI 上任何其他用户账户的等效密钥)。用户可使用密钥对启动您的 AMI 的实例，并在不需要根密码的情况下进行登录。

很多发行版（包括 Amazon Linux 和 Ubuntu）使用 `cloud-init` 软件包为配置的用户插入公有密钥凭证。如果您的发行版不支持 `cloud-init`，则可以将以下代码添加到系统启动脚本（如 `/etc/rc.local`），以提取您在启动时为根用户指定的公有密钥。

Note

在以下示例中，IP 地址 http://169.254.169.254/ 是链路本地地址，仅从该实例有效。

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

这一点适用于任何用户；无需将其限制为 `root` 用户。

Note

根据此 AMI 进行的实例重新捆绑包括启动时所用的密钥。要防止密钥被包含，您必须清除 (或删除) `authorized_keys` 文件或将此文件排除在重新捆绑之外。

禁用 sshd DNS 检查（可选）

禁用 sshd DNS 检查会稍微减弱您的 sshd 安全性。但是，如果 DNS 解析失败，SSH 的登录仍然有效。如果您未禁用 sshd 检查，DNS 解析失败后会阻止所有的登录。

要禁用 sshd DNS 检查

1. 用文字编辑器打开 `/etc/ssh/sshd_config` 文件并查找以下行：

```
#UseDNS yes
```

2. 将行更改为：

```
UseDNS no
```

> **Note**
>
> 若您的发行版不同或您未运行 OpenSSH，此配置文件的位置也会不同。若情况如此，请咨询相关文档。

保护自己

我们不建议您将敏感数据或软件存储在您共享的任何 AMI 上。启动共享 AMI 的用户可能能够重新捆绑 AMI 并能自行注册 AMI。遵循上述指南可助您避免一些容易被忽视的安全风险：

- 我们建议对 `--exclude` *`directory`* 使用 `ec2-bundle-vol` 选项，以跳过包含您不想在捆绑中包含的机密信息的所有目录和子目录。具体而言，在捆绑映像时，排除所有用户拥有的 SSH 公有/私有密钥对和 SSH `authorized_keys` 文件。Amazon 公有 AMI 会将其存储在 `/root/.ssh`（对于根用户）和 `/home/`*`user_name`*`/.ssh/`（对于常规用户）中。有关更多信息，请参阅ec2-bundle-vol (p. 158)。
- 务必在捆绑前删除 Shell 程序历史记录。如果您在同一 AMI 中多次尝试捆绑上传，Shell 程序历史中将包含访问密钥。以下示例应为从实例内部捆绑前您运行的最后一个命令。

```
[ec2-user ~]$ shred -u ~/.*history
```

> **Warning**
>
> 以上警告中描述的 **`shred`** 的限制在此处也适用。
> 请注意，bash 在退出时会将当前会话的历史记录写入磁盘。如果您在删除 `~/.bash_history` 后注销您的实例，然后重新登录，您将发现 `~/.bash_history` 已重新创建且包含上一会话期间运行的所有命令。
> Bash 以外的其他程序也会将历史记录写入磁盘，请谨慎使用并删除或排除不必要的点文件和点目录。

- 捆绑正在运行的实例需要您的私有密钥和 X.509 证书。将上述密钥和凭证以及其他证书放置到未予捆绑的位置 (如实例存储)。

付费 AMI

付费 AMI 是可以从开发人员处购买的 AMI。

Amazon EC2 与 Amazon Web Services Marketplace 集成，使开发人员能够向使用其 AMI 的其他 Amazon EC2 用户收取费用或提供实例支持。

Amazon Web Services Marketplace 是一个在线商店，您可以从中购买在 Amazon 上运行的软件，包括可用来启动 EC2 实例的 AMI。Amazon Web Services Marketplace AMI 分为各种类别（如开发人员工具），

您可以根据自己的要求查找产品。有关 Amazon Web Services Marketplace 的更多信息，请参阅 Amazon Web Services Marketplace 网站。

从付费 AMI 启动实例与从任何其他 AMI 启动实例的方式相同。不需要额外参数。实例根据 AMI 拥有者设置的费率以及相关 Web 服务的标准使用费 (例如，在 Amazon EC2 中运行 m1.small 实例类型的小时费率) 来收费。还可能需要支付其他税款。付费 AMI 拥有者可以确认是否使用该付费 AMI 启动特定实例。

> **Important**
>
> Amazon DevPay 不再接受新的卖家或产品。Amazon Web Services Marketplace 现在是通过 Amazon 销售软件和服务的统一电子商务平台。有关如何从 Amazon Web Services Marketplace 部署和销售软件的信息，请参阅在 Amazon Marketplace 中出售。Amazon Web Services Marketplace 支持受 Amazon EBS 支持的 AMI。

目录

- 出售您的 AMI (p. 134)
- 查找付费 AMI (p. 134)
- 购买付费 AMI (p. 135)
- 获取实例的产品代码 (p. 135)
- 使用付费支持 (p. 136)
- 付费和支持 AMI 的账单 (p. 136)
- 管理您的 Amazon Web Services Marketplace 订阅 (p. 136)

出售您的 AMI

您可以使用 Amazon Web Services Marketplace 销售 AMI。Amazon Web Services Marketplace 提供组织有序的购物体验。此外，Amazon Web Services Marketplace 还支持 Amazon 功能，如 Amazon EBS-backed AMI、预留实例和竞价型实例。

有关如何在 Amazon Web Services Marketplace 中出售 AMI 的信息，请参阅在 Amazon Marketplace 中出售。

查找付费 AMI

有几种方法可查找可供您购买的 AMI。例如，您可以使用 Amazon Web Services Marketplace、Amazon EC2 控制台或命令行。开发人员自己也可能向您介绍付费 AMI。

使用控制台查找付费 AMI

使用控制台查找付费 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMIs。
3. 对于第一个筛选条件，选择公有映像。
4. 在“Search”（搜索）栏中，选择 Owner alias（所有者别名），再选择 =，然后选择 aws-marketplace。
5. 如果您知道产品代码，请选择 Product code（产品代码），再选择 =，然后输入产品代码。

使用 Amazon Web Services Marketplace 查找付费 AMI

使用 Amazon Web Services Marketplace 查找付费 AMI

1. 打开 Amazon Web Services Marketplace。
2. 在搜索字段中输入操作系统的名称，然后选择搜索按钮（放大镜）。

3. 要进一步确定结果范围，请使用一种类别或筛选条件。
4. 每个产品都使用其产品类型进行标记：AMI 或Software as a Service。

使用 Amazon CLI 查找付费 AMI

您可以使用以下 describe-images (Amazon CLI) 查找付费 AMI。

```
aws ec2 describe-images
    --owners aws-marketplace
```

此命令返回描述每个 AMI 的大量详细信息，包括付费 AMI 的产品代码。describe-images 的输出包含一个用于产品代码的条目，如下所示：

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

如果您知道产品代码，可以按产品代码筛选结果。此示例返回具有指定产品代码的最新 AMI。

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

购买付费 AMI

必须先注册 (购买) 付费 AMI，然后才能使用该 AMI 启动实例。

通常情况下，付费 AMI 的卖方会为您提供 AMI 的相关信息，包括其价格以及购买网站链接。单击该链接时，首先会提示您登录 Amazon，然后可以购买 AMI。

使用控制台购买付费 AMI

可以使用 Amazon EC2 启动向导购买付费 AMI。有关更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。

使用 Amazon Web Services Marketplace 订阅产品

要使用 Amazon Web Services Marketplace，必须拥有 Amazon 账户。要从 Amazon Web Services Marketplace 产品启动实例，必须注册以使用 Amazon EC2 服务，并且必须订阅从中启动实例的产品。可通过两种方式在 Amazon Web Services Marketplace 中订阅产品：

- Amazon Web Services Marketplace 网站：您可以使用一键部署功能快速启动预配置的软件。
- Amazon EC2 启动向导：您可以直接从向导搜索 AMI 并启动实例。有关更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。

获取实例的产品代码

可以使用实例元数据检索实例的 Amazon Web Services Marketplace 产品代码。有关检索元数据的更多信息，请参阅 实例元数据和用户数据 (p. 754)。

要检索产品代码，请使用以下命令：

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

如果实例具有产品代码，则 Amazon EC2 将返回产品代码。

使用付费支持

Amazon EC2 还使开发人员可以为软件（或派生 AMI）提供支持。开发人员可以创建您可注册使用的支持产品。在注册支持产品的过程中，开发人员会为您提供产品代码，您必须将该代码与您自己的 AMI 关联起来。这样，开发人员就能确认您的实例有获取支持的权限。此外，还能确保您在运行产品实例时，按照开发人员指定的产品使用条款付费。

> **Important**
>
> 不能将支持产品用于预留实例。通常情况下，您需按支持产品卖方指定的价格付费。

要将产品代码与您的 AMI 相关联，请使用以下命令之一，其中，ami_id 是 AMI 的 ID，product_code 是产品代码：

- modify-image-attribute (Amazon CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (Amazon Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

您设置产品代码属性后，该属性不能被更改或删除。

付费和支持 AMI 的账单

在每个月月底，您会收到一封电子邮件，邮件里注明了该月因使用任何付费和受支持的 AMI 所产生的信用卡付费金额情况。这个账单与您的常规 Amazon EC2 账单是分开的。有关更多信息，请参阅 Amazon Web Services Marketplace 买家指南中的为产品付费。

管理您的 Amazon Web Services Marketplace 订阅

在 Amazon Web Services Marketplace 网站上，您可以检查订阅详细信息，查看供应商的使用说明，管理订阅等。

检查订阅详细信息

1. 登录 Amazon Web Services Marketplace。
2. 选择 Your Marketplace Account。

3. 选择 Manage your software subscriptions。
4. 会列出当前所有订阅。选择 Usage Instructions 以查看使用产品的特定说明，例如，用于连接到运行中的实例的用户名称。

取消 Amazon Web Services Marketplace 订阅

1. 确保您终止了从订阅运行的所有实例。
   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 在导航窗格中，选择实例。
   c. 选择相应实例，然后依次选择 Instance state（实例状态）、Terminate instance（终止实例）。
   d. 当系统提示您确认时，选择终止。
2. 登录到 Amazon Web Services Marketplace，选择 Your Marketplace Account（您的 Marketplace 账户），然后选择 Manage your software subscriptions（管理您的软件订阅）。
3. 选择 Cancel subscription。会提示您确认取消。

   Note

   取消了订阅之后，您无法再从该 AMI 启动任何实例。要再次使用该 AMI，您需要在 Amazon Web Services Marketplace 网站上或通过 Amazon EC2 控制台中的启动向导重新订阅它。

AMI 周期

您可以创建自己的 AMI 并对其进行复制、备份和维护，直到准备弃用或取消注册为止。

目录

- 创建 AMI (p. 137)
- 修改 AMI (p. 172)
- 复制 AMI (p. 172)
- 使用 S3 存储和还原 AMI (p. 178)
- 弃用 AMI (p. 183)
- 注销您的 AMI (p. 188)
- 从回收站恢复 AMI (p. 193)
- 自动化 EBS 支持的 AMI 生命周期 (p. 196)

创建 AMI

您可以创建 Amazon EBS 支持的 Linux AMI 和实例存储支持的 AMI。

主题

- 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)
- 创建由实例存储支持的 Linux AMI (p. 142)

有关如何创建 Windows AMI 的信息，请参阅创建自定义 Windows AMI。

创建一个由 Amazon EBS 支持的 Linux AMI

要创建 Amazon EBS 支持的 Linux AMI，请通过从 Amazon EBS 支持的现有 Linux AMI 启动的实例开始进行。这可以是您从 Amazon Web Services Marketplace 获得的 AMI、您使用 Amazon Server Migration

Service 或 VM Import/Export 创建的 AMI 或您可以访问的任何其他 AMI。根据您的需要自定义实例后，创建并注册新的 AMI，用它来启动具有这些自定义项的新实例。

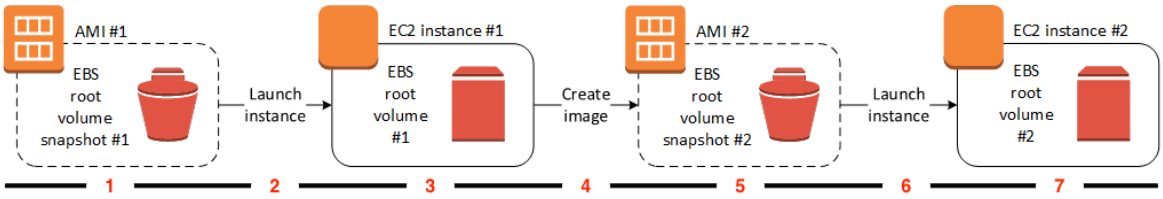
下述过程适用于由加密的 Amazon Elastic Block Store (Amazon EBS) 卷（包括根卷）支持的 Amazon EC2 实例，也适用于未加密卷。

用于由实例存储支持的 AMIs 的 AMI 创建过程有些不同。有关 Amazon EBS 支持的实例和实例存储支持的实例之间的差别，以及如何确定实例的根设备类型的信息，请参阅 根设备存储 (p. 103)。有关创建实例存储支持的 Linux AMI 的信息，请参阅 创建由实例存储支持的 Linux AMI (p. 142)。

有关创建 Amazon EBS 支持的 Windows AMI 的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的创建 Amazon EBS 支持的 Windows AMI。

创建 Amazon EBS-backed AMI 的概述

以下图表概述了从运行中的 EC2 实例创建 Amazon EBS-backed AMI 的流程：从现有 AMI 开始，启动实例，自定义该实例，从该实例创建新 AMI，并最终启动新 AMI 的实例。图中的数字与以下描述中的数字匹配。



1 – AMI #1：从现有的 AMI 开始

查找类似于您要创建的 AMI 的现有 AMI。这可以是您从 Amazon Web Services Marketplace 获得的 AMI、您使用 Amazon Server Migration Service 或 VM Import/Export 创建的 AMI 或您可以访问的任何其他 AMI。您将根据自己的需求自定义此 AMI。

在图中，EBS 根卷快照 #1 表示 AMI 为 Amazon EBS-backed AMI，并且有关根卷的信息存储在此快照中。

2 – 从现有 AMI 启动实例

配置 AMI 的方法是从您希望作为新 AMI 基础的 AMI 启动实例，然后自定义该实例（在图中以 3 表示）。然后，您将创建一个包含自定义项的新 AMI（在图中以 4 表示）。

3 – EC2 实例 #1：自定义实例

连接到您的实例并根据您的需求对其进行自定义。您的新 AMI 将包含这些自定义项。

您可以对您的实例执行以下任何操作，以便自定义该实例：

- 安装软件和应用程序
- 复制数据
- 通过删除临时文件、对您的硬盘进行碎片整理以及将可用空间清零来缩短启动时间
- 附加其他 EBS 卷

4 – 创建映像

当您从实例中创建 AMI 时，Amazon EC2 先切断实例的电源再创建 AMI，以确保创建过程中实例上的所有内容均停止并保持一致状态。如果您确信您的实例处于适合 AMI 创建的一致状态，则可以告知 Amazon EC2 不断电和重启实例。一些文件系统 (例如 XFS) 可以冻结和解冻活动，因此能在不重启实例的情况下安全创建映像。

在 AMI 创建过程中，Amazon EC2 会创建您实例的根卷和附加到您实例的任何其他 EBS 卷的快照。在注销 AMI (p. 188) 并删除快照之前，您需要支付快照的费用。如果有任何附加到实例的卷进行了加密，则新 AMI 只会在支持 Amazon EBS 加密 (p. 1504)的实例上成功启动。

根据卷的大小，可能需要几分钟才能完成 AMI 创建过程 (有时长达 24 小时)。您可能会发现先创建卷的快照，然后再创建 AMI 后会更高效。这样，创建 AMI 时就只需创建小的增量快照，且创建过程完成得更快 (快照创建的总时间保持不变)。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。

5 – AMI #2：新 AMI

该过程完成之后，您便具有从实例的根卷创建的新 AMI 和快照（快照 #2）。如果除了根设备卷之外，您还向实例添加了实例存储卷或 EBS 卷，则新 AMI 的块储存设备映射包含这些卷的信息。

Amazon EC2 自动为您注册 AMI。

6 – 从新 AMI 启动实例

您可以使用新 AMI 启动实例。

7 – EC2 实例 #2：新实例

当您使用新 AMI 启动实例时，Amazon EC2 会使用快照为实例的根卷创建新 EBS 卷。如果您在自定义实例时添加了实例存储卷或 EBS 卷，则新 AMI 的块储存设备映射包含这些卷的信息，并且您从新 AMI 启动的实例的块储存设备映射自动包含这些卷的信息。新实例的块储存设备映射中指定的实例存储卷是新的，不包含用于创建 AMI 的实例的实例存储卷中的任何数据。EBS 卷上的数据会持久保留。有关更多信息，请参阅块设备映射 (p. 1615)。

当您从由 EBS 支持的 AMI 创建新实例时，应该先初始化其根卷及任何额外的 EBS 存储，然后再将其投入生产。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。

从实例创建 Linux AMI

可以使用 Amazon Web Services Management Console 或命令行创建 AMI。

Console

使用控制台从实例创建 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择要从中创建 AMI 的实例，然后选择 Actions（操作）、Image and templates（映像和模板）、Create image（创建映像）。

   Tip

   如果该选项处于禁用状态，则表明您的实例不是由 Amazon EBS 支持的实例。
4. 在 Create image（创建映像）页面上，请指定以下信息：

   a. 对于 Image name（映像名称），请输入映像的唯一名称，最多 127 个字符。
   b. 对于 Image description（映像描述），输入映像的可选描述，最多 255 个字符。
   c. 对于 No reboot（不重启），请保持 Enable（启用）复选框处于清除状态（默认），或将其选中。

      - 如果清除 Enable（启用），Amazon EC2 创建新 AMI 时，会重新启动实例，以便其可以在数据处于静态状态时拍摄附加卷的快照，以确保状态的一致性。
      - 如果选择 Enable（启用），Amazon EC2 创建新 AMI 时，不会关闭和重启实例。

      Warning

      如果您选择启用 No reboot（不重启）选项，则我们无法保证所创建映像的文件系统完整性。
   d. Instance volumes（实例卷）– 您可以修改根卷，并添加其他 Amazon EBS 和实例存储卷，如下所示：

i. 根卷在第一行中定义。

- 要更改根卷的大小，请在 Size (尺寸) 中输入所需的值。
- 如果选择 Delete on Termination (终止时删除)，则当您终止从此 AMI 创建的实例时，将删除 EBS 卷。如果取消选择 Delete on Termination (终止时删除)，则当您终止实例时，不会删除 EBS 卷。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。

ii. 要添加 EBS 卷，请选择 Add New Volume（添加新卷）（这将添加一个新行）。对于存储类型，选择 EBS，并填写行中的字段。当您从新的 AMI 启动实例时，额外的卷会自动附加到该实例。您必须格式化并挂载空卷。您必须挂载基于快照的卷。

iii. 要添加实例存储卷，请参阅 将实例存储卷添加到 AMI (p. 1593)。当您从新的 AMI 启动实例时，这些额外的卷会自动初始化并挂载。这些卷不包含您的 AMI 所基于的运行实例的实例存储卷上的数据。

e. 准备好创建 AMI 时，选择 Create image（创建映像）。

5. 若要在创建 AMI 时查看其状态，请执行以下操作：

a. 在导航窗格中，选择 AMIs。
b. 将筛选条件设置为 Owned by me（我拥有的），然后在列表中查找您的 AMI。

最初，状态是 `pending`，但过几分钟就会变成 `available`。

6. （可选）若要查看为新 AMI 创建的快照，请执行以下操作：

a. 记下您在上一步骤中找到的 AMI ID。
b. 在导航窗格中，选择快照。
c. 将筛选条件设置为 Owned by me（我拥有的），然后在 Description（描述）列中查找具有新 AMI ID 的快照。

您从此 AMI 启动实例时，Amazon EC2 使用此快照创建其根设备卷。

Amazon CLI

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-image (Amazon CLI)
- New-EC2Image (Amazon Tools for Windows PowerShell)

从快照创建 Linux AMI

如果您有实例的根设备卷的快照，则可以使用 Amazon Web Services Management Console 或命令行从此快照创建 AMI。

New console

使用控制台从快照创建 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择从中创建 AMI 的快照并选择 Actions（操作）、Create image from snapshot（从快照创建映像）。
4. 对于 Image name（镜像名称），请输入镜像的描述性名称。
5. 对于 Description（描述），请输入镜像的简短描述。
6. 对于 Architecture（架构），请选择镜像架构。对于 32 位，选择 i386；对于 64 位，选择 x86_64；对于 64 位 ARM，选择 ARM64；对于 64 位 macOS，选择 x86_64。

7. 对于 Root device name（根设备名称），请输入要用于根设备卷的设备名称。有关更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。
8. 对于 Virtualization type（虚拟化类型），请选择从此 AMI 启动的实例要使用的虚拟化类型。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。
9. （仅适用于半虚拟化）对于 Kernel ID（内核 ID），选择镜像的操作系统内核。如果您使用的是实例的根设备卷快照，请选择与原始实例相同的内核 ID。如果您不确定，请使用默认内核。
10. （仅适用于半虚拟化）对于 RAM disk ID（RAM 磁盘 ID），请选择镜像的 RAM 磁盘。如果您选择了一个特定内核，则您可能需要选择带有可支持该内核的驱动程序的某个特定 RAM 磁盘。
11. （可选）在 Block device mappings（块储存设备映射）部分中，自定义根卷并添加其它数据卷。

    对于每个卷，您可以指定大小、类型、性能特征、终止时删除的行为以及加密状态。对于根卷，其大小不能小于快照的大小。
12. 选择创建映像。

Old console

使用控制台从快照创建 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 Elastic Block Store 下，选择 Snapshots。
3. 依次选择快照、Actions 和 Create Image。
4. 在 Create Image from EBS Snapshot 对话框中，填写与创建 AMI 相关的字段，然后选择 Create。如果要重新创建父实例，请选择与父实例相同的选项。

   - Architecture：对 32 位选择 i386，对 64 位选择 x86_64。
   - Root device name：输入相应的根卷名称。有关更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。
   - Virtualization type：选择是从此 AMI 使用半虚拟化 (PV) 还是硬件虚拟机 (HVM) 虚拟化启动实例。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。
   - (仅限 PV 虚拟化类型) Kernel ID 和 RAM disk ID：从列表中选择 AKI 和 ARI。如果选择默认 AKI 或不选择 AKI，则您每次启动使用此 AMI 实例时，都必须指定 AKI。此外，如果默认 AKI 与实例不兼容，对您的实例进行的运行状况检查可能会失败。
   - （可选）Block Device Mappings：添加卷或扩展 AMI 根卷的默认大小。有关调整实例上的文件系统大小以扩展卷的更多信息，请参阅调整卷大小后扩展 Linux 文件系统 (p. 1500)。

Amazon CLI

使用命令行从快照创建 AMI

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- register-image (Amazon CLI)
- Register-EC2Image (Amazon Tools for Windows PowerShell)

从您创建的 AMI 启动实例

您可以从通过实例或快照创建的 AMI 启动实例。

从 AMI 启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，在映像下选择 AMI。
3. 将筛选条件设置为我拥有的，然后选择您的 AMI。

4. 选择 Launch instance from AMI（从 AMI 启动实例）（新控制台）或 Actions（操作）、Launch（启动）（旧控制台）。
5. 在启动实例向导中接受默认值或指定自定义值。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

创建由实例存储支持的 Linux AMI

您在启动实例时指定的 AMI 决定根设备卷的类型

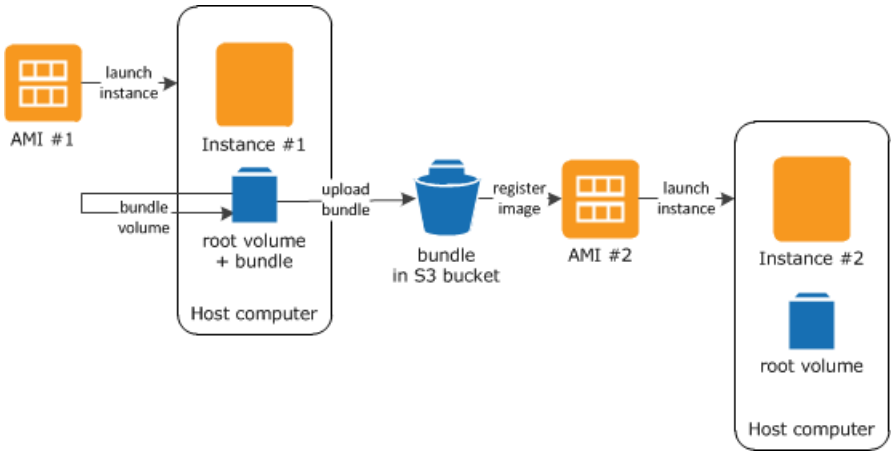
要创建由实例存储支持的 Linux AMI，请通过从由实例存储支持的现有 Linux AMI 启动的实例开始进行。根据您自己的需要自定义该实例之后，请捆绑卷并注册新 AMI，您可以使用该 AMI 启动具有这些自定义项的新实例。

> **Important**
>
> 只有以下实例类型支持将实例存储卷作为根设备：C3、D2、G2、I2、M3 和 R3。

用于 Amazon EBS-backed AMI 的 AMI 创建过程有所不同。有关 Amazon EBS 支持的实例和实例存储支持的实例之间的差别，以及如何确定实例的根设备类型的更多信息，请参阅根设备存储 (p. 103)。如果您需要创建 Amazon EBS 支持的 Linux AMI，请参阅创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。

由实例存储支持的 AMI 的创建过程概述

下图总结了从由实例存储支持的实例创建 AMI 的过程。



首先，从类似于您要创建的 AMI 的 AMI 启动实例。您可以连接到您的实例并进行自定义。根据您的需要设置好实例后，您可以捆绑它。完成捆绑过程需要几分钟的时间。该过程完成之后，您会得到一个捆绑，该捆绑由映像清单 (`image.manifest.xml`) 以及包含根卷模板的文件 (`image.part.xx`) 组成。接下来，将该捆绑上传到 Amazon S3 存储桶，然后注册您的 AMI。

> **Note**
>
> 要将对象上载到实例存储支持的 Linux AMI 的 S3 存储桶，必须为该存储桶启用 ACL。否则，Amazon EC2 将无法在要上载的对象上设置 ACL。如果您的目标存储桶使用存储桶拥有者强制执行的 S3 对象所有权设置，则这将不起作用，因为 ACL 已禁用。有关更多信息，请参阅使用 S3 对象所有权控制已上载对象的所有权。

当您使用新 AMI 启动实例时，我们会使用您上传到 Amazon S3 的捆绑为实例创建根卷。Amazon S3 中的捆绑使用的存储空间会使您的账户产生费用，直到将其删除。有关更多信息，请参阅注销您的 AMI (p. 188)。

如果除了根设备卷之外，您还向实例添加实例存储卷，则新 AMI 的块储存设备映射包含这些卷的信息，并且您从新 AMI 启动的实例的块储存设备映射自动包含这些卷的信息。有关更多信息，请参阅块设备映射 (p. 1615)。

先决条件

必须先完成以下任务才能创建 AMI：

- 安装 AMI 工具。有关更多信息，请参阅设置 AMI 工具 (p. 143)。
- 安装 Amazon CLI。有关更多信息，请参阅开始设置 Amazon Command Line Interface。
- 请确保您具有用于捆绑的 S3 存储桶，并且您的存储桶已启用 ACL。

  要创建 S3 存储桶，请打开 Amazon S3 控制台，然后单击 Create Bucket（创建存储桶）。或者，您可以使用 Amazon CLI mb 命令。
- 确保您拥有您的 Amazon 账户 ID。有关更多信息，请参阅 Amazon General Reference 中的Amazon账户标识符。
- 确保您拥有凭证以使用 Amazon CLI。有关更多信息，请参阅《Amazon Account Management 参考指南》中的 Amazon 账户最佳实践。
- 确保您拥有 X.509 证书以及相应的私有密钥。
  - 如果您需要创建 X.509 证书，请参阅管理签名证书 (p. 145)。X.509 证书和私有密钥用于加密和解密您的 AMI。
  - [中国（北京）] 使用 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem` 证书。
  - [Amazon GovCloud（美国西部）] 使用 `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` 证书。
- 连接到您的 实例并对其进行自定义。例如，您可以安装软件和应用程序、复制数据、删除临时文件及修改 Linux 配置。

任务

- 设置 AMI 工具 (p. 143)
- 通过实例存储支持的 Amazon Linux 实例创建 AMI (p. 146)
- 通过实例存储支持的 Ubuntu 实例创建 AMI (p. 148)
- 将实例存储支持的 AMI 转换为 Amazon EBS-backed AMI (p. 152)

设置 AMI 工具

您可使用 AMI 工具创建和管理实例存储支持的 Linux AMIs。要使用这些工具，必须在 Linux 实例上安装它们。AMI 工具可作为 RPM 提供，也为不支持 RPM 的 Linux 发行版提供 .zip 格式的文件。

使用 RPM 设置 AMI 工具

1. 使用您的 Linux 发行版的程序包管理器 (如 yum) 安装 Ruby。例如：

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. 使用 wget 或 curl 等工具下载 RPM 文件。例如：

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. 使用以下命令验证 RPM 文件的签名：

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

   上述命令应指示该文件的 SHA1 和 MD5 哈希值是 `OK`。如果该命令指示这些哈希值是 `NOT OK`，请使用以下命令查看该文件的标头 SHA1 和 MD5 哈希值：

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

然后，将您的文件的标头 SHA1 和 MD5 哈希值与以下经验证的 AMI 工具哈希值进行比较，以确认文件的真实性：

- 标头 SHA1：a1f662d6f25f69871104e6a62187fa4df508f880
- MD5：9faff05258064e2f7909b66142de6782

如果您的文件的标头 SHA1 和 MD5 哈希值与经验证的 AMI 工具哈希值相匹配，请继续下一步。

4. 使用以下命令安装 RPM：

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. 使用 ec2-ami-tools-version (p. 156) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ ec2-ami-tools-version
```

Note

如果您收到一个加载错误，例如“cannot load such file -- ec2/amitools/version (LoadError)”(无法加载此类文件 -- ec2/amitools/version (LoadError))，请完成下一步骤以将 AMI 工具安装的位置添加到 RUBYLIB 路径。

6. （可选）如果您在上一步中收到了错误，则将您的 AMI 工具的安装位置添加到您的 RUBYLIB 路径中。

   a. 运行以下命令以确定要添加的路径。

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

   在以上示例中，以前加载错误中的丢失文件位于 /usr/lib/ruby/site_ruby 和 /usr/lib64/ruby/site_ruby。

   b. 将上一步的位置添加到您的 RUBYLIB 路径中。

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
```

   c. 使用 ec2-ami-tools-version (p. 156) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ ec2-ami-tools-version
```

使用 .zip 文件设置 AMI 工具

1. 使用您的 Linux 发行版的程序包管理器安装 Ruby 并解压缩，例如 apt-get。例如：

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. 使用 wget 或 curl 等工具下载 .zip 文件。例如：

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. 将文件解压缩到合适的安装目录，如 /usr/local/ec2。

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

请注意，.zip 文件包含文件夹 ec2-ami-tools-*x.x.x*，其中 *x.x.x* 是工具的版本号（例如，ec2-ami-tools-1.5.7）。

4. 将 EC2_AMITOOL_HOME 环境变量设置为工具的安装目录。例如：

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. 将工具添加到您的 PATH 环境变量。例如：

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. 您可以使用 ec2-ami-tools-version (p. 156) 命令验证您的 AMI 工具安装。

```
[ec2-user ~]$ ec2-ami-tools-version
```

管理签名证书

AMI 工具中的某些命令需要签名证书 (也称为 X.509 证书)。您必须创建证书，然后将其上传到 Amazon。例如，您可以使用第三方工具 (例如 OpenSSL) 创建证书。

创建签名证书

1. 安装和配置 OpenSSL。
2. 使用 openssl genrsa 命令创建私有密钥，并将输出保存到 .pem 文件。我们建议您创建 2048 或 4096 位 RSA 密钥。

```
openssl genrsa 2048 > private-key.pem
```

3. 使用 openssl req 命令生成证书。

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

要将证书上传到 Amazon，请使用 upload-signing-certificate 命令。

```
aws iam upload-signing-certificate --user-name user-name --certificate-body file://path/to/
certificate.pem
```

要列出用户的证书，请使用 list-signing-certificates 命令：

```
aws iam list-signing-certificates --user-name user-name
```

要对用户禁用或重新启用签名证书，请使用 update-signing-certificate 命令。以下命令可禁用证书：

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

要删除证书，请使用 delete-signing-certificate 命令：

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX704BEXAMPLE
```

通过实例存储支持的实例创建 AMI

下列步骤用于从实例存储支持的实例创建实例存储支持的 AMI。在开始之前，请您务必阅读先决条件 (p. 143)。

主题

- 通过实例存储支持的 Amazon Linux 实例创建 AMI (p. 146)
- 通过实例存储支持的 Ubuntu 实例创建 AMI (p. 148)

通过实例存储支持的 Amazon Linux 实例创建 AMI

本节介绍如何通过 Amazon Linux 实例创建 AMI。以下过程可能不适用于运行其他 Linux 发行版的实例。有关特定于 Ubuntu 的过程，请参阅 通过实例存储支持的 Ubuntu 实例创建 AMI (p. 148)。

准备使用 AMI 工具 (仅限 HVM 实例)

1. AMI 工具需要有 GRUB Legacy，才能正确启动。使用以下命令安装 GRUB：

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. 使用以下命令安装分区管理程序包：

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

通过实例存储支持的 Amazon Linux 实例创建 AMI

此过程假设您满足先决条件 (p. 143)中的先决条件。

1. 将您的凭证上传到您的实例。我们使用这些凭证确保只有您和 Amazon EC2 才能访问您的 AMI。

   a. 在您的实例上为凭证创建临时目录，如下所示：

      ```
      [ec2-user ~]$ mkdir /tmp/cert
      ```

      这使您可以从创建的映像中排除您的凭证。

   b. 使用安全复制工具 (如 scp (p. 651)) 将 X.509 证书和对应的私有密钥从您的计算机复制到实例上的 /tmp/cert 目录。以下 -i *my-private-key*.pem 命令中的 scp 选项是您用于通过 SSH 连接到实例的私有密钥，而不是 X.509 私有密钥。例如：

      ```
      you@your_computer:~ $ scp -i my-private-key.pem /
      path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
      path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
      user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
      pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
      cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
      ```

      此外，由于这些是纯文本文件，所以您可以在文本编辑器中打开证书和密钥，并将其内容复制到 /tmp/cert 中的新文件。

2. 通过从您的实例内部运行 ec2-bundle-vol (p. 158) 命令，准备捆绑包以便上传到 Amazon S3。请务必指定 -e 选项以排除用于存储您的凭证的目录。默认情况下，捆绑过程不包括可能包含敏感

信息的文件。这些文件包括 *.sw、*.swo、*.swp、*.pem、*.priv、*id_rsa*、*id_dsa* *.gpg、*.jks、*/.ssh/authorized_keys 和 */.bash_history。要包括所有这些文件，请使用 --no-filter 选项。要包括其中部分文件，请使用 --include 选项。

Important

默认情况下，AMI 捆绑过程在表示根卷的 /tmp 目录中创建经过压缩和加密的文件集合。如果您在 /tmp 中没有足够的可用磁盘空间来存储捆绑，则需要使用 -d */path/to/bundle/storage* 选项指定不同的位置来存储捆绑。某些实例会在 /mnt 或 /media/ephemeral0 上挂载您可以使用的短暂存储，您也可以创建 (p. 1344)、附上 (p. 1347)和挂载 (p. 1348)新 Amazon Elastic Block Store（Amazon EBS）卷来存储捆绑包。

a. 您必须以根用户身份运行 ec2-bundle-vol 命令。对于大部分命令，您可以使用 sudo 获取提升的权限，但是在这种情况下，您应运行 sudo -E su 以保留环境变量。

```
[ec2-user ~]$ sudo -E su
```

请注意，在 bash 提示符下现在将您标识为根用户，并且美元符号已替换为哈希标签，表示您现在处于 root Shell 中：

```
[root ec2-user]#
```

b. 要创建 AMI 捆绑，请如下所示运行 ec2-bundle-vol (p. 158) 命令：

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

Note

对于中国（北京）和 Amazon GovCloud（美国西部）区域，请使用 --ec2cert 参数并根据先决条件 (p. 143)指定证书。

创建映像可能需要几分钟时间。该命令完成后，您的 /tmp (非默认) 目录会包含捆绑 (image.manifest.xml 以及多个 image.part.*xx* 文件)。

c. 从 root Shell 退出。

```
[root ec2-user]# exit
```

3. （可选）要添加更多实例存储卷，请在 image.manifest.xml 文件中为您的 AMI 编辑块储存设备映射。有关更多信息，请参阅块设备映射 (p. 1615)。

a. 创建 image.manifest.xml 文件的备份。

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. 重新设置 image.manifest.xml 文件的格式，使其更易于阅读和编辑。

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. 使用文本编辑器编辑 image.manifest.xml 中的块储存设备映射。以下示例显示了 ephemeral1 实例存储卷的一个新条目。

Note

有关排除的文件的列表，请参阅ec2-bundle-vol (p. 158)。

```
<block_device_mapping>
  <mapping>
    <virtual>ami</virtual>
    <device>sda</device>
  </mapping>
  <mapping>
    <virtual>ephemeral0</virtual>
    <device>sdb</device>
  </mapping>
  <mapping>
    <virtual>ephemeral1</virtual>
    <device>sdc</device>
  </mapping>
  <mapping>
    <virtual>root</virtual>
    <device>/dev/sda1</device>
  </mapping>
</block_device_mapping>
```

d. 保存 `image.manifest.xml` 文件并退出文本编辑器。

4. 要将捆绑上传到 Amazon S3，请如下所示运行 ec2-upload-bundle (p. 168) 命令。

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

Important

要在US East (N. Virginia)之外的区域中注册 AMI，则必须指定带 `--region` 选项的目标区域和目标区域中已存在的存储桶路径或可在目标区域中创建的唯一存储桶路径。

5. （可选）将捆绑上传到 Amazon S3 之后，您可以使用以下 `/tmp` 命令将捆绑从实例上的 rm 目录中删除：

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

Important

如果您在 `-d` */path/to/bundle/storage* 中使用 Step 2 (p. 146) 选项指定了路径，请使用该路径，而不是 `/tmp`。

6. 要注册您的 AMI，请按以下所示运行 register-image 命令。

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-
type hvm
```

Important

如果您先前为 ec2-upload-bundle (p. 168) 命令指定了某个区域，请为该命令再次指定该区域。

通过实例存储支持的 Ubuntu 实例创建 AMI

本节介绍如何在将实例存储卷作为根卷的情况下从 Ubuntu Linux 实例创建 AMI。以下过程可能不适用于运行其他 Linux 发行版的实例。有关特定于 Amazon Linux 的过程，请参阅 通过实例存储支持的 Amazon Linux 实例创建 AMI (p. 146)。

准备使用 AMI 工具 (仅限 HVM 实例)

AMI 工具需要有 GRUB Legacy，才能正确启动。不过，Ubuntu 配置为使用 GRUB 2。您必须检查您的实例是否使用传统 GRUB，如果未使用，您需要安装并配置它。

HVM 实例还需要安装分区工具，以便 AMI 工具可以正常工作。

1. GRUB Legacy（版本 0.9*x* 或更早版本）必须安装在您的实例上。检查传统 GRUB 是否存在，并根据需要安装它。

   a. 检查您的 GRUB 安装版本。

   ```
   ubuntu:~$ grub-install --version
   grub-install (GRUB) 1.99-21ubuntu3.10
   ```

   在该示例中，GRUB 版本高于 0.9*x*，因此您必须安装传统 GRUB。继续执行Step 1.b (p. 149)。如果传统 GRUB 已存在，您可以跳到Step 2 (p. 149)。

   b. 使用以下命令安装 grub 程序包。

   ```
   ubuntu:~$ sudo apt-get install -y grub
   ```

2. 使用您的发行版的软件包管理器安装以下分区管理软件包。

   - gdisk（此软件包在某些发行版中可能名为 gptfdisk）
   - kpartx
   - parted

   使用以下命令。

   ```
   ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
   ```

3. 检查您的实例的内核参数。

   ```
   ubuntu:~$ cat /proc/cmdline
   BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
   aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
   ```

   请注意内核和根设备参数之后的选项：ro、console=ttyS0 和 xen_emul_unplug=unnecessary。您的选项可能有所不同。

4. 检查 /boot/grub/menu.lst 中的内核条目。

   ```
   ubuntu:~$ grep ^kernel /boot/grub/menu.lst
   kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
   kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
   kernel  /boot/memtest86+.bin
   ```

   请注意，console 参数指向 hvc0 而不是 ttyS0，并且缺少 xen_emul_unplug=unnecessary 参数。同样，您的选项可能有所不同。

5. 使用您常用的文本编辑器（如 /boot/grub/menu.lst 或 vim）编辑 nano 文件，以更改控制台并将先前确定的参数添加到启动条目中。

   ```
   title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
   root            (hd0)
   kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
    ro console=ttyS0 xen_emul_unplug=unnecessary
   ```

```
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
 single console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, memtest86+
root            (hd0)
kernel          /boot/memtest86+.bin
```

6. 验证您的内核条目现在是否包含正确参数。

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
 xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
 console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7. [仅适用于 Ubuntu 14.04 及更高版本] 从 Ubuntu 14.04 开始，实例存储支持的 Ubuntu AMI 使用 GPT 分区表和装载在 `/boot/efi` 中的单独 EFI 分区。ec2-bundle-vol 命令不会捆绑此引导分区，因此您需要为 EFI 分区的 `/etc/fstab` 条目添加注释，如下所示。

```
LABEL=cloudimg-rootfs   /        ext4   defaults        0 0
#LABEL=UEFI     /boot/efi       vfat    defaults        0 0
/dev/xvdb       /mnt    auto    defaults,nobootwait,comment=cloudconfig 0       2
```

通过实例存储支持的 Ubuntu 实例创建 AMI

此过程假设您满足先决条件 (p. 143)中的先决条件。

1. 将您的凭证上传到您的实例。我们使用这些凭证确保只有您和 Amazon EC2 才能访问您的 AMI。

   a. 在您的实例上为凭证创建临时目录，如下所示：

   ```
   ubuntu:~$ mkdir /tmp/cert
   ```

   这使您可以从创建的映像中排除您的凭证。

   b. 使用安全复制工具（如 scp (p. 651)）将您的 X.509 证书和私有密钥从您的计算机复制到您实例上的 `/tmp/cert` 目录。以下 `-i my-private-key.pem` 命令中的 scp 选项是您用于通过 SSH 连接到实例的私有密钥，而不是 X.509 私有密钥。例如：

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   此外，由于这些是纯文本文件，所以您可以在文本编辑器中打开证书和密钥，并将其内容复制到 `/tmp/cert` 中的新文件。

2. 通过从您的实例内运行 ec2-bundle-vol (p. 158) 命令，准备捆绑包以便上传到 Amazon S3。请务必指定 `-e` 选项以排除用于存储您的凭证的目录。默认情况下，捆绑过程不包括可能包含敏感信息的文件。这些文件包括 `*.sw`、`*.swo`、`*.swp`、`*.pem`、`*.priv`、`*id_rsa*`、`*id_dsa*`

.gpg、.jks、*/.ssh/authorized_keys 和 */.bash_history。要包括所有这些文件，请使用 --no-filter 选项。要包括其中部分文件，请使用 --include 选项。

Important

默认情况下，AMI 捆绑过程在表示根卷的 /tmp 目录中创建经过压缩和加密的文件集合。如果您在 /tmp 中没有足够的可用磁盘空间来存储捆绑，则需要使用 -d */path/to/bundle/storage* 选项指定不同的位置来存储捆绑。某些实例会在 /mnt 或 /media/ephemeral0 上挂载您可以使用的短暂存储，您也可以创建 (p. 1344)、附上 (p. 1347)和挂载 (p. 1348)新 Amazon Elastic Block Store（Amazon EBS）卷来存储捆绑包。

a. 您必须以根用户身份运行 ec2-bundle-vol 命令。对于大部分命令，您可以使用 sudo 获取提升的权限，但是在这种情况下，您应运行 sudo -E su 以保留环境变量。

```
ubuntu:~$ sudo -E su
```

请注意，在 bash 提示符下现在将您标识为根用户，并且美元符号已替换为哈希标签，表示您现在处于 root Shell 中：

```
root@ubuntu:#
```

b. 要创建 AMI 捆绑，请如下所示运行 ec2-bundle-vol (p. 158) 命令。

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
 -c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r
 x86_64 -e /tmp/cert --partition gpt
```

Important

对于 Ubuntu 14.04 及更高版本的 HVM 实例，请添加 --partition mbr 标志以正确捆绑启动指令；否则，新创建的 AMI 不会启动。

创建映像可能需要几分钟时间。该命令完成后，您的 tmp 目录会包含捆绑 (image.manifest.xml 以及多个 image.part.*xx* 文件)。

c. 从 root Shell 退出。

```
root@ubuntu:# exit
```

3. （可选）要添加更多实例存储卷，请在 image.manifest.xml 文件中为您的 AMI 编辑块储存设备映射。有关更多信息，请参阅块设备映射 (p. 1615)。

a. 创建 image.manifest.xml 文件的备份。

```
ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

b. 重新设置 image.manifest.xml 文件的格式，使其更易于阅读和编辑。

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
image.manifest.xml
```

c. 使用文本编辑器编辑 image.manifest.xml 中的块储存设备映射。以下示例显示了 *ephemeral1* 实例存储卷的一个新条目。

```
    <block_device_mapping>
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
```

```
    </mapping>
    <mapping>
      <virtual>ephemeral0</virtual>
      <device>sdb</device>
    </mapping>
    <mapping>
      <virtual>ephemeral1</virtual>
      <device>sdc</device>
    </mapping>
    <mapping>
      <virtual>root</virtual>
      <device>/dev/sda1</device>
    </mapping>
  </block_device_mapping>
```

d. 保存 `image.manifest.xml` 文件并退出文本编辑器。

4. 要将捆绑上传到 Amazon S3，请如下所示运行 ec2-upload-bundle (p. 168) 命令。

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

Important

如果您打算在US East (N. Virginia)之外的区域中注册 AMI，则必须指定带 `--region` 选项的目标区域和目标区域中已存在的存储桶路径或可在目标区域中创建的唯一存储桶路径。

5. （可选）将捆绑上传到 Amazon S3 之后，您可以使用以下 `/tmp` 命令将捆绑从实例上的 rm 目录中删除：

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

Important

如果您在 `-d` */path/to/bundle/storage* 中指定了带有 Step 2 (p. 150) 选项的路径，请在下面使用该路径，而不是 `/tmp`。

6. 要注册您的 AMI，请按以下所示运行 register-image Amazon CLI 命令。

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-
type hvm
```

Important

如果您先前为 ec2-upload-bundle (p. 168) 命令指定了某个区域，请为该命令再次指定该区域。

7. [仅适用于 Ubuntu 14.04 及更高版本] 在 `/etc/fstab` 中取消对 EFI 条目的注释；否则，正在运行的实例不会重启。

将实例存储支持的 AMI 转换为 Amazon EBS-backed AMI

您可以将拥有的实例存储支持的 Linux AMI 转换为 Amazon EBS 支持的 Linux AMI。

Important

您无法将实例存储支持的 Windows AMI 转换为 Amazon EBS 支持的 Windows AMI，并且无法转换您不拥有的 AMI。

将由实例存储支持的 AMI 转换为 Amazon EBS-backed AMI

1. 从 Amazon EBS-backed AMI 启动 Amazon Linux 实例。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。Amazon Linux 实例预先安装了 Amazon CLI 和 AMI 工具。
2. 上传您用于将实例存储支持的 AMI 捆绑到实例的 X.509 私有密钥。我们使用此密钥确保只有您和 Amazon EC2 才能访问您的 AMI。

   a. 在您的实例上为 X.509 私有密钥创建临时目录，如下所示：

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   b. 使用安全复制工具 (如 /tmp/certscp) 将您的 X.509 私有密钥从您的计算机复制到您实例上的 (p. 651) 目录。以下命令中的 *my-private-key* 参数是您用于通过 SSH 连接到实例的私有密钥。例如：

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   ```

3. 配置环境变量以使用 Amazon CLI。有关更多信息，请参阅创建密钥对。

   a. （推荐）为您的 Amazon 访问密钥、私有密钥和会话令牌设置环境变量。

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. 为您的 Amazon 访问密钥和私有密钥设置环境变量。

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. 为新 AMI 准备 Amazon Elastic Block Store (Amazon EBS) 卷。

   a. 使用 create-volume 命令在您的实例所在的同一可用区中创建空 EBS 卷。记下命令输出中的卷 ID。

   > **Important**
   >
   > 此 EBS 卷不小于原始实例存储根卷。

   ```
   [ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --availability-
   zone us-west-2b
   ```

   b. 使用 attach-volume 命令将该卷附加到 Amazon EBS 支持的实例。

   ```
   [ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-id instance_id
    --device /dev/sdb --region us-west-2
   ```

5. 创建用于捆绑的文件夹。

   ```
   [ec2-user ~]$ mkdir /tmp/bundle
   ```

6. 使用 /tmp/bundle 命令将由实例存储支持的 AMI 的捆绑下载到 ec2-download-bundle (p. 164)。

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m
 image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /path/
to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. 使用 ec2-unbundle (p. 168) 命令从捆绑重新构建映像文件。

   a. 将目录更改为捆绑文件夹。

   ```
   [ec2-user ~]$ cd /tmp/bundle/
   ```

   b. 运行 ec2-unbundle (p. 168) 命令。

   ```
   [ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
   HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
   ```

8. 将文件从未捆绑的映像复制到新 EBS 卷。

   ```
   [ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
   ```

9. 探测所有未捆绑的新分区的卷。

   ```
   [ec2-user bundle]$ sudo partprobe /dev/sdb1
   ```

10. 列出块储存设备以查找要装载的设备名称。

    ```
    [ec2-user bundle]$ lsblk
    NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
    /dev/sda    202:0    0   8G  0 disk
    ##/dev/sda1 202:1    0   8G  0 part /
    /dev/sdb    202:80   0  10G  0 disk
    ##/dev/sdb1 202:81   0  10G  0 part
    ```

    在此示例中，要装载的分区是 /dev/sdb1，但您的设备名称可能有所不同。如果您的卷未分区，则要装载的设备类似于 /dev/sdb (没有设备分区尾部数字)。

11. 为新 EBS 卷创建装载点并装载该卷。

    ```
    [ec2-user bundle]$ sudo mkdir /mnt/ebs
    [ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
    ```

12. 使用您常用的文本编辑器（如 /etc/fstab 或 vim）在 EBS 卷上打开 nano 文件，然后删除实例存储（临时）卷的所有条目。因为 EBS 卷装载在 /mnt/ebs 上，所以 fstab 文件位于 /mnt/ebs/etc/fstab 处。

    ```
    [ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
    #
    LABEL=/     /           ext4    defaults,noatime  1   1
    tmpfs       /dev/shm    tmpfs   defaults        0   0
    devpts      /dev/pts    devpts  gid=5,mode=620  0   0
    sysfs       /sys        sysfs   defaults        0   0
    proc        /proc       proc    defaults        0   0
    /dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
    ```

    在本示例中，应删除最后一行。

13. 从实例中卸载和分离该卷。

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. 按如下所示从新 EBS 卷创建 AMI。

    a. 创建新 EBS 卷的快照。

    ```
    [ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
     "your_snapshot_description" --volume-id volume_id
    ```

    b. 检查快照是否完整。

    ```
    [ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
    id snapshot_id
    ```

    c. 使用 `aki` 命令标识在原始 AMI 上使用的处理器架构、虚拟化类型和内核映像 (describe-images)。对于此步骤，您需要实例存储支持的原始 AMI 的 AMI ID。

    ```
    [ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id --
    output text
    IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon available
     public machine aki-fc8f11cc instance-store paravirtual xen
    ```

    在此示例中，架构是 `x86_64`，内核映像 ID 是 `aki-fc8f11cc`。在以下步骤中使用这些值。如果上面命令的输出还列出 `ari` ID，请记下该 ID。

    d. 使用新 EBS 卷的快照 ID 和上一步中得到的值注册新 AMI。如果前一命令输出列出了 `ari` ID，请通过 `--ramdisk-id ari_id` 将其包括在后续命令中。

    ```
    [ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
    name your_new_ami_name --block-device-mappings DeviceName=device-
    name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --architecture
     x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
    ```

15. (可选) 测试了您可以从新 AMI 启动实例之后，您可以删除为此过程创建的 EBS 卷。

```
aws ec2 delete-volume --volume-id volume_id
```

AMI 工具参考

您可以使用 AMI 工具命令创建和管理实例存储支持的 Linux AMI。要设置这些工具，请参阅设置 AMI 工具 (p. 143)。

有关访问密钥的更多信息，请参阅《Amazon Account Management 参考指南》中的 Amazon 账户最佳实践。

命令

- ec2-ami-tools-version (p. 156)
- ec2-bundle-image (p. 156)
- ec2-bundle-vol (p. 158)
- ec2-delete-bundle (p. 162)
- ec2-download-bundle (p. 164)
- ec2-migrate-manifest (p. 166)
- ec2-unbundle (p. 168)

- ec2-upload-bundle (p. 168)
- AMI 工具的常用选项 (p. 171)

ec2-ami-tools-version

描述

描述 AMI 工具的版本。

语法

```
ec2-ami-tools-version
```

输出

版本信息。

示例

此示例命令显示所用 AMI 工具的版本信息。

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

ec2-bundle-image

描述

通过回环文件中创建的操作系统映像创建实例存储支持的 Linux AMI。

语法

```
ec2-bundle-image -c path -k path -u account -i path [-d path] [--ec2cert path]
[-r architecture] [--productcodes code1,code2,...] [-B mapping] [-p prefix]
```

选项

`-c, --cert` 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

`-k, --privatekey` 路径

指向 PEM 编码 RSA 密钥文件的路径。您需要指定此密钥解开此捆绑包，因此，请将其保存在安全的地方。请注意，不需要在您的 Amazon 账户中注册该密钥。

必需：是

`-u, --user` 账户

用户的 Amazon 账户 ID (不包含破折号)。

必需：是

`-i, --image` 路径

指向待捆绑映像的路径。

必需：是

`-d, --destination` 路径

要在其中创建捆绑的目录。

默认值：`/tmp`

必需：否

`--ec2cert` 路径

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

`us-gov-west-1` 和 `cn-north-1` 区域使用非默认公有密钥凭证，必须随该选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 `/opt/aws/amitools/ec2/etc/ec2/amitools/`。如果您将来自 RPM 或 ZIP 文件的 AMI 工具安装在了 设置 AMI 工具 (p. 143) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 `us-gov-west-1` 和 `cn-north-1` 区域。

`-r, --arch` 架构

映像架构。如果您不在命令行上提供架构，则会在绑定开始时提示您输入架构。

有效值：`i386` | `x86_64`

必需：否

`--productcodes` code1,code2,...

在注册时附加到映像的产品代码，用逗号隔开。

必需：否

`-B, --block-device-mapping` 映射

定义块储存设备向此 AMI 的实例公开的方式 (如果其实例类型支持指定的设备)。

指定键值对的逗号分隔列表，每个键是虚拟名称，每个值是相应的设备名称。虚拟名称包括：

- `ami` — 实例所看到的根文件系统设备
- `root` — 内核所看到的根文件系统设备
- `swap` — 实例所看到的交换设备
- `ephemeralN` — 第 N 个实例存储卷

必需：否

`-p, --prefix` prefix

捆绑的 AMI 文件的文件名前缀。

默认：映像文件的名称。例如，如果映像路径为 `/var/spool/my-image/version-2/debian.img`，则默认前缀为 `debian.img`。

必需：否

`--kernel` kernel_id

已淘汰。使用 register-image 设置内核。

必需：否

`--ramdisk` ramdisk_id

已淘汰。使用 register-image 设置 RAM 磁盘 (若需要)。

必需：否

输出

描述捆绑过程的阶段和状态的状态消息。

示例

此示例从回环文件中所创建的操作系统映像创建捆绑的 AMI。

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

描述

通过对实例根设备卷的副本进行压缩、加密和签名来创建实例存储支持的 Linux AMI。

Amazon EC2 将尝试从实例继承产品代码、内核设置、RAM 磁盘设置和块储存设备映射。

默认情况下，捆绑过程不包括可能包含敏感信息的文件。这些文件包括 `*.sw`、`*.swo`、`*.swp`、`*.pem`、`*.priv`、`*id_rsa*`、`*id_dsa*` `*.gpg`、`*.jks`、`*/.ssh/authorized_keys` 和 `*/.bash_history`。要包括所有这些文件，请使用 `--no-filter` 选项。要包括其中部分文件，请使用 `--include` 选项。

有关更多信息，请参阅创建由实例存储支持的 Linux AMI (p. 142)。

语法

ec2-bundle-vol -c *path* -k *path* -u *account* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [--all] [-e *directory1*,*directory2*,...] [-i *file1*,*file2*,...] [--no-filter] [-p *prefix*] [-

s *size*] [--[no-]inherit] [-v *volume*] [-P *type*] [-S *script*] [--fstab *path*] [--generate-fstab] [--grub-config *path*]

选项

`-c, --cert` 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

`-k, --privatekey` 路径

用户的 PEM 编码 RSA 密钥文件的路径。

必需：是

`-u, --user` 账户

用户的 Amazon 账户 ID (不包含破折号)。

必需：是

`-d, --destination` destination

要在其中创建捆绑的目录。

默认值：`/tmp`

必需：否

`--ec2cert` 路径

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

`us-gov-west-1` 和 `cn-north-1` 区域使用非默认公有密钥凭证，必须随该选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 `/opt/aws/amitools/ec2/etc/ec2/amitools/`。如果您将来自 RPM 或 ZIP 文件的 AMI 工具安装在了 设置 AMI 工具 (p. 143) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 `us-gov-west-1` 和 `cn-north-1` 区域。

`-r, --arch` 架构

映像架构。如果您不在命令行上提供架构，则会在绑定开始时提示您提供架构。

有效值：`i386` | `x86_64`

必需：否

`--productcodes` code1,code2,...

在注册时附加到映像的产品代码，用逗号隔开。

必需：否

`-B, --block-device-mapping` 映射

定义块储存设备向此 AMI 的实例公开的方式 (如果其实例类型支持指定的设备)。

指定键值对的逗号分隔列表，每个键是虚拟名称，每个值是相应的设备名称。虚拟名称包括：

- `ami` — 实例所看到的根文件系统设备
- `root` — 内核所看到的根文件系统设备
- `swap` — 实例所看到的交换设备

- ephemeralN — 第 N 个实例存储卷

必需：否

`-a, --all`

捆绑所有目录，包括远程装载的文件系统上的目录。

必需：否

`-e, --exclude` directory1,directory2,...

要从捆绑操作中排除的绝对目录路径和文件的列表。此参数覆盖 `--all` 选项。指定排除时，随此参数列出的目录和子目录将不会随卷捆绑。

必需：否

`-i, --include` file1,file2,...

要在捆绑操作中包含的文件的列表。因为指定的文件可能包含敏感信息，若不指定则会从 AMI 中排除。

必需：否

`--no-filter`

如果指定，则我们不会因为文件可能包含敏感信息而将其从 AMI 排除。

必需：否

`-p, --prefix` prefix

捆绑的 AMI 文件的文件名前缀。

默认值：`image`

必需：否

`-s, --size` size

要创建的映像文件的大小，以 MB (1024 * 1024 字节) 为单位。最大大小为 10240 MB。

默认值：10240

必需：否

`--[no-]inherit`

指示映像是否应当继承实例的元数据 (默认为继承)。如果启用 `--inherit` 但实例元数据不可访问，则捆绑将失败。

必需：否

`-v, --volume` 体积

要从中创建捆绑的装载卷的绝对路径。

默认值：根目录 (/)

必需：否

`-P, --partition` type

指示磁盘映像是否应使用分区表。如果不指定分区表类型，则默认使用卷的父块储存设备上使用的类型 (如果适用)，否则默认为 `gpt`。

有效值：`mbr` |`gpt` |`none`

必需：否

`-S, --script` 脚本

将在捆绑前运行的自定义脚本。该脚本必须获得一个参数，即卷的装载点。

必需：否

`--fstab` 路径

要捆绑到映像中的 fstab 的路径。如果未指定，Amazon EC2 将捆绑 /etc/fstab。

必需：否

`--generate-fstab`

使用 Amazon EC2 提供的 fstab 捆绑卷。

必需：否

`--grub-config`

将捆绑到映像中的备用 GRUB 配置文件的路径。默认情况下，`ec2-bundle-vol` 预计克隆的映像上存在 `/boot/grub/menu.lst` 或 `/boot/grub/grub.conf`。该选项可让您指定备用 GRUB 配置文件的路径，将会复制该文件以覆盖默认值 (若存在)。

必需：否

`--kernel` kernel_id

已淘汰。使用 register-image 设置内核。

必需：否

`--ramdisk`ramdisk_id

已淘汰。使用 register-image 设置 RAM 磁盘 (若需要)。

必需：否

输出

描述捆绑的阶段和状态的状态消息。

示例

此示例通过对本机根文件系统进行压缩、加密和签名创建捆绑的 AMI。

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
```

```
1+0 records in
1+0 records out
mke2fs 1.38 (30-Jun-2005)
warning: 256 blocks unused.

Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

描述

从 Amazon S3 存储中删除指定的捆绑。删除捆绑后，您不能从相应的 AMI 启动实例。

语法

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

选项

`-b, --bucket` 存储桶

包含捆绑的 AMI 的 Amazon S3 存储桶的名称，后跟可选的以“/”分隔的路径前缀

必需：是

`-a, --access-key` access_key_id

Amazon 访问密钥 ID。

必需：是

`-s, --secret-key` secret_access_key

Amazon 秘密访问密钥。

必需：是

`-t, --delegation-token` token

传递到 Amazon 请求的委托令牌。有关更多信息，请参阅使用临时安全凭证。

必需：仅当使用临时安全凭证时是必需的。

默认：`AWS_DELEGATION_TOKEN` 环境变量的值 (若已设置)。

`--region`区域

要在请求签名中使用的区域。

默认值：`us-east-1`

必需：若使用签名版本 4 则必需

`--sigv版本`

对请求进行签名时要使用的签名版本。

有效值：2 | 4

默认值：4

必需：否

`-m, --manifestpath`

清单文件的路径。

必需：您必须指定 `--prefix` 或 `--manifest`。

`-p, --prefix` prefix

捆绑的 AMI 文件名前缀。请提供完整前缀。例如，如果前缀是 image.img，请使用 `-p image.img` 而不是 `-p image`。

必需：您必须指定 `--prefix` 或 `--manifest`。

`--clear`

删除指定的捆绑之后删除 Amazon S3 存储桶 (若为空)。

必需：否

`--retry`

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需：否

`-y, --yes`

自动假定所有提示的回答为 yes。

必需：否

输出

Amazon EC2 显示状态消息以指示删除过程的阶段和状态。

示例

此示例从 Amazon S3 删除捆绑。

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -
s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET1/
image.manifest.xml
DOC-EXAMPLE-BUCKET1/
image.part.00
DOC-EXAMPLE-BUCKET1/
image.part.01
DOC-EXAMPLE-BUCKET1/
image.part.02
DOC-EXAMPLE-BUCKET1/
```

```
image.part.03
DOC-EXAMPLE-BUCKET1/
image.part.04
DOC-EXAMPLE-BUCKET1/
image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
ec2-delete-bundle complete.
```

ec2-download-bundle

描述

从 Amazon S3 存储下载指定的实例存储支持的 Linux AMIs。

语法

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

选项

`-b, --bucket` 存储桶

捆绑所在的 Amazon S3 存储桶的名称，后跟可选的以“/”分隔的路径前缀。

必需：是

`-a, --access-key` access_key_id

Amazon 访问密钥 ID。

必需：是

`-s, --secret-key` secret_access_key

Amazon 秘密访问密钥。

必需：是

`-k, --privatekey` 路径

用于解密清单的私有密钥。

必需：是

`--url` url

Amazon S3 服务 URL。

默认值：`https://s3.amazonaws.com/`

必需：否

`--region` region

要在请求签名中使用的区域。

默认值：`us-east-1`

必需：若使用签名版本 4 则必需

`--sigv` version

对请求进行签名时要使用的签名版本。

有效值：2 | 4

默认值：4

必需：否

`-m, --manifest` file

清单文件的名称 (无路径)。我们建议您指定清单 (`-m`) 或前缀 (`-p`)。

必需：否

`-p, --prefix` prefix

捆绑的 AMI 文件的文件名前缀。

默认值：`image`

必需：否

`-d, --directory` directory

保存下载的捆绑的目录。该目录必须存在。

默认：当前工作目录。

必需：否

`--retry`

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需：否

输出

将显示指示下载过程各个阶段的状态消息。

示例

此示例创建 `bundled` 目录（使用 Linux mkdir 命令）并从 *DOC-EXAMPLE-BUCKET1* Amazon S3 存储桶下载捆绑。

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.00 ...
```

```
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.06 ...
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

ec2-migrate-manifest

描述

修改实例存储支持的 Linux AMI（例如，其证书、内核和 RAM 磁盘）以使其支持其他区域。

语法

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -s
secret_access_key --region region) | (--no-mapping)} [--ec2cert ec2_cert_path]
[--kernel kernel-id] [--ramdisk ramdisk_id]
```

选项

`-c, --cert` 路径

用户的 PEM 编码 RSA 公有密钥凭证文件。

必需：是

`-k, --privatekey` 路径

用户的 PEM 编码 RSA 密钥文件的路径。

必需：是

`--manifest` 路径

清单文件的路径。

必需：是

`-a, --access-key` access_key_id

Amazon 访问密钥 ID。

必需：若使用自动映射则必需。

`-s, --secret-key` secret_access_key

Amazon 秘密访问密钥。

必需：若使用自动映射则必需。

`--region` region

要在映射文件中查找的区域。

必需：若使用自动映射则必需。

`--no-mapping`

禁用内核和 RAM 磁盘的自动映射。

迁移期间，Amazon EC2 会将清单文件中的内核和 RAM 磁盘替换为目标区域指定的内核和 RAM 磁盘。除非提供了 `--no-mapping` 参数，否则 `ec2-migrate-bundle` 便可能使用 `DescribeRegions` 和 `DescribeImages` 操作执行自动映射。

必需：若您不提供用于自动映射的 `-a`、`-s` 和 `--region` 选项，则必需。

`--ec2cert` 路径

用于加密映像清单的 Amazon EC2 X.509 公有密钥凭证的路径。

`us-gov-west-1` 和 `cn-north-1` 区域使用非默认公有密钥凭证，必须随该选项指定该证书的路径。该证书的路径因 AMI 工具的安装方法而异。对于 Amazon Linux，证书位于 `/opt/aws/amitools/ec2/etc/ec2/amitools/`。如果您将来自 ZIP 文件的 AMI 工具安装在 设置 AMI 工具 (p. 143) 中，则证书位于 `$EC2_AMITOOL_HOME/etc/ec2/amitools/`。

必需：仅限 `us-gov-west-1` 和 `cn-north-1` 区域。

`--kernel` kernel_id

要选择的内核的 ID。

> **Important**
>
> 我们建议您使用 PV-GRUB 而不是内核和 RAM 磁盘。有关更多信息，请参阅用户提供的内核 (p. 226)。

必需：否

`--ramdisk` ramdisk_id

供选择的 RAM 磁盘的 ID。

> **Important**
>
> 我们建议您使用 PV-GRUB 而不是内核和 RAM 磁盘。有关更多信息，请参阅用户提供的内核 (p. 226)。

必需：否

输出

描述捆绑过程的阶段和状态的状态消息。

示例

此示例将 `my-ami.manifest.xml` 清单中指定的 AMI 从美国复制到欧洲。

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml --cert cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem
 --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

描述

从实例存储支持的 Linux AMI 重新创建捆绑。

语法

```
ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]
```

选项

`-k, --privatekey` 路径

您的 PEM 编码 RSA 密钥文件的路径。

必需：是

`-m, --manifest` 路径

清单文件的路径。

必需：是

`-s, --source` source_directory

包含捆绑的目录。

默认：当前目录。

必需：否

`-d, --destination` destination_directory

将 AMI 解绑到的目录。目标目录必须存在。

默认：当前目录。

必需：否

示例

此 Linux 和 UNIX 示例解绑 `image.manifest.xml` 文件中指定的 AMI。

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s
 mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

输出

将显示指示解绑过程各个阶段的状态消息。

ec2-upload-bundle

描述

将实例存储支持的 Linux AMI 的捆绑上载到 Amazon S3，并在上载的对象上设置相应的访问控制列表 (ACL)。有关更多信息，请参阅创建由实例存储支持的 Linux AMI (p. 142)。

Note

要将对象上载到实例存储支持的 Linux AMI 的 S3 存储桶，必须为该存储桶启用 ACL。否则，Amazon EC2 将无法在要上载的对象上设置 ACL。如果您的目标存储桶使用存储桶拥有者强制执行的 S3 对象所有权设置，则这将不起作用，因为 ACL 已禁用。有关更多信息，请参阅使用 S3 对象所有权控制已上载对象的所有权。

语法

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t token] -m
path [--url url] [--region region] [--sigv version] [--acl acl] [-d directory]
[--part part] [--retry] [--skipmanifest]
```

选项

`-b, --bucket` 存储桶

用于存储捆绑的 Amazon S3 存储桶的名称，后跟可选的以“/”分隔的路径前缀。如果存储桶不存在，则创建一个 (若存储桶名称可用)。

必需：是

`-a, --access-key` access_key_id

您的 Amazon 访问密钥 ID。

必需：是

`-s, --secret-key` secret_access_key

您的 Amazon 秘密访问密钥。

必需：是

`-t, --delegation-token` token

传递到 Amazon 请求的委托令牌。有关更多信息，请参阅使用临时安全凭证。

必需：仅当使用临时安全凭证时是必需的。

默认：`AWS_DELEGATION_TOKEN` 环境变量的值 (若已设置)。

`-m, --manifest` 路径

清单文件的路径。清单文件是在捆绑过程中创建的，可以在包含捆绑的目录中找到。

必需：是

`--url` url

已淘汰。请使用 `--region` 选项，除非您的存储桶被限制到 EU 位置 (且不是 `eu-west-1`)。`--location` 标记是确定该特定位置限制的唯一途径。

Amazon S3 终端节点服务 URL。

默认值：`https://s3.amazonaws.com/`

必需：否

`--region` region

要在请求签名中为目标 S3 存储桶使用的区域。

- 如果存储桶不存在，您也没有指定区域，则该工具将创建无位置限制的存储桶（在 us-east-1 中）。
- 如果存储桶不存在，而您指定了区域，则该工具将在指定区域创建存储桶。
- 如果存储桶存在，而您没有指定区域，则该工具将使用存储桶的位置。
- 如果存储桶存在，并且您指定 us-east-1 为区域，则该工具将使用存储桶的实际位置而不会显示任何错误消息，并将覆盖任何现有的匹配文件。
- 如果存储桶存在，并且您指定与存储桶的实际位置不符的区域（非 us-east-1），则该工具将报错退出。

如果您的存储桶被限制到 EU 位置 (不是 eu-west-1)，请改用 --location 标记。--location 标记是确定该特定位置限制的唯一途径。

默认值：us-east-1

必需：若使用签名版本 4 则必需

--sigv version

对请求进行签名时要使用的签名版本。

有效值：2 | 4

默认值：4

必需：否

--acl acl

捆绑的映像的访问控制列表策略。

有效值：public-read | aws-exec-read

默认值：aws-exec-read

必需：否

-d, --directory directory

包含捆绑的 AMI 段的目录。

默认：包含清单文件的目录 (参阅 -m 选项)。

必需：否

--part part

开始上传指定的段及所有后续段。例如：--part 04。

必需：否

--retry

在所有 Amazon S3 错误后自动重试，每个操作最多五次。

必需：否

--skipmanifest

不上传清单。

必需：否

--location 位置

已淘汰。请使用 --region 选项，除非您的存储桶被限制到 EU 位置 (且不是 eu-west-1)。--location 标记是确定该特定位置限制的唯一途径。

目标 Amazon S3 存储桶的位置限制。如果存储桶存在，而您指定的位置与存储桶的实际位置不符，则该工具将报错退出。如果存储桶存在，而您没有指定位置，则该工具将使用存储桶的位置。如果存储桶不存在，而您指定了位置，则该工具将在指定位置创建存储桶。如果存储桶不存在，您也没有指定位置，则该工具将创建无位置限制的存储桶 (在 us-east-1 中)。

默认：如果指定 --region，则将位置设置为该指定区域。如果未指定 --region，则位置默认为 us-east-1。

必需：否

输出

Amazon EC2 显示状态消息以指示上传过程的阶段的状态。

示例

此示例上传 image.manifest.xml 清单所指定的捆绑。

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

AMI 工具的常用选项

大多数 AMI 工具接受以下可选参数。

--help, -h

显示帮助消息。

--version

显示版本和版权声明。

--manual

显示手动输入。

`--batch`

以批处理模式运行，不显示交互提示。

`--debug`

显示对故障排除可能有帮助的信息。

修改 AMI

您可以修改一组有限的亚马逊云机器镜像（AMI）属性，例如 AMI 的描述和共享属性。但是，AMI 内容（二进制卷数据）无法修改。要修改 AMI 内容，必须创建新的 AMI (p. 137)。

Important

您无法修改由 EBS 支持的 AMI 内容（二进制卷数据），因为支持这些内容的快照是不可变的。您也无法修改由实例存储支持（由 S3 支持）的 AMI 内容（二进制卷数据），因为内容已签名，如果签名不匹配会导致实例启动失败。

有关可修改的 AMI 属性，请参阅《Amazon EC2 API 参考》中的 ModifyImageAttribute。

以下主题提供有关使用 Amazon EC2 控制台和 Amazon CLI 来修改 AMI 属性的说明：

- 将 AMI 设为公用 (p. 124)
- ???
- 与特定 Amazon 账户共享 AMI (p. 126)
- 使用付费支持 (p. 136)
- 配置 AMI (p. 762)

复制 AMI

您可以在 Amazon 区域内或跨区域复制 Amazon Machine Image (AMI)。可以复制 Amazon EBS-backed AMIs 和实例存储支持的 AMIs。您可以复制带加密快照的 AMI，并在复制过程中更改加密状态。您可以复制与共享给您的 AMI。

复制源 AMI 将生成完全相同但独立的目标 AMI（具有自己的唯一标识符）。您可以更改或注销源 AMI，这不会对目标 AMI 产生任何影响。反之亦然。

借助 Amazon EBS-backed AMI，每个支持快照将会复制到完全相同但独立的目标快照。如果您将 AMI 复制到新区域，则快照是完整的（非增量）副本。如果您加密未加密的备份快照或将其加密到新 KMS 密钥，则快照是完整（非增量）副本。后续的 AMI 复制操作会生成备份快照的增量副本。

目录

- 注意事项 (p. 173)
- 成本 (p. 173)
- 用于复制实例存储支持的 AMI 的权限 (p. 173)
- 复制 AMI (p. 174)
- 停止待处理的 AMI 复制操作 (p. 175)
- 跨区域复制 (p. 176)
- 跨账户复制 (p. 177)
- 加密和复制 (p. 177)

注意事项

- 您可以使用 IAM policy 授予或拒绝用户复制 AMI 的权限。为 CopyImage 操作指定的资源级权限仅适用于新 AMI。您不能为源 AMI 指定资源级权限。
- Amazon 不会将启动许可或 Amazon S3 存储桶许可从源 AMI 复制到新 AMI。复制操作完成之后，您可以将启动许可和 Amazon S3 存储桶权限应用于新的 AMI。
- 您只能复制附加到 AMI 的用户定义的 AMI 标签。不会复制系统标签（前缀为 aws:）和由其他 Amazon Web Services 账户 附加的用户定义标签。
- 复制从另一个账户共享的 Amazon Web Services Marketplace AMI 不支持 CopyImage 操作。相反，如果您想在另一个账户中复制 Amazon Web Services Marketplace AMI，则必须执行以下操作：与另一个账户共享 Amazon Web Services Marketplace AMI，然后在另一个账户中使用 Amazon Web Services Marketplace AMI 启动 EC2 实例。然后，您可以使用 CreateImage 操作从实例中创建 AMI。新的 AMI 保留了所有 Amazon Web Services Marketplace 代码。请注意，此过程也适用于直接或间接从 Amazon Web Services Marketplace AMI 派生的任何 AMI。有关创建从实例创建 AMI 的更多信息，请参阅 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。

成本

复制 AMI 没有任何费用。但要收取标准存储和数据传输费。如果您复制由 EBS 支持的 AMI，则任何其他 EBS 快照的存储将会产生费用。

用于复制实例存储支持的 AMI 的权限

要复制由实例存储支持的 AMI，用户必须具有以下 Amazon S3 权限：s3:CreateBucket、s3:GetBucketAcl、s3:ListAllMyBuckets、s3:GetObject、s3:PutObject 和 s3:PutObjectAcl。

以下示例策略允许用户将指定的存储桶中的 AMI 源复制到指定的区域。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::ami-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
              "s3:CreateBucket",
              "s3:GetBucketAcl",
              "s3:PutObjectAcl",
              "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-123456789012-in-us-east-1*"
            ]
        }
```

```
    ]
}
```

要查找 AMI 源存储桶的 Amazon Resource Name (ARN)，请访问 https://console.aws.amazon.com/ec2/，打开 Amazon EC2 控制台，在导航窗格中选择 AMIs (AMI)，然后在 Source (源) 列中找到该存储桶名称。

Note

仅在用户首次将实例存储支持的 AMI 复制到单个区域时，才需要 `s3:CreateBucket` 权限。在此之后，将使用已在该区域中创建的 Amazon S3 存储桶来存储您将来复制到该区域的所有 AMIs。

复制 AMI

您可以使用 Amazon Web Services Management Console、Amazon Command Line Interface 或开发工具包，或者 Amazon EC2 API（三者都支持 `CopyImage` 操作）复制 AMI。

先决条件

创建或获取 Amazon EBS 快照支持的 AMI。请注意，您可以使用 Amazon EC2 控制台搜索 Amazon 提供的各种 AMI。有关更多信息，请参阅 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)和查找 AMI。

New console

使用控制台复制 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从控制台导航栏中，选择包含 AMI 的区域。
3. 在导航窗格中，选择映像和 AMI 以显示区域中可供您使用的 AMIs 列表。
4. 选择要复制的 AMI，然后选择操作和复制 AMI。
5. 在 Copy AMI（复制 AMI）页上，请指定以下信息：
   - AMI copy name（AMI 副本名称）：新 AMI 的名称。您可以在名称中包含操作系统信息，因为我们在显示有关 AMI 的详情时不提供该信息。
   - AMI copy description（AMI 副本描述）：默认情况下，描述包括源 AMI 的相关信息，以便您能区分副本和原本。您可以按需更改此描述。
   - Destination Region（目标区域）：在其中复制 AMI 的区域。有关更多信息，请参阅跨区域复制 (p. 176)。
   - Copy tags（复制标签）：选中此复选框可在复制 AMI 时包含用户定义的 AMI 标签。不会复制系统标签（前缀为 `aws:`）和由其他 Amazon Web Services 账户 附加的用户定义标签。
   - Encrypt EBS snapshots of AMI copy（加密 AMI 副本的 EBS 快照）：选择此复选框可加密目标快照，或使用不同的密钥对它们进行重新加密。如果您启用默认加密 (p. 1507)，Encrypt EBS snapshots of AMI copy（加密 AMI 副本的 EBS 快照）复选框处于选中状态，无法清除。有关更多信息，请参阅加密和复制 (p. 177)。
   - KMS 密钥：用于加密目标快照的 KMS 密钥。
6. 选择 Copy AMI（复制 AMI）。

   新 AMI 的初始状态是 `Pending`。当状态为 `Available` 时，AMI 复制操作完成。

Old console

使用控制台复制 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从控制台导航栏中，选择包含 AMI 的区域。在导航窗格中，选择映像和 AMI 以显示区域中可供您使用的 AMIs 列表。

3. 选择要复制的 AMI，然后选择操作和复制 AMI。
4. 在复制 AMI 对话框中，请指定以下信息，然后选择复制 AMI：
   - 目标区域：在其中复制 AMI 的区域。有关更多信息，请参阅跨区域复制 (p. 176)。
   - 名称：新 AMI 的名称。您可以在名称中包含操作系统信息，因为我们在显示有关 AMI 的详情时不提供该信息。
   - Description：默认情况下，描述包括源 AMI 的相关信息，以便您能区分副本和原本。您可以按需更改此描述。
   - Encryption：选择此字段可加密目标快照，或使用不同的密钥对它们进行重新加密。如果启用了默认加密 (p. 1507)，则会设置加密选项，且无法取消设置。有关更多信息，请参阅加密和复制 (p. 177)。
   - KMS 密钥：用于加密目标快照的 KMS 密钥。
5. 我们将显示一个确认页面，以告知您复制操作已启动，并为您提供新 AMI 的 ID。

   若要立即查看复制操作的进度，请访问提供的链接。若要稍后查看进度，请选择完成，然后在您需要时使用导航栏切换到目标区域（如果适用）并在 AMI 列表中找到您的 AMI。

   目标 AMI 的初始状态为 `pending`，当状态为 `available` 时，此操作完成。

要使用 Amazon CLI 来复制 AMI

您可使用 copy-image 命令复制 AMI。您必须指定源和目标区域。您可以使用 `--source-region` 参数指定源区域。您可以使用 `--region` 参数或环境变量指定目标区域。有关更多信息，请参阅配置 Amazon 命令行界面。

在复制期间加密目标快照时，您必须指定这些额外参数：`--encrypted` 和 `--kms-key-id`。

有关示例命令，请参阅《Amazon CLI 命令参考》中 copy-image 下的示例。

使用 Tools for Windows PowerShell 来复制 AMI

您可使用 Copy-EC2Image 命令复制 AMI。您必须指定源和目标区域。您可以使用 `-SourceRegion` 参数指定源区域。您可以使用 `-Region` 参数或 `Set-AWSDefaultRegion` 命令指定目标区域。有关更多信息，请参阅指定 Amazon 区域。

在复制期间加密目标快照时，您必须指定这些额外参数：`-Encrypted` 和 `-KmsKeyId`。

停止待处理的 AMI 复制操作

您可以按如下方式停止待处理的 AMI 复制。

New console

使用控制台停止 AMI 复制操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中，从区域选择器中选择目标区域。
3. 在导航窗格中，选择 AMIs。
4. 选择要停止复制的 AMI，然后选择 Actions（操作）和 Deregister AMI（取消注册 AMI）。
5. 当系统要求您确认时，选择 Deregister AMI（取消注册 AMI）。

Old console

使用控制台停止 AMI 复制操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 从导航栏中，从区域选择器中选择目标区域。
3. 在导航窗格中，选择 AMIs。
4. 选择要停止复制的 AMI，然后选择操作和取消注册。
5. 当系统要求确认时，请选择 Continue。

使用命令行停止 AMI 复制操作

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

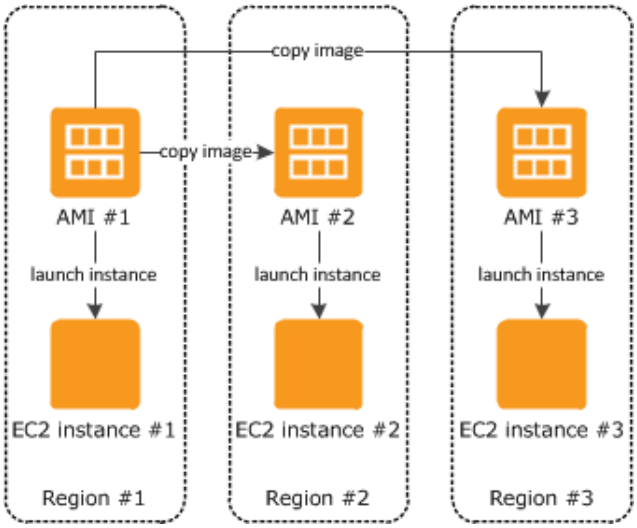
- deregister-image (Amazon CLI)
- Unregister-EC2Image（Amazon Tools for Windows PowerShell）

跨区域复制

跨不同地理位置复制 AMI 具有以下优势：

- 一致的全球部署：通过将 AMI 从一个区域复制到另一个区域，您可以根据相同的 AMI 在不同的区域中启动一致的实例。
- 可扩展性：无论用户身处何处，您都可以更轻松地设计和构建能满足他们需求的全球应用程序。
- 性能：您可以通过分发您的应用程序以及找到较接近您用户的应用程序的关键组件来提高性能。您还可以利用区域特定的功能，例如，实例类型或其他 Amazon 服务。
- 高可用性：您可以跨 Amazon 区域设计和部署应用程序以提高可用性。

下图显示源 AMI、在不同的区域中复制的两个 AMIs 以及从它们中启动的 EC2 实例之间的关系。从 AMI 中启动实例时，该实例位于 AMI 所在的区域中。如果您更改源 AMI，并希望在目标区域中的 AMIs 上反映这些更改，您必须将源 AMI 重新复制到目标区域中。



在首次将实例存储支持的 AMI 复制到一个区域时，我们为复制到该区域的 AMIs 创建一个 Amazon S3 存储桶。复制到该区域的所有实例存储支持的 AMIs 存储在该存储桶中。存储桶名称具有以下格式：amis-for-*account*-in-*region*-*hash*。例如：`amis-for-123456789012-in-us-east-2-yhjmxvp6`。

先决条件

在复制 AMI 之前，您必须确保更新源 AMI 的内容以支持在不同的区域中运行。例如，您应更新任何数据库连接字符串或相似的应用程序配置数据，以指向适当的资源。否则，从目标区域上的新 AMI 中启动的实例可能仍会使用源区域中的资源，这可能会影响性能和成本。

Limits

- 目标区域限制为 100 个并发 AMI 副本。
- 您无法将半虚拟化 (PV) AMI 复制到不支持 PV AMI 的区域。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。

跨账户复制

您可以与其他 Amazon 账户共享 AMI。共享 AMI 不影响 AMI 的所有权。拥有它的账户需要支付区域中的存储费用。有关更多信息，请参阅与特定 Amazon 账户共享 AMI (p. 126)。

如果您复制已与您的账户共享的 AMI，则您是您的账户中的目标 AMI 的所有者。源 AMI 的所有者需要支付标准 Amazon EBS 或 Amazon S3 传输费用，您需要支付目标区域中的目标 AMI 的存储费用。

资源权限

若要从另一个账户复制与您共享的 AMI，源 AMI 的所有者必须授予您对支持 AMI 的存储的读取权限。存储是关联的 EBS 快照（用于 Amazon EBS-backed AMI）或关联的 S3 存储桶（用于实例存储支持的 AMI）。如果共享 AMI 带有加密快照，拥有者必须同时与您共享一个或多个密钥。有关授予资源权限的更多信息，对于 EBS 快照，请参阅 共享 Amazon EBS 快照 (p. 1403)，对于 S3 存储桶，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon S3 中的 Identity and Access Management。

> **Note**
>
> 若要复制 AMI 及其标签，您必须具有源 AMI 的启动权限。

加密和复制

下表显示了各种 AMI 复制场景的加密支持。尽管可以复制未加密快照来生成加密快照，但是不能复制加密快照来生成未加密快照。

场景	描述	支持
1	未加密到未加密	是
2	加密到加密	是
3	未加密到加密	是
4	加密到未加密	否

> **Note**
>
> 在 CopyImage 操作期间加密仅适用于 Amazon EBS-backed AMI。因为实例存储支持的 AMI 不依赖于快照，所以不能使用复制来更改器加密状态。

默认情况下（即未指定加密参数的情况）将复制 AMI 的备份快照并保持其原始加密状态。复制未加密快照支持的 AMI 将生成完全相同、也未加密的目标快照。如果源 AMI 受加密快照支持，则复制它将生成一个由相同 Amazon KMS 密钥加密的相同目标快照。在默认情况下，复制多个快照支持的 AMI 将保留其在每个目标快照中的源加密状态。

如果您在复制 AMI 的过程中指定对应加密参数，可以将其备份快照加密或重新加密。以下示例显示为 CopyImage 操作提供加密参数以更改目标 AMI 的加密状态的一个非默认案例。

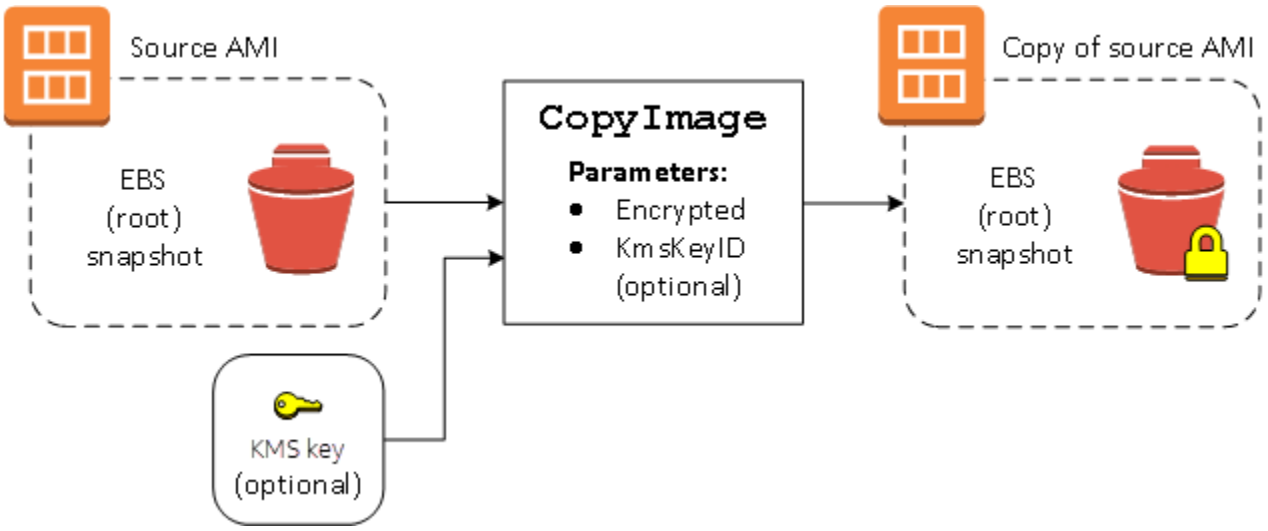
将未加密的源 AMI 复制到加密目标 AMI

在这种情况下，由未加密根快照支持的 AMI 会复制到带加密根快照的 AMI。CopyImage 操作将使用两个加密参数（包括一个客户托管密钥）调用。因此，根快照的加密状态发生变化，这样目标 AMI 由与原快照具有

相同数据的根快照支持，但使用指定的密钥进行加密。在两个 AMI 中，您都会产生快照的存储成本，以及从任一 AMI 启动的任何实例的费用。

Note

启用默认加密 (p. 1507)与将 AMI 中所有快照的 `Encrypted` 参数设置为 `true` 具有相同的效果。



设置 `Encrypted` 参数会加密此实例的单个快照。如果您未指定 `KmsKeyId` 参数，会使用默认客户托管密钥来加密快照副本。

有关复制带加密快照的 AMIs 的更多信息，请参阅将加密与 EBS 支持的 AMI 结合使用 (p. 196)。

使用 S3 存储和还原 AMI

您可以将 Amazon Machine Image (AMI) 存储在 Amazon S3 存储桶中、将 AMI 复制到另一个 S3 存储桶，然后从 S3 存储桶还原它。通过使用 S3 存储桶存储和还原 AMI，您可以将 AMI 从一个 Amazon 分区复制到另一个分区，例如，从主商业分区到 Amazon GovCloud (US) 分区。您还可以通过将 AMI 存储在 S3 存储桶中为其创建存档副本。

支持使用 S3 存储和还原 AMI 的 API 是 `CreateStoreImageTask`、`DescribeStoreImageTasks` 和 `CreateRestoreImageTask`。

`CopyImage` 是推荐用于在 Amazon 分区内复制 AMI 的 API。但是，`CopyImage` 无法将 AMI 复制到另一个分区。

有关 Amazon 分区的信息，请参阅《Amazon 一般参考》中 Amazon 资源名称（ARN）页面的##。

Warning

在 Amazon 分区或 Amazon 区域之间移动数据时，请确保遵守所有适用法律和业务要求，包括但不限于任何适用的政府法规和数据驻留要求。

主题

- 使用案例 (p. 179)
- AMI 存储和还原 API 的工作原理 (p. 179)
- 限制 (p. 181)
- 成本 (p. 181)
- 保护您的 AMI (p. 181)
- 使用 S3 存储和还原 AMI 的权限 (p. 181)
- 使用 AMI 存储和还原 API (p. 182)

使用案例

使用存储和还原 API 执行以下操作：

- 将 AMI 从一个 Amazon 分区复制到另一个 Amazon 分区 (p. 179)
- 制作 AMI 的存档副本 (p. 179)

将 AMI 从一个 Amazon 分区复制到另一个 Amazon 分区

通过使用 S3 存储桶存储和还原 AMI，您可以将 AMI 从一个 Amazon 分区复制到另一个分区，或从一个 Amazon 区域复制到另一个区域。在以下示例中，您可将 AMI 从主商业分区复制到 Amazon GovCloud (US) 分区，尤其是从 `us-east-2` 区域复制到 `us-gov-east-1` 区域。

要将 AMI 从一个分区复制到另一个分区，请执行以下步骤：

- 使用 `CreateStoreImageTask` 将 AMI 存储在当前区域内的 S3 存储桶中。在此示例中，S3 存储桶位于 `us-east-2` 中。有关示例命令，请参阅 将 AMI 存储在 S3 存储桶中 (p. 182)。
- 使用 `DescribeStoreImageTasks` 监控存储任务的进度。任务完成后，对象将在 S3 存储桶中可见。有关示例命令，请参阅 描述 AMI 存储任务的进度 (p. 182)。
- 使用您选择的程序将存储的 AMI 对象复制到目标分区中的 S3 存储桶。在此示例中，S3 存储桶位于 `us-gov-east-1` 中。

  Note

  由于每个分区均需要不同的 Amazon 凭证，因此无法将 S3 对象从一个分区直接复制到另一个分区。跨分区复制 S3 对象的过程不在本文档的讨论范围之内。我们提供以下复制过程作为示例，但您必须使用符合安全要求的复制过程。

  - 要跨分区复制某一 AMI，复制过程可能非常简单，如下所示：从源存储桶下载对象到中间主机（例如，EC2 实例或笔记本电脑），然后从中间主机上传对象到目标存储桶。对于该过程的每个阶段，请对分区使用 Amazon 凭证。
  - 要实现更持久的使用，请考虑开发一个管理副本的应用程序（可能使用 S3 分段下载和上传）。
- 使用 `CreateRestoreImageTask` 从目标分区中的 S3 存储桶还原 AMI。在此示例中，S3 存储桶位于 `us-gov-east-1` 中。有关示例命令，请参阅 从 S3 存储桶还原 AMI (p. 183)。
- 通过对需要检查其状态何时变为可用的 AMI 进行描述来监控还原任务的进度。您还可以通过描述快照来监控构成所还原 AMI 的快照的进度百分比。

制作 AMI 的存档副本

您可以通过将 AMI 存储在 S3 存储桶中为其创建存档副本。有关示例命令，请参阅 将 AMI 存储在 S3 存储桶中 (p. 182)。

AMI 被打包到 S3 内的单个对象中，所有 AMI 元数据（不包括共享信息）都作为存储 AMI 的一部分得到保留。AMI 数据将作为存储流程的一部分进行压缩。由于 AMI 包含可轻松压缩的数据，因此 S3 中的对象较小。为了降低成本，您可以使用更便宜的 S3 存储套餐。有关更多信息，请参阅 Amazon S3 存储类和 Amazon S3 定价

AMI 存储和还原 API 的工作原理

要使用 S3 存储和还原 AMI，请使用以下 API：

- `CreateStoreImageTask` – 将 AMI 存储在 S3 存储桶中
- `DescribeStoreImageTasks` – 提供 AMI 存储任务的进度
- `CreateRestoreImageTask` – 从 S3 存储桶还原 AMI

API 的工作原理

- CreateStoreImageTask (p. 180)
- DescribeStoreImageTasks (p. 180)
- CreateRestoreImageTask (p. 180)

CreateStoreImageTask

CreateStoreImageTask (p. 182) API 将 AMI 作为单个对象存储在 S3 存储桶中。

API 创建一个任务，从 AMI 及其快照中读取所有数据，然后使用 S3 分段上传将数据存储在 S3 对象中。API 获取 AMI 的所有组件，包括大多数非区域特定的 AMI 元数据以及 AMI 中包含的所有 EBS 快照，然后将它们打包到 S3 内的单个对象中。数据将作为上传流程的一部分进行压缩，以减少 S3 中使用的空间量，因此 S3 中的对象可能小于 AMI 中快照大小总和。

如果调用此 API 的账户有可见的 AMI 和快照标签，则会保留它们。

S3 中的对象的 ID 与 AMI 的相同，但带有 `.bin` 扩展名。以下数据还作为 S3 对象上的 S3 元数据标签存储：AMI 名称、AMI 描述、AMI 注册日期、AMI 拥有者账户以及存储操作的时间戳。

完成任务所需的时间取决于 AMI 的大小。它还取决于有多少其他任务正在进行，因为任务需要排队。您可以通过调用 DescribeStoreImageTasks (p. 182) API 来跟踪任务的进度。

所有正在进行的 AMI 的大小总和限制为每个账户 600 GB 的 EBS 快照数据。进一步的任务创建将被拒绝，直到正在进行的任务低于限制。例如，如果当前正在存储快照数据为 100 GB 的 AMI 和另一个快照数据为 200 GB 的 AMI，则将接受另一个请求，因为正在进行的总量为 300 GB，低于限制。但是，如果当前正在存储的单个 AMI 的快照数据为 800 GB，则在任务完成之前，将会拒绝进一步的任务。

DescribeStoreImageTasks

DescribeStoreImageTasks (p. 182) API 描述 AMI 存储任务的进度。您可以描述指定 AMI 的任务。如果未指定 AMI，则会获得过去 31 天内处理的所有存储映像任务的分页列表。

对于每个 AMI 任务，响应会指示任务是 `InProgress`、`Completed` 还是 `Failed`。对于任务 `InProgress`，响应会将估计进度显示为百分比值。

任务按反向的时间顺序列出。

目前，只能查看上个月的任务。

CreateRestoreImageTask

CreateRestoreImageTask (p. 183) API 启动一个任务，该任务可从先前使用 CreateStoreImageTask (p. 182) 请求创建的 S3 对象还原 AMI。

执行还原任务的区域可以与执行存储任务的区域相同，也可以不同。

要从中还原 AMI 对象的 S3 存储桶必须位于请求执行还原任务的相同区域中。AMI 将在此区域中还原。

AMI 将使用其元数据还原，例如与存储的 AMI 值对应的名称、描述和块储存设备映射。名称对该账户在该区域中的 AMI 必须唯一。如果未提供名称，则新 AMI 获得的名称与原始 AMI 的名称相同。AMI 获得在还原流程中生成的新 AMI ID。

完成 AMI 还原任务所需的时间取决于 AMI 的大小。它还取决于有多少其他任务正在进行，因为任务需要排队。您可以通过描述 AMI (describe-images) 或其 EBS 快照 (describe-snapshots) 来查看任务的进度。如果任务失败，AMI 和快照将移至失败状态。

所有正在进行的 AMI 的大小总和限制为每个账户的 EBS 快照数据 300 GB（根据还原后的大小）。进一步的任务创建将被拒绝，直到正在进行的任务低于限制。

限制

- 使用这些 API 只能存储由 EBS 支持的 AMI。
- 不支持半虚拟化 (PV) AMI。
- 可存储的 AMI 的大小（压缩前）限制为 5,000 GB。
- 存储映像 (p. 182)请求的限额：600 GB 的存储工作（快照数据）正在进行中。
- 还原映像 (p. 183)请求的限额：300 GB 的还原工作（快照数据）正在进行中。
- 在存储任务的持续时间内，不得删除快照，执行存储的 IAM 委托人必须有权访问快照，否则存储流程将会失败。
- 您不能在同一 S3 存储桶中创建 AMI 的多个副本。
- 存储在 S3 存储桶中的 AMI 无法使用其原始 AMI ID 进行还原。您可以使用 AMI 别名来缓解这种情况。
- 目前，仅支持使用 Amazon Command Line Interface、Amazon 开发工具包和 Amazon EC2 API 存储和还原 API。您无法使用 Amazon EC2 控制台存储和还原 AMI。

成本

使用 S3 存储和还原 AMI 时，您需要为存储和还原 API 使用的服务以及数据传输付费。API 使用 S3 和 EBS Direct API（由这些 API 在内部使用以访问快照数据）。有关更多信息，请参阅 Amazon S3 定价和 Amazon EBS 定价。

保护您的 AMI

要使用存储和还原 API，S3 存储桶和 AMI 必须位于同一区域中。务必确保 S3 存储桶配置有足够的安全性来保护 AMI 的内容，并确保只要 AMI 对象仍保留在存储桶中，安全性将保持不变。如果无法做到这一点，建议不要使用这些 API。确保不允许对 S3 存储桶进行公共访问。我们建议为存储 AMI 的 S3 存储桶启用服务器端加密，但不是必需要求。

有关如何为 S3 存储桶设置适当的安全设置的信息，请查看以下安全主题：

- 阻止对 Amazon S3 存储的公有访问
- 设置 Amazon S3 存储桶的默认服务器端加密行为
- 要符合 Amazon Config 规则 s3-bucket-ssl-requests-only，我要使用什么 S3 存储桶策略？
- 启用 Amazon S3 服务器访问日志记录

当 AMI 快照复制到 S3 对象时，将通过 TLS 连接复制数据。您可以使用加密快照存储 AMI，但是快照会作为存储流程的一部分进行解密。

使用 S3 存储和还原 AMI 的权限

如果您的 IAM 主体将使用 Amazon S3 来存储或还原 AMI，则需要向其授予所需权限。

以下示例策略包括允许 IAM 委托人执行存储和还原任务需要的所有操作。

此外，您还可以创建向主体授予仅访问指定资源权限的 IAM policy。如需了解更多示例策略，请参阅《IAM 用户指南》中的 Amazon 资源的访问管理。

> **Note**
>
> 如果构成 AMI 的快照已加密，或者账户默认启用了加密功能，您的 IAM 主体必须具有使用 KMS 密钥的权限。有关更多信息，请参阅Amazon KMS keys 使用权限 (p. 1423)。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

使用 AMI 存储和还原 API

主题

- 将 AMI 存储在 S3 存储桶中 (p. 182)
- 描述 AMI 存储任务的进度 (p. 182)
- 从 S3 存储桶还原 AMI (p. 183)

将 AMI 存储在 S3 存储桶中

存储 AMI (Amazon CLI)

使用 create-store-image-task 命令。指定 AMI 的 ID 以及要在其中存储 AMI 的 S3 存储桶的名称。

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket myamibucket
```

预期输出

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

描述 AMI 存储任务的进度

描述 AMI 存储任务的进度 (Amazon CLI)

使用 describe-store-image-tasks 命令。

```
aws ec2 describe-store-image-tasks
```

预期输出

```
{
  "AmiId": "ami-1234567890abcdef0",
  "Bucket": "myamibucket",
  "ProgressPercentage": 17,
  "S3ObjectKey": "ami-1234567890abcdef0.bin",
  "StoreTaskState": "InProgress",
  "StoreTaskFailureReason": null,
  "TaskStartTime": "2021-01-01T01:01:01.001Z"
}
```

从 S3 存储桶还原 AMI

还原 AMI (Amazon CLI)

使用 create-restore-image-task 命令。使用来自 S3ObjectKey 输出的 Bucket 和 describe-store-image-tasks 的值，请指定 AMI 的对象键以及要将 AMI 复制到的 S3 存储桶的名称。还可以为还原的 AMI 指定名称。名称对该账户在该区域中的 AMI 必须唯一。

> **Note**
>
> 还原的 AMI 将获得一个新 AMI ID。

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket myamibucket \
    --name "New AMI Name"
```

预期输出

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
}
```

弃用 AMI

您可以弃用 AMI，以表明该 AMI 已过期且不应使用。您还可以为 AMI 指定未来弃用日期，表明 AMI 何时过期。例如，您可能会弃用不再主动维护的 AMI，或是已被较新版本取代的 AMI。默认情况下，已弃用的 AMI 不会显示在 AMI 列表中，防止新用户使用过期的 AMI。但是，现有用户和启动服务（如启动模板和 Auto Scaling 组）可以通过指定其 ID 来继续使用已弃用的 AMI。要删除 AMI 以便使用户和服务无法使用，您必须取消注册 (p. 188)。

AMI 弃用后：

- 对于 AMI 用户，已弃用的 AMI 不会显示在 DescribeImages API 调用中，除非您指定其 ID 或要求必须显示已弃用的 AMI。AMI 拥有者可继续在 DescribeImages API 调用中看到已弃用的 AMI。
- 对于 AMI 用户，已弃用的 AMI 无法通过 EC2 控制台进行选择。例如，已弃用的 AMI 不会出现在启动实例向导的 AMI 目录中。AMI 拥有者可继续在 EC2 控制台中看到已弃用的 AMI。
- 对于 AMI 用户，如果您知道已弃用的 AMI 的 ID，则可以通过 API、CLI 或开发工具包继续使用已弃用的 AMI 启动实例。
- 启动服务（如启动模板和 Auto Scaling 组）可以继续引用已弃用的 AMI。
- 使用随后被弃用的 AMI 启动的 EC2 实例不会受到影响，可以停止、启动和重新启动。

您可以弃用私有和公用 AMI。

您还可以创建 Amazon Data Lifecycle Manager EBS 支持的 AMI 策略，以自动化 EBS 支持的 AMI 的弃用。有关更多信息，请参阅自动化 AMI 生命周期 (p. 1462)。

Note

默认情况下，所有公用 AMI 的弃用日期设置为自 AMI 创建日期起的两年。您可以将弃用日期设置为早于两年。要取消弃用日期，或将弃用移至未来某一日期，您必须通过仅将 AMI 与特定 Amazon 账户共享 (p. 126)来将其设为私有。

主题

- 成本 (p. 184)
- 限制 (p. 181)
- 弃用 AMI (p. 184)
- 描述已弃用的 AMI (p. 185)
- 取消弃用 AMI (p. 187)

成本

当您弃用 AMI 时，不会删除该 AMI。AMI 拥有者须继续为 AMI 的快照付费。要停止支付快照费用，AMI 拥有者必须通过取消注册 (p. 188)删除 AMI。

限制

- 要弃用 AMI，您必须是 AMI 的拥有者。

弃用 AMI

您可以在特定日期和时间弃用 AMI。您必须是 AMI 拥有者才能执行此过程。

Console

在特定日期弃用 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航器中选择 AMI。
3. 从筛选栏中选择 Owned by me（我拥有的）。
4. 选取相应 AMI，然后选择 Actions（操作）、Manage AMI Deprecation（管理 AMI 弃用）。您可以选择多个 AMI，一次性为多个 AMI 设置同一弃用日期。
5. 选择 Enable（启用）复选框，然后输入弃用日期和时间。

   弃用日期的上限为从当前日期起 10 年，但公有 AMI 除外，其上限为自创建之日起 2 年。您不能指定一个过去的日期。
6. 选择 Save（保存）。

Amazon CLI

在特定日期弃用 AMI

使用 enable-image-deprecation 命令。指定 AMI 的 ID 以及弃用 AMI 的日期和时间。如果指定以秒为单位的值，Amazon EC2 会将秒四舍五入到最近的分钟数。

`deprecate-at` 的上限为从当前日期起 10 年，但公有 AMI 除外，后者的上限为自创建之日起 2 年。您不能指定一个过去的日期。

```
aws ec2 enable-image-deprecation \
```

```
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

预期输出

```
{
  "Return": "true"
}
```

上次启动时间

LastLaunchedTime 是一个时间戳，指示您上次使用 AMI 启动实例时的时间戳。最近未用于启动实例的 AMI 可能需要弃用或注销 (p. 188)。

Note

- 在使用 AMI 启动实例时，使用情况报告会有 24 小时的延迟。
- lastLaunchedTime 数据从 2017 年 4 月开始可用。

Console

查看 AMI 的上次启动时间

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航器中选择 AMI。
3. 从筛选栏中选择 Owned by me（我拥有的）。
4. 选择 AMI，然后检查 Last launched time（上次启动时间）字段 [选择 AMI 旁边的复选框后，该字段将在 Details（详细信息）选项卡中显示]。此字段显示了上次使用 AMI 启动实例的日期和时间。

Amazon CLI

查看 AMI 的上次启动时间

运行 describe-image-attribute 命令并指定 --attribute lastLaunchedTime。您必须是 AMI 的拥有者才能执行此命令。

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

输出示例

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

描述已弃用的 AMI

您可以查看 AMI 的弃用日期和时间，然后按弃用日期对所有 AMI 进行筛选。您也可以使用 Amazon CLI 来描述已弃用的所有 AMI（即已超出弃用日期）。

Console

查看 AMI 的弃用日期

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航器中选择 AMIs，然后选择相应 AMI。
3. 查看 Depreation time（弃用时间）字段 [如果选中了 AMI 旁边的复选框，则该字段位于 Details（详细信息）选项卡]。该字段将显示 AMI 的弃用日期和时间。如果该字段为空，表示该 AMI 未遭弃用。

按弃用日期筛选 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航器中选择 AMI。
3. 从筛选栏中选择 Owned by me（我拥有的）或 Private images（私有映像）（私有映像包括与您共享的 AMI 以及您拥有的 AMI）。
4. 在搜索栏中输入 **`Deprecation time`**（输入字母时会出现 Deprecation time（弃用时间）筛选器），然后选择运算符以及日期和时间。

Amazon CLI

当您使用 describe-images 命令时，结果会因您是 AMI 用户或 AMI 拥有者而有所不同。

- 如果您是 AMI 用户：

  默认情况下，当您使用 describe-images 命令描述所有 AMI 时，不属于您但与您共享的已弃用 AMI 不会出现在结果中。这是因为默认值为 `--no-include-deprecated`。要在结果中包括已弃用的 AMI，您必须指定 `--include-deprecated` 参数。
- 如果您是 AMI 拥有者：

  当您使用 describe-images 命令描述所有 AMI 时，您拥有的所有 AMI（包括已弃用的 AMI）均会显示在结果中。您无需指定 `--include-deprecated` 参数。此外，您不能通过使用 `--no-include-deprecated` 从结果中排除已弃用的 AMI。

如果 AMI 被弃用，`DeprecationTime` 字段将显示在结果中。

> **Note**
>
> 已弃用的 AMI 是指弃用日期在过去的 AMI。如果您已将弃用日期设置为将来的日期，则 AMI 尚未弃用。

在描述所有 AMI 时包括所有已弃用的 AMI

使用 describe-images 命令并指定 `--include-deprecated` 参数，以在结果中包括非您所有的所有已弃用的 AMI。

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

描述 AMI 的弃用日期

使用 describe-images 命令并指定 AMI 的 ID。

请注意，如果您同时指定 `--no-include-deprecated` 与 AMI ID，则会在结果中返回已弃用的 AMI。

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

预期输出

`DeprecationTime` 字段显示将 AMI 设置为已弃用的日期。如果 AMI 未设置为已弃用，则 `DeprecationTime` 字段不会显示在输出结果中。

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

取消弃用 AMI

您可以取消弃用 AMI，即删除 Deprecation time（弃用时间）字段（控制台），或从 describe-images 输出 (Amazon CLI) 中删除 `DeprecationTime` 字段。您必须是 AMI 拥有者才能执行此过程。

Console

取消弃用 AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在左侧导航器中选择 AMI。
3. 从筛选栏中选择 Owned by me（我拥有的）。
4. 选取相应 AMI，然后选择 Actions（操作）、Manage AMI Deprecation（管理 AMI 弃用）。您可以选择多个 AMI，一次性取消对多个 AMI 的弃用。
5. 取消选中 Enable（启用）复选框，然后选择 Save（保存）。

Amazon CLI

取消弃用 AMI

使用 disable-image-deprecation 命令并指定 AMI 的 ID。

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

预期输出

```
{
  "Return": "true"
}
```

注销您的 AMI

使用完 AMI 之后，可以注销它。注销 AMI 之后，便无法将其用于启动新实例。

在注销 AMI 时，不会影响已从 AMI 创建的任何实例或在创建 AMI 的过程中创建的任何快照。这些实例和快照的存储成本将继续对您产生使用费用。因此，您应终止您已使用完的任何实例并删除任何快照。

用于清除 AMI 的过程取决于它是由 Amazon EBS 还是由实例存储支持。有关更多信息，请参阅确定 AMI 的根设备类型 (p. 104)。

目录

- 注意事项 (p. 188)
- 清除Amazon EBS-backed AMI (p. 188)
- 清除由实例存储支持的 AMI (p. 191)
- 上次启动时间 (p. 192)

注意事项

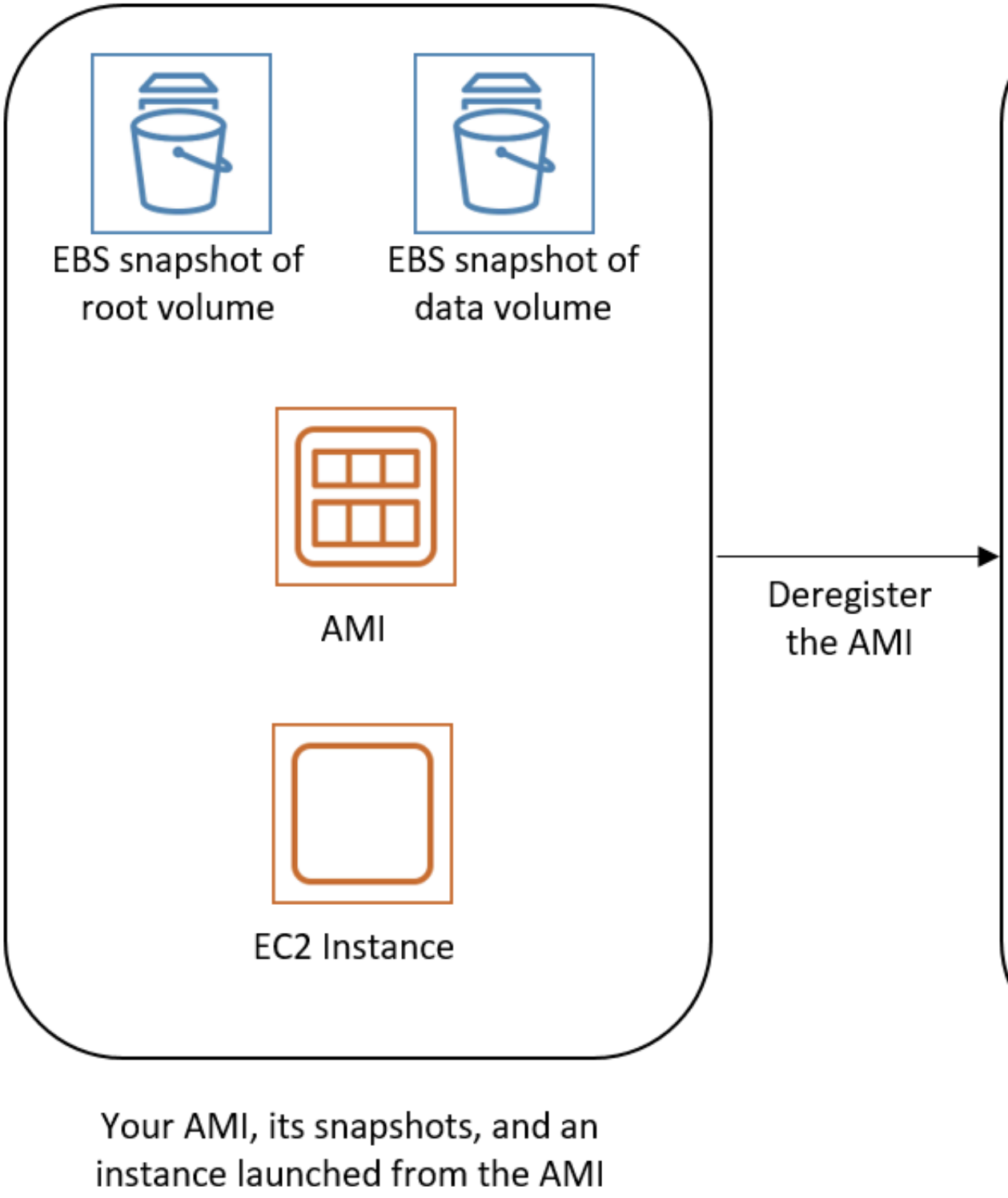
取消注册 AMI 时需考虑以下事项：

- 您无法取消注册不属于您账户所有的 AMI。
- 您无法取消注册由 Amazon Backup 服务使用 Amazon EC2 管理的 AMI。而是应该使用 Amazon Backup 删除备份文件库中相应的恢复点。有关更多信息，请参阅 Amazon Backup 开发人员指南中的删除备份。

清除Amazon EBS-backed AMI

在注销Amazon EBS-backed AMI 时，不会影响在 AMI 创建过程中为实例的卷创建的快照。这些快照将继续产生存储费用。因此，如果使用完这些快照，应将其删除。

下图演示了清除Amazon EBS-backed AMI 的过程。



您可以使用下面的任意一种方法清除 Amazon EBS-backed AMI。

New console

清除Amazon EBS-backed AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 注销 AMI
   a. 在导航窗格中，选择 AMIs。
   b. 选择要取消注册的 AMI，记下它的 ID – 这有助于您在下一步骤中找到要删除的快照。
   c. 选择 Actions（操作）、Deregister AMI（取消注册 AMI）。当系统提示您确认时，选择 Deregister AMI（取消注册 AMI）。

      Note

      控制台可能需要几分钟才能从列表中删除该 AMI。选择 Refresh 以刷新状态。
3. 删除不再需要的快照
   a. 在导航窗格中，选择快照。
   b. 选择要删除的快照（在 Description 列中查找上一步中的 AMI ID）。
   c. 选择 Actions（操作）、Delete snapshot（删除快照）。当系统提示进行确认时，选择 Delete（删除）。
4. （可选）终止实例

   如果您使用完从 AMI 启动的实例，则可以终止该实例。
   a. 在导航窗格中，选择 Instances（实例），然后选择要终止的实例。
   b. 依次选择实例状态、终止实例。当系统提示您确认时，选择终止。

Old console

清除Amazon EBS-backed AMI

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 注销 AMI
   a. 在导航窗格中，选择 AMIs。
   b. 选择要注销的 AMI，记下它的 ID — 这有助于您在下一步中找到要删除的快照。
   c. 选择 Actions、Deregister。当系统提示进行确认时，请选择 Continue。

      Note

      控制台可能需要几分钟时间才能从列表中删除该 AMI。选择 Refresh 以刷新状态。
3. 删除不再需要的快照
   a. 在导航窗格中，选择快照。
   b. 选择要删除的快照（在 Description 列中查找上一步中的 AMI ID）。
   c. 依次选择 Actions（操作）和 Delete（删除）。当系统提示进行确认时，选择 Yes, Delete（是，删除）。
4. （可选）终止实例

   如果您使用完从 AMI 启动的实例，则可以终止该实例。
   a. 在导航窗格中，选择 Instances（实例），然后选择要终止的实例。
   b. 依次选择 Actions（操作）、Instance State（实例状态）和 Terminate（终止）。当系统提示您确认时，选择 Yes, Terminate（是，终止）。

Amazon CLI

请按照以下步骤清除Amazon EBS-backed AMI

1. 注销 AMI

   使用 deregister-image 命令注销 AMI：

   ```
   aws ec2 deregister-image --image-id ami-12345678
   ```

2. 删除不再需要的快照

   使用 delete-snapshot 命令删除不再需要的快照：

   ```
   aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0
   ```

3. 终止实例（可选）

   如果您使用完从 AMI 启动的实例，则可以使用 terminate-instances 命令终止该实例：

   ```
   aws ec2 terminate-instances --instance-ids i-12345678
   ```

PowerShell

请按照以下步骤清除Amazon EBS-backed AMI

1. 注销 AMI

   使用 Unregister-EC2Image cmdlet 注销 AMI：

   ```
   Unregister-EC2Image -ImageId ami-12345678
   ```

2. 删除不再需要的快照

   使用 Remove-EC2Snapshot cmdlet 删除不再需要的快照：

   ```
   Remove-EC2Snapshot -SnapshotId snap-12345678
   ```

3. 终止实例（可选）

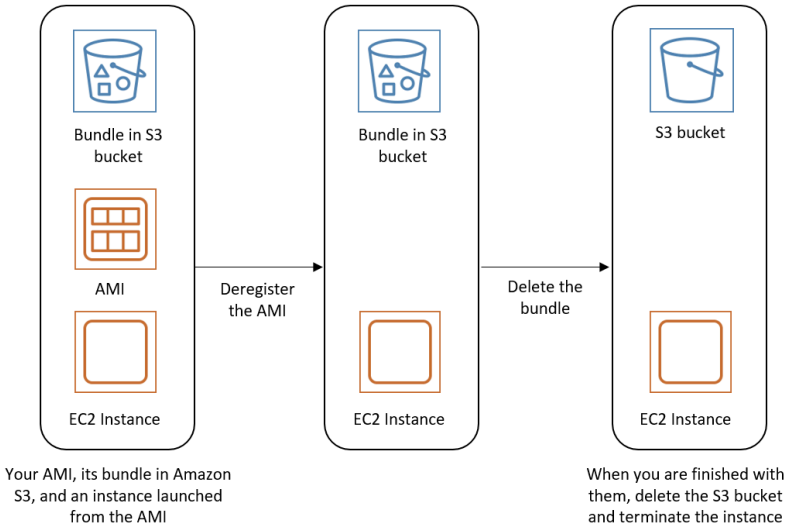
   如果您使用完从 AMI 启动的实例，则可以使用 Remove-EC2Instance cmdlet 终止该实例：

   ```
   Remove-EC2Instance -InstanceId i-12345678
   ```

清除由实例存储支持的 AMI

注销某个由实例存储支持的 AMI 时，不会影响您在创建该 AMI 时上传到 Amazon S3 的文件。这些文件将继续在 Amazon S3 中对您产生使用费用。因此，如果您使用完这些文件，应删除它们。

下图说明清除由实例存储支持的 AMI 的过程。



清除由实例存储支持的 AMI

1. 使用 deregister-image 命令取消注册 AMI，如下所示。

```
aws ec2 deregister-image --image-id ami_id
```

2. 使用 ec2-delete-bundle (p. 162)（AMI 工具）命令删除 Amazon S3 中的捆绑包，如下所示。

```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -s your_secret_access_key
 -p image
```

3. （可选）如果您使用完从 AMI 启动的实例，则可以使用 terminate-instances 命令终止该实例，如下所示。

```
aws ec2 terminate-instances --instance-ids instance_id
```

4. （可选）如果您使用完将捆绑上传到的 Amazon S3 存储桶，则可以删除该存储桶。要删除 Amazon S3 存储桶，请打开 Amazon S3 控制台，选择存储桶，再选择 Actions，然后选择 Delete。

上次启动时间

`LastLaunchedTime` 是一个时间戳，指示您上次使用 AMI 启动实例时的时间戳。最近未用于启动实例的 AMI 可能需要注销或启用 (p. 183)。

Note

- 在使用 AMI 启动实例时，使用情况报告会有 24 小时的延迟。
- `lastLaunchedTime` 数据从 2017 年 4 月开始可用。

Console

查看 AMI 的上次启动时间

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在左侧导航器中选择 AMI。
3. 从筛选栏中选择 Owned by me（我拥有的）。
4. 选择 AMI，然后检查 Last launched time（上次启动时间）字段 [选择 AMI 旁边的复选框后，该字段将在 Details（详细信息）选项卡中显示]。此字段显示了上次使用 AMI 启动实例的日期和时间。

Amazon CLI

查看 AMI 的上次启动时间

运行 describe-image-attribute 命令并指定 `--attribute lastLaunchedTime`。您必须是 AMI 的拥有者才能执行此命令。

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

输出示例

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

从回收站恢复 AMI

回收站是一项数据恢复功能，支持您还原意外删除的 Amazon EBS 快照和 EBS 支持的 AMI。使用回收站时，如果资源被删除，回收站功能将在您指定的时间段内保留快照，而后永久删除资源。

在资源保留期到期之前，您可以随时从回收站还原资源。从回收站还原资源后，资源将从回收站中删除，您可以像使用账户中任何该类型的其他资源的一样使用此资源。如果保留期过期且资源未还原，则资源将从回收站中永久删除，并且不再可用于恢复。

回收站中的 AMI 不会产生任何额外费用。

有关更多信息，请参阅回收站 (p. 1627)。

主题

- 使用回收站中的 AMI 的权限 (p. 193)
- 查看回收站中的 AMI (p. 194)
- 从回收站还原 AMI (p. 195)

使用回收站中的 AMI 的权限

默认情况下，用户无权使用回收站中的 AMI。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

要查看和恢复回收站中的 AMI，用户必须具有以下权限：

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

要管理回收站中 AMI 的标签，用户需要以下额外权限。

- ec2:CreateTags
- ec2:DeleteTags

要使用回收站控制台，用户需要 ec2:DescribeTags 权限。

以下是 IAM policy 示例。其中包括控制台用户的 ec2:DescribeTags 权限，以及用于管理标签的 ec2:CreateTags 和 ec2:CreateTags 权限。如果不需要上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用回收站所需权限的更多信息，请参阅 使用回收站和保留规则的权限 (p. 1631)。

查看回收站中的 AMI

如果 AMI 位于回收站中，则只能查看该 AMI 的有限信息，包括：

- AMI 的名称、描述和唯一 ID。
- AMI 被删除并放入回收站的日期和时间。
- 保留期到期的日期和时间。此后，系统会永久删除 AMI。

您可以使用以下某种方法查看回收站中的 AMI。

Recycle Bin console

使用控制台查看回收站中的已删除 AMI

1. 在以下位置打开回收站控制台 console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该表格列出了当前在回收站中的所有资源。要查看特定 AMI 的详细信息，请在表格中选择所需 AMI，然后选择 Actions（操作）、View details（查看详细信息）。

Amazon CLI

使用 Amazon CLI 查看回收站中的已删除 AMI

使用 list-images-in-recycle-bin Amazon CLI 命令。要查看特定 AMI，请在命令中包括 `--image-id` 选项并指定要查看的 AMI 的 ID。在单个请求中，您最多可以指定 20 个 ID。

要查看回收站中的所有 AMI，请省略 `--image-id` 选项。如果没有为 `--max-items` 指定值，命令默认每页将返回 1000 个项目。有关更多信息，请参阅《Amazon EC2 API 参考》中的分页。

```
$ aws ec2 list-images-in-recycle-bin --image-id ami_id
```

例如，以下命令提供回收站中 AMI `ami-01234567890abcdef` 的相关信息。

```
$ aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

输出示例：

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

Important

如果您收到以下错误，您可能需要更新 Amazon CLI 版本。有关更多信息，请参阅找不到命令错误。

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

从回收站还原 AMI

当 AMI 在回收站中时，您不能以任何方式使用它。要使用该 AMI，您必须先还原它。从回收站还原 AMI 时，该 AMI 立即可供使用，回收站会将其删除。还原 AMI 后，您可以像使用账户中任何其他 AMI 一样使用它。

您可以使用以下方法之一从回收站还原 AMI。

Recycle Bin console

使用控制台从回收站还原 AMI

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com//rbin/home/
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该表格列出了当前在回收站中的所有资源。选择要还原的 AMI，然后选择 Recover（恢复）。
4. 系统提示时，选择 Recover（还原）。

Amazon CLI

使用 Amazon CLI 从回收站还原已删除的 AMI

使用 restore-image-from-recycle-bin Amazon CLI 命令。对于 `--image-id`，指定需还原 AMI 的 ID。

```
$ aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

例如，以下命令将 AMI `ami-01234567890abcdef` 从回收站中还原。

```
$ aws restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

命令成功后，不返回任何输出。

Important

如果您收到以下错误，您可能需要更新 Amazon CLI 版本。有关更多信息，请参阅找不到命令错误。

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

自动化 EBS 支持的 AMI 生命周期

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留、复制、弃用和取消注册 Amazon EBS-backed AMIs 及其备份快照。有关更多信息，请参阅Amazon Data Lifecycle Manager (p. 1448)。

将加密与 EBS 支持的 AMI 结合使用

由 Amazon EBS 快照支持的 AMI 可以利用 Amazon EBS 加密。可以将数据和根卷的快照加密并附加到 AMI。在启动实例和复制映像时，您可以包含 EBS 完全加密支持。在提供了 Amazon KMS 的所有区域中，支持在这些操作中使用加密参数。

从 AMIs 中启动带加密 EBS 卷的 EC2 实例的方式与其他实例相同。另外，从未加密 EBS 快照支持的 AMI 中启动实例时，您可以在启动过程中将部分或全部卷加密。

与 EBS 卷相似，可使用默认 Amazon KMS key 或您指定的客户托管密钥加密 AMI 中的快照。在所有情况下，您都必须拥有使用所选 KMS 密钥 的权限。

带加密快照的 AMI 可以跨 Amazon 账户共享。有关更多信息，请参阅共享 AMI (p. 121)。

“将加密与 EBS 支持的 AMI 结合使用”相关主题

- 启动实例场景 (p. 197)
- 映像复制场景 (p. 199)

启动实例场景

Amazon EC2 实例是通过 Amazon Web Services Management Console 或者直接使用 Amazon EC2 API 或 CLI，使用 `RunInstances` 操作以及通过块储存设备映射提供的参数在 AMI 中启动的。有关数据块设备映射的更多信息，请参阅数据块设备映射。有关通过 Amazon CLI 控制数据块设备映射的示例，请参阅启动、列出和终止 EC2 实例。

如果不使用显式加密参数，在默认情况下，`RunInstances` 操作会在从 AMI 的源快照中还原 EBS 卷时保持这些快照的现有加密状态。如果启用默认加密 (p. 1507)，从 AMI 中（无论使用加密还是未加密的快照）创建的所有卷都会被加密。如果在默认情况下并未启用加密，则实例保持 AMI 的加密状态。

您也可以启动实例，同时通过提供加密参数来对结果卷应用新的加密状态。因此，会观察到以下行为：

启动时不指定加密参数

- 未加密快照会还原为未加密卷，除非已在默认情况下启用加密，那么所有新创建的所有卷都将加密。
- 您拥有的加密快照会还原为使用相同 KMS 密钥 加密的卷。
- 您未拥有的加密快照（例如，与您共享了 AMI）会还原到由您的 Amazon 账户的默认 KMS 密钥加密的卷。

可以通过提供加密参数覆盖默认行为。可用参数包括 `Encrypted` 和 `KmsKeyId`。仅设置 `Encrypted` 参数会得到以下结果：

已设置 **`Encrypted`**，但未指定 **`KmsKeyId`** 时的实例启动行为

- 未加密快照会还原到由您的 Amazon 账户的默认 KMS 密钥加密的 EBS 卷。
- 您拥有的加密快照会还原到由相同 KMS 密钥 加密的 EBS 卷。（也就是说，`Encrypted` 参数没有影响。）
- 您未拥有的加密快照（即，与您共享了 AMI）会还原到由您的 Amazon 账户的默认 KMS 密钥加密的卷。（也就是说，`Encrypted` 参数没有影响。）

如果同时设置 `Encrypted` 和 `KmsKeyId` 参数，可以为加密操作指定非默认 KMS 密钥。会实现以下行为：

同时设置 **`Encrypted`** 和 **`KmsKeyId`** 的实例

- 未加密快照会还原到由指定 KMS 密钥 加密的 EBS 卷。
- 加密快照还原为未使用原始 KMS 密钥 加密，而是使用指定 KMS 密钥 加密的 EBS 卷。

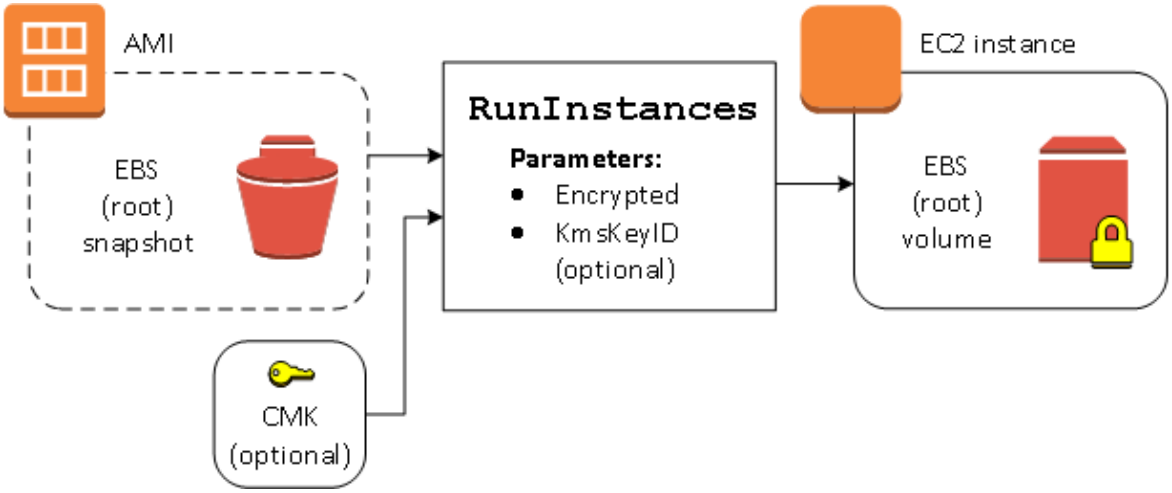
提交 `KmsKeyId` 但没有同时设置 `Encrypted` 参数会导致错误。

以下部分提供使用非默认加密参数从 AMI 中启动实例的示例。在以下每个场景中，提供给 `RunInstances` 操作的参数会导致在使用快照还原卷的过程中加密状态发生变化。

有关使用控制台从 AMI 启动实例的信息，请参阅 启动实例 (p. 574)。

在启动过程中加密卷

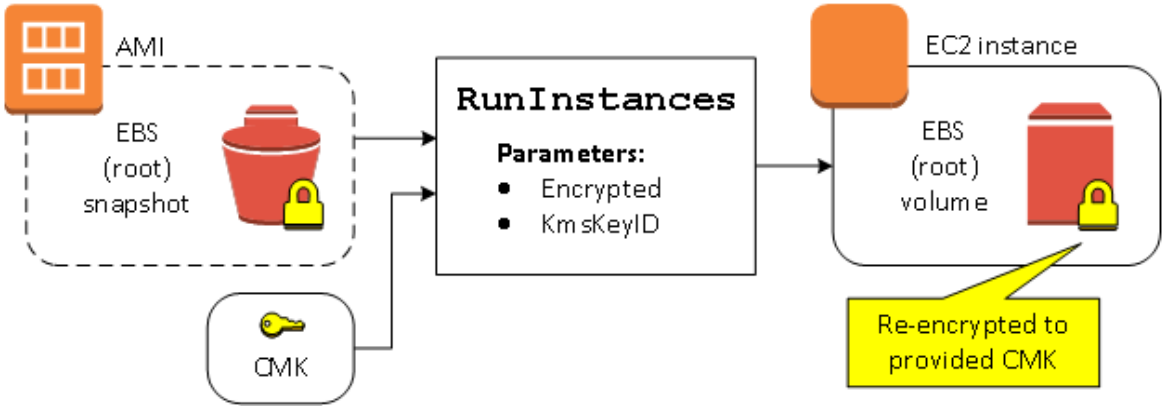
在该示例中，使用未加密快照支持的 AMI 启动带加密 EBS 卷的 EC2 实例。



仅使用 `Encrypted` 参数的结果是对该实例中的卷行加密。提供 `KmsKeyId` 参数是可选的。如果未指定 KMS 密钥 ID，会使用 Amazon 账户的默认 KMS 密钥加密卷。要使用您拥有的不同 KMS 密钥 加密卷，请提供 `KmsKeyId` 参数。

在启动过程中重新加密卷

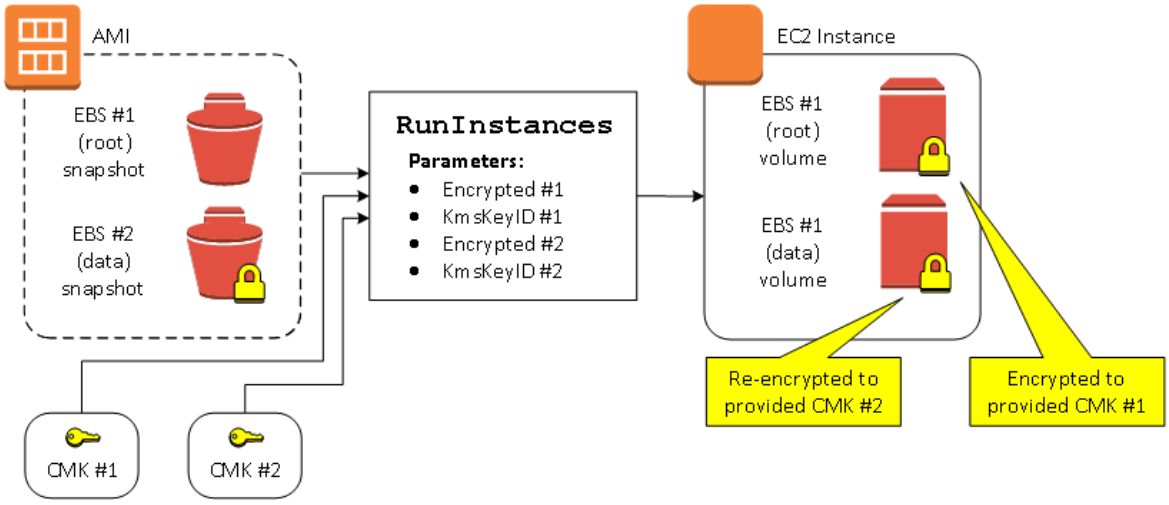
在该示例中，使用加密快照支持的 AMI 启动带有由新 KMS 密钥 加密的 EBS 卷的 EC2 实例。



如果您拥有 AMI 且未提供加密参数，则生成的实例具有由与快照相同的 KMS 密钥 加密的卷。如果 AMI 是与他人共享而不是由您拥有，且您未提供加密参数，则由您的默认 KMS 密钥 对卷进行加密。如果按所示提供加密参数，则会由指定 KMS 密钥 对卷进行加密。

在启动过程中更改多个卷的加密状态

在这一更为复杂的示例中，会使用多个快照（分别具有自己的加密状态）支持的 AMI 启动带有新加密卷和重新加密卷的 EC2 实例。



在这种情况下，会为 RunInstances 操作提供用于各个源快照的加密参数。在指定所有可用的加密参数后，无论您是否拥有 AMI，结果实例都相同。

映像复制场景

可通过 Amazon Web Services Management Console 或者直接使用 Amazon EC2 API 或 CLI，使用 CopyImage 操作复制 Amazon EC2 AMI。

如果不使用显式加密参数，在默认情况下，CopyImage 操作会在复制 AMI 的源快照时保持这些快照的现有加密状态。您也可以复制 AMI，同时通过提供加密参数来对其关联的 EBS 快照应用新的加密状态。因此，会观察到以下行为：

复制时不指定加密参数

- 未加密快照会复制为另一个未加密快照，除非已在默认情况下启用加密，那么所有新创建的快照都将加密。
- 您拥有的加密快照会复制为使用相同 KMS 密钥 加密的快照。
- 您未拥有的加密快照（例如，与您共享了 AMI）会复制为由您的 Amazon 账户的默认 KMS 密钥加密的快照。

可以通过提供加密参数覆盖以上所有默认行为。可用参数包括 Encrypted 和 KmsKeyId。仅设置 Encrypted 参数会得到以下结果：

已设置 **Encrypted**，但未指定 **KmsKeyId** 时的复制映像行为

- 未加密快照会复制为由 Amazon 账户的默认 KMS 密钥加密的快照。
- 加密快照会复制为由相同 KMS 密钥 加密的快照。（也就是说，Encrypted 参数没有影响。）
- 您未拥有的加密快照（即，与您共享了 AMI）会复制为由您的 Amazon 账户的默认 KMS 密钥加密的卷。（也就是说，Encrypted 参数没有影响。）

通过同时设置 Encrypted 和 KmsKeyId 参数，可以为加密操作指定客户托管的 KMS 密钥。会实现以下行为：

同时设置 **Encrypted** 和 **KmsKeyId** 时的复制映像行为

- 未加密快照会复制为由指定 KMS 密钥 加密的快照。
- 加密快照会复制为未使用原始 KMS 密钥 加密，而是使用指定 KMS 密钥 加密的快照。

提交 KmsKeyId 但没有同时设置 Encrypted 参数会导致错误。

以下部分提供使用非默认加密参数复制 AMI，导致更改加密状态的示例。

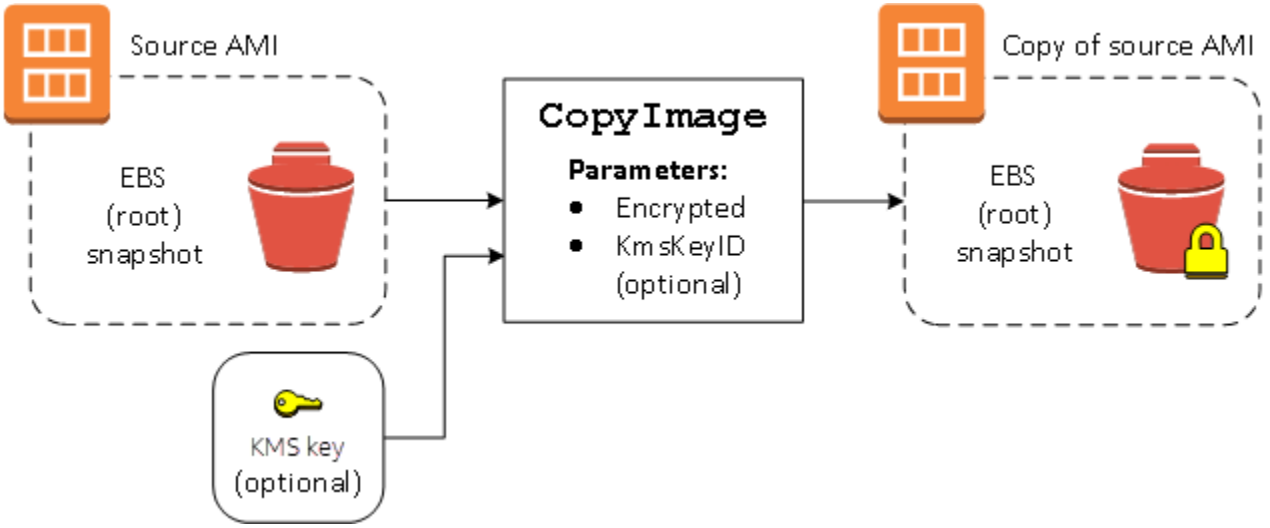
有关使用控制台的说明，请参阅 复制 AMI (p. 172)。

在复制过程中将未加密映像加密

在这种情况下，由未加密根快照支持的 AMI 会复制到带加密根快照的 AMI。CopyImage 操作将使用两个加密参数（包括一个客户托管密钥）调用。因此，根快照的加密状态发生变化，这样目标 AMI 由与原快照具有相同数据的根快照支持，但使用指定的密钥进行加密。在两个 AMI 中，您都会产生快照的存储成本，以及从任一 AMI 启动的任何实例的费用。

Note

启用默认加密 (p. 1507)与将 AMI 中所有快照的 Encrypted 参数设置为 true 具有相同的效果。



设置 Encrypted 参数会加密此实例的单个快照。如果您未指定 KmsKeyId 参数，会使用默认客户托管密钥来加密快照副本。

Note

您也可以复制带多个快照的映像，并单独配置每个快照的加密状态。

使用 Amazon EventBridge 监控 AMI 事件

当 Amazon Machine Image（AMI）状态发生变化时，Amazon EC2 将生成发送到 Amazon EventBridge（以前称为 Amazon CloudWatch Events）的事件。您可以使用 Amazon EventBridge 检测并响应这些事件。要做到这一点，您可以在 EventBridge 中创建触发操作以响应事件的规则。例如，您可以创建 EventBridge 规则，以检测 AMI 创建过程何时完成，然后调用 Amazon SNS 主题以向您发送电子邮件通知。

当 AMI 进入以下任何状态时，Amazon EC2 将生成事件：

- available
- failed
- deregistered

当以下 AMI 操作之一运行时，AMI 可以进入 available 或 failed 状态：

- CreateImage
- CopyImage
- RegisterImage
- CreateRestoreImageTask

当以下 AMI 操作运行时，AMI 可以进入 `deregistered` 状态：

- DeregisterImage

事件将尽最大努力生成。

主题

- AMI 事件 (p. 201)
- 创建 Amazon EventBridge 规则 (p. 203)

AMI 事件

这里有三个 EC2 AMI State Change 事件：

- available (p. 201)
- failed (p. 202)
- deregistered (p. 202)

事件以 JSON 格式发送到默认的 EventBridge 事件总线。

事件中的以下字段可用于创建触发操作的规则：

`"source": "aws.ec2“`

识别来自 Amazon EC2 的事件。

`"detail-type": "EC2 AMI State Change"`

识别事件名称。

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

提供以下信息：

- AMI ID – 如果您想要跟踪特定 AMI。
- AMI 的状态（`available`、`failed` 或 `deregistered`）。

available

以下是 Amazon EC2 在 AMI 于 CreateImage、CopyImage、RegisterImage 或 CreateRestoreImageTask 操作成功后进入 `available` 状态时所生成的事件的示例。

`"State": "available"` 表明操作成功。

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

failed

以下是 Amazon EC2 在 AMI 于 CreateImage、CopyImage、RegisterImage 或 CreateRestoreImageTask 操作失败后进入 `failed` 状态时所生成的事件的示例。

以下字段提供相关信息：

- `"State": "failed"` – 指示操作失败。
- `"ErrorMessage": ""` – 提供操作失败的原因。

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
        "ErrorMessage": "Description of failure"
    }
}
```

deregistered

以下是 Amazon EC2 在 AMI 于 DeregisterImage 操作成功后进入 `deregistered` 状态时所生成的事件的示例。如果操作失败，则不会生成任何事件。由于 DeregisterImage 是同步操作，任何故障都能被立即知晓。

`"State": "deregistered"` 表明 DeregisterImage 操作成功。

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

创建 Amazon EventBridge 规则

您可以创建 Amazon EventBridge 规则，以指定当 EventBridge 收到与规则中的事件模式匹配的事件时要采取的措施。当事件匹配时，EventBridge 会将事件发送到指定的目标并触发规则中定义的操作。

事件模式与它们匹配的事件具有相同的结构。事件模式匹配或不匹配事件。

为 AMI 状态更改事件创建规则时，您可以在事件模式中包含以下字段：

`"source": "aws.ec2“`

识别来自 Amazon EC2 的事件。

`"detail-type": "EC2 AMI State Change"`

识别事件名称。

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

提供以下信息：

- AMI ID – 如果您想要跟踪特定 AMI。
- AMI 的状态（`available`、`failed` 或 `deregistered`）。

示例：创建 EventBridge 规则以发送通知

下面的示例可创建 EventBridge 规则，以便在任何 AMI 在 CreateImage 操作成功完成后处于 `available` 时发送电子邮件、文本消息或移动推送通知。

创建 EventBridge 规则之前，您必须为电子邮件、短信或移动推送通知创建 Amazon SNS 主题。

要创建 EventBridge 规则以在 AMI 创建并处于 **`available`** 状态时发送通知

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于定义规则详细信息，请执行以下操作：

   a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

      规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

   b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。

   c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。

   d. 选择 Next（下一步）。

4. 对于 Build event pattern（构建事件模式），执行以下操作：

   a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。

   b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 AMI 进入 `available` 状态时生成的任何 `EC2 AMI State Change` 事件：

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 AMI State Change"],
 "detail": {"State": ["available"]}
}
```

      要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

i. 要使用模板创建事件模式，请执行以下操作：

A. 选择 Event pattern form（事件模式表）。
B. 对于 Event source（事件源），选择 Amazon services（服务）。
C. 对于 Amazon 服务，选择 EC2。
D. 对于 Event type（事件类型），选择 EC2 AMI State Change（EC2 AMI 状态更改）。
E. 要自定义模板，请选择 Edit pattern（编辑模式），然后进行更改以匹配示例事件模式。

ii. 要指定自定义事件模式，请执行以下操作：

A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。
B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。

c. 选择 Next（下一步）。

5. 对于 Select target(s)（选择目标），请执行以下操作：

a. 对于 Target types（目标类型），选择 Amazon service（服务）。
b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。
c. 对于 Topic（主题），选择现有主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。
d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。
e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。
7. 对于 Review and create（查看与创建），执行以下操作：

a. 查看规则的详细信息并根据需要对其进行修改。
b. 选择 Create rule（创建规则）。

有关更多信息，请参阅《Amazon EventBridge 用户指南》中的以下主题：

- Amazon EventBridge 事件
- Amazon EventBridge 事件模式
- Amazon EventBridge 规则

有关如何创建 Lambda 函数和运行 Lambda 函数的 EventBridge 规则的教程，请参阅《Amazon Lambda 开发人员指南》中的教程：使用 EventBridge 记录 Amazon EC2 实例的状态。

了解 AMI 账单信息

启动实例时，有许多 Amazon Machine Image (AMI) 可供选择，它们支持各种操作系统平台和功能。要了解您在启动实例时选择的 AMI 如何影响 Amazon 账单的底线，您可以研究相关的操作系统平台和账单信息。在启动任何按需或竞价型实例之前执行此操作，或者购买预留实例。

下面是关于提前研究 AMI 如何帮助您选择最适合自己需求的 AMI 的两个示例：

- 对于竞价型实例，您可以使用 AMI Platform details (平台详细信息) 来确认对于竞价型实例支持 AMI。
- 购买时 Reserved Instance 时，您可以确保选择映射到 AMI Platform details (平台详细信息) 的操作系统平台（Platform [平台]）。

有关实例定价的更多信息，请参阅 Amazon EC2 定价。

目录

- AMI 账单信息字段 (p. 205)
- 查找 AMI 账单和使用详细信息 (p. 206)
- 验证账单上的 AMI 费用 (p. 208)

AMI 账单信息字段

以下字段提供与 AMI 关联的账单信息：

平台详细信息

与 AMI 的账单代码关联的平台详细信息。例如：`Red Hat Enterprise Linux`。

使用情况操作

Amazon EC2 实例的操作以及与 AMI 关联的账单代码。例如：`RunInstances:0010`。Usage operation (使用情况操作) 对应于 Amazon 成本和使用情况报告 (CUR) 和 Amazon 价目表 API 中的 lineitem/Operation 列。

您可以在 Amazon EC2 控制台的 Instances (实例) 或 AMI 页面上查看这些字段，或者在 describe-images 命令返回的响应中查看这些字段。

示例数据：按平台划分的使用情况操作

下表列出了一些平台详细信息和使用情况操作值，这些信息显示在 Amazon EC2 控制台的 Instances (实例) 或 AMI 页面上，或者显示在由 describe-images 命令返回的响应中。

平台详细信息	使用情况操作 **
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
采用 SQL Server 标准版和 HA 的 Red Hat Enterprise Linux	RunInstances:1014
采用 SQL Server 企业版和 HA 的 Red Hat Enterprise Linux	RunInstances:1110
采用 SQL Server 标准版的 Red Hat Enterprise Linux	RunInstances:0014
采用 SQL Server Web 的 Red Hat Enterprise Linux	RunInstances:0210
采用 SQL Server 企业版的 Red Hat Enterprise Linux	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200

平台详细信息	使用情况操作 **
SUSE Linux	RunInstances:000g
Windows	RunInstances:0002
Windows BYOL	RunInstances:0800
使用 SQL Server Enterprise 的 Windows *	RunInstances:0102
使用 SQL Server Standard 的 Windows *	RunInstances:0006
使用 SQL Server Web 的 Windows *	RunInstances:0202

* 如果两个软件许可证与 AMI 关联，则 Platform details (平台详细信息) 字段将显示两者。

** 如果您正在运行竞价型实例，则 Amazon 成本和使用情况报告上的 `lineitem/Operation` 可能与此处列出的 Usage operation (使用情况操作) 值不同。例如，如果 `lineitem/Operation` 显示 `RunInstances:0010:SV006`，则表示 Amazon EC2 正在 VPC 区域 #6 中的美国东部（弗吉尼亚）运行 Red Hat Enterprise Linux 竞价型实例小时。

查找 AMI 账单和使用详细信息

在 Amazon EC2 控制台中，您可以从 AMI 页面或 Instances (实例) 页面查看 AMI 账单信息。您也可以使用 Amazon CLI 或实例元数据服务查找账单信息。

下列字段可以帮助您验证账单上的 AMI 费用：

- 平台详细信息
- 使用情况操作
- AMI ID

查找 AMI 账单信息（控制台）

请按照以下步骤在 Amazon EC2 控制台中查看 AMI 账单信息：

从 AMI 页面查找 AMI 账单信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 AMI，然后选择 AMI。
3. 在 Details (详细信息) 选项卡上，检查 Platform details (平台详细信息) 和 Usage operation (使用情况操作) 的值。

从 Instances (实例) 页面查找 AMI 账单信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择一个实例。
3. 在 Details (详细信息) 选项卡（如果您使用的是以前版本的控制台，则为 Description (描述) 选项卡）中，检查 Platform details (平台详细信息) 和 Usage operation (使用情况操作) 的值。

查找 AMI 账单信息 (Amazon CLI)

要使用 Amazon CLI 查找 AMI 账单信息，您需要知道 AMI ID。如果您不知道 AMI ID，则可以使用 describe-instances 命令从实例获取该 AMI ID。

查找 AMI ID

如果您知道实例 ID，则可以使用 describe-instances 命令获取实例的 AMI ID。

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

在输出中，在 ImageId 字段中指定了 AMI ID。

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

查找 AMI 账单信息

如果您知道 AMI ID，则可以使用 describe-images 命令获取 AMI 平台和使用情况操作详细信息。

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

以下示例输出显示了 PlatformDetails 和 UsageOperation 字段。在此示例中，ami-0123456789EXAMPLE 平台是 Red Hat Enterprise Linux，使用情况操作和账单代码是 RunInstances:0010。

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-1112223333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
```

```
}
```

验证账单上的 AMI 费用

为确保您不会产生计划外费用，您可以验证 Amazon 成本和使用情况报告 (CUR) 中某个实例的账单信息和与您用于启动实例的 AMI 关联的账单信息匹配。

要验证账单信息，请在 CUR 中找到实例 ID 并检查 `lineitem/Operation` 列中的相应值。该值应和与 AMI 关联的 Usage operation (使用情况操作) 的值相匹配。

例如，AMI `ami-0123456789EXAMPLE` 具有以下账单信息：

- Platform details (平台详细信息) = `Red Hat Enterprise Linux`
- Usage operation (使用情况操作) = `RunInstances:0010`

如果您使用此 AMI 启动了实例，您可以在 CUR 中找到实例 ID 并检查 `lineitem/Operation` 列中的相应值。在这个例子中，值应该是 `RunInstances:0010`。

Amazon Linux

Amazon Linux 由 Amazon Web Services (Amazon) 提供。它旨在为 Amazon EC2 上运行的应用程序提供稳定、安全和高性能的执行环境。此外，它还包括让您能够与 Amazon 轻松集成的程序包，包括启动配置工具和许多常见的 Amazon 库及工具。Amazon 为运行 Amazon Linux 的所有实例提供持续的安全性和维护更新。许多在 CentOS (及类似发行版) 上开发的应用程序在 Amazon Linux 上运行。

目录

- Amazon Linux 可用性 (p. 208)
- 连接到 Amazon Linux 实例 (p. 209)
- 识别 Amazon Linux 映像 (p. 209)
- Amazon 命令行工具 (p. 210)
- 程序包存储库 (p. 211)
- Extras 库 (Amazon Linux 2) (p. 213)
- Amazon Linux 2 支持的内核 (p. 213)
- 访问源软件包以获取参考信息 (p. 214)
- cloud-init (p. 215)
- 订阅 Amazon Linux通知 (p. 216)
- 作为虚拟机本地运行 Amazon Linux 2 (p. 218)
- Amazon Linux 2 上的内核实时修补 (p. 221)

Amazon Linux 可用性

Amazon 提供 Amazon Linux 2 和 Amazon Linux AMI。如果您要从其他 Linux 发行版迁移至 Amazon Linux，我们建议您迁移至 Amazon Linux 2。

Amazon Linux AMI 的最后一个版本 2018.03 已于 2020 年 12 月 31 日终止标准支持。有关更多信息，请参阅以下博客文章：Amazon Linux AMI 生命周期终止。如果您目前使用的是 Amazon Linux AMI，则建议您迁移至 Amazon Linux 2。要迁移至 Amazon Linux 2，请启动实例或使用当前 Amazon Linux 2 映像创建虚拟机。安装您的应用程序以及所有必需的软件包。测试您的应用程序，并进行使其在 Amazon Linux 2 上运行所需的任何更改。

有关更多信息，请参阅 Amazon Linux 2 和 Amazon Linux AMI。有关 Amazon Linux Docker 容器映像，请参阅 Docker Hub 上的 amazonlinux。

连接到 Amazon Linux 实例

默认情况下，Amazon Linux 不支持远程根安全 Shell（SSH）。此外，密码验证已禁用，以防止强力 (brute-force) 密码攻击。要在 Amazon Linux 实例上启用 SSH 登录，您必须在实例启动时为其提供密钥对。您还必须设置用于启动实例的安全组以允许 SSH 访问。默认情况下，唯一可以使用 SSH 进行远程登录的账户是 ec2-user；此账户还拥有 sudo 特权。如果您启用远程根登录，请注意，其安全性低于依靠密钥对和辅助用户。

识别 Amazon Linux 映像

每个映像都包含用于识别它的唯一的 `/etc/image-id` 文件。此文件包含有关映像的以下信息：

- `image_name`、`image_version`、`image_arch` – Amazon 用于构建映像的构建配方中的值。
- `image_stamp` - 映像创建期间随机生成的一个唯一的十六进制值。
- `image_date` – 映像创建的 UTC 时间，采用 YYYYMMDDhhmmss 格式。
- `recipe_name`、`recipe_id` - Amazon 用于构建映像的构建配方的名称和 ID。

Amazon Linux 包含 `/etc/system-release` 文件，用于指定当前已安装的版本。此文件使用 yum 进行更新，是 `system-release` RPM Package Manager（RPM）的一部分。

Amazon Linux 还包含遵循 Common Platform Enumeration（CPE）规范的 `/etc/system-release` 的机器可读版本；请参阅 `/etc/system-release-cpe`。

Amazon Linux 2

以下是当前 Amazon Linux 2 版本的 `/etc/image-id` 示例。

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn2-ami-hvm"
image_version="2"
image_arch="x86_64"
image_file="amzn2-ami-hvm-2.0.20180810-x86_64.xfs.gpt"
image_stamp="8008-2abd"
image_date="20180811020321"
recipe_name="amzn2 ami"
recipe_id="c652686a-2415-9819-65fb-4dee-9792-289d-1e2846bd"
```

以下是当前 Amazon Linux 2 版本的 `/etc/system-release` 示例。

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux 2
```

以下是 Amazon Linux 2 的 `/etc/os-release` 示例。

```
[ec2-user ~]$ cat /etc/os-release
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
```

```
HOME_URL="https://amazonlinux.com/"
```

Amazon Linux AMI

以下是当前 Amazon Linux AMI 版本的 `/etc/image-id` 示例。

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn-ami-hvm"
image_version="2018.03"
image_arch="x86_64"
image_file="amzn-ami-hvm-2018.03.0.20180811-x86_64.ext4.gpt"
image_stamp="cc81-f2f3"
image_date="20180811012746"
recipe_name="amzn ami"
recipe_id="5b283820-dc60-a7ea-d436-39fa-439f-02ea-5c802dbd"
```

以下是当前 Amazon Linux AMI 版本的 `/etc/system-release` 示例。

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux AMI release 2018.03
```

Amazon 命令行工具

以下 Amazon 集成命令行工具及使用方法包含在 Amazon Linux AMI 中或 Amazon Linux 2 的默认存储库中。有关 Amazon Linux AMI 中的程序包的完整列表，请参阅 Amazon Linux AMI 2017.09 程序包。

- aws-amitools-ec2
- aws-apitools-as
- aws-apitools-cfn
- aws-apitools-elb
- aws-apitools-mon
- aws-cfn-bootstrap
- aws-cli

Amazon Linux 2 和最低版本的 Amazon Linux（`amzn-ami-minimal-*` 和 `amzn2-ami-minimal-*`）并不总是包含所有这些程序包；但您可以使用以下命令来从默认存储库中安装它们：

```
[ec2-user ~]$ sudo yum install -y package_name
```

对于使用 IAM 角色启动的实例，提供了一个简单脚本，用于在安装凭证文件后准备 `AWS_CREDENTIAL_FILE`、`JAVA_HOME`、`AWS_PATH`、`PATH` 和产品特定的环境变量，以简化这些工具的配置。

此外，为了支持您安装多个版本的 API 和 AMI 工具，我们还在 `/opt/aws` 中提供了指向所需工具版本的符号链接，如下所述：

`/opt/aws/bin`

指向每个已安装工具目录中的 `/bin` 目录的符号链接。

`/opt/aws/{apitools|amitools}`

产品安装在形式为 *name*`--`*version* 的目录中，符号链接 *name* 附加到最近安装的版本。

`/opt/aws/{apitools|amitools}/`*name*`/environment.sh`

由 `/etc/profile.d/aws-apitools-common.sh` 用于设置产品特定的环境变量，如 `EC2_HOME`。

程序包存储库

Amazon Linux 2 和 Amazon Linux AMI 旨在与每个 Amazon EC2 Amazon 区域中托管的在线程序包存储库结合使用。这些存储库为 Amazon Linux 2 和 Amazon Linux AMI 中的程序包提供持续更新，还可访问数百个常见的开源服务器应用程序。这些存储库在所有区域中提供，可使用 yum 更新工具进行访问。通过在每个区域托管存储库，我们可以快速部署更新，不会产生任何数据传输费。

Amazon Linux 2 和 Amazon Linux AMI 会定期进行更新，增强安全性及功能。如果您不需要保留实例的数据或自定义项，则只需使用当前 AMI 启动新实例。如果您需要保留实例的数据或自定义项，则可以通过 Amazon Linux 程序包存储库维护这些实例。这些存储库包含所有更新后的程序包。您可以选择将这些更新应用到正在运行的实例中。即使新版本发布后，旧版的 AMI 和更新程序包仍继续可用。

> **Important**
>
> 您的实例必须具有 Internet 访问权限才能访问该存储库。

要安装程序包，请使用以下命令：

```
[ec2-user ~]$ sudo yum install package
```

对于 Amazon Linux AMI，系统配置了对 Extra Packages for Enterprise Linux (EPEL) 存储库的访问权限，但默认情况下未启用。Amazon Linux 2 未配置为使用 EPEL 存储库。除了 存储库中的软件包以外，EPEL 还提供了第三方软件包。Amazon 不支持第三方软件包。您可以使用以下命令来启用 EPEL 存储库：

- 对于 Amazon Linux 2：

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- 对于 Amazon Linux AMI：

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

如果您发现 Amazon Linux 不包含您需要的应用程序，您只需直接在 Amazon Linux 实例上安装该应用程序即可。Amazon Linux 使用 RPM 和 yum 进行程序包管理，这可能是安装新应用程序最简单的方法。您始终应该首先查看我们的中央 Amazon Linux 存储库，确定其中是否有您需要应用程序，因为许多应用程序在那里都可以找到。您可以轻松地将这些应用程序添加到 Amazon Linux 实例。

要将应用程序上传到正在运行的 Amazon Linux 实例，请使用 scp 或 sftp，然后通过登录实例来配置应用程序。您还可以使用内置 cloud-init 程序包中的 PACKAGE_SETUP 操作，在实例启动时，上传应用程序。有关更多信息，请参阅cloud-init (p. 215)。

安全更新

安全更新通过程序包存储库提供，而更新后的 AMI 安全警报在 Amazon Linux 安全中心中发布。有关 Amazon 安全策略的更多信息，或要报告安全问题，请访问 Amazon 云安全。

Amazon Linux 配置为在启动时下载和安装关键或重要安全更新。我们建议您在启动后针对您的用例进行必要的更新。例如，您可能希望在启动时应用所有更新（而不仅仅是安全更新），或者评估各个更新并仅应用适用于您系统的更新。这是使用以下 cloud-init 设置进行控制的：`repo_upgrade`。下方 cloud-init 配置片段显示了如何修改传递到实例初始化用户数据文本中的设置：

```
#cloud-config
repo_upgrade: security
```

`repo_upgrade` 的可能值如下所示：

`critical`

应用未完成的关键安全更新。

`important`

应用未完成的关键和重要安全更新。

`medium`

应用未完成的关键、重要和中等安全更新。

`low`

应用所有未完成的安全更新，包括具有低严重性的安全更新。

`security`

应用 Amazon 标记为安全更新的明显关键或重要更新。

`bugfix`

应用 Amazon 标记为缺陷修正的更新。缺陷修正是一组较大的更新，其中包括安全更新和针对各种其他小漏洞的修正更新。

`all`

应用全部适用更新 (不论类别)。

`none`

实例启动时不应用任何更新。

`repo_upgrade` 的默认设置是安全的。也就是说，如果您未在用户数据中指定其他值，在默认情况下，Amazon Linux 会在启动时执行针对所有已安装程序包的安全升级。Amazon Linux 还会使用 `/etc/motd` 文件列出登录时可用更新的数量，通知您已安装程序包的任何更新。要安装这些更新，您需要在实例上运行 sudo yum upgrade。

存储库配置

利用 Amazon Linux，AMI 将被视为实时快照，因此当您运行 yum update -y 时，存储库和更新结构可始终为您提供最新的程序包。

存储库结构进行了配置以提供不间断的更新流，可让您从一个版本的 Amazon Linux 滚动到下一版本。举例来说，如果从较旧版本的 Amazon Linux AMI（如 2017.09 或更低版本）启动实例并运行 yum update -y，则会得到最新程序包。

您可通过启用 lock-on-launch 功能禁用滚动更新。lock-on-launch 功能会锁定您的实例，使其仅接收来自指定版本的 AMI 的更新。举例来说，您可以启动 2017.09 AMI，使其仅接收早于 2018.03 AMI 发布的更新，直至您准备好迁移到 2018.03 AMI 为止。

Important

如果锁定到并非最新的存储库版本，则您不会收到后续更新。要接收连续更新流，您必须使用最新的 AMI，或持续更新您的 AMI，使存储库指向最新版本。

要在新实例中启用 lock-on-launch 功能，请使用已传递到 cloud-init 的以下用户数据启动它：

```
#cloud-config
repo_releasever: 2017.09
```

将现有实例锁定到当前 AMI 版本

1. 编辑 `/etc/yum.conf`。

2. 注释 `releasever=latest`。
3. 要清除缓存，请运行 yum clean all。

Extras 库 (Amazon Linux 2)

利用 Amazon Linux 2，您可以使用 Extras 库来在您的实例上安装应用程序和软件更新。这些软件更新称为主题。您可以安装主题的某特定版本或忽略要使用最新版本的版本信息。

要列出可用的主题，请使用以下命令：

```
[ec2-user ~]$ amazon-linux-extras list
```

要启用主题并安装其程序包的最新版本以确保最新，请使用以下命令：

```
[ec2-user ~]$ sudo amazon-linux-extras install topic
```

要启用主题并安装其程序包的特定版本以确保稳定性，请使用以下命令：

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

要删除从主题中安装的程序包，请使用以下命令：

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk '{ print
 $1 }')
```

Note

该命令不会删除作为 Extra 依赖项安装的程序包。

要禁用主题并使 yum 程序包管理器无法访问程序包，请使用以下命令：

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

Important

该命令适用于高级用户。如果未正确使用该命令，可能会导致程序包兼容性冲突。

Amazon Linux 2 支持的内核

支持的内核版本

目前，Amazon Linux 2（AL2）AMI 可用于内核版本 4.14 和 5.10，默认版本为 5.10。您还可以选择使用额外存储库将 AL2 上的内核升级到 5.15 版。请注意，升级到 5.15 版需要重新启动才能使新内核生效。在决定使用案例是否需要升级之前，请查看 AL2 上内核 5.15 版的新功能和限制。如果您需要实时修补支持，我们建议您将 AL2 AMI 与内核 5.10 结合使用。

内核 5.15 中的新功能

- 基于内核的虚拟机（KVM）现在默认使用新的 x86 TDP MMU，并添加了 AMD SVM 5 级分页，以便实现与原来的 KVM x86 MMU 代码相比更高的并行性和可扩展性。
- OverlayFS 提高了性能，现在还可以处理不可变/附加/同步/noatime 属性的复制。
- 为 EXT4 添加了新的优化和改进，例如新增了全新的 orphan_file 功能，以消除大规模并行截断、文件删除和将 DISCARD 工作移出 JBD2 提交线程的瓶颈，以帮助 DISCARD 行为缓慢的设备，而不会阻止 JBD2 提交 KThread。

- 为 XFS 添加了新的优化和改进，例如在每个 CPU 后台线程中进行可缩短目录树删除时间的批量索引节点激活，以及启用流水线以帮助提高处理大量元数据更新的性能。
- 更好地支持 DAMON，其作为主动内存回收和性能分析的数据访问监控框架。

内核 5.15 的限制

- 不支持 LustreFSx（稍后将添加支持）。
- 不支持内核实时修补。

内核 5.15 安装说明

您可以使用以下命令从具有内核 4.14 的 Amazon Linux 2 AMI 和具有内核 5.10 的 AL2 AMI 升级到内核 5.15：

1. 在 `amazon-linux-extras` 中启用 `kernel-5.15` 主题，然后在主机上安装内核 5.15。

```
sudo amazon-linux-extras install kernel-5.15
```

2. 使用已安装的内核 5.15 重新启动主机。

```
sudo reboot
```

3. 检查系统内核版本。

```
uname -r
```

支持时间范围

在 Amazon Linux 2 AMI 的标准支持结束之前，Amazon Linux 2（4.14、5.10 和 5.15）上可用的所有 Linux 内核都将受支持。

实时修补支持

Amazon Linux 2 kernel version	Kernel live patching supported
4.14	Yes
5.10	Yes
5.15	No

访问源软件包以获取参考信息

您可以使用 Amazon Linux 中提供的工具，查看您已在实例上安装的软件包的源，获取参考信息。您可以查看 Amazon Linux 和在线软件包存储库中包含的全部软件包的源软件包。只需确定您要安装的源软件包的名称，并使用 yumdownloader --source 命令在您正在运行的实例中查看源。例如：

```
[ec2-user ~]$ yumdownloader --source bash
```

您可以对源 RPM 进行解压缩，并可以使用标准 RPM 工具查看源树进行参考。完成调试之后，该软件包可供使用。

cloud-init

cloud-init 程序包是由 Canonical 构建的开源应用程序，用于在云计算环境（例如 Amazon EC2）中引导 Linux 映像。Amazon Linux 包含 cloud-init 的自定义版本。它使您能够指定实例启动时应执行的操作。启动实例时，您可以通过用户数据字段将需要的操作传递到 cloud-init。这意味着，您可以将通用 AMI 用于许多使用案例，并在启动时进行动态配置。Amazon Linux 还使用 cloud-init 来执行 ec2-user 账户的初始配置。

有关更多信息，请参阅 cloud-init 文档。

Amazon Linux 使用在 `/etc/cloud/cloud.cfg.d` 和 `/etc/cloud/cloud.cfg` 中发现的 cloud-init 操作。您可以在 `/etc/cloud/cloud.cfg.d` 中创建自己的 cloud-init 操作文件。此目录中的所有文件均由 cloud-init 读取。它们是按词典顺序进行读取的，并且文件随后将覆盖之前文件中的值。

cloud-init 程序包将在启动时对实例执行这些 (以及其他) 常见配置任务：

- 设置默认区域设置。
- 设置主机名。
- 解析并处理用户数据。
- 生成主机私有 SSH 密钥。
- 将用户的公有 SSH 密钥添加到 `.ssh/authorized_keys`，以便于登录和管理。
- 准备存储库以进行程序包管理。
- 处理用户数据中定义的软件包操作。
- 执行在用户数据中找到的用户脚本。
- 装载实例存储卷 (如果适用)。
  - 默认情况下，`ephemeral0` 实例存储卷装载在 `/media/ephemeral0` (如果它存在且包含有效的文件系统；否则将不会安装)。
  - 默认情况下，将装载与实例关联的所有交换卷 (仅适用于 `m1.small` 和 `c1.medium` 实例类型)。
  - 您可以使用以下 cloud-init 指令覆盖默认实例存储卷安装：

    ```
    #cloud-config
    mounts:
    - [ ephemeral0 ]
    ```

    有关对安装的更多控制，请参阅 cloud-init 文档中的安装。
  - 在实例启动时，不会格式化支持 TRIM 的实例存储卷，因此，您必须先对这些卷进行分区和格式化，然后才能装载它们。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。您可以在启动时使用 `disk_setup` 模块对您的实例存储卷进行分区和格式化。有关更多信息，请参阅 cloud-init 文档中的磁盘设置。

支持的用户数据格式

cloud-init 软件包可处理多种格式的用户数据：

- Gzip
  - 如果用户数据是经过 gzip 压缩过的，cloud-init 可解压缩数据，并进行适当处理。
- MIME 多部分内容型
  - 使用 MIME 多部分内容型文件，您可以指定多种数据类型。例如，您可以指定用户数据脚本和云配置类型。如果多部分内容型文件的格式是受支持的格式，则 cloud-init 可以处理它的各部分内容。
- Base64 解码
  - 如果用户数据是使用 base64 编码的，cloud-init 将决定它能否将解码后的数据当作其中一种受支持的数据类型进行理解。如果它能理解解码后的数据，则会解码数据，并进行适当处理。如果不能，它将完整地返回 base64 数据。

- 用户数据脚本
  - 开头为 `#!` 或 `Content-Type: text/x-shellscript`。
  - 该脚本由 `/etc/init.d/cloud-init-user-scripts` 在首轮启动过程中运行。此操作会在启动过程的后期发生 (即执行初始配置操作后)。
- 包含文件
  - 开头为 `#include` 或 `Content-Type: text/x-include-url`。
  - 此内容是一个包含文件。该文件包含一个 URL 列表，每行一个 URL。系统会读取每个 URL，其内容会通过此相同规则集验证。从 URL 读取的内容可使用 gzip 进行压缩、采用 MIME 分段处理或存储为纯文本。
- 云配置数据
  - 开头为 `#cloud-config` 或 `Content-Type: text/cloud-config`。
  - 此内容是云配置数据。要了解支持的配置格式的带注释示例，请查看示例。
- Upstart 作业（Amazon Linux 2 上不支持）
  - 开头为 `#upstart-job` 或 `Content-Type: text/upstart-job`。
  - 此内容存储在 `/etc/init` 中的一个文件里，upstart 使用内容的方式与其他 upstart 作业相同。
- Cloud Boothook
  - 开头为 `#cloud-boothook` 或 `Content-Type: text/cloud-boothook`。
  - 此内容为 boothook 数据。它存储在 `/var/lib/cloud` 下的一个文件中并会立即运行。
  - 这是最早可用的 hook。尚无仅供运行一次的机制。boothook 必须自行解决此问题。它的环境变量 `INSTANCE_ID` 中包含实例 ID。可使用此变量来提供一组一个实例可用一次的 boothook 数据。

订阅 Amazon Linux通知

要收到新 AMI 发布通知，可使用 Amazon SNS 订阅。

订阅 Amazon Linux 通知

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。
2. 如果需要，可在导航栏中将区域更改为美国东部（弗吉尼亚北部）。必须选择所订阅的 SNS 通知在创建时所在的区域。
3. 在导航窗格中，依次选择 Subscriptions 和 Create subscription。
4. 对于 Create subscription 对话框，执行以下操作：
   a. [Amazon Linux 2] 对于主题 ARN，复制并粘贴以下 Amazon Resource Name (ARN)：**`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`**。
   b. [Amazon Linux] 对于主题 ARN，复制并粘贴以下 Amazon Resource Name (ARN)：**`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`**。
   c. 对于协议，选择电子邮件。
   d. 对于终端节点，输入可以用于接收通知的电子邮件地址。
   e. 选择 Create subscription。
5. 您将收到一封主题行为“Amazon Notification - Subscription Confirmation”的确认电子邮件。打开电子邮件，然后选择 Confirm subscription 以完成订阅。

每当发布新的 AMI 时，我们都会向相应主题的订阅者发送通知。若不想再接收这些通知，请使用以下过程取消订阅。

取消订阅 Amazon Linux 通知

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。

2. 如果需要，可在导航栏中将区域更改为美国东部（弗吉尼亚北部）。必须使用创建 SNS 通知的区域。
3. 在导航窗格中，选择订阅，选择订阅，然后选择操作和删除订阅。
4. 当系统提示进行确认时，选择 Delete（删除）。

Amazon Linux AMI SNS 消息格式

SNS 消息的架构如下所示。

```
{
    "description": "Validates output from AMI Release SNS message",
    "type": "object",
    "properties": {
        "v1": {
            "type": "object",
            "properties": {
                "ReleaseVersion": {
                    "description": "Major release (ex. 2018.03)",
                    "type": "string"
                },
                "ImageVersion": {
                    "description": "Full release (ex. 2018.03.0.20180412)",
                    "type": "string"
                },
                "ReleaseNotes": {
                    "description": "Human-readable string with extra information",
                    "type": "string"
                },
                "Regions": {
                    "type": "object",
                    "description": "Each key will be a region name (ex. us-east-1)",
                    "additionalProperties": {
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "Name": {
                                    "description": "AMI Name (ex. amzn-ami-
hvm-2018.03.0.20180412-x86_64-gp2)",
                                    "type": "string"
                                },
                                "ImageId": {
                                    "description": "AMI Name (ex.ami-467ca739)",
                                    "type": "string"
                                }
                            },
                            "required": [
                                "Name",
                                "ImageId"
                            ]
                        }
                    }
                }
            },
            "required": [
                "ReleaseVersion",
                "ImageVersion",
                "ReleaseNotes",
                "Regions"
            ]
        }
    },
    "required": [
        "v1"
```

```
    ]
}
```

作为虚拟机本地运行 Amazon Linux 2

使用 Amazon Linux 2 虚拟机 (VM) 映像进行本地开发和测试。我们为受支持的每个虚拟化平台提供不同的 Amazon Linux 2 VM 映像。您可以在 Amazon Linux 2 虚拟机映像页面查看支持的平台列表。

要将 Amazon Linux 2 虚拟机映像用于受支持的虚拟化平台之一，请执行以下操作：

- 步骤 1：准备 seed.iso 启动映像 (p. 218)
- 步骤 2：下载 Amazon Linux 2 VM 映像 (p. 219)
- 步骤 3：启动并连接到新 VM (p. 219)

步骤 1：准备 seed.iso 启动映像

seed.iso 启动映像包含启动新虚拟机所需的初始配置信息，如网络配置、主机名和用户数据。

> **Note**
>
> seed.iso 启动映像仅包括启动 VM 所需的配置信息。不包括 Amazon Linux 2 操作系统文件。

要生成 seed.iso 启动映像，需要两个配置文件：

- meta-data – 此文件包括 VM 的主机名和静态网络设置。
- user-data - 此文件配置用户账户，并指定其密码、密钥对以及访问机制。默认情况下，Amazon Linux 2 VM 映像会创建 ec2-user 用户账户。使用 user-data 配置文件设置默认用户账户的密码。

创建 **seed.iso** 启动盘

1. 创建一个名为 seedconfig 的新文件夹并导航到该文件夹。
2. 创建 meta-data 配置文件。
   a. 创建名为 meta-data 的新文件。
   b. 使用首选编辑器打开 meta-data 文件，并添加以下内容。

      ```
      local-hostname: vm_hostname
      # eth0 is the default network interface enabled in the image. You can configure
       static network settings with an entry like the following.
      network-interfaces: |
        auto eth0
        iface eth0 inet static
        address 192.168.1.10
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.254
      ```

      将 *vm_hostname* 替换为您选择的 VM 主机名，并根据需要配置网络设置。
   c. 保存并关闭 meta-data 配置文件。

   有关示例 meta-data 配置文件（用于指定 VM 主机名 (amazonlinux.onprem)、配置默认网络接口 (eth0) 并为必要的网络设备指定静态 IP 地址），请参阅示例 Seed.iso 文件。
3. 创建 user-data 配置文件。
   a. 创建名为 user-data 的新文件。

b. 使用首选编辑器打开 user-data 文件，并添加以下内容。

```
#cloud-config
#vim:syntax=yaml
users:
# A user by the name `ec2-user` is created in the image by default.
  - default
chpasswd:
  list: |
    ec2-user:plain_text_password
# In the above line, do not add any spaces after 'ec2-user:'.
```

将 *plain_text_password* 替换为您为默认 ec2-user 用户账户选择的密码。

c. （可选）默认情况下，VM 每次启动时，cloud-init 都会应用网络设置。添加以下内容，以防止 cloud-init 在每次启动时都应用网络设置，并保留首次启动期间应用的网络设置。

```
# NOTE: Cloud-init applies network settings on every boot by default. To retain
 network settings
# from first boot, add the following 'write_files' section:
write_files:
  - path: /etc/cloud/cloud.cfg.d/80_disable_network_after_firstboot.cfg
    content: |
      # Disable network configuration after first boot
      network:
        config: disabled
```

d. 保存并关闭 user-data 配置文件。

还可以创建其他用户账户并指定其访问机制、密码和密钥对。有关受支持指令的更多信息，请参阅模块参考。有关创建三个其他用户并为默认 user-data 用户账户指定自定义密码的示例 ec2-user 文件，请参阅示例 Seed.iso 文件。

4. 使用 seed.iso 和 meta-data 配置文件创建 user-data 启动映像。

对于 Linux，请使用类似 genisoimage 的工具。导航到 seedconfig 文件夹，并运行以下命令。

```
$ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

对于 macOS，请使用类似 hdiutil 的工具。从 seedconfig 文件夹往上导航一级，运行以下命令。

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
 seedconfig/
```

步骤 2：下载 Amazon Linux 2 VM 映像

我们为受支持的每个虚拟化平台提供不同的 Amazon Linux 2 VM 映像。您可以查看支持的平台列表，并在 Amazon Linux 2 虚拟机映像页面中为所选平台下载对应的 VM 映像。

步骤 3：启动并连接到新 VM

要启动和连接到新 VM，必须要有 seed.iso 启动映像（在步骤 1 (p. 218) 中创建）和 Amazon Linux 2 VM 映像（在步骤 2 (p. 219) 中下载）。具体步骤因您选择的 VM 平台而异。

VMware vSphere

适用于 VMware 的虚拟机映像以 OVF 格式提供。

要使用 VMware vSphere 引导虚拟机

1. 为 `seed.iso` 文件创建新的数据存储，或将其添加到现有的数据存储中。
2. 部署 OVF 模板，但先不启动虚拟机。
3. 在 Navigator (导航器) 面板中，右键单击新虚拟机，然后选择 Edit Settings (编辑设置)。
4. 在 Virtual Hardware (虚拟硬件) 选项卡上，为 New device (新设备) 选择 CD/DVD Drive (CD/DVD 驱动器)，然后选择 Add (添加)。
5. 对于 New CD/DVD Drive (新 CD/DVD 驱动器)，请选择 Datastore ISO File (数据存储 ISO 文件)。选择将 `seed.iso` 文件添加到的数据存储，浏览到并选择 `seed.iso` 文件，然后选择 OK (确定)。
6. 对于新 CD/DVD 驱动器，请选择连接，然后选择确定。

在将数据存储与虚拟机关联后，您应该能够引导该虚拟机。

KVM

使用 KVM 引导虚拟机

1. 打开 Create new VM (创建新的虚拟机) 向导。
2. 对于步骤 1，选择 Import existing disk image (导入现有的磁盘映像)。
3. 对于步骤 2，浏览到并选择虚拟机映像。对于 OS type（操作系统类型）和 Version（版本），分别选择 Linux 和 Red Hat Enterprise Linux 7.0。
4. 对于步骤 3，请指定要使用的 RAM 量和 CPU 数量。
5. 对于步骤 4，输入新虚拟机的名称，然后选择 Customize configuration before install (安装前自定义配置)，然后选择 Finish (完成)。
6. 在虚拟机的 Configuration (配置) 窗口中，选择 Add Hardware (添加硬件)。
7. 在 Add New Virtual Hardware (添加新的虚拟硬件) 窗口中，选择 Storage (存储)。
8. 在 Storage configuration (存储配置) 中，选择 Select or create custom storage (选择或创建自定义存储)。对于 Device type (设备类型)，选择 CDROM device (CDROM 设备)。选择 Manage (管理)，选择 Browse Local (浏览本地)，然后导航到并选择 `seed.iso` 文件。选择 Finish。
9. 选择 Begin Installation (开始安装)。

Oracle VirtualBox

使用 Oracle VirtualBox 引导虚拟机

1. 打开 Oracle VirtualBox，然后选择新建。
2. 对于 Name（名称），输入虚拟机的描述性名称；对于 Type（类型）和 Version（版本），分别选择 Linux 和 Red Hat (64-bit) [Red Hat（64 位）]。选择 Continue (继续)。
3. 对于内存大小，请指定要分配给虚拟机的内存容量，然后选择继续。
4. 对于硬盘，选择使用现有虚拟硬盘文件，浏览并打开虚拟机映像，然后选择创建。
5. 在启动虚拟机之前，您必须在虚拟机的虚拟光驱中加载 `seed.iso` 文件：
   a. 选择新的虚拟机，选择 Settings (设置)，然后选择 Storage (存储)。
   b. 在存储设备列表中，在控制器: IDE 下选择空的光驱。
   c. 在光驱的 Attributes (属性) 部分中，选择浏览按钮，选择 Choose Virtual Optical Disk File (选择虚拟光盘文件)，然后选择 `seed.iso` 文件。选择确定，以应用更改并关闭“设置”。

在将 `seed.iso` 文件添加到虚拟光驱后，您应该能够启动该虚拟机。

Microsoft Hyper-V

Microsoft Hyper-V 的虚拟机映像压缩为一个 zip 文件。您必须提取该 zip 文件的内容。

使用 Microsoft Hyper-V 引导虚拟机

1. 打开新建虚拟机向导。
2. 在提示您选择代时，选择 Generation 1 (第一代)。
3. 在提示您配置网络适配器时，为 Connection (连接) 选择 External (外部)。
4. 在提示您连接虚拟硬盘时，选择 Use an existing virtual hard disk (使用现有的虚拟硬盘)，选择 Browse (浏览)，然后导航到并选择虚拟机映像。选择 Finish (完成) 以创建虚拟机。
5. 右键单击新虚拟机，然后选择 Settings (设置)。在 Settings (设置) 窗口中，在 IDE Controller 1 (IDE 控制器 1) 下面选择 DVD Drive (DVD 驱动器)。
6. 对于 DVD 驱动器，选择 Image file (映像文件)，然后浏览到并选择 `seed.iso` 文件。
7. 应用更改并启动虚拟机。

在 VM 启动后，使用在 `user-data` 配置文件中定义的用户账户之一登录。在您第一次登录之后，就可以断开 `seed.iso` 启动映像与 VM 的连接。

Amazon Linux 2 上的内核实时修补

适用于 Amazon Linux 2 的内核实时修补使您能够将安全漏洞和严重错误修补程序应用于正在运行的 Linux 内核，而无需重启或中断正在运行的应用程序。这使您能够从改进的服务和应用程序可用性中受益，同时保持基础设施的安全和最新状态。

Amazon 发布了两种适用于 Amazon Linux 2 的内核实时修补程序：

- 安全更新 - 包括 Linux 常见漏洞和风险（CVE）的更新。通常使用 Amazon Linux 安全公告评级将这些更新评为重要 或关键。它们通常对应于通用漏洞评分系统 (CVSS) 的 7 分或更高。在某些情况下，Amazon 可能会在分配 CVE 之前提供更新。在这些情况下，修补程序可能会显示为错误修复。
- 错误修复 - 包括与 CVE 无关的关键错误和稳定性问题的修复。

Amazon 为 Amazon Linux 2 内核版本提供内核实时修补程序，最长可在发布后 3 个月内使用。在 3 个月期限之后，您必须更新到更高版本的内核才能继续接收内核实时修补程序。

Amazon Linux 2 内核实时修补程序在现有 Amazon Linux 2 存储库中作为签名的 RPM 软件包提供。补丁可以使用现有 yum 工作流安装在单个实例上，也可以使用 Amazon Systems Manager 安装在一组托管实例上。

在 Amazon Linux 2 上提供内核实时修补功能，无需额外费用。

主题

- 支持的配置和先决条件 (p. 221)
- 使用内核实时修补 (p. 223)
- 限制 (p. 226)
- 常见问题 (p. 226)

支持的配置和先决条件

运行 Amazon Linux 2 的 Amazon EC2 实例和本地虚拟机 (p. 218)支持内核实时修补。

要在 Amazon Linux 2 上使用内核实时修补，必须使用：

- `x86_64` 架构的内核版本 `4.14` 或 `5.10`
- `ARM64` 架构的内核版本 `5.10`

策略要求

要从 Amazon Linux 存储库下载程序包，Amazon Elastic Compute Cloud 需要访问服务拥有的 Amazon S3 存储桶。如果您在环境中使用 Amazon S3 的 Amazon Virtual Private Cloud（VPC）端点，则需要确保您的 VPC 端点策略允许访问这些公有存储桶。

此表介绍了 EC2 访问“内核实时修补”可能需要的每种 Amazon S3 存储桶。

S3 存储桶 ARN	描述
arn:aws:s3:::packages.*region*.amazonaws.com/*	包含 Amazon Linux AMI 程序包的 Amazon S3 存储桶
arn:aws:s3:::repo.*region*.amazonaws.com/*	包含 Amazon Linux AMI 存储库的 Amazon S3 存储桶
arn:aws:s3:::amazonlinux.*region*.amazonaws.com/*	包含 Amazon Linux 2 存储库的 Amazon S3 存储桶
arn:aws:s3:::amazonlinux-2-repos-*region*/*	包含 Amazon Linux 2 存储库的 Amazon S3 存储桶

以下策略说明了如何限制对属于您组织的身份和资源的访问权，以及如何提供对“内核实时修补”所需的 Amazon S3 存储桶的访问权。使用您组织的相应值替换 *region*、*principal-org-id* 和 *resource-org-id*。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRequestsByOrgsIdentitiesToOrgsResources",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "principal-org-id",
          "aws:ResourceOrgID": "resource-org-id"
        }
      }
    },
    {
      "Sid": "AllowAccessToAmazonLinuxAMIRepositories",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
```

```
}
```

使用内核实时修补

对于单个实例，您可以在实例本身上使用命令行启用并使用内核实时修补，或者使用 Amazon Systems Manager 在一组托管实例上启用和使用内核实时修补。

以下各节说明如何使用命令行在单个实例上启用并使用内核实时修补。

有关在一组托管实例上启用并使用内核实时修补的更多信息，请参阅 Amazon Systems Manager 用户指南中的在 Amazon Linux 2 实例上使用内核实时修补。

主题

- 启用内核实时修补 (p. 223)
- 查看可用的内核实时修补程序 (p. 224)
- 应用内核实时补丁 (p. 225)
- 查看应用的内核实时修补程序 (p. 225)
- 禁用内核实时修补功能 (p. 226)

启用内核实时修补

默认情况下，在 Amazon Linux 2 上内核实时修补处于禁用状态。要使用实时修补，必须为内核实时修补安装 yum 插件，并启用实时修补功能。

先决条件

内核实时修补需要 `binutils`。如果尚未安装 `binutils`，请使用以下命令进行安装：

```
$ sudo yum install binutils
```

启用内核实时修补

1. 内核实时补丁支持下列 Amazon Linux 2 内核版本。

   - `x86_64` 架构的内核版本 `4.14` 或 `5.10`
   - `ARM64` 架构的内核版本 `5.10`

   要检查内核版本，请运行以下命令。

   ```
   $ sudo yum list kernel
   ```

2. 如果您已经拥有受支持的内核版本，请跳过此步骤。如果您没有受支持的内核版本，请运行以下命令将内核更新到最新版本并重启实例。

   ```
   $ sudo yum install -y kernel
   ```

   ```
   $ sudo reboot
   ```

3. 为内核实时修补安装 yum 插件。

   ```
   $ sudo yum install -y yum-plugin-kernel-livepatch
   ```

4. 为内核实时修补启用 yum 插件。

```
$ sudo yum kernel-livepatch enable -y
```

此命令还会从配置的存储库安装最新版本的内核实时修补程序 RPM。

5. 要确认用于内核实时修补的 yum 插件已成功安装，请运行以下命令。

```
$ rpm -qa | grep kernel-livepatch
```

启用内核实时修补时，将自动应用空的内核实时修补程序 RPM。如果成功启用了内核实时修补功能，此命令将返回一个列表，其中包括初始的空内核实时修补程序 RPM。下面是示例输出。

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. 安装 kpatch 软件包。

```
$ sudo yum install -y kpatch-runtime
```

7. 如果之前安装过 kpatch 服务，请更新它。

```
$ sudo yum update kpatch-runtime
```

8. 启动 kpatch 服务。此服务在初始化或启动时会加载所有内核实时修补程序。

```
$ sudo systemctl enable kpatch.service
```

9. 在 Amazon Linux 2 额外资源库中启用内核实时修补主题。本主题包含内核实时修补程序。

```
$ sudo amazon-linux-extras enable livepatch
```

查看可用的内核实时修补程序

Amazon Linux 安全警报会发布到 Amazon Linux 安全中心。有关 Amazon Linux 2 安全警报（包括内核实时修补程序的警报）的信息，请参阅 Amazon Linux 安全中心。内核实时修补程序的前缀为 ALASLIVEPATCH。Amazon Linux 安全中心可能不会列出解决错误的内核实时修补程序。

您还可以使用命令行搜索公告和 CVE 的可用内核实时修补程序。

列出所有可用的内核实时修补程序以获取公告

使用以下命令。

```
$ yum updateinfo list
```

下面显示了示例输出。

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-motd
ALAS2LIVEPATCH-2020-002 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
ALAS2LIVEPATCH-2020-005 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

列出 CVE 的所有可用内核实时修补程序

使用以下命令。

```
$ yum updateinfo list cves
```

下面显示了示例输出。

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motdamzn2-core/2/x86_64 | 2.4 kB 00:00:00
CVE-2019-15918 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2019-20096 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2020-8648 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

应用内核实时补丁

您可以使用 yum 程序包管理器应用内核实时修补程序，方式与应用定期更新相同。用于内核实时修补功能的 yum 插件可管理要应用的内核实时修补程序，无需重启。

Tip

我们建议您使用内核实时修补功能定期更新内核，以确保内核保持安全和最新状态。

您可以选择应用特定的内核实时修补程序，或者应用任何可用的内核实时修补程序以及定期安全更新。

应用特定内核实时修补程序

1. 使用 查看可用的内核实时修补程序 (p. 224) 中描述的命令之一获取内核实时修补程序版本。
2. 为您的 Amazon Linux 2 内核应用内核实时修补程序。

   ```
   $ sudo yum install kernel-livepatch-kernel_version.x86_64
   ```

   例如，以下命令为 Amazon Linux 2 内核版本 `5.10.102-99.473` 应用内核实时修补程序。

   ```
   $ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
   ```

应用任何可用的内核实时修补程序以及定期安全更新

使用以下命令。

```
$ sudo yum update --security
```

省略 `--security` 选项将包含错误修复。

Important

- 应用内核实时修补程序后，内核版本不会更新。仅当实例重启后，版本才会更新到新版本。
- Amazon Linux 2 内核在三个月的时间段内接收内核实时修补程序。三个月的时间段过去后，不会为该内核版本发布新的内核实时修补程序。要在三个月后继续接收内核实时修补程序，您必须重启实例以移动到新的内核版本，然后该版本将在接下来的三个月内继续接收内核实时修补程序。要检查内核版本的支持窗口，请运行 `yum kernel-livepatch supported`。

查看应用的内核实时修补程序

查看应用的内核实时修补程序

使用以下命令。

```
$ kpatch list
```

该命令返回已加载和已安装的安全更新内核实时修补程序的列表。下面是示例输出。

```
Loaded patch modules:
livepatch_cifs_lease_buffer_len [enabled]
livepatch_CVE_2019_20096 [enabled]
livepatch_CVE_2020_8648 [enabled]

Installed patch modules:
livepatch_cifs_lease_buffer_len (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2019_20096 (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2020_8648 (5.10.102-99.473.amzn2.x86_64)
```

Note

单个内核实时修补程序可以包含和安装多个实时修补程序。

禁用内核实时修补功能

如果您不再需要使用内核实时修补，可以随时禁用它。

禁用内核实时修补功能

1. 删除应用的内核实时修补程序的 RPM 软件包。

```
$ sudo yum kernel-livepatch disable
```

2. 卸载内核实时修补功能的 yum 插件。

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

3. 重启实例。

```
$ sudo reboot
```

限制

内核实时修补功能具有以下限制：

- 在应用内核实时修补程序时，无法执行休眠、使用高级调试工具（例如 SystemTap、kprobes 和基于 eBPF 的工具）或者访问内核实时修补基础设施使用的 ftrace 输出文件。

常见问题

有关 Amazon Linux 2 的内核实时修补的常见问题，请参阅 Amazon Linux 2 内核实时修补常见问题。

用户提供的内核

如果您的 Amazon EC2 实例上需要自定义内核，您可以从接近于您想要的内核的 AMI 开始，在您的实例上编译自定义内核，并更新引导加载程序以指向新内核。该过程根据您的AMI所使用的虚拟化类型而异。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。

目录

- HVM AMIs (GRUB) (p. 227)
- 半虚拟化 AMIs (PV-GRUB) (p. 227)

HVM AMIs (GRUB)

HVM 实例卷就像是物理磁盘。引导过程类似于带分区磁盘和引导加载程序的裸机操作系统，使它能够在当前支持的所有 Linux 发行版中工作。最常见的引导加载程序是 GRUB 或 GRUB2。

默认情况下，GRUB 不会将其输出发送到实例控制台，因为它会造成额外启动延迟。有关更多信息，请参阅实例控制台输出 (p. 1724)。如果要安装自定义内核，则应考虑启用 GRUB 输出。

无需指定后备内核，但是我们建议您在测试新内核时准备好后备内核。如果新内核发生故障时，GRUB 可以退回到另一个内核。如果有后备内核，实例即使没有找到新内核也能进行引导。

旧版 GRUB for Amazon Linux 使用 `/boot/grub/menu.lst`。GRUB2 for Amazon Linux 2 使用 `/etc/default/grub`。有关更新引导加载程序中的默认内核的更多信息，请参阅 Linux 发行版的文档。

半虚拟化 AMIs (PV-GRUB)

使用半虚拟化 (PV) 的 Amazon 系统映像 会在启动过程中使用名为 PV-GRUB 的系统。PV-GRUB 是半虚拟化引导加载程序，运行经过修补的 GNU GRUB 0.97 版本。当您启动实例时，PV-GRUB 会启动引导过程，然后链式加载由映像的 `menu.lst` 文件指定的内核。

PV-GRUB 理解标准 `grub.conf` 或 `menu.lst` 命令，可与当前支持的所有 Linux 发行版配合使用。较旧发行版（如 Ubuntu 10.04 LTS、Oracle Enterprise Linux 或 CentOS 5.x）需要特殊的“ec2”或“xen”内核软件包，而较新发行版在默认内核软件包中包含所需驱动程序。

大多数新半虚拟化 AMI 在默认情况下使用 PV-GRUB AKI (包括 Amazon EC2 Launch Wizard Quick Start 菜单中提供的所有半虚拟化 Linux AMI)，无需执行额外步骤即可在实例上使用不同的内核，前提是要使用的内核与您的发行版兼容。在实例上运行自定义内核的最佳方式是从接近于您想要的内核的 AMI 开始，然后在实例上编译自定义内核并修改 `menu.lst` 文件以使用该内核进行引导。

您可以验证 AMI 的内核映像是否为 PV-GRUB AKI。运行以下 describe-images 命令（替换为您的内核映像 ID），并检查 `Name` 字段是否以 `pv-grub` 开头：

```
aws ec2 describe-images --filters Name=image-id,Values=aki-880531cd
```

目录

- PV-GRUB 的限制 (p. 227)
- 为半虚拟化 AMIs 配置 GRUB (p. 228)
- Amazon PV-GRUB Kernel Image ID (p. 228)
- 更新 PV-GRUB (p. 230)

PV-GRUB 的限制

PV-GRUB 具有以下限制：

- 您不能使用 64 位版本的 PV-GRUB 来启动 32 位的内核，反之亦然。
- 当您使用 PV-GRUB AKI 时，不能指定 Amazon Ramdisk Image (ARI)。
- Amazon 经测试确认 PV-GRUB 可与以下文件系统格式配合使用：EXT2、EXT3、EXT4、JFS、XFS 和 ReiserFS。其他文件系统格式可能不适用。
- PV-GRUB 可以引导使用 gzip、bzip2、lzo 和 xz 压缩格式压缩的内核。
- 集群 AMI 不支持也不需要 PV-GRUB，因为它们使用完全硬件虚拟化 (HVM)。当半虚拟化实例使用 PV-GRUB 来启动时，HVM 实例卷用作实际磁盘，并且启动过程与带已分区磁盘和引导加载程序的裸机操作系统的类似。
- PV-GRUB 版本 1.03 及更低版本不支持 GPT 分区；它们仅支持 MBR 分区。

- 如果您计划通过 Amazon Elastic Block Store (Amazon EBS) 卷使用逻辑卷管理 (LVM)，则需要在 LVM 外有一个独立的引导分区。然后，您可以通过 LVM 创建逻辑卷。

为半虚拟化 AMIs 配置 GRUB

要引导 PV-GRUB，GRUB `menu.lst` 文件必须存在于映像中；此文件的最常见位置是 `/boot/grub/menu.lst`。

以下是用于启动带 PV-GRUB AKI 的 AMI 的 `menu.lst` 配置文件示例。在该示例中，可在两个内核条目中进行选择：Amazon Linux 2018.03（此 AMI 的原始内核），以及 Vanilla Linux 4.16.4（来自 https://www.kernel.org/ 的较新 Vanilla Linux 内核版本）。Vanilla 条目是从此 AMI 的原始条目复制的，`kernel` 和 `initrd` 路径已更新为新位置。`default 0` 参数将引导加载程序指向其发现的第一个条目 (在此例中为 Vanilla 条目)，`fallback 1` 参数在引导第一个条目的过程中发生问题时，将引导加载程序指向下一个条目。

```
default 0
fallback 1
timeout 0
hiddenmenu

title Vanilla Linux 4.16.4
root (hd0)
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.16.4

title Amazon Linux 2018.03 (4.14.26-46.32.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.14.26-46.32.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.14.26-46.32.amzn1.x86_64.img
```

无需在 `menu.lst` 文件中指定后备内核，但是我们建议您在测试新内核时准备好后备内核。如果新内核发生故障，PV-GRUB 可以回退到其他内核。如果有后备内核，实例即使没有找到新内核也能进行引导。

PV-GRUB 检查以下位置是否存在 `menu.lst`，使用找到的第一项：

- `(hd0)/boot/grub`
- `(hd0,0)/boot/grub`
- `(hd0,0)/grub`
- `(hd0,1)/boot/grub`
- `(hd0,1)/grub`
- `(hd0,2)/boot/grub`
- `(hd0,2)/grub`
- `(hd0,3)/boot/grub`
- `(hd0,3)/grub`

请注意，PV-GRUB 1.03 及更低版本仅检查此列表中的前两个位置。

Amazon PV-GRUB Kernel Image ID

PV-GRUB AKI 在所有 Amazon EC2 区域（不包括亚太地区（大阪））中都可用。同时存在适用于 32 位和 64 位架构类型的 AKI。大多数新 AMI 在默认情况下使用 PV-GRUB AKI。

我们建议您始终使用最新版本的 PV-GRUB AKI，因为并不是所有的 PV-GRUB AKI 版本都能与全部实例类型兼容。使用以下 describe-images 命令可获取当前区域的 PV-GRUB AKI 列表：

```
aws ec2 describe-images --owners amazon --filters Name=name,Values=pv-grub-*.gz
```

PV-GRUB 是 ap-southeast-2 区域中唯一可用的 AKI。您应验证要复制到此区域的任何 AMI 是否使用此区域中可用的 PV-GRUB 版本。

以下是每个区域的当前 AKI ID。使用 hd0 AKI 注册新 AMI。

Note

在之前提供 hd00 AKI 的区域，我们将继续提供 hd00 AKI，以实现向后兼容性。

ap-northeast-1，亚太区域（东京）

映像 ID	映像名称
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-1、亚太区域（新加坡）

映像 ID	映像名称
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2、亚太区域（悉尼）

映像 ID	映像名称
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1、欧洲（法兰克福）

映像 ID	映像名称
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1、欧洲（爱尔兰）

映像 ID	映像名称
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1、南美洲（圣保罗）

映像 ID	映像名称
aki-7cd34110	pv-grub-hd0_1.05-i386.gz

映像 ID	映像名称
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

us-east-1、US East (N. Virginia)

映像 ID	映像名称
aki-04206613	pv-grub-hd0_1.05-i386.gz
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

us-gov-west-1、Amazon GovCloud（美国西部）

映像 ID	映像名称
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

us-west-1、美国西部（加利福尼亚北部）

映像 ID	映像名称
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2、美国西部（俄勒冈）

映像 ID	映像名称
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

更新 PV-GRUB

我们建议您始终使用最新版本的 PV-GRUB AKI，因为并不是所有的 PV-GRUB AKI 版本都能与全部实例类型兼容。较旧版本的 PV-GRUB 也并非在所有区域都可用，因此如果您将使用较旧版本的 AMI 复制到不支持该版本的区域，则无法引导从该 AMI 启动的实例，直至您更新内核映像。使用以下过程可检查您的实例的 PV-GRUB 版本并在必要时更新它。

检查您的 PV-GRUB 版本

1. 查找您的实例的内核 ID。

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute kernel --
region region

{
    "InstanceId": "instance_id",
    "KernelId": "aki-70cb0e10"
}
```

此实例的内核 ID 是 aki-70cb0e10。

2. 查看该内核 ID 的版本信息。

```
aws ec2 describe-images --image-ids aki-70cb0e10 --region region

{
    "Images": [
        {
            "VirtualizationType": "paravirtual",
            "Name": "pv-grub-hd0_1.05-x86_64.gz",
            ...
            "Description": "PV-GRUB release 1.05, 64-bit"
        }
    ]
}
```

此内核映像是 PV-GRUB 1.05。如果您的 PV-GRUB 版本不是最新版本（如 Amazon PV-GRUB Kernel Image ID (p. 228) 所示），则应使用以下过程更新它。

更新您的 PV-GRUB 版本

如果您的实例使用较旧版本的 PV-GRUB，则您应将它更新为最新版本。

1. 通过 Amazon PV-GRUB Kernel Image ID (p. 228) 确定您的区域和处理器架构的最新 PV-GRUB AKI。
2. 停止您的实例。您的实例必须停止才能修改所使用的内核映像。

```
aws ec2 stop-instances --instance-ids instance_id --region region
```

3. 修改用于您的实例的内核映像。

```
aws ec2 modify-instance-attribute --instance-id instance_id --kernel kernel_id --
region region
```

4. 重新启动您的实例。

```
aws ec2 start-instances --instance-ids instance_id --region region
```

配置 Amazon Linux 2 MATE 桌面连接

MATE 桌面环境 已在 AMI 中预装和预配置，描述如下：

".NET Core *x.x*, Mono *x.xx*, PowerShell *x.x*, and MATE DE pre-installed to run your .NET applications on Amazon Linux 2 with Long Term Support (LTS)."

该环境提供了一个直观的图形用户界面，无需使用命令行即可管理 Amazon Linux 2 实例。该界面使用图形化表示，例如图标、窗口、工具栏、文件夹、壁纸和桌面小部件。基于 GUI 的内置工具可用于执行常见任务。例如，有一些工具可用于添加和删除软件、应用更新、组织文件、启动程序和监视系统运行状况。

Important

xrdp 是 AMI 中捆绑的远程桌面软件。默认情况下，xrdp 使用自签名 TLS 证书来加密远程桌面会话。Amazon 和 xrdp 的维护人员都不建议在生产中使用自签名证书，而是从相应的证书颁发机构

(CA) 获取证书并将其安装在您的实例上。有关 TSL 配置的更多信息，请参阅 xrdp Wiki 上的 TLS 安全层。

先决条件

要运行本主题中显示的命令，必须安装 Amazon Command Line Interface (Amazon CLI) 或 Amazon Tools for Windows PowerShell，然后配置您的 Amazon 个人资料。

选项

1. 安装 Amazon CLI – 有关详细信息，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI 和配置基础。
2. 安装 Tools for Windows PowerShell – 有关详细信息，请参阅《Amazon Tools for Windows PowerShell 用户指南》中的安装 Amazon Tools for Windows PowerShell 和共享凭证。

配置 RDP 连接

按照以下步骤设置远程桌面协议 (RDP) 连接，从本地计算机指向运行 MATE 桌面环境的 Amazon Linux 2 实例。

1. 要获取 AMI 名称中包含 MATE 的 Amazon Linux 2 的 AMI ID，可以使用本地命令行工具中的 describe-images 命令。如果尚未安装命令行工具，可以直接从 Amazon CloudShell 会话执行以下查询。有关如何从 CloudShell 启动 Shell 会话的信息，请参阅开始使用 Amazon CloudShell。从 Amazon EC2 控制台中，您可以启动实例，然后在 AMI 搜索栏中输入 MATE，以查找包含 MATE 的 AMI。预安装了 MATE 的 Amazon Linux 2 Quick Start 将出现在搜索结果中。

```
aws ec2 describe-images --filters "Name=name,Values=amzn2*MATE*" --query "Images[*].
[ImageId,Name,Description]"
[
    [
        "ami-0123example0abc12",
        "amzn2-x86_64-MATEDE_DOTNET-2020.12.04",
        ".NET Core 5.0, Mono 6.12, PowerShell 7.1, and MATE DE pre-installed to run
 your .NET applications on Amazon Linux 2 with Long Term Support (LTS)."
    ],
    [
        "ami-0456example0def34",
        "amzn2-x86_64-MATEDE_DOTNET-2020.04.14",
        "Amazon Linux 2 with .Net Core, PowerShell, Mono, and MATE Desktop Environment"
    ]
]
```

   选择适合您使用的 AMI。
2. 使用您在上一步中找到的 AMI 启动 EC2 实例。将安全组配置为允许到端口 3389 的入站 TCP 流量。有关配置安全组的更多信息，请参阅 VPC 的安全组。此配置使您能够使用 RDP 客户端连接到实例。
3. 使用 SSH 连接到实例。
4. 更新实例上的软件和内核。

```
[ec2-user ~]$ sudo yum update
```

   在更新完成后，重启实例以确保实例使用的是来自更新的最新程序包和库；重启发生前不会加载内核更新。

```
[ec2-user ~]$ sudo reboot
```

5. 重新连接到实例并在 Linux 实例上运行以下命令以设置 ec2-user 的密码。

```
[ec2-user ~]$ sudo passwd ec2-user
```

6. 安装证书和密钥。

   如果您已经拥有证书和密钥，将它们复制到 /etc/xrdp/ 目录，如下所示：

   - 证书 — /etc/xrdp/cert.pem
   - 密钥 — /etc/xrdp/key.pem

   如果您没有证书和密钥，则使用以下命令在 /etc/xrdp 目录中生成。

```
$ sudo openssl req -x509 -sha384 -newkey rsa:3072 -nodes -keyout /etc/xrdp/key.pem -
out /etc/xrdp/cert.pem -days 365
```

   Note

   此命令会生成有效期达 365 天的证书。

7. 在要连接到实例的计算机上打开 RDP 客户端（例如，运行 Microsoft Windows 的计算机上的远程桌面连接）。输入 ec2-user 作为用户名，然后输入您在上一步中设置的密码。

在您的 Amazon EC2 实例上禁用 **xrdp**

您可以通过在 Linux 实例上运行以下命令之一随时禁用 xrdp。以下命令不会影响您通过 X11 服务器使用 MATE 的能力。

```
[ec2-user ~]$ sudo systemctl disable xrdp
```

```
[ec2-user ~]$ sudo systemctl stop xrdp
```

在您的 Amazon EC2 实例上启用 **xrdp**

要重新启用 xrdp，以便您能连接到运行 MATE 桌面环境的 Amazon Linux 2 实例，请在您的 Linux 实例上运行以下命令之一。

```
[ec2-user ~]$ sudo systemctl enable xrdp
```

```
[ec2-user ~]$ sudo systemctl start xrdp
```

AMI 限额

以下限额适用于创建和共享 AMI。限额按 Amazon Web Services 区域应用。

配额名称	描述	每个区域的默认限额
AMI	每个区域允许的最大公有和私有 AMI 数量。这包括可用和待处理的 AMI 以及回收站中的 AMI。	50000

配额名称	描述	每个区域的默认限额
公有 AMI	每个区域允许的最大公有 AMI 数量，包括回收站中的公有 AMI。	5
AMI 共享	某一区域内可以共享 AMI 的最大实体（组织、组织部门 (OU) 和账户）数量。请注意，如果您与某个组织或 OU 共享一个 AMI，则该组织或 OU 中的账户数量不计入该限额。	1000

如果您超出限额，但想创建或共享更多 AMI，可以执行以下操作：

- 如果您超出总 AMI 或公有 AMI 限额，请考虑取消注册未使用的映像。
- 如果您超出公有 AMI 限额，请考虑将一个或多个公有 AMI 设为私有。
- 如果您超出 AMI 共享限额，请考虑与某个组织或 OU（而不是单独的账户）共享您的 AMI。
- 请求增加 AMI 的限额。

请求增加 AMI 的限额

如果您需要的 AMI 超出其默认限额，您可以请求增加限额。

请求增加 AMI 的限额

1. 访问 https://console.aws.amazon.com/servicequotas/home，打开 Service Quotas 控制台。
2. 在导航窗格中，选择 Amazon services（Amazon 服务）。
3. 从列表中选择 Amazon Elastic Compute Cloud (Amazon EC2)，或在搜索框中键入服务的名称。
4. 选择 AMI 限额以请求增加限额。您可以选择的 AMI 限额包括：
   - AMI
   - 公有 AMI
   - AMI 共享
5. 选择 Request quota increase (请求增加配额)。
6. 对于 Change quota value（更改限额值），输入新的限额值，然后选择 Request（请求）。

要查看任何待处理或最近解决的请求，请从导航窗格选择 Dashboard (控制面板)。对于待处理的请求，请选择请求状态以打开收到的请求。请求的初始状态为 Pending（待处理）。状态更改为 Quota requested（已请求限额）后，您将在 Support Center case number（支持中心案例编号）下看到案例编号。选择案例编号以打开请求服务单。

解决请求后，配额的 Applied quota value (应用的配额值) 设置为新值。

有关更多信息，请参阅 Service Quotas 用户指南。

Amazon EC2 实例

如果您是首次接触 Amazon EC2，请参阅以下主题了解其用法：

- 什么是 Amazon EC2？ (p. 1)
- 设置以使用 Amazon EC2 (p. 5)
- 教程：Amazon EC2 Linux 实例入门 (p. 9)
- 实例生命周期 (p. 570)

您需先回答以下问题，然后才能启动生产环境。

问：哪种实例类型最能满足我的需求？

Amazon EC2 提供不同的实例类型，以便您可以选择需要的 CPU、内存、存储和网络容量来运行您的应用程序。有关更多信息，请参阅实例类型 (p. 238)。

问：哪个购买选项最能满足我的需求？

Amazon EC2 支持按需型实例（默认值）、竞价型实例和预留实例。有关更多信息，请参阅实例购买选项 (p. 404)。

问：哪种类型的根卷能满足我的需求？

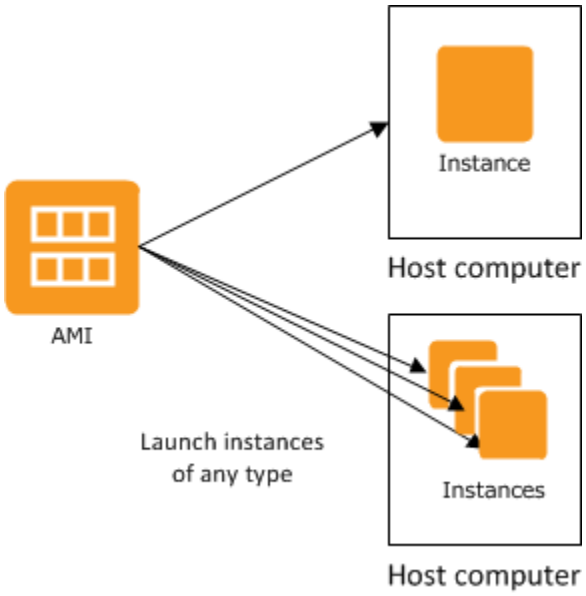
由 Amazon EBS 或实例存储支持的每一个实例。根据您需要的根卷类型选择 AMI。有关更多信息，请参阅根设备存储 (p. 103)。

问：我能否在混合环境中远程管理 EC2 实例以及设备的队列？

Amazon Systems Manager 可让您在混合环境中安全地远程管理 Amazon EC2 实例、本地实例和虚拟机 (VM)（包括来自其他云提供商的虚拟机）的配置。有关更多信息，请参阅 Amazon Systems Manager 用户指南。

实例和 AMI

Amazon Machine Image (AMI) 是一种包含软件配置 (例如，操作系统、应用程序服务器和应用程序) 的模板。通过 AMI，您可以启动实例，实例是作为云中虚拟服务器运行的 AMI 的副本。您可以启动多个 AMI 实例，如下图所示。



您的实例会保持运行，直到您停止、休眠或终止实例，或者实例失败为止。如果实例失败了，您可以从 AMI 启动一个新实例。

实例

实例是云中的虚拟服务器。启动时的实例配置是您在启动实例时指定的 AMI 的副本。

您可以从一个单一的 AMI 启动不同类型的实例。实例类型从本质上决定了用于您的实例的主机硬件。每一个实例类型提供不同的计算和存储能力。选择一种基于您打算在实例上运行的应用程序或软件所需的存储容量和计算能力的实例类型。有关更多信息，请参阅 Amazon EC2 实例类型。

启动一个实例后，该实例看上去像一个传统主机，您可以像与任何计算机交互一样与其进行交互。您对实例有完全控制权；您可以使用 sudo 运行需要根权限的命令。

您的 Amazon 账户对于保持运行状态的实例数量有限制。有关此限制的更多信息，以及如何请求调高限制，请参阅“Amazon EC2 一般常见问题”中的我能在 Amazon EC2 中运行多少个实例。

实例的存储

实例的根设备包含用于启动实例的映像。根卷是一个 Amazon Elastic Block Store (Amazon EBS) 卷或是实例存储卷。有关更多信息，请参阅Amazon EC2 实例根设备卷 (p. 1608)。

实例可能包括本地存储卷 (称为实例存储卷)，可以在启动时使用块储存设备映射配置这些卷。有关更多信息，请参阅块设备映射 (p. 1615)。这些卷已添加到实例并进行映射之后，便可供您进行装载和使用。如果实例失败，或是实例停止或终止，则这些卷上的数据会丢失；因此，这些卷最好用于临时数据。为保证重要数据的安全，应对多个实例使用复制策略，或将持久性数据存储在 Amazon S3 或 Amazon EBS 卷中。有关更多信息，请参阅存储 (p. 1322)。

安全最佳实践

- 使用 Amazon Identity and Access Management (IAM) 控制对Amazon资源（包括您的实例）的访问。有关更多信息，请参阅适用于 Amazon EC2 的 Identity and Access Management (p. 1223)。
- 通过仅允许受信任主机或网络访问实例的端口来限制访问。例如，您可以通过限制端口 22 的入站流量来限制 SSH 访问。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

- 定期审查安全组中的规则，并确保应用最小权限原则 — 即仅开启您需要的权限。您还可以创建不同的安全组来处理具有不同安全要求的实例。考虑创建一个可允许外部登录的堡垒安全组，同时在不允许外部登录的组内保留实例提醒程序。
- 对于从 AMI 启用的实例，禁用基于密码的登录。由于密码可以被查到或破解，因此存在安全风险。有关更多信息，请参阅对根用户禁用基于密码的远程登录 (p. 130)。有关安全共享 AMI 的更多信息，请参阅共享 AMI (p. 121)。

停止和终止实例

您可以随时停止或终止运行的实例。

停止实例

实例停止后，该实例将执行正常关闭操作，然后过渡到 `stopped` 状态。其所有 Amazon EBS 卷都将保持附加状态，并且您可以在稍后重新启动实例。

当实例处于停止状态时，您不必支付额外的实例使用费用。而每次从停止状态过渡到运行状态时，都需要支付一个最低一分钟费用。当实例停止时，如果实例类型发生变化，则在实例启动后，您需要就新实例类型支付费用。您实例的所有相关 Amazon EBS 用量（包括根设备用量）都按照一般 Amazon EBS 价格计费。

当实例处于停止状态时，您可以附加或分离 Amazon EBS 卷。您还可以从实例创建 AMI，以及更改内核、RAM 磁盘和实例类型。

终止实例

当终止实例后，实例将执行正常关闭操作。根设备卷在默认情况下会被删除，但任何附加的 Amazon EBS 卷在默认情况下会被保留，这由每个卷的 `deleteOnTermination` 属性设置确定。实例本身也将被删除，并且您不能在稍后重新启动该实例。

要防止意外终止，您可以禁用实例终止。如果禁用，请确保将实例的 `disableApiTermination` 属性设置为 `true`。若要控制实例关闭时的行为 (如在 Linux 中为 `shutdown -h`，在 Windows 中为 `shutdown`)，则可根据需要将 `instanceInitiatedShutdownBehavior` 实例属性设为 `stop` 或 `terminate`。根设备的 Amazon EBS 卷默认为 `stop` 的实例和带有实例存储根设备的实例，总会因实例关闭而终止。

有关更多信息，请参阅实例生命周期 (p. 570)。

> **Note**
>
> 一些Amazon资源（如 Amazon EBS 卷和弹性 IP 地址）无论实例的状态如何，都将产生费用。有关更多信息，请参阅 Amazon Billing 用户指南中的避免意外费用。有关 Amazon EBS 成本的更多信息，请参阅 Amazon EBS 定价。

AMI

Amazon Web Services (Amazon) 发布了许多包含常见软件配置的 Amazon Machine Image (AMI) 供公众使用。此外，Amazon 开发人员社区的会员也发布了他们的自定义 AMI。您也可以创建一个或多个自定义 AMI；这样能让您快速轻松地启动能满足您一切需求的新实例。例如，如果您的应用程序是网站或 Web 服务，则您的 AMI 可能包含 Web 服务器、相关静态内容和动态页面代码。因此，您从这个 AMI 启动实例之后，您的 Web 服务器将启动，并且您的应用程序已准备好接受请求。

所有 AMI 都被分类为由 Amazon EBS 支持或由实例存储支持，前者意味着从 AMI 启动的实例的根设备是 Amazon EBS 卷，后者意味着从 AMI 启动的实例的根设备是依据 Amazon S3 中存储的模板创建的实例存储卷。

对 AMI 的描述显示了根设备类型 (`ebs` 或 `instance store`)。这很重要，因为您使用每种 AMI 可进行的操作有很大区别。有关这些区别的更多信息，请参阅 根设备存储 (p. 103)。

使用完 AMI 之后，可以注销它。注销 AMI 之后，便无法将其用于启动新实例。从 AMI 启动的现有实例不受影响。因此，如果您也使用完从这些 AMI 中启动的实例，应终止这些实例。

实例类型

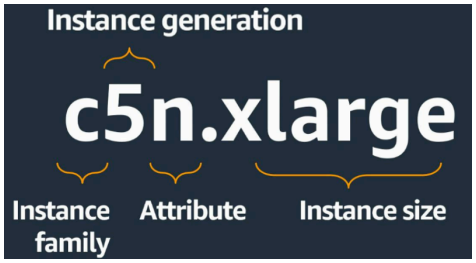
启动实例时，您指定的实例类型 决定了用于您的实例的主机硬件。每个实例类型提供不同的计算、内存和存储功能，并按照这些功能分组到实例系列。选择一种基于您打算在实例上运行的应用程序或软件的需求的实例类型。

Amazon EC2 会将主机的一些资源（例如 CPU、内存和实例存储）专用于特定实例。Amazon EC2 在实例间共享主机的其他资源，例如网络和磁盘子系统。如果一个主机上的每个实例都试图尽可能多地使用这些共享的资源，那么每个实例都将获得该资源相等份额。但是，当某个资源利用不充分时，会有实例会在该资源可用时消耗其更多的份额。

每种实例类型均从共享资源提供更高或更低的起始性能。例如，高 I/O 性能的实例类型能获取共享资源的更高份额。分配更大份额的共享资源也降低了 I/O 性能的方差。对于大多数应用程序，中等 I/O 是绰绰有余的。然而，对于需要更大或一致性更高的 I/O 性能的应用程序，可考虑使用更高 I/O 性能的实例类型。

实例类型名称

Amazon EC2 提供多种实例类型，让您能够选择最适合自己需求的类型。实例类型的命名基于其系列、代系、附加功能和型号。实例类型名称的第一位表示实例系列，例如 `c`。第二位表示实例代系，例如 `5`。句点之前的剩余字母表示附加功能，例如实例存储卷。句点 (`.`) 之后是实例型号，这是一个数字加一个大小（例如 `9xlarge`），或者是 `metal`，用来表示裸机实例。



以下是实例类型名称所表示的其他功能：

- a – AMD 处理器
- g – Amazon Graviton 处理器
- i – 英特尔处理器
- d – 实例存储卷
- n – 网络优化
- b – 数据块存储优化
- e – 额外的存储或内存
- z – 高频率

目录

- 可用实例类型 (p. 239)
- 硬件规格 (p. 245)
- AMI 虚拟化类型 (p. 246)
- 基于 Nitro 系统构建的实例 (p. 246)
- 联网和存储功能 (p. 247)
- 实例限制 (p. 252)
- 通用实例 (p. 252)
- 计算优化型实例 (p. 305)

- 内存优化型实例 (p. 322)
- 存储优化型实例 (p. 347)
- Linux 加速计算实例 (p. 358)
- 查找 Amazon EC2 实例类型 (p. 396)
- 获取实例类型建议 (p. 397)
- 更改实例类型 (p. 399)

可用实例类型

Amazon EC2 提供各种不同的实例类型，这些实例类型经过优化，适合不同的使用案例。实例类型包括 CPU、内存、存储和网络容量的不同组合，便于您灵活选择适合应用程序的资源组合。每种实例类型都包含一个或多个实例大小，您可以根据目标工作负载的要求扩展资源。

> **Note**
>
> 上一代实例仍然得到完全支持，并且特性和功能保持不变。我们建议您使用最新一代的实例以获得最佳性能。

要确定哪些实例类型满足您的要求（例如支持的区域、计算资源或存储资源），请参阅查找 Amazon EC2 实例类型 (p. 396)。

主题

- 当前一代实例 (p. 239)
- 上一代实例 (p. 244)

当前一代实例

为了获得最佳性能，我们建议您在启动新实例时使用以下实例类型。有关更多信息，请参阅 Amazon EC2 实例类型。

实例

- 通用型 (p. 239)
- 计算优化 (p. 241)
- 内存优化 (p. 242)
- 存储优化 (p. 243)
- 加速计算 (p. 244)

通用型

类型	尺寸	
M4	`m4.large` | `m4.xlarge` | `m4.2xlarge` | `m4.4xlarge` | `m4.10xlarge` | `m4.16xlarge`	
M5	`m5.large` | `m5.xlarge` | `m5.2xlarge` | `m5.4xlarge` | `m5.8xlarge` | `m5.12xlarge` | `m5.16xlarge` | `m5.24xlarge` | `m5.metal`	
M5a	`m5a.large` | `m5a.xlarge` | `m5a.2xlarge` | `m5a.4xlarge` | `m5a.8xlarge` | `m5a.12xlarge` | `m5a.16xlarge` | `m5a.24xlarge`	
M5ad	`m5ad.large` | `m5ad.xlarge` | `m5ad.2xlarge` | `m5ad.4xlarge` | `m5ad.8xlarge` | `m5ad.12xlarge` | `m5ad.16xlarge` | `m5ad.24xlarge`	

类型	尺寸	
M5d	m5d.large | m5d.xlarge | m5d.2xlarge | m5d.4xlarge | m5d.8xlarge | m5d.12xlarge | m5d.16xlarge | m5d.24xlarge | m5d.metal	
M5dn	m5dn.large | m5dn.xlarge | m5dn.2xlarge | m5dn.4xlarge | m5dn.8xlarge | m5dn.12xlarge | m5dn.16xlarge | m5dn.24xlarge | m5dn.metal	
M5n	m5n.large | m5n.xlarge | m5n.2xlarge | m5n.4xlarge | m5n.8xlarge | m5n.12xlarge | m5n.16xlarge | m5n.24xlarge | m5n.metal	
M5zn	m5zn.large | m5zn.xlarge | m5zn.2xlarge | m5zn.3xlarge | m5zn.6xlarge | m5zn.12xlarge | m5zn.metal	
M6a	m6a.large | m6a.xlarge | m6a.2xlarge | m6a.4xlarge | m6a.8xlarge | m6a.12xlarge | m6a.16xlarge | m6a.24xlarge | m6a.32xlarge | m6a.48xlarge | m6a.metal	
M6g	m6g.medium | m6g.large | m6g.xlarge | m6g.2xlarge | m6g.4xlarge | m6g.8xlarge | m6g.12xlarge | m6g.16xlarge | m6g.metal	
M6gd	m6gd.medium | m6gd.large | m6gd.xlarge | m6gd.2xlarge | m6gd.4xlarge | m6gd.8xlarge | m6gd.12xlarge | m6gd.16xlarge | m6gd.metal	
M6i	m6i.large | m6i.xlarge | m6i.2xlarge | m6i.4xlarge | m6i.8xlarge | m6i.12xlarge | m6i.16xlarge | m6i.24xlarge | m6i.32xlarge | m6i.metal	
M6id	m6id.large | m6id.xlarge | m6id.2xlarge | m6id.4xlarge | m6id.8xlarge | m6id.12xlarge | m6id.16xlarge | m6id.24xlarge | m6id.32xlarge | m6id.metal	
M6idn	m6idn.large | m6idn.xlarge | m6idn.2xlarge | m6idn.4xlarge | m6idn.8xlarge | m6idn.12xlarge | m6idn.16xlarge | m6idn.24xlarge | m6idn.32xlarge | m6idn.metal	
M6in	m6in.large | m6in.xlarge | m6in.2xlarge | m6in.4xlarge | m6in.8xlarge | m6in.12xlarge | m6in.16xlarge | m6in.24xlarge | m6in.32xlarge | m6in.metal	
M7g	m7g.medium | m7g.large | m7g.xlarge | m7g.2xlarge | m7g.4xlarge | m7g.8xlarge | m7g.12xlarge | m7g.16xlarge | m7g.metal	
Mac1	mac1.metal	
Mac2	mac2.metal	
T2	t2.nano | t2.micro | t2.small | t2.medium | t2.large | t2.xlarge | t2.2xlarge	
T3	t3.nano | t3.micro | t3.small | t3.medium | t3.large | t3.xlarge | t3.2xlarge	
T3a	t3a.nano | t3a.micro | t3a.small | t3a.medium | t3a.large | t3a.xlarge | t3a.2xlarge	
T4g	t4g.nano | t4g.micro | t4g.small | t4g.medium | t4g.large | t4g.xlarge | t4g.2xlarge	

计算优化

类型	尺寸	
C4	c4.large | c4.xlarge | c4.2xlarge | c4.4xlarge | c4.8xlarge	
C5	c5.large | c5.xlarge | c5.2xlarge | c5.4xlarge | c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5.metal	
C5a	c5a.large | c5a.xlarge | c5a.2xlarge | c5a.4xlarge | c5a.8xlarge | c5a.12xlarge | c5a.16xlarge | c5a.24xlarge	
C5ad	c5ad.large | c5ad.xlarge | c5ad.2xlarge | c5ad.4xlarge | c5ad.8xlarge | c5ad.12xlarge | c5ad.16xlarge | c5ad.24xlarge	
C5d	c5d.large | c5d.xlarge | c5d.2xlarge | c5d.4xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5d.metal	
C5n	c5n.large | c5n.xlarge | c5n.2xlarge | c5n.4xlarge | c5n.9xlarge | c5n.18xlarge | c5n.metal	
C6a	c6a.large | c6a.xlarge | c6a.2xlarge | c6a.4xlarge | c6a.8xlarge | c6a.12xlarge | c6a.16xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6a.metal	
C6g	c6g.medium | c6g.large | c6g.xlarge | c6g.2xlarge | c6g.4xlarge | c6g.8xlarge | c6g.12xlarge | c6g.16xlarge | c6g.metal	
C6gd	c6gd.medium | c6gd.large | c6gd.xlarge | c6gd.2xlarge | c6gd.4xlarge | c6gd.8xlarge | c6gd.12xlarge | c6gd.16xlarge | c6gd.metal	
C6gn	c6gn.medium | c6gn.large | c6gn.xlarge | c6gn.2xlarge | c6gn.4xlarge | c6gn.8xlarge | c6gn.12xlarge | c6gn.16xlarge	
C6i	c6i.large | c6i.xlarge | c6i.2xlarge | c6i.4xlarge | c6i.8xlarge | c6i.12xlarge | c6i.16xlarge | c6i.24xlarge | c6i.32xlarge | c6i.metal	
C6id	c6id.large | c6id.xlarge | c6id.2xlarge | c6id.4xlarge | c6id.8xlarge | c6id.12xlarge | c6id.16xlarge | c6id.24xlarge | c6id.32xlarge | c6id.metal	
C6in	c6in.large | c6in.xlarge | c6in.2xlarge | c6in.4xlarge | c6in.8xlarge | c6in.12xlarge | c6in.16xlarge | c6in.24xlarge | c6in.32xlarge | c6in.metal	
C7g	c7g.medium | c7g.large | c7g.xlarge | c7g.2xlarge | c7g.4xlarge | c7g.8xlarge | c7g.12xlarge | c7g.16xlarge | c7g.metal	
CC2	cc2.8xlarge	
Hpc6a	hpc6a.48xlarge	

内存优化

类型	尺寸	
CR1	cr1.8xlarge	
Hpc6id	hpc6id.32xlarge	
R4	r4.large | r4.xlarge | r4.2xlarge | r4.4xlarge | r4.8xlarge | r4.16xlarge	
R5	r5.large | r5.xlarge | r5.2xlarge | r5.4xlarge | r5.8xlarge | r5.12xlarge | r5.16xlarge | r5.24xlarge | r5.metal	
R5a	r5a.large | r5a.xlarge | r5a.2xlarge | r5a.4xlarge | r5a.8xlarge | r5a.12xlarge | r5a.16xlarge | r5a.24xlarge	
R5ad	r5ad.large | r5ad.xlarge | r5ad.2xlarge | r5ad.4xlarge | r5ad.8xlarge | r5ad.12xlarge | r5ad.16xlarge | r5ad.24xlarge	
R5b	r5b.large | r5b.xlarge | r5b.2xlarge | r5b.4xlarge | r5b.8xlarge | r5b.12xlarge | r5b.16xlarge | r5b.24xlarge | r5b.metal	
R5d	r5d.large | r5d.xlarge | r5d.2xlarge | r5d.4xlarge | r5d.8xlarge | r5d.12xlarge | r5d.16xlarge | r5d.24xlarge | r5d.metal	
R5dn	r5dn.large | r5dn.xlarge | r5dn.2xlarge | r5dn.4xlarge | r5dn.8xlarge | r5dn.12xlarge | r5dn.16xlarge | r5dn.24xlarge | r5dn.metal	
R5n	r5n.large | r5n.xlarge | r5n.2xlarge | r5n.4xlarge | r5n.8xlarge | r5n.12xlarge | r5n.16xlarge | r5n.24xlarge | r5n.metal	
R6a	r6a.large | r6a.xlarge | r6a.2xlarge | r6a.4xlarge | r6a.8xlarge | r6a.12xlarge | r6a.16xlarge | r6a.24xlarge | r6a.32xlarge | r6a.48xlarge | r6a.metal	
R6g	r6g.medium | r6g.large | r6g.xlarge | r6g.2xlarge | r6g.4xlarge | r6g.8xlarge | r6g.12xlarge | r6g.16xlarge | r6g.metal	
R6gd	r6gd.medium | r6gd.large | r6gd.xlarge | r6gd.2xlarge | r6gd.4xlarge | r6gd.8xlarge | r6gd.12xlarge | r6gd.16xlarge | r6gd.metal	
R6i	r6i.large | r6i.xlarge | r6i.2xlarge | r6i.4xlarge | r6i.8xlarge | r6i.12xlarge | r6i.16xlarge | r6i.24xlarge | r6i.32xlarge | r6i.metal	
R6idn	r6idn.large | r6idn.xlarge | r6idn.2xlarge | r6idn.4xlarge | r6idn.8xlarge | r6idn.12xlarge | r6idn.16xlarge | r6idn.24xlarge | r6idn.32xlarge | r6idn.metal	
R6in	r6in.large | r6in.xlarge | r6in.2xlarge | r6in.4xlarge | r6in.8xlarge | r6in.12xlarge | r6in.16xlarge | r6in.24xlarge | r6in.32xlarge | r6in.metal	
R6id	r6id.large | r6id.xlarge | r6id.2xlarge | r6id.4xlarge | r6id.8xlarge | r6id.12xlarge | r6id.16xlarge | r6id.24xlarge | r6id.32xlarge | r6id.metal	

类型	尺寸	
R7g	r7g.medium | r7g.large | r7g.xlarge | r7g.2xlarge | r7g.4xlarge | r7g.8xlarge | r7g.12xlarge | r7g.16xlarge | r7g.metal	
U-3tb1	u-3tb1.56xlarge	
U-6tb1	u-6tb1.56xlarge | u-6tb1.112xlarge | u-6tb1.metal	
U-9tb1	u-9tb1.112xlarge | u-9tb1.metal	
U-12tb1	u-12tb1.112xlarge | u-12tb1.metal	
U-18tb1	u-18tb1.metal	
U-24tb1	u-24tb1.metal	
X1	x1.16xlarge | x1.32xlarge	
X2gd	x2gd.medium | x2gd.large | x2gd.xlarge | x2gd.2xlarge | x2gd.4xlarge | x2gd.8xlarge | x2gd.12xlarge | x2gd.16xlarge | x2gd.metal	
X2idn	x2idn.16xlarge | x2idn.24xlarge | x2idn.32xlarge | x2idn.metal	
X2iedn	x2iedn.xlarge | x2iedn.2xlarge | x2iedn.4xlarge | x2iedn.8xlarge | x2iedn.16xlarge | x2iedn.24xlarge | x2iedn.32xlarge | x2iedn.metal	
X2iezn	x2iezn.2xlarge | x2iezn.4xlarge | x2iezn.6xlarge | x2iezn.8xlarge | x2iezn.12xlarge | x2iezn.metal	
X1e	x1e.xlarge | x1e.2xlarge | x1e.4xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge	
z1d	z1d.large | z1d.xlarge | z1d.2xlarge | z1d.3xlarge | z1d.6xlarge | z1d.12xlarge | z1d.metal	

存储优化

类型	尺寸	
D2	d2.xlarge | d2.2xlarge | d2.4xlarge | d2.8xlarge	
D3	d3.xlarge | d3.2xlarge | d3.4xlarge | d3.8xlarge	
D3en	d3en.xlarge | d3en.2xlarge | d3en.4xlarge | d3en.6xlarge | d3en.8xlarge | d3en.12xlarge	
H1	h1.2xlarge | h1.4xlarge | h1.8xlarge | h1.16xlarge	
HS1	hs1.8xlarge	
I3	i3.large | i3.xlarge | i3.2xlarge | i3.4xlarge | i3.8xlarge | i3.16xlarge | i3.metal	
I3en	i3en.large | i3en.xlarge | i3en.2xlarge | i3en.3xlarge | i3en.6xlarge | i3en.12xlarge | i3en.24xlarge | i3en.metal	

类型	尺寸	
I4i	i4i.large | i4i.xlarge | i4i.2xlarge | i4i.4xlarge | i4i.8xlarge | i4i.16xlarge | i4i.32xlarge | i4i.metal	
Im4gn	im4gn.large | im4gn.xlarge | im4gn.2xlarge | im4gn.4xlarge | im4gn.8xlarge | im4gn.16xlarge	
Is4gen	is4gen.medium | is4gen.large | is4gen.xlarge | is4gen.2xlarge | is4gen.4xlarge | is4gen.8xlarge	

加速计算

类型	尺寸	
DL1	dl1.24xlarge	
F1	f1.2xlarge | f1.4xlarge | f1.16xlarge	
G3	g3.4xlarge | g3.8xlarge | g3.16xlarge	
G4ad	g4ad.xlarge | g4ad.2xlarge | g4ad.4xlarge | g4ad.8xlarge | g4ad.16xlarge	
G4dn	g4dn.xlarge | g4dn.2xlarge | g4dn.4xlarge | g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal	
G5	g5.xlarge | g5.2xlarge | g5.4xlarge | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge | g5.48xlarge	
G5g	g5g.xlarge | g5g.2xlarge | g5g.4xlarge | g5g.8xlarge | g5g.16xlarge | g5g.metal	
Inf1	inf1.xlarge | inf1.2xlarge | inf1.6xlarge | inf1.24xlarge	
P2	p2.xlarge | p2.8xlarge | p2.16xlarge	
P3	p3.2xlarge | p3.8xlarge | p3.16xlarge	
P3dn	p3dn.24xlarge	
P4d	p4d.24xlarge	
P4de	p4de.24xlarge	
Trn1	trn1.2xlarge | trn1.32xlarge	
VT1	vt1.3xlarge | vt1.6xlarge | vt1.24xlarge	

上一代实例

Amazon Web Services 为根据上一代实例类型优化了应用程序但尚未升级的用户提供了上一代实例类型。我们鼓励您使用当前一代实例类型以获得最佳性能，但我们将继续支持下面的上一代实例类型。有关哪些当前一代实例类型是适合的升级的更多信息，请参阅上一代实例。

类型	尺寸
A1	a1.medium | a1.large | a1.xlarge | a1.2xlarge | a1.4xlarge | a1.metal
C1	c1.medium | c1.xlarge
C3	c3.large | c3.xlarge | c3.2xlarge | c3.4xlarge | c3.8xlarge
G2	g2.2xlarge | g2.8xlarge
I2	i2.xlarge | i2.2xlarge | i2.4xlarge | i2.8xlarge
M1	m1.small | m1.medium | m1.large | m1.xlarge
M2	m2.xlarge | m2.2xlarge | m2.4xlarge
M3	m3.medium | m3.large | m3.xlarge | m3.2xlarge
R3	r3.large | r3.xlarge | r3.2xlarge | r3.4xlarge | r3.8xlarge
T1	t1.micro

硬件规格

有关更多信息，请参阅 Amazon EC2 实例类型。

要确定最适合您的需求的实例类型，我们建议启动一个实例，并使用自己的基准测试应用程序。由于您是按实例秒付费的，因此在做出决策前测试多个实例类型将会既方便又经济。如果您的需求有变化，甚至是在做出决策后，您可以在以后更改您的实例类型。有关更多信息，请参阅更改实例类型 (p. 399)。

处理器功能

Intel 处理器功能

在 Intel 处理器上运行的 Amazon EC2 实例可能包括以下功能。并非所有实例类型都支持以下所有处理器功能。有关每种实例类型可用哪些功能的详细信息，请参阅 Amazon EC2实例类型。

- Intel AES New Instructions (AES-NI) — Intel AES-NI 加密指令集改进了原先 Advanced Encryption Standard (AES) 的算法，可以提供更快的数据保护和更好的安全性。所有最新一代 EC2 实例都支持此处理器功能。
- Intel Advanced Vector Extensions（Intel AVX、Intel AVX2 和 Intel AVX-512）— ：Intel AVX/Intel AVX2 和 Intel AVX-512 分别是 256 位和 512 位指令集扩展，专为浮点 (FP) 密集型应用程序而设计。Intel AVX 指令可以提升诸如图像和音频/视频处理、科学模拟、财务分析、3D 建模与分析等应用的性能。这些功能仅在使用 HVM AMI 启动的实例上可用。
- Intel 睿频加速技术 — Intel 睿频加速技术处理器以比基本操作频率快的速度自动运行核心。
- Intel Deep Learning Boost (Intel DL Boost) — 加速 AI 深度学习使用案例。第二代 Intel Xeon 可扩展处理器能够扩展采用全新矢量神经网络指令 (VNNI/INT8) 的 Intel AVX-512，与上一代 Intel Xeon 可扩展处理器（配有 FP32）相比，深度学习推理性能显著提高，适用于图像识别/分割、对象检测、语音识别、语言翻译、推荐系统和强化学习等。VNNI 可能不会兼容所有 Linux 发行版。

  以下实例支持 VNNI：M5n、R5n、M5dn、M5zn、R5b、R5dn、D3、D3en 和 C6i。C5 和 C5d 实例仅支持 12xlarge、24xlarge 和 metal 实例的 VNNI。

64 位 CPU 的命名约定可能会导致混淆。芯片制造商 Advanced Micro Devices (AMD) 成功引入了第一款基于 Intel x86 指令集的商用 64 位架构。因此，不论芯片制造商是谁，这一架构被普遍称为

AMD64。Windows 和多个 Linux 发行版遵循这一实践。这说明了为什么实例即使运行在 Intel 硬件上，但 Ubuntu 或 Windows 上的内部系统信息仍将 CPU 架构显示为 AMD64。

AMI 虚拟化类型

实例的虚拟化类型由用于启动该实例的 AMI 决定。最新一代实例类型仅支持硬件虚拟机 (HVM)。某些上一代实例类型支持半虚拟化 (PV)，某些 Amazon 区域支持半虚拟化实例。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。

为获得最佳性能，我们建议您使用 HVM AMI。此外，HVM AMI 还需要利用增强联网。HVM 虚拟化使用 Amazon 平台提供的硬件辅助技术。借助 HVM 虚拟化，访客虚拟机如同在本地硬件平台上运行一样，除了仍然使用半虚拟 (PV) 网络和存储驱动程序以提高性能。

基于 Nitro 系统构建的实例

Nitro 系统是由 Amazon 打造的硬件和软件组件集合，可实现高性能、高可用性和高安全性。有关更多信息，请参阅 Amazon Nitro 系统。

Nitro 系统提供了裸机功能，从而消除了所有虚拟化开销并支持需要完全访问主机硬件的工作负载。裸机实例非常适合以下用途：

- 需要访问虚拟环境中不可用或不完整支持的低级硬件功能 (如 Intel VT) 的工作负载
- 需要非虚拟化环境进行许可或支持的应用程序

Nitro 组件

以下组件属于 Nitro 系统的一部分：

- Nitro 卡
  - 本地 NVMe 存储卷
  - 联网硬件支持
  - 管理
  - 监控
  - 安全性
- Nitro 安全芯片，集成到主板中
- Nitro 管理程序 - 一种轻量级管理程序，可管理内存和 CPU 分配并为多数工作负载提供了与裸机不相上下的性能。

虚拟化实例

以下虚拟化实例基于 Nitro 系统而构建：

- 通用
  型：A1、M5、M5a、M5ad、M5d、M5dn、M5n、M5zn、M6a、M6g、M6gd、M6i、M6id、M6idn、M6in、M7g、T3、和 T4g
- 计算优化型：C5、C5a、C5ad、C5d、C5n、C6a、C6g、C6gd、C6gn、C6i、C6id、C6in、C7g 和 Hpc6a
- 内存优化
  型：Hpc6id、R5、R5a、R5ad、R5b、R5d、R5dn、R5n、R6a、R6g、R6gd、R6i、R6idn、R6in、R6id、R7g、U-3t 和 z1d
- 存储优化型：D3、D3en、I3en、I4i、Im4gn 和 Is4gen
- 加速计算型：DL1、G4ad、G4dn、G5、G5g、Inf1、P3dn、P4d、P4de、Trn1 和 VT1

裸机实例

以下裸机实例基于 Nitro 系统而构建：

- 通用型：a1.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | m5zn.metal | m6a.metal | m6g.metal | m6gd.metal | m6i.metal | m6id.metal | m6idn.metal | m6in.metal | m7g.metal | mac1.metal | mac2.metal
- 计算优化型：c5.metal | c5d.metal | c5n.metal | c6a.metal | c6g.metal | c6gd.metal | c6i.metal | c6id.metal | c6in.metal | c7g.metal
- 内存优化型：r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal | r6a.metal | r6g.metal | r6gd.metal | r6i.metal | r6idn.metal | r6in.metal | r6id.metal | r7g.metal | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | x2gd.metal | x2idn.metal | x2iedn.metal | x2iezn.metal | z1d.metal
- 存储优化型：i3.metal | i3en.metal | i4i.metal
- 加速计算型：g4dn.metal | g5g.metal

联网和存储功能

当您选择实例类型时，您同时选择了可用的联网和存储功能。要描述实例类型，请使用 describe-instance-types 命令。

联网功能

- 所有当前生成实例类型以及 C3、R3 和 I2 以前生成实例类型都支持 IPv6。
- 为了最大程度提高您的实例类型的联网和带宽性能，您可以执行以下操作：
  - 将支持的实例类型启动到集群置放群组中，以针对高性能计算 (HPC) 应用程序优化您的实例。通用集群置放群组中的实例可以受益于高带宽、低延迟的联网。有关更多信息，请参阅置放群组 (p. 1177)。
  - 为受支持的最新一代实例类型启用增强联网，从而显著提高每秒数据包数 (PPS) 性能、减弱网络抖动和减少网络延迟。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。
- 为增强网络启用的当前生成实例类型具有以下网络性能属性：
  - 通过私有 IPv4 或 IPv6 位于相同区域内的流量可以支持 5 Gbps 用于单流流量，以及最多 25 Gbps 用于多流流量（取决于实例类型）。
  - 在同一个区域中，通过公有 IP 地址空间或者通过 VPC 终端节点往返于 Amazon S3 存储桶之间的流量可以使用所有可用的实例聚合带宽。
- 支持的最大传输单位 (MTU) 因实例类型而异。所有 Amazon EC2 实例类型都支持标准以太网 V2 1500 MTU 框架。所有最新一代实例都支持 9001 MTU (巨型帧)，某些上一代实例也支持它们。有关更多信息，请参阅EC2 实例的网络最大传输单位 (MTU) (p. 1192)。

存储功能

- 一些实例类型支持 EBS 卷和实例存储卷，而另一些实例类型仅支持 EBS 卷。一些支持实例存储卷的实例类型使用固态硬盘 (SSD) 来提供非常高的随机 I/O 性能。一些实例类型支持 NVMe 实例存储卷。一些实例类型支持 NVMe EBS 卷。有关更多信息，请参阅Linux 实例上的 Amazon EBS 和 NVMe (p. 1518) 和 NVMe SSD 卷 (p. 1596)。
- 若要获得 Amazon EBS I/O 的额外专用容量，您可以将某些实例类型作为 EBS 优化实例启动。某些实例类型在默认情况下会进行 EBS 优化。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

联网和存储功能摘要

下表总结了最新一代实例类型支持的联网和存储功能。

实例

- 通用型 (p. 248)
- 计算优化 (p. 249)
- 内存优化 (p. 249)
- 存储优化 (p. 250)
- 加速计算 (p. 251)
- 上一代实例类型 (p. 251)

通用型

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
M4	是	否	否	是	ENA
M5	是	是	否	是	ENA
M5a	是	是	否	是	ENA
M5ad	否	是	NVMe	是	ENA
M5d	否	是	NVMe	是	ENA
M5dn	否	是	NVMe	是	ENA | EFA
M5n	是	是	否	是	ENA | EFA
M5zn	是	是	否	是	ENA | EFA
M6a	是	是	否	是	ENA | EFA
M6g	是	是	否	是	ENA
M6gd	否	是	NVMe	是	ENA
M6i	是	是	否	是	ENA | EFA
M6id	否	是	NVMe	是	ENA | EFA
M6idn	否	是	NVMe	是	ENA | EFA
M6in	是	是	否	是	ENA | EFA
M7g	是	是	否	是	ENA | EFA
Mac1	是	是	否	是	ENA
Mac2	是	是	否	是	ENA
T2	是	否	否	是	不支持
T3	是	是	否	是	ENA
T3a	是	是	否	是	ENA
T4g	是	是	否	是	ENA

计算优化

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
C4	是	否	否	是	不支持
C5	是	是	否	是	ENA
C5a	是	是	否	是	ENA
C5ad	否	是	NVMe	是	ENA
C5d	否	是	NVMe	是	ENA
C5n	是	是	否	是	ENA | EFA
C6a	是	是	否	是	ENA | EFA
C6g	是	是	否	是	ENA
C6gd	否	是	NVMe	是	ENA
C6gn	是	是	否	是	ENA | EFA
C6i	是	是	否	是	ENA | EFA
C6id	否	是	NVMe	是	ENA | EFA
C6in	是	是	否	是	ENA | EFA
C7g	是	是	否	是	ENA | EFA
CC2	否	否	HDD	是	不支持
Hpc6a	是	是	否	是	ENA | EFA

内存优化

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
CR1	否	否	HDD	是	不支持
Hpc6id	否	是	NVMe	是	ENA | EFA
R4	是	否	否	是	ENA
R5	是	是	否	是	ENA
R5a	是	是	否	是	ENA
R5ad	否	是	NVMe	是	ENA
R5b	是	是	否	是	ENA
R5d	否	是	NVMe	是	ENA
R5dn	否	是	NVMe	是	ENA | EFA
R5n	是	是	否	是	ENA | EFA

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
R6a	是	是	否	是	ENA | EFA
R6g	是	是	否	是	ENA
R6gd	否	是	NVMe	是	ENA
R6i	是	是	否	是	ENA | EFA
R6idn	否	是	NVMe	是	ENA | EFA
R6in	是	是	否	是	ENA | EFA
R6id	否	是	NVMe	是	ENA | EFA
R7g	是	是	否	是	ENA | EFA
U-3tb1	是	是	否	是	ENA
U-6tb1	是	是	否	是	ENA
U-9tb1	是	是	否	是	ENA
U-12tb1	是	是	否	是	ENA
U-18tb1	是	是	否	是	ENA
U-24tb1	是	是	否	是	ENA
X1	否	否	SSD	是	ENA
X2gd	否	是	NVMe	是	ENA
X2idn	否	是	NVMe	是	ENA | EFA
X2iedn	否	是	NVMe	是	ENA | EFA
X2iezn	是	是	否	是	ENA | EFA
X1e	否	否	SSD	是	ENA
z1d	否	是	NVMe	是	ENA

存储优化

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
D2	否	否	HDD	是	不支持
D3	否	是	NVMe	是	ENA
D3en	否	是	NVMe	是	ENA
H1	否	否	HDD	是	ENA
HS1	否	是	HDD	是	不支持
I3	否	是	NVMe	是	ENA
I3en	否	是	NVMe	是	ENA | EFA

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
I4i	否	是	NVMe	是	ENA | EFA
Im4gn	否	是	NVMe	是	ENA | EFA
Is4gen	否	是	NVMe	是	ENA

加速计算

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
DL1	否	是	NVMe	是	ENA | EFA
F1	否	是	NVMe	是	不支持
G3	是	否	否	是	ENA
G4ad	否	是	NVMe	是	ENA
G4dn	否	是	NVMe	是	ENA | EFA
G5	否	是	NVMe	是	ENA | EFA
G5g	是	是	否	是	ENA
Inf1	是	是	否	是	ENA | EFA
P2	是	否	否	是	ENA
P3	是	否	否	是	ENA
P3dn	否	是	NVMe	是	ENA | EFA
P4d	否	是	NVMe	是	ENA | EFA
P4de	否	是	NVMe	是	ENA | EFA
Trn1	否	是	NVMe	是	ENA | EFA
VT1	是	是	否	是	ENA | EFA

上一代实例类型

下表总结了前一代实例类型支持的联网和存储功能。

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
A1	是	是	否	是	ENA
C1	否	否	HDD	是	不支持
C3	否	否	SSD	是	不支持
G2	否	否	SSD	是	不支持
I2	否	否	SSD	是	不支持

实例类型	仅限于 EBS	NVME EBS	实例存储	置放群组	增强联网
M1	否	否	HDD	是	不支持
M2	否	否	HDD	是	不支持
M3	否	否	SSD	是	不支持
R3	否	否	SSD	是	不支持
T1	是	否	否	是	不支持

实例限制

在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。

有关默认限制的更多信息，请参阅我可以在 Amazon EC2 中运行多少个实例？

有关查看当前限制或请求提高当前限制的更多信息，请参阅 Amazon EC2 Service Quotas (p. 1678)。

通用实例

通用型实例提供平衡的计算、内存和网络资源，可用于各种不同的工作负载。

M5 和 M5a 实例

这些实例提供了理想的云基础设施，面向部署在云中的广泛应用程序，提供平衡的计算、内存和网络资源。它们非常适合以下用途：

- 中小型数据库
- 需要额外内存的数据处理任务
- 缓存机群
- 为 SAP、Microsoft SharePoint、集群计算和其他企业应用程序运行后端服务器

裸机实例（如 `m5.metal`、`m5n.metal` 和 `m5zn.metal` ）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

M5zn

这些实例非常适合从极高的单线程性能、高吞吐量和低延迟网络受益的应用程序。它们非常适合以下用途：

- 游戏
- 高性能计算
- 模拟建模

M6g 和 M6gd 实例

这些实例由 Amazon Graviton2 处理器提供支持，并为各种不同的通用工作负载提供平衡的计算、内存和网络。它们非常适合以下用途：

- 应用程序服务器
- 微服务
- 游戏服务器

- 中型数据存储
- 缓存机群

裸机实例（如 m6g.metal）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。有关更多信息，请参阅 Amazon EC2 M6g 实例。

M6i 和 M6id 实例

这些实例非常适合通用型工作负载，例如：

- 应用程序服务器和 Web 服务器
- 微服务
- 高性能计算
- 应用程序开发
- 中小型数据库
- 缓存机群

裸机实例（如 m6i.metal）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

M6in 和 M6idn 实例

这些实例非常适合网络密集型工作负载，例如：

- 高性能文件系统
- 分布式 Web 级内存缓存
- 缓存机群
- 实时大数据分析
- 电信应用程序，例如 5G 用户面功能（UPF）

有关更多信息，请参阅 Amazon EC2 M6i 实例。

T2、T3、T3a 和 T4g 实例

这些实例提供基准水平的 CPU 性能，并且能够在您的工作负载需要时突增到更高的性能。无限实例可以将较高的 CPU 性能保持所需的任意时间。有关更多信息，请参阅可突增性能实例 (p. 274)。它们非常适合以下用途：

- 网站和 Web 应用程序
- 代码存储库
- 开发、构建、测试和存放环境
- 微服务

目录

- 硬件规格 (p. 254)
- 实例性能 (p. 260)
- 网络性能 (p. 260)
- Amazon EBS I/O 性能 (p. 271)
- 基于 SSD 的实例存储卷的 I/O 性能 (p. 271)
- 发布说明 (p. 273)
- 可突增性能实例 (p. 274)

硬件规格

以下是通用型实例的硬件规格摘要。虚拟中央处理单元（vCPU）表示分配给虚拟机（VM）的物理 CPU 的一部分。对于 x86 实例，每个内核有两个 vCPU。对于 Graviton 实例，每个内核有一个 vCPU。

实例类型	默认 vCPU	内存（GiB）
a1.medium	1	2.00
a1.large	2	4.00
a1.xlarge	4	8.00
a1.2xlarge	8	16.00
a1.4xlarge	16	32.00
a1.metal	16	32.00
m1.small	1	1.70
m1.medium	1	3.70
m1.large	2	7.50
m1.xlarge	4	15.00
m2.xlarge	2	17.10
m2.2xlarge	4	34.20
m2.4xlarge	8	68.40
m3.medium	1	3.75
m3.large	2	7.50
m3.xlarge	4	15.00
m3.2xlarge	8	30.00
m4.large	2	8.00
m4.xlarge	4	16.00
m4.2xlarge	8	32.00
m4.4xlarge	16	64.00
m4.10xlarge	40	160.00
m4.16xlarge	64	256.00
m5.large	2	8.00
m5.xlarge	4	16.00
m5.2xlarge	8	32.00
m5.4xlarge	16	64.00
m5.8xlarge	32	128.00

实例类型	默认 vCPU	内存（GiB）
m5.12xlarge	48	192.00
m5.16xlarge	64	256.00
m5.24xlarge	96	384.00
m5.metal	96	384.00
m5a.large	2	8.00
m5a.xlarge	4	16.00
m5a.2xlarge	8	32.00
m5a.4xlarge	16	64.00
m5a.8xlarge	32	128.00
m5a.12xlarge	48	192.00
m5a.16xlarge	64	256.00
m5a.24xlarge	96	384.00
m5ad.large	2	8.00
m5ad.xlarge	4	16.00
m5ad.2xlarge	8	32.00
m5ad.4xlarge	16	64.00
m5ad.8xlarge	32	128.00
m5ad.12xlarge	48	192.00
m5ad.16xlarge	64	256.00
m5ad.24xlarge	96	384.00
m5d.large	2	8.00
m5d.xlarge	4	16.00
m5d.2xlarge	8	32.00
m5d.4xlarge	16	64.00
m5d.8xlarge	32	128.00
m5d.12xlarge	48	192.00
m5d.16xlarge	64	256.00
m5d.24xlarge	96	384.00
m5d.metal	96	384.00
m5dn.large	2	8.00
m5dn.xlarge	4	16.00

实例类型	默认 vCPU	内存（GiB）
m5dn.2xlarge	8	32.00
m5dn.4xlarge	16	64.00
m5dn.8xlarge	32	128.00
m5dn.12xlarge	48	192.00
m5dn.16xlarge	64	256.00
m5dn.24xlarge	96	384.00
m5dn.metal	96	384.00
m5n.large	2	8.00
m5n.xlarge	4	16.00
m5n.2xlarge	8	32.00
m5n.4xlarge	16	64.00
m5n.8xlarge	32	128.00
m5n.12xlarge	48	192.00
m5n.16xlarge	64	256.00
m5n.24xlarge	96	384.00
m5n.metal	96	384.00
m5zn.large	2	8.00
m5zn.xlarge	4	16.00
m5zn.2xlarge	8	32.00
m5zn.3xlarge	12	48.00
m5zn.6xlarge	24	96.00
m5zn.12xlarge	48	192.00
m5zn.metal	48	192.00
m6a.large	2	8.00
m6a.xlarge	4	16.00
m6a.2xlarge	8	32.00
m6a.4xlarge	16	64.00
m6a.8xlarge	32	128.00
m6a.12xlarge	48	192.00
m6a.16xlarge	64	256.00
m6a.24xlarge	96	384.00

实例类型	默认 vCPU	内存（GiB）
m6a.32xlarge	128	512.00
m6a.48xlarge	192	768.00
m6a.metal	192	768.00
m6g.medium	1	4.00
m6g.large	2	8.00
m6g.xlarge	4	16.00
m6g.2xlarge	8	32.00
m6g.4xlarge	16	64.00
m6g.8xlarge	32	128.00
m6g.12xlarge	48	192.00
m6g.16xlarge	64	256.00
m6g.metal	64	256.00
m6gd.medium	1	4.00
m6gd.large	2	8.00
m6gd.xlarge	4	16.00
m6gd.2xlarge	8	32.00
m6gd.4xlarge	16	64.00
m6gd.8xlarge	32	128.00
m6gd.12xlarge	48	192.00
m6gd.16xlarge	64	256.00
m6gd.metal	64	256.00
m6i.large	2	8.00
m6i.xlarge	4	16.00
m6i.2xlarge	8	32.00
m6i.4xlarge	16	64.00
m6i.8xlarge	32	128.00
m6i.12xlarge	48	192.00
m6i.16xlarge	64	256.00
m6i.24xlarge	96	384.00
m6i.32xlarge	128	512.00
m6i.metal	128	512.00

实例类型	默认 vCPU	内存（GiB）
m6id.large	2	8.00
m6id.xlarge	4	16.00
m6id.2xlarge	8	32.00
m6id.4xlarge	16	64.00
m6id.8xlarge	32	128.00
m6id.12xlarge	48	192.00
m6id.16xlarge	64	256.00
m6id.24xlarge	96	384.00
m6id.32xlarge	128	512.00
m6id.metal	128	512.00
m6idn.large	2	8.00
m6idn.xlarge	4	16.00
m6idn.2xlarge	8	32.00
m6idn.4xlarge	16	64.00
m6idn.8xlarge	32	128.00
m6idn.12xlarge	48	192.00
m6idn.16xlarge	64	256.00
m6idn.24xlarge	96	384.00
m6idn.32xlarge	128	512.00
m6idn.metal	128	512.00
m6in.large	2	8.00
m6in.xlarge	4	16.00
m6in.2xlarge	8	32.00
m6in.4xlarge	16	64.00
m6in.8xlarge	32	128.00
m6in.12xlarge	48	192.00
m6in.16xlarge	64	256.00
m6in.24xlarge	96	384.00
m6in.32xlarge	128	512.00
m6in.metal	128	512.00
m7g.medium	1	4.00

实例类型	默认 vCPU	内存（GiB）
m7g.large	2	8.00
m7g.xlarge	4	16.00
m7g.2xlarge	8	32.00
m7g.4xlarge	16	64.00
m7g.8xlarge	32	128.00
m7g.12xlarge	48	192.00
m7g.16xlarge	64	256.00
m7g.metal	64	256.00
mac1.metal	12	32.00
mac2.metal	8	16.00
t1.micro	1	0.61
t2.nano	1	0.50
t2.micro	1	1.00
t2.small	1	2.00
t2.medium	2	4.00
t2.large	2	8.00
t2.xlarge	4	16.00
t2.2xlarge	8	32.00
t3.nano	2	0.50
t3.micro	2	1.00
t3.small	2	2.00
t3.medium	2	4.00
t3.large	2	8.00
t3.xlarge	4	16.00
t3.2xlarge	8	32.00
t3a.nano	2	0.50
t3a.micro	2	1.00
t3a.small	2	2.00
t3a.medium	2	4.00
t3a.large	2	8.00
t3a.xlarge	4	16.00

实例类型	默认 vCPU	内存（GiB）
t3a.2xlarge	8	32.00
t4g.nano	2	0.50
t4g.micro	2	1.00
t4g.small	2	2.00
t4g.medium	2	4.00
t4g.large	2	8.00
t4g.xlarge	4	16.00
t4g.2xlarge	8	32.00

通用型实例使用以下处理器。

Amazon Graviton 处理器

- Amazon Graviton2：M6g、M6gd、T4g

AMD 处理器

- AMD EPYC 7000 系列处理器（AMD EPYC 7571）：M5a、M5ad、T3a
- 第三代 AMD EPYC 处理器（AMD EPYC 7R13）：M6a

英特尔处理器

- 英特尔至强可扩展处理器（Haswell E5-2676 v3 i 或 Broadwell E5-2686 v4）：M4、T2
- 英特尔至强可扩展处理器（Skylake 8175M 或 Cascade Lake 8259CL）：M5、M5d、T3
- 第二代英特尔至强可扩展处理器（Cascade Lake 8259CL）：M5n
- 第二代英特尔至强可扩展处理器（Cascade Lake 8252C）：M5zn
- 第三代英特尔至强可扩展处理器（Ice Lake 8375C）：M6i、M6id

有关更多信息，请参阅 Amazon EC2 实例类型。

实例性能

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。有些通用型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

一些通用型实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅您的 EC2 实例的处理器状态控制 (p. 707)。

网络性能

您可以为受支持的实例类型启用增强联网，以提供更低的延迟、更低的网络抖动和更高的每秒数据包数 (PPS) 性能。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。

以下是支持增强联网的通用型实例的网络性能摘要。

Note

标有 † 的实例类型具备基准带宽，并且可以通过网络输入/输出积分机制，尽可能将其基准带宽突增到基准以上。有关更多信息，请参阅实例网络带宽 (p. 1141)。

实例类型	网络性能	增强联网功能
a1.medium †	高达 10Gb	ENA
a1.large †	高达 10Gb	ENA
a1.xlarge †	高达 10Gb	ENA
a1.2xlarge †	高达 10Gb	ENA
a1.4xlarge †	高达 10Gb	ENA
a1.metal †	高达 10Gb	ENA
m1.small †	低	不支持
m1.medium †	中	不支持
m1.large †	中	不支持
m1.xlarge †	高	不支持
m2.xlarge †	中	不支持
m2.2xlarge †	中	不支持
m2.4xlarge †	高	不支持
m3.medium †	中	不支持
m3.large †	中	不支持
m3.xlarge †	高	不支持
m3.2xlarge †	高	不支持
m4.large †	中	不支持
m4.xlarge †	高	不支持
m4.2xlarge †	高	不支持
m4.4xlarge †	高	不支持
m4.10xlarge †	10Gb	不支持
m4.16xlarge †	25Gb	ENA
m5.large †	高达 10Gb	ENA
m5.xlarge †	高达 10Gb	ENA
m5.2xlarge †	高达 10Gb	ENA
m5.4xlarge †	高达 10Gb	ENA

实例类型	网络性能	增强联网功能
m5.8xlarge	10Gb	ENA
m5.12xlarge	12Gb	ENA
m5.16xlarge	20Gb	ENA
m5.24xlarge	25Gb	ENA
m5.metal	25Gb	ENA
m5a.large †	高达 10Gb	ENA
m5a.xlarge †	高达 10Gb	ENA
m5a.2xlarge †	高达 10Gb	ENA
m5a.4xlarge †	高达 10Gb	ENA
m5a.8xlarge †	高达 10Gb	ENA
m5a.12xlarge	10Gb	ENA
m5a.16xlarge	12Gb	ENA
m5a.24xlarge	20Gb	ENA
m5ad.large †	高达 10Gb	ENA
m5ad.xlarge †	高达 10Gb	ENA
m5ad.2xlarge †	高达 10Gb	ENA
m5ad.4xlarge †	高达 10Gb	ENA
m5ad.8xlarge †	高达 10Gb	ENA
m5ad.12xlarge	10Gb	ENA
m5ad.16xlarge	12Gb	ENA
m5ad.24xlarge	20Gb	ENA
m5d.large †	高达 10Gb	ENA
m5d.xlarge †	高达 10Gb	ENA
m5d.2xlarge †	高达 10Gb	ENA
m5d.4xlarge †	高达 10Gb	ENA
m5d.8xlarge	10Gb	ENA
m5d.12xlarge	12Gb	ENA
m5d.16xlarge	20Gb	ENA
m5d.24xlarge	25Gb	ENA
m5d.metal	25Gb	ENA
m5dn.large †	高达 25Gb	ENA

实例类型	网络性能	增强联网功能
m5dn.xlarge †	高达 25Gb	ENA
m5dn.2xlarge †	高达 25Gb	ENA
m5dn.4xlarge †	高达 25Gb	ENA
m5dn.8xlarge	25Gb	ENA
m5dn.12xlarge	50Gb	ENA
m5dn.16xlarge	75Gb	ENA
m5dn.24xlarge	100Gb	ENA | EFA
m5dn.metal	100Gb	ENA | EFA
m5n.large †	高达 25Gb	ENA
m5n.xlarge †	高达 25Gb	ENA
m5n.2xlarge †	高达 25Gb	ENA
m5n.4xlarge †	高达 25Gb	ENA
m5n.8xlarge	25Gb	ENA
m5n.12xlarge	50Gb	ENA
m5n.16xlarge	75Gb	ENA
m5n.24xlarge	100Gb	ENA | EFA
m5n.metal	100Gb	ENA | EFA
m5zn.large †	高达 25Gb	ENA
m5zn.xlarge †	高达 25Gb	ENA
m5zn.2xlarge †	高达 25Gb	ENA
m5zn.3xlarge †	高达 25Gb	ENA
m5zn.6xlarge	50Gb	ENA
m5zn.12xlarge	100Gb	ENA | EFA
m5zn.metal	100Gb	ENA | EFA
m6a.large †	高达 12.5Gb	ENA
m6a.xlarge †	高达 12.5Gb	ENA
m6a.2xlarge †	高达 12.5Gb	ENA
m6a.4xlarge †	高达 12.5Gb	ENA
m6a.8xlarge	12.5Gb	ENA
m6a.12xlarge	18.75Gb	ENA
m6a.16xlarge	25Gb	ENA

实例类型	网络性能	增强联网功能
m6a.24xlarge	37.5Gb	ENA
m6a.32xlarge	50Gb	ENA
m6a.48xlarge	50Gb	ENA | EFA
m6a.metal	50Gb	ENA | EFA
m6g.medium †	高达 10Gb	ENA
m6g.large †	高达 10Gb	ENA
m6g.xlarge †	高达 10Gb	ENA
m6g.2xlarge †	高达 10Gb	ENA
m6g.4xlarge †	高达 10Gb	ENA
m6g.8xlarge	12Gb	ENA
m6g.12xlarge	20Gb	ENA
m6g.16xlarge	25Gb	ENA
m6g.metal	25Gb	ENA
m6gd.medium †	高达 10Gb	ENA
m6gd.large †	高达 10Gb	ENA
m6gd.xlarge †	高达 10Gb	ENA
m6gd.2xlarge †	高达 10Gb	ENA
m6gd.4xlarge †	高达 10Gb	ENA
m6gd.8xlarge	12Gb	ENA
m6gd.12xlarge	20Gb	ENA
m6gd.16xlarge	25Gb	ENA
m6gd.metal	25Gb	ENA
m6i.large †	高达 12.5Gb	ENA
m6i.xlarge †	高达 12.5Gb	ENA
m6i.2xlarge †	高达 12.5Gb	ENA
m6i.4xlarge †	高达 12.5Gb	ENA
m6i.8xlarge	12.5Gb	ENA
m6i.12xlarge	18.75Gb	ENA
m6i.16xlarge	25Gb	ENA
m6i.24xlarge	37.5Gb	ENA
m6i.32xlarge	50Gb	ENA | EFA

实例类型	网络性能	增强联网功能
m6i.metal	50Gb	ENA | EFA
m6id.large †	高达 12.5Gb	ENA
m6id.xlarge †	高达 12.5Gb	ENA
m6id.2xlarge †	高达 12.5Gb	ENA
m6id.4xlarge †	高达 12.5Gb	ENA
m6id.8xlarge	12.5Gb	ENA
m6id.12xlarge	18.75Gb	ENA
m6id.16xlarge	25Gb	ENA
m6id.24xlarge	37.5Gb	ENA
m6id.32xlarge	50Gb	ENA | EFA
m6id.metal	50Gb	ENA | EFA
m6idn.large †	高达 25Gb	ENA
m6idn.xlarge †	高达 30Gb	ENA
m6idn.2xlarge †	高达 40Gb	ENA
m6idn.4xlarge †	高达 50Gb	ENA
m6idn.8xlarge	50Gb	ENA
m6idn.12xlarge	75Gb	ENA
m6idn.16xlarge	100Gb	ENA
m6idn.24xlarge	150Gb	ENA
m6idn.32xlarge	200Gb	ENA | EFA
m6idn.metal	200Gb	ENA | EFA
m6in.large †	高达 25Gb	ENA
m6in.xlarge †	高达 30Gb	ENA
m6in.2xlarge †	高达 40Gb	ENA
m6in.4xlarge †	高达 50Gb	ENA
m6in.8xlarge	50Gb	ENA
m6in.12xlarge	75Gb	ENA
m6in.16xlarge	100Gb	ENA
m6in.24xlarge	150Gb	ENA
m6in.32xlarge	200Gb	ENA | EFA
m6in.metal	200Gb	ENA | EFA

实例类型	网络性能	增强联网功能
m7g.medium †	高达 12.5Gb	ENA
m7g.large †	高达 12.5Gb	ENA
m7g.xlarge †	高达 12.5Gb	ENA
m7g.2xlarge †	高达 15Gb	ENA
m7g.4xlarge †	高达 15Gb	ENA
m7g.8xlarge	15Gb	ENA
m7g.12xlarge	22.5Gb	ENA
m7g.16xlarge	30Gb	ENA | EFA
m7g.metal	30Gb	ENA | EFA
mac1.metal	25Gb	ENA
mac2.metal	10Gb	ENA
t1.micro †	非常低	不支持
t2.nano †	低到中	不支持
t2.micro †	低到中	不支持
t2.small †	低到中	不支持
t2.medium †	低到中	不支持
t2.large †	低到中	不支持
t2.xlarge †	中	不支持
t2.2xlarge †	中	不支持
t3.nano †	高达 5Gb	ENA
t3.micro †	高达 5Gb	ENA
t3.small †	高达 5Gb	ENA
t3.medium †	高达 5Gb	ENA
t3.large †	高达 5Gb	ENA
t3.xlarge †	高达 5Gb	ENA
t3.2xlarge †	高达 5Gb	ENA
t3a.nano †	高达 5Gb	ENA
t3a.micro †	高达 5Gb	ENA
t3a.small †	高达 5Gb	ENA
t3a.medium †	高达 5Gb	ENA
t3a.large †	高达 5Gb	ENA

实例类型	网络性能	增强联网功能
t3a.xlarge †	高达 5Gb	ENA
t3a.2xlarge †	高达 5Gb	ENA
t4g.nano †	高达 5Gb	ENA
t4g.micro †	高达 5Gb	ENA
t4g.small †	高达 5Gb	ENA
t4g.medium †	高达 5Gb	ENA
t4g.large †	高达 5Gb	ENA
t4g.xlarge †	高达 5Gb	ENA
t4g.2xlarge †	高达 5Gb	ENA

对于支持 200Gbps 的 32xlarge 和 metal 实例类型，实例上至少需要 2 个 ENI，并且每个 ENI 需要连接到不同的网卡，才能达到 200Gbps 的吞吐量。连接到网卡的每个 ENI 最大可达到 170Gbps。

下表显示了实例类型的基准带宽和突增带宽，这些实例类型通过网络输入/输出积分机制将其基准带宽突增到基准以上。

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
a1.medium	0.5	10.0
a1.large	0.75	10.0
a1.xlarge	1.25	10.0
a1.2xlarge	2.5	10.0
a1.4xlarge	5.0	10.0
a1.metal	5.0	10.0
m1.small	0.3	1.2
m1.medium	0.3	1.2
m1.large	0.7	2.8
m1.xlarge	1.0	10.0
m2.xlarge	0.3	1.2
m2.2xlarge	0.7	2.8
m2.4xlarge	1.0	10.0
m3.medium	0.3	1.2
m3.large	0.7	2.8
m3.xlarge	1.0	10.0
m3.2xlarge	1.0	10.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
m4.large	0.45	1.2
m4.xlarge	0.75	2.8
m4.2xlarge	1.0	10.0
m4.4xlarge	2.0	10.0
m4.10xlarge	5.0	10.0
m4.16xlarge	5.0	10.0
m5.large	0.75	10.0
m5.xlarge	1.25	10.0
m5.2xlarge	2.5	10.0
m5.4xlarge	5.0	10.0
m5a.large	0.75	10.0
m5a.xlarge	1.25	10.0
m5a.2xlarge	2.5	10.0
m5a.4xlarge	5.0	10.0
m5a.8xlarge	7.5	10.0
m5ad.large	0.75	10.0
m5ad.xlarge	1.25	10.0
m5ad.2xlarge	2.5	10.0
m5ad.4xlarge	5.0	10.0
m5ad.8xlarge	7.5	10.0
m5d.large	0.75	10.0
m5d.xlarge	1.25	10.0
m5d.2xlarge	2.5	10.0
m5d.4xlarge	5.0	10.0
m5dn.large	2.1	25.0
m5dn.xlarge	4.1	25.0
m5dn.2xlarge	8.125	25.0
m5dn.4xlarge	16.25	25.0
m5n.large	2.1	25.0
m5n.xlarge	4.1	25.0
m5n.2xlarge	8.125	25.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
m5n.4xlarge	16.25	25.0
m5zn.large	3.0	25.0
m5zn.xlarge	5.0	25.0
m5zn.2xlarge	10.0	25.0
m5zn.3xlarge	15.0	25.0
m6a.large	0.781	12.5
m6a.xlarge	1.562	12.5
m6a.2xlarge	3.125	12.5
m6a.4xlarge	6.25	12.5
m6g.medium	0.5	10.0
m6g.large	0.75	10.0
m6g.xlarge	1.25	10.0
m6g.2xlarge	2.5	10.0
m6g.4xlarge	5.0	10.0
m6gd.medium	0.5	10.0
m6gd.large	0.75	10.0
m6gd.xlarge	1.25	10.0
m6gd.2xlarge	2.5	10.0
m6gd.4xlarge	5.0	10.0
m6i.large	0.781	12.5
m6i.xlarge	1.562	12.5
m6i.2xlarge	3.125	12.5
m6i.4xlarge	6.25	12.5
m6id.large	0.781	12.5
m6id.xlarge	1.562	12.5
m6id.2xlarge	3.125	12.5
m6id.4xlarge	6.25	12.5
m6idn.large	3.125	25.0
m6idn.xlarge	6.25	30.0
m6idn.2xlarge	12.5	40.0
m6idn.4xlarge	25.0	50.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
m6in.large	3.125	25.0
m6in.xlarge	6.25	30.0
m6in.2xlarge	12.5	40.0
m6in.4xlarge	25.0	50.0
m7g.medium	0.52	12.5
m7g.large	0.937	12.5
m7g.xlarge	1.876	12.5
m7g.2xlarge	3.75	15.0
m7g.4xlarge	7.5	15.0
t1.micro	0.07	0.28
t2.nano	0.032	0.512
t2.micro	0.064	1.024
t2.small	0.128	1.024
t2.medium	0.256	1.024
t2.large	0.512	1.024
t2.xlarge	0.75	1.024
t2.2xlarge	1.0	1.024
t3.nano	0.032	5.0
t3.micro	0.064	5.0
t3.small	0.128	5.0
t3.medium	0.256	5.0
t3.large	0.512	5.0
t3.xlarge	1.024	5.0
t3.2xlarge	2.048	5.0
t3a.nano	0.032	5.0
t3a.micro	0.064	5.0
t3a.small	0.128	5.0
t3a.medium	0.256	5.0
t3a.large	0.512	5.0
t3a.xlarge	1.024	5.0
t3a.2xlarge	2.048	5.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
t4g.nano	0.032	5.0
t4g.micro	0.064	5.0
t4g.small	0.128	5.0
t4g.medium	0.256	5.0
t4g.large	0.512	5.0
t4g.xlarge	1.024	5.0
t4g.2xlarge	2.048	5.0

Amazon EBS I/O 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 Amazon EBS 卷提供最佳性能。

有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

基于 SSD 的实例存储卷的 I/O 性能

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您最高可以获得下表所列的 IOPS（4096 字节的数据块大小）性能（在队列深度饱和时）。否则，您将获得较低的 IOPS 性能。

实例大小	100% 随机读取 IOPS	写入 IOPS
m5ad.large	30000	15000
m5ad.xlarge	59,000	29,000
m5ad.2xlarge	117,000	57,000
m5ad.4xlarge	234,000	114,000
m5ad.8xlarge	466666	233333
m5ad.12xlarge	700,000	340,000
m5ad.16xlarge	933333	466666
m5ad.24xlarge	1400000	680,000
m5d.large	30000	15000
m5d.xlarge	59,000	29,000
m5d.2xlarge	117,000	57,000
m5d.4xlarge	234,000	114,000
m5d.8xlarge	466666	233333
m5d.12xlarge	700,000	340,000
m5d.16xlarge	933333	466666

实例大小	100% 随机读取 IOPS	写入 IOPS
m5d.24xlarge	1400000	680,000
m5d.metal	1400000	680,000
m5dn.large	30000	15000
m5dn.xlarge	59,000	29,000
m5dn.2xlarge	117,000	57,000
m5dn.4xlarge	234,000	114,000
m5dn.8xlarge	466666	233333
m5dn.12xlarge	700,000	340,000
m5dn.16xlarge	933333	466666
m5dn.24xlarge	1400000	680,000
m5dn.metal	1400000	680,000
m6gd.medium	13438	5625
m6gd.large	26875	11250
m6gd.xlarge	53750	22500
m6gd.2xlarge	107500	45000
m6gd.4xlarge	215000	90000
m6gd.8xlarge	430000	180,000
m6gd.12xlarge	645000	270000
m6gd.16xlarge	860000	360,000
m6gd.metal	860000	360,000
m6id.large	33,542	16,771
m6id.xlarge	67,083	33,542
m6id.2xlarge	134,167	67,084
m6id.4xlarge	268,333	134,167
m6id.8xlarge	536,666	268,334
m6id.12xlarge	804,999	402,501
m6id.16xlarge	1,073,332	536,668
m6id.24xlarge	1,609,998	805,002
m6id.32xlarge	2,146,664	1,073,336
m6id.metal	2,146,664	1,073,336
m6idn.large	33,542	16,771

实例大小	100% 随机读取 IOPS	写入 IOPS
m6idn.xlarge	67,083	33,542
m6idn.2xlarge	134,167	67,084
m6idn.4xlarge	268,333	134,167
m6idn.8xlarge	536,666	268,334
m6idn.12xlarge	804,999	402,501
m6idn.16xlarge	1,073,332	536,668
m6idn.24xlarge	1,609,998	805,002
m6idn.32xlarge	2,146,664	1,073,336
m6idn.metal	2,146,664	1,073,336

随着您不断在您的实例的基于 SSD 的实例存储卷中填充数据，您可以达到的写入 IOPS 将不断减少。这是因为，SSD 控制器必须执行额外的工作，即查找可用空间、重写现有数据，以及擦除未使用的空间以使之可供重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为 实例提供的基于 SSD 的实例存储卷不会为超额配置预保留空白间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。

发布说明

- 实例基于 Nitro 系统 (p. 246)构建，M4、t2.large 及更大实例、t3.large 及更大实例以及 t3a.large 及更大的实例类型需要 64 位 HVM AMI。它们具有高内存，需要 64 位操作系统才能利用这一容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- 基于 Nitro 系统 (p. 246)构建的实例具有以下要求：
  - 必须安装有 NVMe 驱动程序 (p. 1518)。
  - 必须安装有 Elastic Network Adapter (ENA) (p. 1143) 驱动程序。

  以下 Linux AMI 满足这些要求：
  - Amazon Linux 2
  - Amazon Linux AMI 2018.03
  - Ubuntu 14.04 或更高版本（采用 linux-aws 内核）

    Note

    Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 linux-aws 内核）
  - Red Hat Enterprise Linux 7.4 或更高版本
  - SUSE Linux Enterprise Server 12 SP2 或更高版本

  - CentOS 7.4.1708 或更高版本
  - FreeBSD 11.1 或更高版本
  - Debian GNU/Linux 9 或更高版本
- 具有 Amazon Graviton 处理器的实例具有以下要求：
  - 使用适用于 64 位 Arm 架构的 AMI。
  - 支持通过带有 ACPI 表的 UEFI 进行引导，以及支持 ACPI 热插拔 PCI 设备。

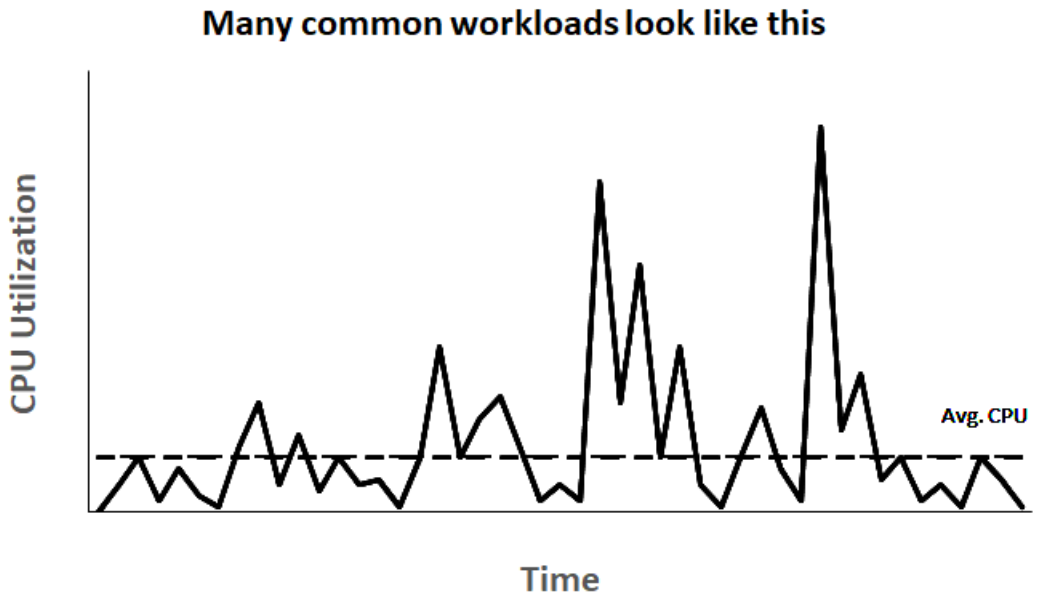
  以下 Linux AMI 满足这些要求：
  - Amazon Linux 2（64 位 Arm）
  - Ubuntu 16.04 或更高版本（64 位 Arm）
  - Red Hat Enterprise Linux 8.0 或更高版本（64 位 Arm）
  - SUSE Linux Enterprise Server 15 或更高版本（64 位 Arm）
  - Debian 10 或更高版本（64 位 Arm）
- 为了从 M6i 实例获得最佳性能，请确保它们的 ENA 驱动程序版本为 2.2.9 或更高版本。将早于 1.2 版本的 ENA 驱动程序用于这些实例会导致网络接口连接失败。以下 AMI 具备兼容的 ENA 驱动程序。
  - 内核版本为 4.14.186 的 Amazon Linux 2
  - 内核版本为 5.4.0-1025-aws 的 Ubuntu 20.04
  - 内核版本为 4.18.0-240.1.1.el8_3.ARCH 的 Red Hat Enterprise Linux 8.3
  - 内核版本为 5.3.18-24.15.1 的 SUSE Linux Enterprise Server 15 SP2
- Amazon EC2 Mac 实例支持 macOS Mojave（10.14 版）、macOS Catalina（10.15 版）和 macOS Big Sur（11 版）。
- 在 Nitro 系统上构建的实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。有关更多信息，请参阅Nitro 系统卷限制 (p. 1607)。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 在 Nitro 系统实例上构建的实例应已登录系统或安装 acpid，以支持通过 API 请求执行干净关闭。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅 Amazon EC2 常见问题解答中的我可以在 Amazon EC2 中运行多少个实例？。

可突增性能实例

许多通用型工作负载通常不繁忙，并且不需要高水平的持续 CPU 性能。下图展示了当前客户在 Amazon 云中运行的许多常见工作负载的 CPU 利用率。



这些低至中等 CPU 利用率工作负载会导致 CPU 周期浪费，因此，您需要支付的费用超过使用量。为了解决这个问题，您可以利用低成本可突增通用型实例，即 T 实例。

T 实例系列提供基准 CPU 性能，而且只要有需要，就能随时突增到基准线以上。基准 CPU 旨在满足大多数通用型工作负载的需求，包括大型微服务、Web 服务器、中小型数据库、数据记录、代码存储库、虚拟桌面、开发和测试环境以及业务关键型应用程序。T 实例平衡了计算、内存和网络资源，并为您提供最经济高效的方式来运行各种具有低至中等 CPU 利用率的通用型应用程序。与 M 实例相比，它们可以为您节省高达 15% 的成本，并且可以通过更小、更经济的实例大小节约更多成本，提供低至 2 个 vCPU 和 0.5GiB 的内存。较小的 T 实例大小（例如纳型、微型、小型和中型）非常适合需要少量内存且无需高 CPU 利用率的工作负载。

Note

本主题介绍可突增 CPU。有关可突增网络性能的信息，请参阅 Amazon EC2 实例网络带宽 (p. 1141)。

EC2 可突增实例类型

EC2 可突增实例包括 T4g、T3a 和 T3 实例类型，以及上一代 T2 实例类型。

T4g 实例类型是最新一代可突增实例。它们提供最好的性价比，并为您提供所有 EC2 实例类型中最低的成本。T4g 实例类型由基于 Arm 的 Amazon Graviton2 处理器提供动力，并且具有操作系统供应商、独立软件供应商以及流行的 Amazon 服务和应用程序广泛的生态系统支持。

下表总结了可突增实例类型之间的主要区别。

类型	描述	处理器系列
最新一代		
T4g	成本最低的 EC2 实例类型，与 T3 相比，性价比高 40%，成本低 20%	采用 Arm Neoverse N1 核心的 Amazon Graviton2 处理器
T3a	成本最低的基于 x86 的实例，与 T3 实例相比，成本低 10%	AMD 第一代 EPYC 处理器

类型	描述	处理器系列
T3	适用于 x86 工作负载的最佳峰值性价比，同等性能的价格比上一代 T2 实例低 30%	英特尔至强可扩展（Skylake、Cascade Lake 处理器）
上一代		
T2	上一代可突增实例	英特尔至强处理器

有关实例定价以及其他规格的信息，请参阅 Amazon EC2 定价和 Amazon EC2 实例类型。有关可突增网络性能的信息，请参阅 Amazon EC2 实例网络带宽 (p. 1141)。

如果您的账户不到 12 个月，您可以在特定使用限制下免费使用 `t2.micro` 实例（或者在 `t3.micro` 不可用的区域中使用 `t2.micro` 实例）。有关更多信息，请参阅 AmazonFree tier（免费套餐）。

T 实例支持的购买选项

- On-Demand Instances
- Reserved Instances
- 专用实例（仅限 T3）
- 专属主机（仅限 T3，仅处于 `standard` 模式）
- 竞价型实例

有关更多信息，请参阅实例购买选项 (p. 404)。

目录

- 最佳实践 (p. 276)
- 具爆发能力的实例的关键概念和定义 (p. 276)
- 可突增性能实例的无限模式 (p. 282)
- 可突增性能实例的标准模式 (p. 288)
- 使用可突增性能实例 (p. 297)
- 监控您的 CPU 积分以获得具爆发能力的实例 (p. 302)

最佳实践

按照这些最佳实践可以从可突增性能实例获得最大的好处。

- 确保您选择的实例大小达到您的操作系统和应用程序的最低内存要求。在许多使用案例中，带有消耗大量内存和 CPU 资源的图形用户界面的操作系统（例如，Windows）可能需要 `t3.micro` 或更大的实例。随着您的工作负载对内存和 CPU 的需求随时间增加，您可以通过 T 实例灵活地扩展到相同实例类型更大实例大小，或者选择其他实例类型。
- 为您的账户启用 Amazon Compute Optimizer 并审查针对您的工作负载的 Compute Optimizer 推荐。Compute Optimizer 可以帮助评估是应该扩大实例规模以提高性能，还是应该缩小实例规模以节省成本。Compute Optimizer 还可以根据您的场景推荐不同的实例类型。有关更多信息，请参阅《Amazon Compute Optimizer 用户指南》中的查看 EC2 实例建议。
- 有关其他要求，请参阅发布说明 (p. 273)。

具爆发能力的实例的关键概念和定义

传统 Amazon EC2 实例类型提供固定的 CPU 资源，而可突增性能实例提供基准水平的 CPU 利用率并能够将 CPU 利用率突增到基准水平之上。这样确保您只需为基准 CPU 以及任何额外的突增 CPU 使用量付费，

从而降低计算成本。基准利用率和突增能力由 CPU 积分控制。可突增性能实例是唯一将积分用于 CPU 使用的实例类型。

当每个具爆发能力的实例保持在 CPU 基准以下时，它会持续获得积分，并且在突增超过基准时持续花费积分。获得或花费的积分数量取决于实例的 CPU 利用率：

- 如果 CPU 利用率低于基准，则所获得的积分将会大于所花费的积分。
- 如果 CPU 利用率等于基准，则所获得的积分将会等于所花费的积分。
- 如果 CPU 利用率高于基准，则所花费的积分将会高于所获得的积分。

当获得的积分大于花费的积分时，差额称为“累积积分”，这些积分以后可以用于突增超过基准的 CPU 利用率。同样，当花费的积分超过获得的积分时，实例行为取决于信用配置模式 – 标准模式或无限模式。

在标准模式下，当花费的积分超过获得的积分时，实例将使用累积积分来突增到基准 CPU 利用率之上。如果没有剩余的累积积分，则实例将逐渐下降到基准 CPU 利用率，并且在累积更多积分之前不能突增到基准之上。

在无限模式下，如果实例突发超过基准 CPU 利用率，则实例首先使用累积积分进行突增。如果没有剩余的累积积分，则实例将花费剩余积分进行突增。在该实例的 CPU 使用率低于基准时，实例会使用它获得的 CPU 积分支付以前花费的超额积分。凭借获得 CPU 积分来支付超额积分的能力，Amazon EC2 可以在 24 小时周期内将实例的 CPU 使用率保持在平均水平。如果 24 小时的平均 CPU 使用率超过基准，则会按每 vCPU 小时的固定额外费率对实例收取额外的使用费用。

目录

- 关键概念和定义 (p. 277)
- 赢取 CPU 积分 (p. 279)
- CPU 积分获得率 (p. 281)
- CPU 积分累积限制 (p. 281)
- 累积的 CPU 积分生命期 (p. 281)
- 基准利用率 (p. 281)

关键概念和定义

以下关键概念和定义适用于具爆发能力的实例。

CPU 使用率

CPU 利用率是当前正在实例上使用的已分配 EC2 计算单位的百分率。此指标衡量实例上正在利用的已分配 CPU 周期的百分比。CPU 利用率 CloudWatch 指标显示每个实例的 CPU 利用率，而不是每个核心的 CPU 利用率。实例的基准 CPU 规范还基于每个实例的 CPU 利用率。要测量 CPU 利用率，请使用 Amazon Web Services Management Console 或 Amazon CLI，请参阅 获取特定实例的统计数据 (p. 1013)。

CPU 积分

vCPU 时间的单位。

示例：

1 个 CPU 积分 = 1 个 vCPU * 100% 利用率 * 1 分钟。

1 个 CPU 积分 = 1 个 vCPU * 50% 利用率 * 2 分钟

1 个 CPU 积分 = 2 个 vCPU * 25% 利用率 * 2 分钟

基准利用率

基准利用率 是当获得的 CPU 积分数与所使用的 CPU 积分数相等时，CPU 在净积分余额为零时的利用率水平。基准利用率也称为基准。基准利用率表示为 vCPU 利用率的百分比，计算方式如下：基准利用率 % =（获得的积分数/vCPU 数）/60 分钟。

有关每种具有可爆发性能实例类型的基准利用率，请参阅 积分表 (p. 279)。

获得的积分

实例在运行时连续获得的积分。

每小时获得的积分数 = % 基准利用率 * vCPU 数 * 60 分钟

例如：

具有 2 个 vCPU 且基准利用率为 5% 的 T3.nano 每小时可获得 6 积分，计算方式如下：

2 个 vCPU * 5% 基准 * 60 分钟 = 每小时 6 积分

已花费或使用的积分

实例在运行时连续使用的积分。

每分钟花费的 CPU 积分 = vCPU 数 * CPU 利用率 * 1 分钟

累积积分

当实例使用的积分少于基准利用率所需的积分时，未使用的 CPU 积分。换句话说，累积积分 = 低于基准的（获得的积分 - 已使用的积分）。

例如：

如果 t3.nano 以 2% 的 CPU 利用率运行，在一小时内低于 5% 的基准，则累积积分的计算方式如下：

累积 CPU 积分 =（每小时获得的积分 - 每小时使用的积分）= 6 - 2 个 vCPU * 2% CPU 利用率 * 60 分钟 = 6 - 2.4 = 每小时 3.6 积分

积分累积限制

取决于实例大小，但通常等于 24 小时内获得的最大积分数。

例如：

对于 t3.nano，积分累积限额 = 24 * 6 = 144 积分

启动积分

仅适用于为标准模式配置的 T2 实例。启动积分是分配给新 T2 实例的有限数量的 CPU 积分，这样在标准模式下启动时，它可以突增到基准以上。

剩余积分

实例在耗尽其累积积分余额后花费的积分。剩余积分专为可突增实例而设计，以便在较长时间内保持高性能，并且仅在无限模式下使用。剩余积分余额用于确定实例在无限模式下使用了多少积分。

标准模式

积分配置模式，允许实例通过支出积分余额中累积的积分突增到基准以上。

无限模式

积分配置模式，允许实例通过承受所需的任何时段的高 CPU 利用率来突增到基准以上。如果在滚动 24 小时或实例生命周期（以较短者为准）内实例的平均 CPU 使用率等于或低于基准，实例的每小时价格自动涵盖所有 CPU 使用峰值。如果实例长时间以较高的 CPU 使用率运行，可能会按每 vCPU 小时的固定费率收取额外的费用。

下表总结了可突增实例类型之间的主要积分区别。

类型	支持的 CPU 积分类型	积分配置模式	实例启动和停止之间的累积的 CPU 积分生命周期
最新一代			
T4g	获得的积分、累积积分、已使用的积分、剩余积分（仅无限模式）	标准、无限（默认值）	7 天（积分在实例停止后持续 7 天）
T3a	获得的积分、累积积分、已使用的积分、剩余积分（仅无限模式）	标准、无限（默认值）	7 天（积分在实例停止后持续 7 天）
T3	获得的积分、累积积分、已使用的积分、剩余积分（仅无限模式）	标准、无限（默认值）	7 天（积分在实例停止后持续 7 天）
上一代			
T2	获得的积分、累积积分、已使用的积分、启动积分（标准模式）、剩余积分（仅无限模式）	标准（默认值）、无限	0 天（实例停止时积分会丢失）

Note

在专属主机上启动的 T3 实例不支持无限制模式。

赢取 CPU 积分

每个可突增性能实例以设定的每小时速率（以毫秒级精度）持续获得 CPU 积分，具体取决于实例大小。用于加减积分的核算过程也以毫秒级精度进行，因此您不必担心 CPU 积分超支；CPU 的短时间突增只消耗少量 CPU 积分。

如果可突增性能实例使用的 CPU 资源少于基准利用率所需的数量（例如，处于空闲状态时），则未使用的 CPU 积分将累积到 CPU 积分余额中。如果可突增性能实例需要突增至基准利用率水平以上，它将花费累积积分。可突增性能实例累积的积分越多，在需要更高 CPU 利用率时，它突增到基准以上的时间就越长。

下表列出了可突增性能实例类型、每小时获得 CPU 积分的速率、实例可以累积获得的最大 CPU 积分数、每个实例的 vCPU 数以及以完整核心百分比形式表示的基准利用率（使用单个 vCPU）。

实例类型	每小时获得的 CPU 积分	可累积获得的最大积分数*	vCPU***	每个 vCPU 的基准利用率
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**

实例类型	每小时获得的 CPU 积分	可累积获得的最大积分数*	vCPU***	每个 vCPU 的基准利用率
t2.xlarge	54	1296	4	22.5%**
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.2xlarge	192	4608	8	40%**

* 可累积的积分数等于可在 24 小时周期内获得的积分数。

** 表中的基准利用率百分比按每个 vCPU 计算。在 CloudWatch 中，CPU 使用率按各个 vCPU 显示。例如，以基准水平运行的 t3.large 实例的 CPU 利用率在 CloudWatch CPU 指标中显示为 30%。有关如何计算基准利用率的信息，请参阅基准利用率 (p. 281)。

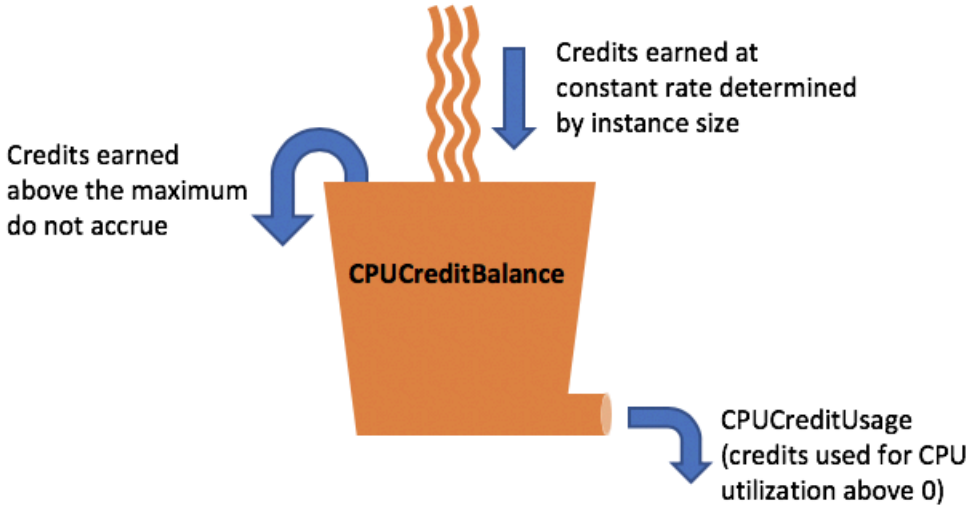
*** 每个 vCPU 都是英特尔至强核心或 AMD EPYC 核心的线程，但 T2 和 T4g 实例除外。

CPU 积分获得率

每小时获得的 CPU 积分数是由实例大小决定的。例如，`t3.nano` 每小时获得 6 积分，而 `t3.small` 每小时获得 24 积分。上表列出了所有实例的积分获得率。

CPU 积分累积限制

虽然获得的积分在运行的实例上从不过期，但实例可累积获得的积分数存在限制。该限制由 CPU 积分余额限制决定。在到达限制后，获得的任何新积分都会被丢弃，如下图所示。存储桶已满表示达到 CPU 积分余额限制，而溢出指示超出限制的新获得积分。



对于每种 实例大小，CPU 积分余额限制是不同的。例如，`t3.micro` 实例可在 CPU 积分余额中累积最多 288 个获得的 CPU 积分。上表列出了每个 实例可以累积获得的最大积分数。

T2 标准实例也获得启动积分。启动积分不计入 CPU 积分余额限制。如果 T2 实例尚未使用其启动积分，并保持闲置状态 24 小时，同时累积获得的积分，则其 CPU 积分余额将超过限制。有关更多信息，请参阅启动积分 (p. 289)。

T4g、T3a 和 T3 实例不会获得启动积分。默认情况下，这些实例以 `unlimited` 模式启动，因此可以在启动时立即突增，无需任何启动积分。预设情况下 T3 实例在专属主机启动时启动为 `standard`；de>`unlimited` 模式不支持专属主机上的 T3 实例。

累积的 CPU 积分生命期

运行的实例上的 CPU 积分不会过期。

对于 T2，CPU 积分余额在实例停止与启动之间不保留。如果您停止 T2 实例，实例将失去其所有累积积分。

对于 T4g、T3a 和 T3，CPU 积分余额将在实例停止后保留七天，然后丢失。如果在七天内启动实例，则不会丢失积分。

有关更多信息，请参阅 CloudWatch 指标表 (p. 303)中的 `CPUCreditBalance`。

基准利用率

基准利用率 是当获得的 CPU 积分数与所使用的 CPU 积分数相等时，CPU 在净积分余额为零时的利用率水平。基准利用率也称为基准。

基准利用率表示为 vCPU 利用率的百分比，计算方法如下：

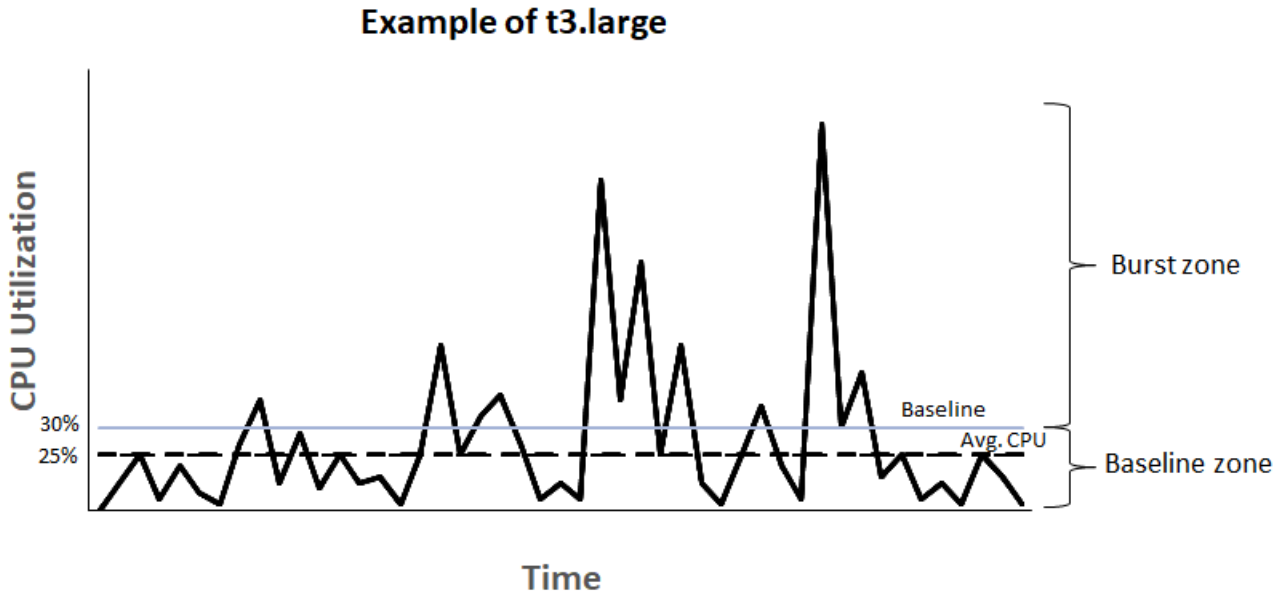
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline utilization
```

例如，一个 t3.nano 实例具有 2 个 vCPU，每小时获得 6 积分，得到的基准利用率为 5%，计算方法如下：

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

一个 t3.xlarge 实例具有 4 个 vCPU，每小时获得 96 积分，得到的基准利用率为 40% ((96/4)/60)。

下图提供了平均 CPU 利用率低于基准的 t3.large 示例。



可突增性能实例的无限模式

配置为 unlimited 的可突增性能实例可以承受所需的任何时段的高 CPU 利用率。如果在滚动 24 小时或实例生命周期（以较短者为准）内实例的平均 CPU 使用率等于或低于基准，实例的每小时价格自动涵盖所有 CPU 使用峰值。

对于绝大多数通用型工作负载，配置为 unlimited 的实例可提供足够高的性能，而不会收取任何额外的费用。如果实例长时间以较高的 CPU 利用率运行，可能会按每 vCPU 小时的固定费率收取额外的费用。有关定价的信息，请参阅 Amazon EC2 定价和 T2/T3 无限模式定价。

如果您使用的 t2.micro 或 t3.micro 实例享受 AmazonFree Tier（免费套餐）优惠并在 unlimited 模式下使用，则在连续 24 小时内的平均利用率超过实例的 基准利用率 (p. 281) 时，您可能需要支付相应费用。

T4g、T3a 和 T3 实例默认情况下作为 unlimited 启动（除非您更改默认值 (p. 301)）。如果滚动 24 小时内的平均 CPU 使用率超过基准，将会产生超额积分费用。如果您以 unlimited 模式启动 Spot 实例 并计划立即短时间使用它们（没有空闲时间来累积 CPU 积分），则会产生超额积分费用。建议您以标准 (p. 288)模式启动 Spot 实例，以避免支付更高的费用。有关更多信息，请参阅 超额积分会产生费用 (p. 285) 和 具爆发能力的实例 (p. 504)：

> **Note**
>
> 预设情况下 T3 实例在专属主机启动时启动为 standard；unlimited 模式不支持专属主机上的 T3 实例。

目录

- 无限模式概念 (p. 283)
  - 无限可突增性能实例的工作原理 (p. 283)
  - 何时使用无限模式与固定 CPU (p. 283)
  - 超额积分会产生费用 (p. 285)
  - T2 无限实例没有启动积分 (p. 285)
  - 启用无限模式 (p. 286)
  - 在无限模式和标准模式之间切换时，积分会出现什么情况 (p. 286)
  - 监控积分使用情况 (p. 286)
- 无限模式示例 (p. 286)
  - 示例 1：介绍 T3 无限版的积分使用情况 (p. 286)
  - 示例 2：介绍 T2 无限版的积分使用情况 (p. 287)

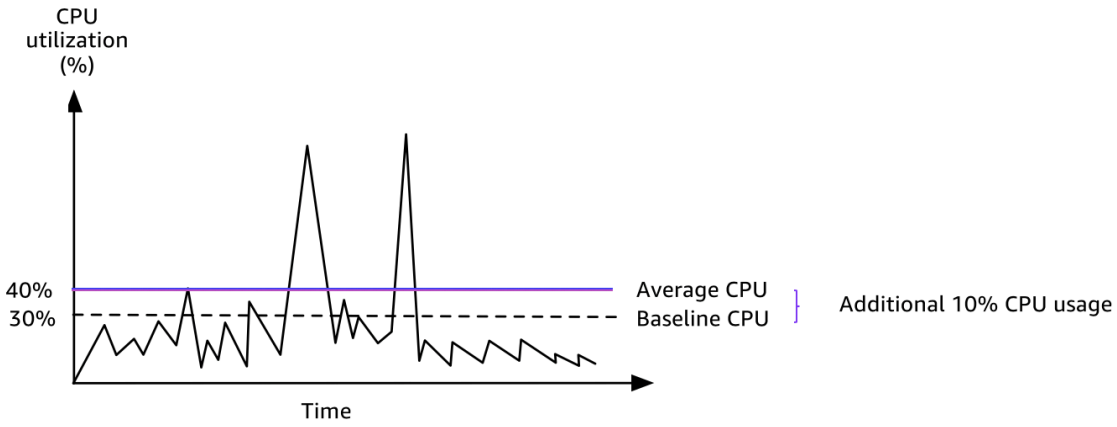
无限模式概念

unlimited 是用于可突增性能实例的积分配置选项。可以随时对正在运行或已停止的实例启用或禁用它。您可以在每个 Amazon 区域的账户级别将 unlimited 设置为每个可突增性能实例系列的默认积分选项 (p. 301)，以便账户中所有新的可突增性能实例都使用默认积分选项启动。

无限可突增性能实例的工作原理

如果配置为 unlimited 的可突增性能实例用完其 CPU 积分余额，它可能会花费超额积分以突增到基准 (p. 281)以上。在该实例的 CPU 使用率低于基准时，实例会使用它获得的 CPU 积分支付以前花费的超额积分。凭借获得 CPU 积分来支付超额积分的能力，Amazon EC2 可以在 24 小时周期内将实例的 CPU 使用率保持在平均水平。如果 24 小时的平均 CPU 使用率超过基准，则会按每 vCPU 小时的固定额外费率对实例收取额外的使用费用。

下图显示 t3.large 的 CPU 使用率。t3.large 的基准 CPU 使用率为 30%。如果实例在 24 小时内以平均 30% CPU 使用率或更低运行，则没有额外费用，因为费用已由实例每小时价格所涵盖。但是，如果实例在 24 小时内以平均 40% 的 CPU 使用率运行（如图中所示），则会按每 vCPU 小时的固定额外费率对实例收取额外的 10% CPU 使用率费用。



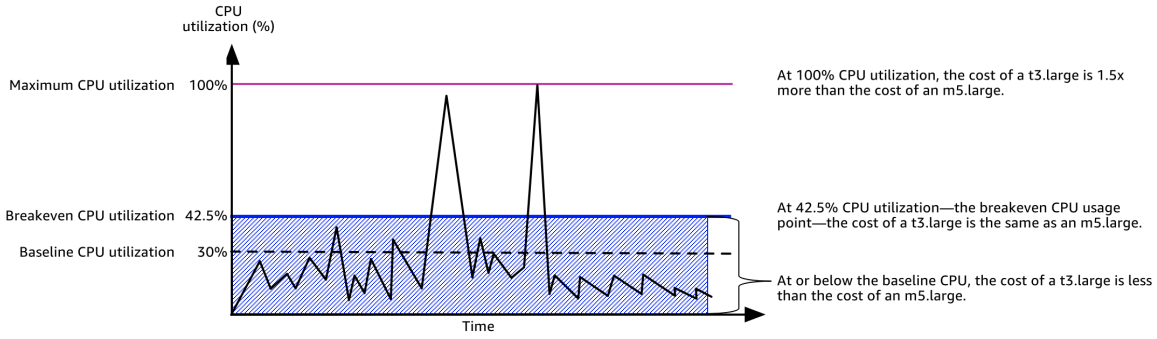
有关每个实例类型的每个 vCPU 的基准利用率以及每个实例类型可获得的积分数的更多信息，请参阅积分表 (p. 279)。

何时使用无限模式与固定 CPU

当确定您在 unlimited 模式下是应使用可突增性能实例（如 T3）还是固定性能实例（如 M5）时，您需要确定收支平衡 CPU 使用率。可突增性能实例的收支平衡 CPU 使用率是可突增性能实例与固定性能实例的费用相同的点。收支平衡 CPU 使用率可帮助您确定以下内容：

- 如果 24 小时内的平均 CPU 使用率等于或低于收支平衡 CPU 使用率，请在 unlimited 模式下使用可突增性能实例，以便您可以受益于可突增性能实例的较低价格，同时获得与固定性能实例相同的性能。
- 如果 24 小时内的平均 CPU 使用率高于收支平衡 CPU 使用率，可突增性能实例将花费比同等大小的固定性能实例更多的费用。如果 T3 实例以 100% CPU 持续突增，则您最终要支付的价格约为同等大小 M5 实例的价格的 1.5 倍。

下图显示了其中 t3.large 花费与 m5.large 花费相同的收支平衡 CPU 使用率点。t3.large 的收支平衡 CPU 使用率点为 42.5%。如果平均 CPU 使用率为 42.5%，则运行 t3.large 的费用与 m5.large 的运行费用相同，如果平均 CPU 使用率高于 42.5%，则前者费用更高。如果工作负载需要低于 42.5% 的平均 CPU 使用率，您可以受益于 t3.large 的较低价格，同时获得与 m5.large 相同的性能。



下表显示了如何计算收支平衡的 CPU 使用率阈值，以便您可以确定何时使用 unlimited 模式的可突增性能实例或固定性能实例将更为便宜。表中的列标记为 A 到 K。

实例类型	vCPU	T3 价格*/小时	M5 价格*/小时	价格差异	T3 的每个 vCPU 的基准利用率 (%)	向超额积分每 vCPU 小时收取费用	每 vCPU 分钟收费	每 vCPU 可用的额外突增分钟数	可用的额外 CPU %	收支平衡 CPU %
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	0.0835 美元	0.096 美元	0.0125 USD	30%	$0.05	0.000833 美元	15	12.5%	42.5%

* 价格基于 us-east-1 和 Linux OS。

该表提供以下信息：

- 列 A 显示实例类型 t3.large。
- 列 B 显示 t3.large 的 vCPU 数。
- 列 C 显示每小时 t3.large 的价格。
- 列 D 显示每小时 m5.large 的价格。
- 列 E 显示 t3.large 和 m5.large 之间的价格差异。
- F 列显示的是 t3.large 的每个 vCPU 的基准利用率，即 30%。在基准时，实例的每小时成本涵盖 CPU 使用率的成本。

- 列 G 显示向实例收取的每 vCPU 小时的固定额外费率（如果实例在耗尽其获得的积分后以 100% CPU 突增）。
- 列 H 显示向实例收取的每 vCPU 分钟的固定额外费率（如果实例在耗尽其获得的积分后以 100% CPU 突增）。
- 列 I 显示 `t3.large` 可每小时以 100% CPU 突增的同时支付与 `m5.large` 相同的每小时价格的额外分钟数。
- 列 J 显示该实例可突增的同时支付与 `m5.large` 相同的每小时价格的超过基准的额外 CPU 使用率（单位为 %）。
- 列 K 显示 `t3.large` 在支付不超过 `m5.large` 的费用的情况下可突增的收支平衡 CPU 使用率（单位为 %）。除此之外，`t3.large` 的费用超过 `m5.large`。

下表显示了与类似大小的 M5 实例类型相比 T3 实例类型的收支平衡 CPU 使用率（单位为 %）。

T3 实例类型	T3 的收支平衡 CPU 使用率（单位为 %）（与 M5 相比）
`t3.large`	42.5%
`t3.xlarge`	52.5%
`t3.2xlarge`	52.5%

超额积分会产生费用

如果实例的平均 CPU 使用率等于或低于基准，则实例不会产生额外的费用。由于实例在 24 小时周期内可获得最大数量的积分 (p. 279)（例如，`t3.micro` 实例可在 24 小时周期内获得最多 288 积分）的原因，因此在花费的超额积分不超过最大积分数时，不会立即向您收费。

但是，如果 CPU 利用率保持在基准以上，则实例无法获得足够的积分来支付已花费的超额积分。对于未支付的超额积分，按每 vCPU 小时的固定费率收取额外的费用。有关费率的信息，请参阅 T2/T3 无限模式定价。

在出现以下任一情况时，将对之前花费的超额积分收费：

- 花费的超额积分超出实例可在 24 小时周期内获得的最大积分数 (p. 279)。对于超出最大积分数的所花费超额积分，将在该小时结束时向您收费。
- 实例已停止或终止。
- 实例从 `unlimited` 切换为 `standard`。

花费的超额积分是通过 CloudWatch 指标 `CPUSurplusCreditBalance` 跟踪的。通过 CloudWatch 指标 `CPUSurplusCreditsCharged` 来跟踪收费的超额积分。有关更多信息，请参阅可突增性能实例的其他 CloudWatch 指标 (p. 302)。

T2 无限实例没有启动积分

T2 标准实例可收到启动积分 (p. 289)，但 T2 无限实例不会收到启动积分。T2 无限实例可以随时突增到基准以上，而不会收取额外的费用，但前提是在滚动 24 小时时间段或其生命周期（以较短者为准）内实例的平均 CPU 使用率等于或低于基准。因此，T2 无限实例不需要启动积分，即可在启动后立即达到较高的性能。

如果 T2 实例从 `standard` 切换到 `unlimited`，则将从 `CPUCreditBalance` 中扣除所有累积的启动积分，然后再结转剩余的 `CPUCreditBalance`。

T4g、T3a 和 T3 实例从来不会收到启动积分，因为它们支持无限模式。无限模式积分配置使 T4g、T3a 和 T3 实例能够根据需要使用尽可能多的 CPU，以便在需要的时间内突增超出基准。

启用无限模式

您可以随时在正在运行或停止的实例上从 unlimited 切换到 standard 以及从 standard 切换到 unlimited。有关更多信息，请参阅以无限或标准模式启动可突增性能实例 (p. 298) 和 修改可突增性能实例的积分规范 (p. 300)。

您可以在每个Amazon区域的账户级别将 unlimited 设置为每个可突增性能实例系列的默认积分选项，以便账户中所有新的可突增性能实例都使用默认积分选项启动。有关更多信息，请参阅设置账户的默认积分规范 (p. 301)。

您可以使用 Amazon EC2 控制台或 Amazon CLI，检查可突增性能实例已配置为 unlimited 还是 standard。有关更多信息，请参阅查看可突增性能实例的积分规范 (p. 300) 和 查看默认积分规范 (p. 302)。

在无限模式和标准模式之间切换时，积分会出现什么情况

CPUCreditBalance 是跟踪实例产生的积分数的 CloudWatch 指标。CPUSurplusCreditBalance 是跟踪实例所用超额积分数的 CloudWatch 指标。

当您将配置为 unlimited 的实例更改为 standard 时，会出现以下情况：

- CPUCreditBalance 值保持不变并进行结转。
- 立即针对 CPUSurplusCreditBalance 值进行收费。

在 standard 实例切换到 unlimited 时，会出现以下情况：

- 将结转包含已累积获得的积分的 CPUCreditBalance 值。
- 对于 T2 标准实例，将从 CPUCreditBalance 值中扣除所有启动积分，并且将结转包含已累积获得的积分的剩余 CPUCreditBalance 值。

监控积分使用情况

要了解您实例花费的积分是否超过基准提供的积分，您可以使用 CloudWatch 指标来跟踪使用情况，并且可以设置小时警报，以便获得积分使用情况通知。有关更多信息，请参阅监控您的 CPU 积分以获得具爆发能力的实例 (p. 302)。

无限模式示例

以下示例介绍当实例配置为 unlimited 时的积分使用情况。

示例

- 示例 1：介绍 T3 无限版的积分使用情况 (p. 286)
- 示例 2：介绍 T2 无限版的积分使用情况 (p. 287)

示例 1：介绍 T3 无限版的积分使用情况

在此示例中，您可以查看作为 t3.nano 启动的 unlimited 实例的 CPU 利用率，以及它如何花费获得 的积分和超额 积分来保持 CPU 利用率。

t3.nano 实例在 24 小时滚动周期内获得 144 个 CPU 积分，这些积分可兑换 144 分钟 vCPU 使用时间。在实例用完 CPU 积分余额（由 CloudWatch 指标 CPUCreditBalance表示）时，它会花费超额 CPU 积分—（尚未获得的 积分）—以突增所需的时间。由于 t3.nano 实例在 24 小时周期内最多可获得 144 积分，因此，在花费的超额积分不超过该最大积分数时，不会立即向您收费。如果花费 144 个以上的 CPU 积分，则会在该小时结束时对超出的部分进行收费。

下图所示的示例旨在说明实例如何使用超额积分突增到基准以上，甚至在用完 CPUCreditBalance 后。以下工作流程引用图中的编号数据点：

P1 – 在图表中的 0 小时处，实例以 unlimited 模式启动并立即开始获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%），不使用任何积分。所有未使用的积分都累积到积分余额中。对于前 24 小时，CPUCreditUsage 为 0，而 CPUCreditBalance 值达到其最大值 144。

P2 – 对于接下来的 12 小时，CPU 利用率为 2.5%，这低于 5% 基准。实例获得的积分多于花费的积分，但 CPUCreditBalance 值不能超过其最大值 144 积分。

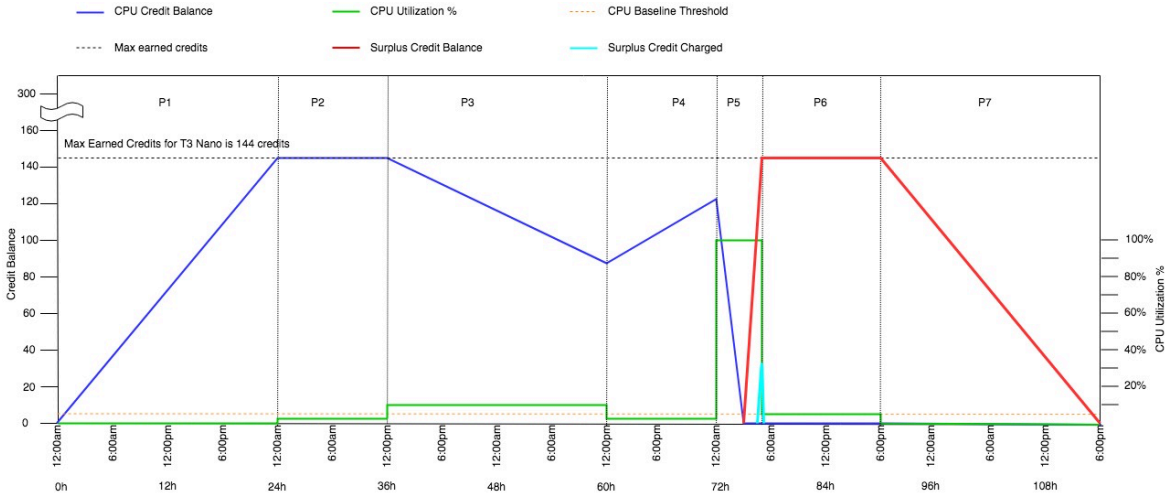
P3 – 对于接下来的 24 小时，CPU 利用率为 7%（高于基准），这要求花费 57.6 积分。实例花费的积分多于获得的积分，CPUCreditBalance 值降至 86.4 积分。

P4 – 对于接下来的 12 小时，CPU 利用率降至 2.5%（低于基准），这要求花费 36 积分。同时，实例获得 72 积分。实例获得的积分多于花费的积分，CPUCreditBalance 值增至 122 积分。

P5 – 对于接下来的 5 小时，实例突增至 100% CPU 利用率，并花费总计 570 积分来持续突增。在进入此期间的大约一小时内，此实例用完其整个 CPUCreditBalance 122 积分，并开始花费超额积分来维持高的 CPU 利用率，在此期间总共花费 448 个超额积分 (570-122=448)。当 CPUSurplusCreditBalance 值达到 144 个 CPU 积分（t3.nano 实例在 24 小时内可获得的最大值）时，之后任何花费的超额积分都无法由获得的积分抵消。之后花费的超额积分总计为 304 积分 (448-144=304)，这会导致这一小时结束后对于这 304 积分收取很小的一笔附加费。

P6 – 对于接下来的 13 小时，CPU 利用率为 5%（基准）。实例获得的积分与花费的积分一样多，而无需额外支付 CPUSurplusCreditBalance 的费用。CPUSurplusCreditBalance 值保持为 144 积分。

P7 – 对于本例中的最后 24 小时，实例空闲，CPU 利用率为 0%。在此期间，实例获得 144 积分，用于支付 CPUSurplusCreditBalance 的费用。



示例 2：介绍 T2 无限版的积分使用情况

在此示例中，您可以查看作为 t2.nano 启动的 unlimited 实例的 CPU 利用率，以及它如何花费获得 的积分和超额 积分来保持 CPU 利用率。

t2.nano 实例在 24 小时滚动周期内获得 72 个 CPU 积分，这些积分可兑换 72 分钟 vCPU 使用时间。在实例用完 CPU 积分余额（由 CloudWatch 指标 CPUCreditBalance表示）时，它会花费超额 CPU 积分—（尚未获得的 积分）—以突增所需的时间。由于 t2.nano 实例在 24 小时周期内最多可获得 72 积分，因此，在花费的超额积分不超过该最大积分数时，不会立即向您收费。如果花费 72 个以上的 CPU 积分，则会在该小时结束时对超出的部分进行收费。

下图所示的示例旨在说明实例如何使用超额积分突增到基准以上，甚至在用完 CPUCreditBalance 后。您可以假定，在图表的时间线开始时，实例累积的积分余额等于它可在 24 小时内获得的最大积分数。以下工作流程引用图中的编号数据点：

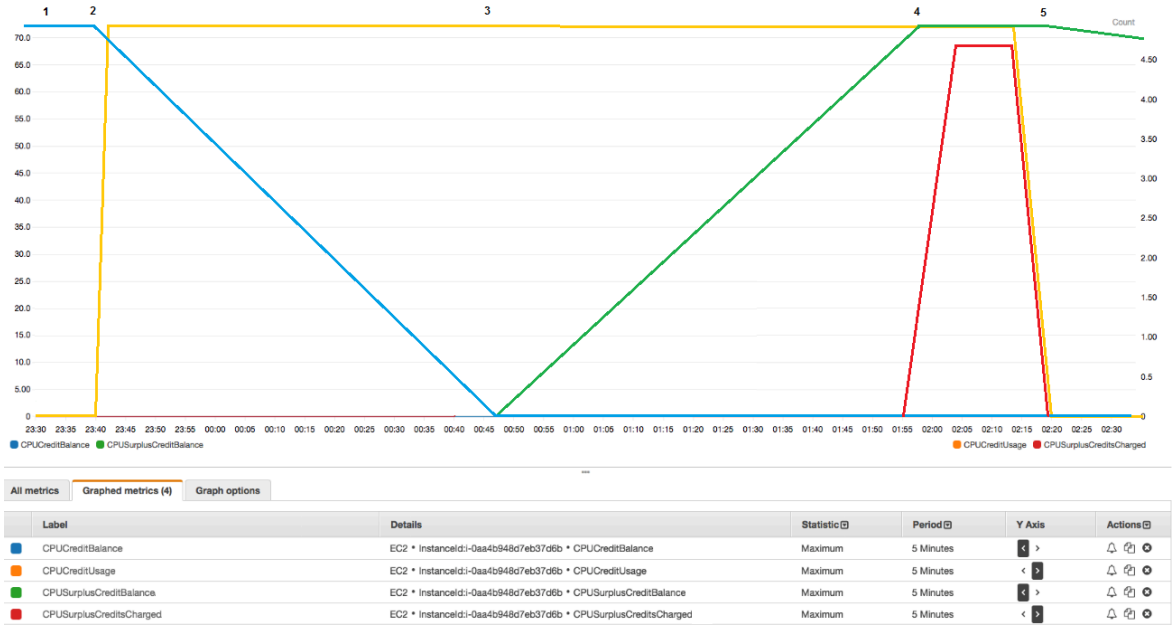
1 – 在前 10 分钟内，CPUCreditUsage 设置为 0 并且 CPUCreditBalance 值始终为最大值 72。

2 – 在 23:40，随着 CPU 使用率增加，实例花费 CPU 积分并且 CPUCreditBalance 值减少。

3 – 在大约 00:47，实例用完全部 CPUCreditBalance，并开始花费超额积分以保持较高的 CPU 利用率。

4 – 一直花费超额积分，直到 1:55，此时 CPUSurplusCreditBalance 值达到 72 个 CPU 积分。这等于 t2.nano 实例在 24 小时周期内可获得的最大积分数。以后花费的任何超额积分无法由 24 小时周期内获得的积分抵消，这会导致在该小时结束时收取少量的额外费用。

5 – 在大约 2:20，实例继续花费超额积分。此时，CPU 使用率低于基准并且实例开始获得积分，每小时 3 积分 (或每 5 分钟 0.25 积分)，它使用这些积分来支付 CPUSurplusCreditBalance。在 CPUSurplusCreditBalance 值减少到 0 后，实例开始在其 CPUCreditBalance 中累积获得积分（每 5 分钟 0.25 积分）。



计算账单

超额积分每 vCPU 小时收取 0.05 USD。在 1:55 和 2:20 之间，实例大约花费 25 个超额积分，这相当于 0.42 个 vCPU 小时。

该实例产生的额外费用为 0.42 vCPU 小时 x 0.05 美元/vCPU 小时 = 0.021 美元，舍入到 0.02 美元。

下面是该 T2 无限实例的月末账单：

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

您可以设置账单提醒以每小时通知一次产生的任何费用，并在必要时采取相应的措施。

可突增性能实例的标准模式

配置为 standard 的可突增性能实例适用于具有平均 CPU 利用率的工作负载，它始终低于实例的基准 CPU 利用率。为了突增到基准以上，实例会花费在其 CPU 积分余额中累积的积分。如果实例累积的积分较少，CPU 利用率将逐渐下降到基准水平，因此，在累积的 CPU 积分余额用完时，实例的性能不会急剧下降。有关更多信息，请参阅具爆发能力的实例的关键概念和定义 (p. 276)。

目录

- 标准模式概念 (p. 289)
  - 标准可突增性能实例的工作原理 (p. 289)
  - 启动积分 (p. 289)
  - 启动积分限制 (p. 290)
  - 启动积分和获得的积分之间的区别 (p. 290)
- 标准模式示例 (p. 291)
  - 示例 1：介绍 T3 标准版的积分使用情况 (p. 291)
  - 示例 2：介绍 T2 标准版的积分使用情况 (p. 292)
    - 第 1 个时段：1 – 24 小时 (p. 292)
    - 第 2 个时段：25 – 36 小时 (p. 293)
    - 第 3 个时段：37 – 61 小时 (p. 293)
    - 第 4 个时段：62 – 72 小时 (p. 294)
    - 第 5 个时段：73 – 75 小时 (p. 295)
    - 第 6 个时段：76 – 90 小时 (p. 295)
    - 第 7 个时段：91 – 96 小时 (p. 296)

标准模式概念

`standard` 是用于可突增性能实例的配置选项。可以随时对正在运行或已停止的实例启用或禁用它。您可以在每个 Amazon 区域的账户级别将 `standard` 设置为每个可突增性能实例系列的默认积分选项 (p. 301)，以便账户中所有新的可突增性能实例都使用默认积分选项启动。

标准可突增性能实例的工作原理

当配置为 `standard` 的可突增性能实例处于运行状态时，它会以设定的每小时速率（以毫秒级精度）持续获得积分。对于 T2 标准模式，在实例停止后，会丢失积累的全部积分，积分余额会重置为零。在它重新启动后，会接受一组新的启动积分，并开始累积获得积分。对于 T4g、T3a 和 T3 标准实例，CPU 积分余额将在实例停止后保留七天，随后丢失。如果在七天内启动实例，则不会丢失积分。

T2 标准实例会收到两种类型的 CPU 积分 (p. 277)：获得的积分以及启动积分。在 T2 标准实例处于运行状态时，它会以固定的每小时速率 (以毫秒级精度) 持续获得积分。在一开始，该实例尚未获得积分来提供良好的初始体验；因此为了提供良好的初始体验，一开始会收到启动积分，可以先花费，同时累积获得积分。

T4g、T3a 和 T3 实例不会收到启动积分，因为它们支持无限模式。无限模式积分配置使 T4g、T3a 和 T3 实例能够根据需要使用尽可能多的 CPU，以便在需要的时间内突增超出基准。

启动积分

在启动时，T2 标准实例的每个 vCPU 会获得 30 个启动积分，而 T1 标准实例会获得 15 个启动积分。例如，`t2.micro` 实例具有一个 vCPU 并获得 30 个启动积分，而 `t2.xlarge` 实例具有 4 个 vCPU 并获得 120 个启动积分。启动积分旨在提供良好的初始体验，以使实例能够在启动后 (没有累积获得积分之前) 立即突增到更高的性能。

首先花费启动积分，再使用获得的积分。未花费的启动积分将累积到 CPU 积分余额中，但不会计入 CPU 积分余额限制。例如，`t2.micro` 实例的 CPU 积分余额限制为 144 个获得的积分。如果实例启动并保持空闲状态 24 小时，其 CPU 积分余额将达到 174 (30 个启动积分 + 144 个获得的积分)，这已超过限制。不过，在实例花费 30 个启动积分后，积分余额就不能超过 144 个。有关每种实例大小的 CPU 积分余额限制的更多信息，请参阅积分表 (p. 279)。

下表列出了在启动时分配的初始 CPU 积分以及 vCPU 数。

实例类型	启动积分	vCPU
`t1.micro`	15	1

实例类型	启动积分	vCPU
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

启动积分限制

T2 标准实例接收启动积分的次数存在限制。在每个区域，每 24 个小时的滚动周期内，每个账户中所有 T2 标准实例组合的默认限制是 100 次启动。例如，当一个实例在 24 小时周期内停止并启动 100 次时，或当 100 个实例在 24 小时周期内启动时，或者其他组合等同于 100 次启动时，将达到此限制。新账户可能具有较低的限制，该限制随着时间根据您的使用情况而增加。

> **Tip**
>
> 要确保您的工作负载始终获得所需的性能，请切换到可突增性能实例的无限模式 (p. 282)或考虑使用更大的实例。

启动积分和获得的积分之间的区别

下表列出了启动积分和获得的积分之间的区别。

	启动积分	获得的积分
积分获得率	在启动时，T2 标准实例的每个 vCPU 获得 30 个启动积分。 如果 T2 实例从 unlimited 切换到 standard，则在切换时不会获得启动积分。	每个 T2 实例以固定的每小时速率 (以毫秒级精度) 持续获得 CPU 积分，具体取决于实例大小。有关每种实例大小获得的 CPU 积分数量的更多信息，请参阅积分表 (p. 279)。
积分获得限制	对于每个区域，在每 24 个小时的滚动周期内，每个账户中所有 T2 标准实例组合的启动积分接收限制是 100 次启动。新账户可能具有较低的限制，该限制随着时间根据您的使用情况而增加。	T2 实例累积的积分数不能超过 CPU 积分余额限制。如果 CPU 积分余额已达到其限制，则将丢弃在达到限制后获得的任何积分。启动积分不计入限制。有关每种 T2 实例大小的 CPU 积分余额限制的更多信息，请参阅积分表 (p. 279)。
积分使用	首先花费启动积分，再使用获得的积分。	只有花完所有启动积分后才能花费获得的积分。
过期积分	在 T2 标准实例运行过程中，启动积分不会过期。当 T2 标准实例停止或切换至“T2 无限”时，所有启动积分都将丢失。	在 T2 实例运行过程中，已累积获得的积分不会过期。T2 实例停止后，将丢失所有已累积获得的积分。

CloudWatch 指标 CPUCreditBalance 可跟踪已累积的启动积分和已累积获得的积分数。有关更多信息，请参阅 CloudWatch 指标表 (p. 303)中的 CPUCreditBalance。

标准模式示例

以下示例介绍当实例配置为 standard 时的积分使用情况。

示例

- 示例 1：介绍 T3 标准版的积分使用情况 (p. 291)
- 示例 2：介绍 T2 标准版的积分使用情况 (p. 292)

示例 1：介绍 T3 标准版的积分使用情况

在本示例中，您将了解作为 t3.nano 启动的 standard 实例如何获得、累积和使用获得 的积分。您可以看到积分余额如何反映累积的获得 的积分。

运行的 t3.nano 实例每 24 小时获得 144 积分。其积分余额限制为 144 个获得的积分。达到该限制后，将丢弃获得的任何新积分。有关可获得和可累积的积分数的更多信息，请参阅积分表 (p. 279)。

您可启动 T3 标准实例并立即使用它。或者，您可能在启动 T3 标准实例后让其闲置几天，再在该实例上运行应用程序。实例是正在被使用还是闲置决定积分是消耗还是累积。如果实例从启动时开始保持闲置状态 24 小时，则积分余额将达到其限制，这是可以累积的获得积分的最大数目。

本示例介绍启动后闲置 24 小时的实例，并向您分析 96 小时内共 7 个时段的积分情况，演示获得、累积、使用和丢弃积分的速率以及每个时段结束时的积分余额值。

以下工作流程引用图中的编号数据点：

P1 – 在图表中的 0 小时处，实例以 standard 模式启动并立即开始获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%），不使用任何积分。所有未使用的积分都累积到积分余额中。对于前 24 小时，CPUCreditUsage 为 0，而 CPUCreditBalance 值达到其最大值 144。

P2 – 对于接下来的 12 小时，CPU 利用率为 2.5%，这低于 5% 基准。实例获得的积分多于花费的积分，但 CPUCreditBalance 值不能超过其最大值 144 积分。所获得的超过限制的所有积分都会被丢弃。

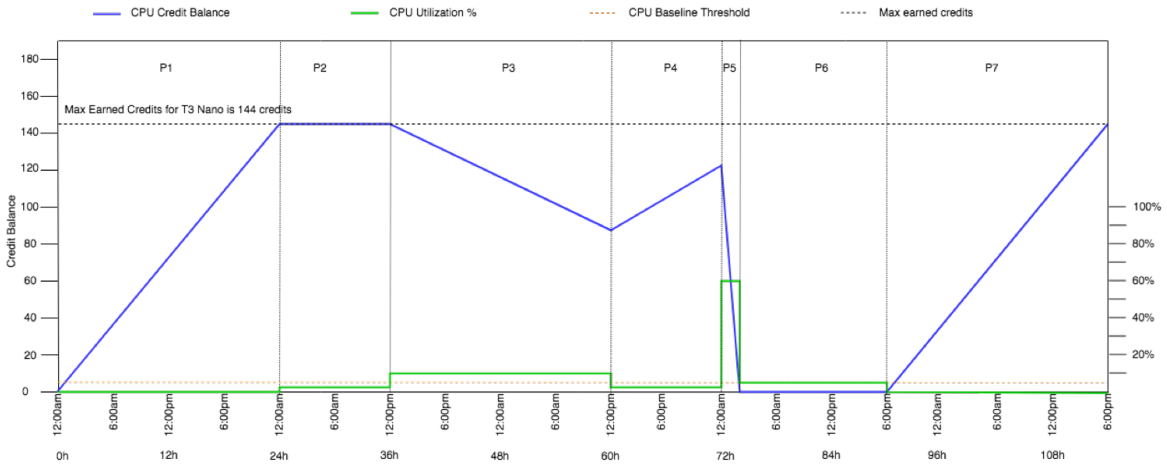
P3 – 对于接下来的 24 小时，CPU 利用率为 7%（高于基准），这要求花费 57.6 积分。实例花费的积分多于获得的积分，CPUCreditBalance 值降至 86.4 积分。

P4 – 对于接下来的 12 小时，CPU 利用率降至 2.5%（低于基准），这要求花费 36 积分。同时，实例获得 72 积分。实例获得的积分多于花费的积分，CPUCreditBalance 值增至 122 积分。

P5 – 对于接下来的两个小时，实例突增至 60% CPU 利用率，并耗尽其整个 CPUCreditBalance 值的 122 积分。在此期间结束时，CPUCreditBalance 为零，CPU 利用率会被强制降低到基准利用率级别 5%。在基准时，实例获得的积分与花费的积分一样多。

P6 – 对于接下来的 14 小时，CPU 利用率为 5%（基准）。实例获得的积分与花费的积分一样多。CPUCreditBalance 值保持为 0。

P7 – 对于本例中的最后 24 小时，实例空闲，CPU 利用率为 0%。在此期间，实例获得 144 积分，这些积分将累积到其 CPUCreditBalance 中。



示例 2：介绍 T2 标准版的积分使用情况

在本示例中，您将了解作为 t2.nano 启动的 standard 实例如何获得、累积和使用启动积分和获得的积分。您还可以了解积分余额如何反映累积获得的积分和累积启动积分。

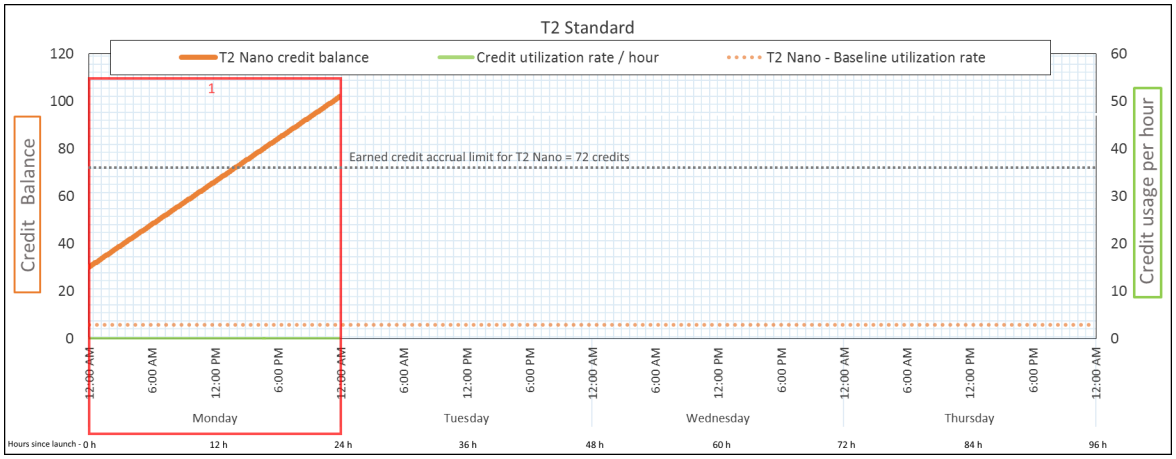
启动时，t2.nano 实例获得 30 启动积分，之后每 24 小时获得 72 积分。其积分余额限制是获得的 72 积分；启动积分不计入该限制。达到该限制后，将丢弃获得的任何新积分。有关可获得和可累积的积分数的更多信息，请参阅积分表 (p. 279)。有关 限制的更多信息，请参阅 启动积分限制 (p. 290)。

您可启动 T2 标准实例并立即使用它。或者，您可能在启动 T2 标准实例后让其闲置几天，再在该实例上运行应用程序。实例是正在被使用还是闲置决定积分是消耗还是累积。如果实例自启动后闲置 24 小时，积分余额将超过其限制，因为积分余额同时反映累积获得的积分和累积启动积分。不过，使用 CPU 后，会先使用启动积分。此后，积分余额限制始终反映可累积获得的最大积分。

本示例介绍启动后闲置 24 小时的实例，并向您分析 96 小时内共 7 个时段的积分情况，演示获得、累积、使用和丢弃积分的速率以及每个时段结束时的积分余额值。

第 1 个时段：1 – 24 小时

在图上的第 0 小时，T2 实例作为 standard 启动并立即获得 30 启动积分。当它处于运行状态时，会获得积分。实例自启动后保持闲置状态（CPU 利用率为 0%），不使用任何积分。所有未使用的积分都累积到积分余额中。在启动后大约 14 小时，积分余额为 72 (30 启动积分 + 获得的 42 积分)，这与实例在 24 小时内获得的积分相同。在启动后 24 小时，积分余额超过 72，因为未使用的启动积分累积到了积分余额中 (积分余额为 —102 积分：30 启动积分 + 72 获得积分)。



积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 0 积分
积分余额	102 积分 (30 启动积分 + 获得的 72 积分)

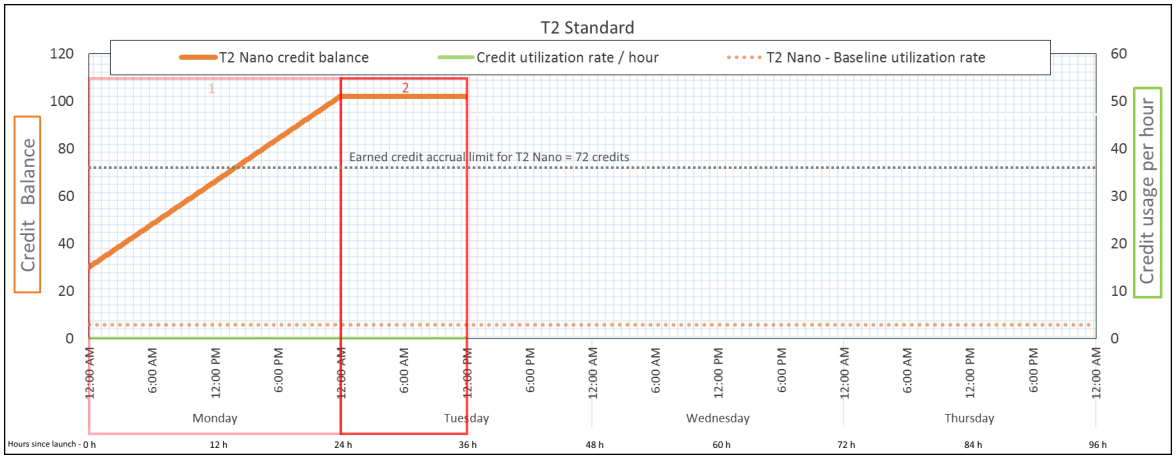
结论

如果启动后没有 CPU 利用率，实例累积的积分将超过其在 24 小时内获得的积分 (30 启动积分 + 获得的 72 积分 = 102 积分)。

在真实场景中，EC2 实例在启动和运行时会使用少量积分，以防止积分余额达到本实例中的最大理论值。

第 2 个时段：25 – 36 小时

在接下来 12 小时，实例继续保持闲置状态并获得积分，但积分余额不会增加。积分余额保持在 102 (30 启动积分 + 获得的 72 积分)。积分余额已达到 72 累积获得的积分限制，因此会丢弃新获得的积分。



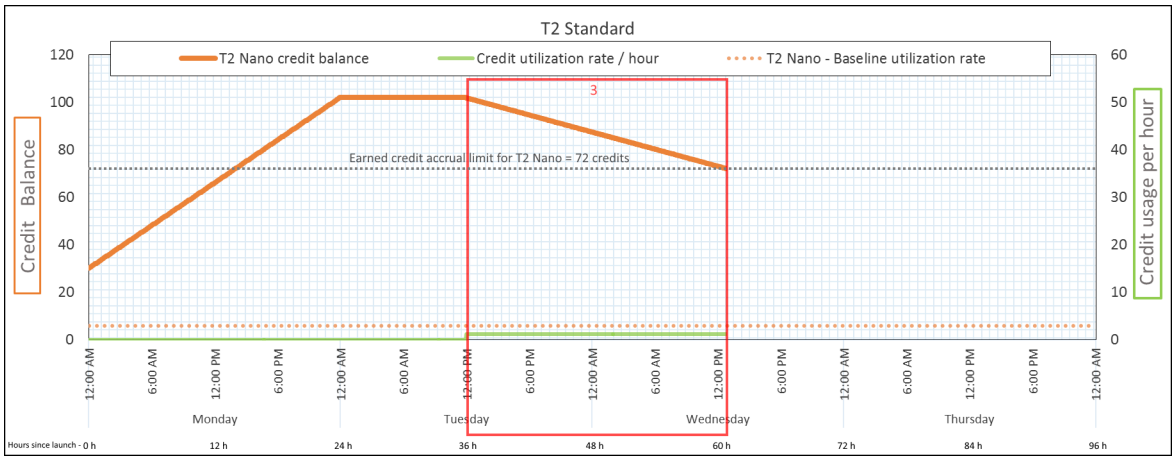
积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分 (每小时 3 积分)
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	102 积分 (30 启动积分 + 72 获得积分) — 余额保持不变

结论

如果积分余额已达到其限制，实例会继续获得积分，但不会累积更多获得的积分。达到该限制后，会丢弃新获得的积分。启动积分不计入 积分余额限制。如果余额包含累积的启动积分，余额将超过该限制。

第 3 个时段：37 – 61 小时

在接下来 25 小时，实例使用 2% CPU，需要 30 积分。在同一周期，它获得 75 积分，但积分余额减少。余额减少的原因是先使用累积的启动 积分，并且由于积分余额已达到其获得的 72 积分限制，因此丢弃了新获得的积分。



积分使用率	24 小时 28.8 积分 (每小时 1.2 积分，2% CPU 利用率，40% 积分获得率) — 25 小时 30 积分
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	72 积分 (使用了 30 启动积分；剩余获得的 72 积分未使用)

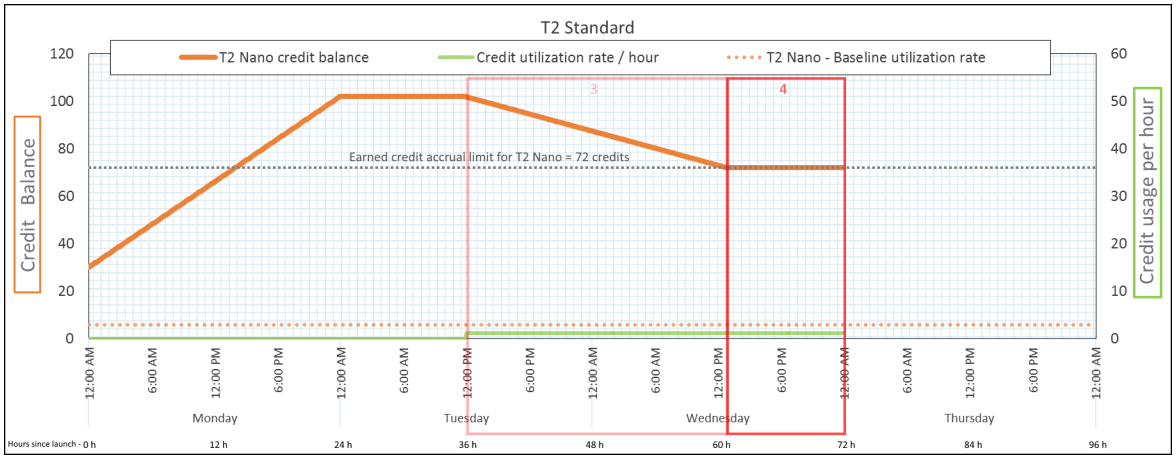
结论

实例先使用启动积分，再使用获得的积分。启动积分不计入积分限制。使用启动积分后，积分余额永远不会超过在 24 小时内可获得的积分。此外，实例运行时，不会获得更多启动积分。

第 4 个时段：62 – 72 小时

在接下来 11 小时，实例使用 2% CPU，需要 13.2 积分。这与上一周期的 CPU 利用率相同，但积分余额不会减少。它保持在 72 积分。

积分余额不减少的原因是积分获得率高于积分使用率。实例使用 13.2 积分的同时，获得 33 积分。不过，由于余额限制是 72 积分，因此会丢弃获得的超过该限制的任何积分。积分余额保持在 72 积分，这与第 2 个时段保持在 102 积分不同，因为没有累积的启动积分。



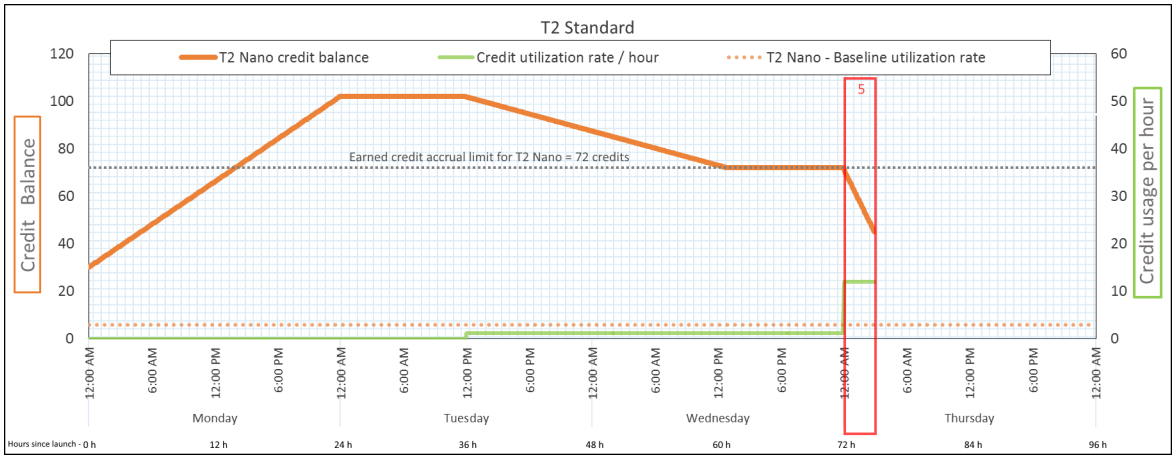
积分使用率	24 小时 28.8 积分 (每小时 1.2 积分，2% CPU 利用率，40% 积分获得率) — 11 小时 13.2 积分
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 43.2 积分 (60% 积分获得率)
积分余额	72 积分 (0 启动积分，获得的 72 积分) — 余额达到其限制

结论

使用启动积分后，积分余额限制由实例在 24 小时内可获得的积分数决定。如果实例获得的积分多于使用的积分，则会丢弃新获得的超过限制的积分。

第 5 个时段：73 – 75 小时

在接下来 3 小时，实例的 CPU 利用率激增至 20%，需要 36 积分。在相同的 3 小时内，实例获得 9 积分，导致净余额减少 27 积分。在这 3 小时结束时，积分余额为累积获得的 45 积分。



积分使用率	24 小时 288 积分 (每小时 12 积分，20% CPU 利用率，400% 积分获得率) — 3 小时 36 积分
积分获得率	每 24 小时 72 积分 (3 小时 9 积分)
积分丢弃率	每 24 小时 0 积分
积分余额	45 积分 (以前的余额 (72) - 使用的积分 (36) + 获得的积分 (9)) — 余额按每 24 小时 216 积分的速率减少 (使用率 288/24 + 获得率 72/24 = 余额减少率 216/24)

结论

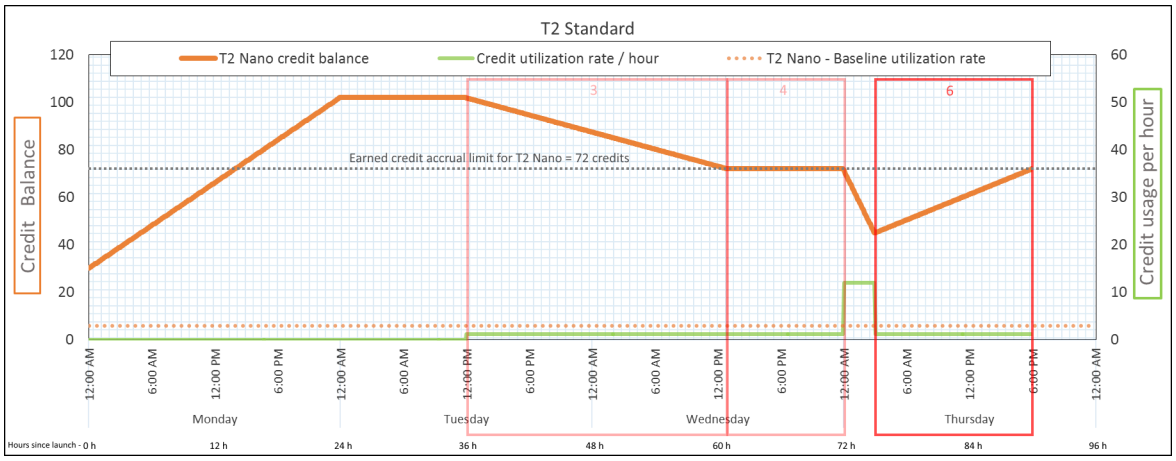
如果实例使用的积分多于获得的积分，则其积分余额将减少。

第 6 个时段：76 – 90 小时

在接下来 15 小时，实例使用 2% CPU，需要 18 积分。这与第 3 个和第 4 个时段的 CPU 利用率相同。不过，此周期的积分余额增加，而第 3 个时段的积分余额减少，第 4 个时段的保持不变。

在第 3 个时段，使用累积的启动积分，并会丢弃获得的超过积分限制的任何积分，导致积分余额减少。在第 4 个时段，实例发挥的积分数少于其获得的积分数。所获得的任何超出限制的积分将丢弃，因此余额保持在其最大值 72 积分。

在本周期，没有累积的启动积分，余额中累积获得的积分数低于限制。不会丢弃获得的任何积分。此外，实例获得的积分多于使用的积分，导致积分余额增加。



积分使用率	24 小时 28.8 积分 (每小时 1.2 积分，2% CPU 利用率，40% 积分获得率) — 15 小时 18 积分
积分获得率	每 24 小时 72 积分 (15 小时 45 积分)
积分丢弃率	每 24 小时 0 积分
积分余额	72 积分 (余额按每 24 小时 43.2 积分的速率增加 — 更改率 = 使用率 28.8/24 + 获得率 72/24)

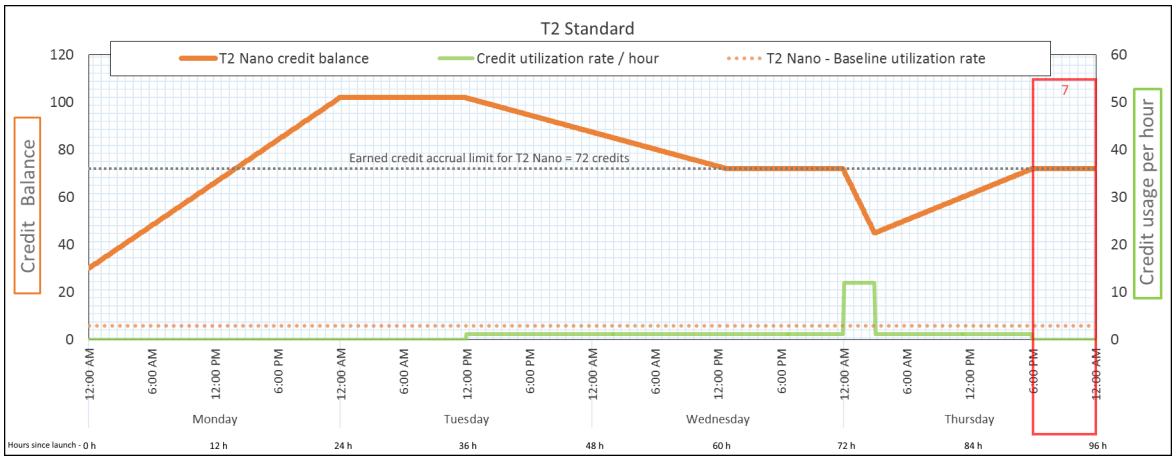
结论

如果实例使用的积分少于获得的积分，则其积分余额将增加。

第 7 个时段：91 – 96 小时

在接下来六小时，实例保持闲置状态— (CPU 利用率为 0%) ，—不使用任何积分。这与第 2 个时段的 CPU 利用率相同，但积分余额不保持在 102 积分，而保持在 72 积分，—这是实例的积分余额限制。

在第 2 个时段，积分余额中包含累积的 30 启动积分。启动积分在第 3 个时段使用。正在运行的实例无法获得更多启动积分。达到积分余额限制后，会丢弃获得的超过限制的任何积分。



积分使用率	每 24 小时 0 积分 (0% CPU 利用率)
积分获得率	每 24 小时 72 积分
积分丢弃率	每 24 小时 72 积分 (100% 积分获得率)
积分余额	72 积分 (0 启动积分，获得的 72 积分)

结论

如果已达到积分余额限制，实例会继续获得积分，但不会累积更多获得的积分。达到该限制后，会丢弃新获得的积分。积分余额限制由实例在 24 小时内可获得的积分数决定。有关积分余额限制的更多信息，请参阅积分表 (p. 279)。

使用可突增性能实例

用于启动、监控和修改这些实例的步骤是类似的。主要差别在于它们启动时的默认积分规范。

每个可突增性能实例系列都具有以下默认积分规范：

- T4g、T3a 和 T3 实例以 `unlimited` 模式启动
- 专属主机上的 T3 实例仅可以作为 `standard` 启动
- T2 实例以 `standard` 模式启动

您可以更改账户的默认积分规范 (p. 301)。

目录

- 以无限或标准模式启动可突增性能实例 (p. 298)
- 使用 Auto Scaling 组以“无限”模式启动可突增性能实例 (p. 298)
- 查看可突增性能实例的积分规范 (p. 300)
- 修改可突增性能实例的积分规范 (p. 300)
- 设置账户的默认积分规范 (p. 301)
- 查看默认积分规范 (p. 302)

以无限或标准模式启动可突增性能实例

您可以使用 Amazon EC2 控制台、Amazon开发工具包、命令行工具或者 Auto Scaling 组，以 `unlimited` 或 `standard` 模式启动实例。有关更多信息，请参阅使用 Auto Scaling 组以“无限”模式启动可突增性能实例 (p. 298)。

要求

- 您必须将 Amazon EBS 卷作为根设备以启动实例。有关更多信息，请参阅Amazon EC2 实例根设备卷 (p. 1608)。
- 有关这些实例的 AMI 和驱动程序要求的更多信息，请参阅发布说明 (p. 273)。

Console

以无限或标准模式启动可突增性能实例

1. 按照程序启动实例 (p. 576)。
2. 在 Instance type（实例类型）下，选择一个 T 实例类型。
3. 展开 Advanced details（高级详细信息），找到 Credit specification（积分规范），然后选择一积分规范。如果不进行选择，则使用默认选项，即为 T2 默认选择 `standard`，为 T4g、、T3a 和 T3 默认选择 `unlimited`。
4. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

Amazon CLI

以无限或标准模式启动可突增性能实例

使用 run-instances 命令启动您的实例。使用 `--credit-specification CpuCredits=` 参数指定积分规范。有效的积分规范为 `unlimited` 和 `standard`。

- 对于 T4g、T3a 和 T3，如果不包含 `--credit-specification` 参数，实例将默认以 `unlimited` 模式启动。
- 对于 T2，如果不包含 `--credit-specification` 参数，实例默认作为 `standard` 启动。

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

使用 Auto Scaling 组以“无限”模式启动可突增性能实例

在启动可突增性能实例时，它们需要具有 CPU 积分才能获得良好的引导体验。如果您使用 Auto Scaling 组启动实例，建议您将实例配置为 `unlimited`。如果这样做，实例会在自动启动或者由 Auto Scaling 组重新启动时使用超额积分。使用超额积分可以防止受到性能限制。

创建启动模板

在 Auto Scaling 组中以 `unlimited` 模式启动实例时，您必须使用启动模板。启动配置不支持以 `unlimited` 模式启动实例。

Note

`unlimited` 模式不支持在专属主机上启动的 T3 实例。

Console

创建以无限模式启动实例的启动模板

1. 按照为 Auto Scaling 组创建启动模板的过程操作。
2. 在启动模板内容中，对于实例类型，请选择实例大小。
3. 要在 Auto Scaling 组中以 unlimited 模式启动实例，请在高级详细信息下，对于积分规范选择无限。
4. 在您完成后，定义启动模板参数，选择创建启动模板。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的为 Auto Scaling 组创建启动模板。

Amazon CLI

创建以无限模式启动实例的启动模板

使用 create-launch-template 命令并将 unlimited 指定为积分规范。

- 对于 T4g、T3a 和 T3，如果不包含 CreditSpecification={CpuCredits=unlimited} 值，实例将默认以 unlimited 模式启动。
- 对于 T2，如果不包含 CreditSpecification={CpuCredits=unlimited} 值，实例默认作为 standard 启动。

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
    --version-description FirstVersion \
    --launch-template-data
 ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

关联 Auto Scaling 组与启动模板

要将启动模板与一个 Auto Scaling 组相关联，请使用启动模板创建 Auto Scaling 组，或者将启动模板添加到现有 Auto Scaling 组中。

Console

使用启动模板创建自动扩缩组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，选择在创建启动模板时使用的同一区域。
3. 在导航窗格中，依次选择 Auto Scaling 组和创建 Auto Scaling 组。
4. 选择启动模板，选择您的启动模板，然后选择下一步。
5. 填写 Auto Scaling 组的各个字段。当您在审核页面上完成审核配置设置时，选择创建 Auto Scaling 组。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的使用启动模板创建 Auto Scaling 组 。

Amazon CLI

使用启动模板创建自动扩缩组

使用 create-auto-scaling-group Amazon CLI 命令并指定 --launch-template 参数。

Console

添加启动模板到现有自动扩缩组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，选择在创建启动模板时使用的同一区域。
3. 在导航窗格中，选择 Auto Scaling Groups。
4. 从 Auto Scaling 组列表中选择一个 Auto Scaling 组，然后依次选择操作和编辑。
5. 在详细信息选项卡上，对于启动模板，选择一个启动模板，然后选择保存。

Amazon CLI

添加启动模板到现有自动扩缩组

使用 update-auto-scaling-group Amazon CLI 命令并指定 `--launch-template` 参数。

查看可突增性能实例的积分规范

您可以查看正在运行或停止的实例的积分规范（`unlimited` 或 `standard`）。

Console

查看可突增实例的积分规范

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择实例。
4. 选择详细信息并查看积分规范字段。该值为 `unlimited` 或 `standard`。

Amazon CLI

描述可突增性能实例的积分规范

使用 describe-instance-credit-specifications 命令。如果您指定一个或多个实例 ID，则将返回具有积分规范 `unlimited` 的所有实例，以及以前使用 `unlimited` 积分规范配置的实例。例如，如果您将 T3 实例大小调整为 M4 实例，而该实例配置为 `unlimited`，Amazon EC2 将返回 M4 实例。

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

下面是示例输出。

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

修改可突增性能实例的积分规范

您可以随时将正在运行或停止的实例的积分规范在 `unlimited` 与 `standard` 之间切换。

请注意，在 unlimited 模式中，实例可能会花费超额积分，从而产生额外费用。有关更多信息，请参阅超额积分会产生费用 (p. 285)。

Console

修改可突增性能实例的积分规范

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择实例。要一次修改若干个实例的规范，请选择所有适用的实例。
4. 依次选择操作、实例设置和更改积分规范。仅当您选择了可突增性能实例时，此选项才会启用。
5. 要将积分规范更改为 unlimited，请选中实例 ID 旁边的复选框。要将积分规范更改为 standard，请清除实例 ID 旁边的复选框。

Amazon CLI

修改可突增性能实例的积分规范 (Amazon CLI)

使用 modify-instance-credit-specification 命令。请使用 --instance-credit-specification 参数指定实例及其积分规范。有效的积分规范为 unlimited 和 standard。

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

下面是示例输出。

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

设置账户的默认积分规范

每个可突增性能实例系列都有默认积分规范 (p. 297)。您可以在每个 Amazon 区域的账户级别更改每个可突增性能实例系列的默认积分规范。

如果您使用 EC2 控制台中的启动实例向导来启动实例，则您为积分规范选择的值会覆盖账户级别的默认积分规范。如果您使用 Amazon CLI 启动实例，则账户中所有新的可突增性能实例都使用默认积分规范启动。现有正在运行或已停止的实例的积分规范不受影响。

考虑因素

实例系列的默认积分规范在 5 分钟滚动周期内只能修改一次，在 24 小时滚动周期内最多可修改四次。

Console

在每个区域的账户级别设置默认积分规范

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（区域选择器）。

3. 在左侧导航窗格上，选择 EC2 Dashboard (EC2 控制面板)。
4. 从 Account attributes (账户属性) 中，选择 Default credit specification (默认积分规范)。
5. 选择管理。
6. 对于每个实例系列，选择 Unlimited (无限) 或 Standard (标准)，然后选择 Update (更新)。

Amazon CLI

在账户级别设置默认积分规范 (Amazon CLI)

使用 modify-default-credit-specification 命令。使用 `--cpu-credits` 参数指定Amazon区域、实例系列和默认积分规范。有效的默认积分规范为 `unlimited` 和 `standard`。

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

查看默认积分规范

您可以在每个Amazon区域的账户级别查看可突增性能实例系列的默认积分规范。

Console

在账户级别查看默认积分规范（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（区域选择器）。
3. 在左侧导航窗格上，选择 EC2 Dashboard (EC2 控制面板)。
4. 从 Account attributes (账户属性) 中，选择 Default credit specification (默认积分规范)。

Amazon CLI

在账户级别查看默认积分规范 (Amazon CLI)

使用 get-default-credit-specification 命令。指定Amazon区域和实例系列。

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

监控您的 CPU 积分以获得具爆发能力的实例

EC2 将指标发送到 Amazon CloudWatch。您可以在 CloudWatch 控制台的 Amazon EC2 每个实例指标中查看 CPU 积分指标，也可以使用 Amazon CLI 列出每个实例的指标。有关更多信息，请参阅 使用控制台列出指标 (p. 1009) 和 使用 Amazon CLI 列出指标 (p. 1011)：

目录

- 可突增性能实例的其他 CloudWatch 指标 (p. 302)
- 计算使用的 CPU 积分 (p. 304)

可突增性能实例的其他 CloudWatch 指标

可突增性能实例具有这些额外的 CloudWatch 指标，将每 5 分钟更新一次这些指标：

- CPUCreditUsage – 在测量周期内花费的 CPU 积分数。
- CPUCreditBalance – 实例产生的 CPU 积分数量。在 CPU 突增以及 CPU 积分的花费速度比获得速度快时，该余额将用完。
- CPUSurplusCreditBalance – 在 CPUCreditBalance 值为零时，用于保持 CPU 利用率而花费的超额 CPU 积分数。
- CPUSurplusCreditsCharged – 超过可在 24 小时内获得的 CPU 积分数上限 (p. 279)的超额 CPU 积分数，因而会产生额外的费用。

最后两个指标仅适用于配置为 unlimited 的实例。

下表描述了可突增性能实例的 CloudWatch 指标。有关更多信息，请参阅列出实例的可用 CloudWatch 指标 (p. 1002)。

指标	描述
CPUCreditUsage	实例为保持 CPU 使用率而花费的 CPU 积分数。一个 CPU 积分等于一个 vCPU 按 100% 利用率运行一分钟，或者 vCPU、利用率和时间的等效组合（例如， 一个 vCPU 按 50% 利用率运行两分钟，或者两个 vCPU 按 25% 利用率运行两分钟）。 CPU 积分指标仅每 5 分钟提供一次。如果您指定一个大于五分钟的时间段，请使用Sum 统计数据，而非 Average 统计数据。 单位：积分 (vCPU 分钟)
CPUCreditBalance	实例自启动后已累积获得的 CPU 积分数。对于 T2 标准，CPUCreditBalance 还包含已累积的启动积分数。 在获得积分后，积分将在积分余额中累积；在花费积分后，将从积分余额中扣除积分。积分余额具有最大值限制，这是由实例大小决定的。在达到限制后，将丢弃获得的任何新积分。对于 T2 标准，启动积分不计入限制。 实例可以花费 CPUCreditBalance 中的积分，以便突增到基准 CPU 使用率以上。 在实例运行过程中，CPUCreditBalance 中的积分不会过期。在 T4g、T3a 和 T3 实例停止时，CPUCreditBalance 值将保留七天。之后，所有累积的积分都将丢失。在 T2 实例停止时，CPUCreditBalance 值不会保留，并且所有累积的积分都将丢失。 CPU 积分指标仅每 5 分钟提供一次。 单位：积分 (vCPU 分钟)
CPUSurplusCreditBalance	在 unlimited 值为零时，CPUCreditBalance 实例花费的超额积分数。 CPUSurplusCreditBalance 值由获得的 CPU 积分支付。如果超额积分数超出实例可在 24 小时周期内获得的最大积分数，则超出最大积分数的已花费超额积分将产生额外费用。 单位：积分 (vCPU 分钟)
CPUSurplusCreditsCharged	未由获得的 CPU 积分支付并且会产生额外费用的已花费超额积分数。 在出现以下任一情况时，将对花费的超额积分收费：

指标	描述
	• 花费的超额积分超出实例可在 24 小时周期内获得的最大积分数。对于超出最大积分数的所花费超额积分，将在该小时结束时向您收费。 • 实例已停止或终止。 • 实例从 `unlimited` 切换为 `standard`。 单位：积分 (vCPU 分钟)

计算使用的 CPU 积分

实例使用的 CPU 积分使用上表中所述的实例 CloudWatch 指标计算。

Amazon EC2 每 5 分钟向 CloudWatch 发送一次指标。在任何时间点引用的以前 指标值是指 5 分钟前 发送的以前指标值。

计算标准实例使用的 CPU 积分

- 如果 CPU 使用率低于基准，此时花费的积分低于前 5 分钟间隔获得的积分，CPU 积分余额将增加。
- 如果 CPU 使用率高于基准，此时花费的积分超过前 5 分钟间隔获得的积分，CPU 积分余额将减少。

从数学上讲，这是使用以下公式得出的：

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

实例大小确定实例每小时可获得的积分数以及实例可在积分余额中累积获得的积分数。有关每小时获得的积分数的信息，以及每个实例大小的积分余额限制，请参阅积分表 (p. 279)。

示例

该示例使用 `t3.nano` 实例。要计算实例的 `CPUCreditBalance` 值，请按以下方式使用前面的公式：

- `CPUCreditBalance` – 要计算的当前积分余额。
- `prior CPUCreditBalance` – 5 分钟前的积分余额。在该示例中，实例累积了两积分。
- `Credits earned per hour` – `t3.nano` 实例每小时获得 6 积分。
- `5/60` – 表示 CloudWatch 指标发布的 5 分钟间隔。将每小时获得的积分乘以 5/60（5 分钟）以计算实例在过去 5 分钟获得的积分数。`t3.nano` 实例每 5 分钟获得 0.5 积分。
- `CPUCreditUsage` – 实例在过去 5 分钟内花费的积分数。在该示例中，实例在过去 5 分钟内花费 1 积分。

您可以使用这些值计算 `CPUCreditBalance` 值：

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

计算无限实例使用的 CPU 积分

在可突增性能实例需要突增到基准以上时，它始终先花费累积的积分，然后再花费超额积分。在用完累积的 CPU 积分余额时，它会花费超额积分以将 CPU 突增所需的时间。在 CPU 使用率低于基准时，在实例累积获得的积分之前始终先支付超额积分。

我们在以下公式中使用 Adjusted balance 项以反映在该 5 分钟间隔内发生的活动。我们使用该值计算 CPUCreditBalance 和 CPUSurplusCreditBalance CloudWatch 指标的值。

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

如果 0 的值为 Adjusted balance，表示实例花费获得的所有积分来进行突增，而未花费任何超额积分。因此，CPUCreditBalance 和 CPUSurplusCreditBalance 均设置为 0。

正的 Adjusted balance 值表示实例累积获得了积分，并支付了以前的超额积分 (如果有)。因此，将 Adjusted balance 值分配给 CPUCreditBalance，并将 CPUSurplusCreditBalance 设置为 0。实例大小决定了可累积的最大积分数 (p. 279)。

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

负的 Adjusted balance 值表示实例花费了其累积获得的所有积分，并且还花费了超额积分来进行突增。因此，将 Adjusted balance 值分配给 CPUSurplusCreditBalance，并将 CPUCreditBalance 设置为 0。此外，实例大小决定了它可累积的最大积分数 (p. 279)。

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

如果花费的超额积分超过了实例可累积的最大积分，超额积分余额将设置为最大值，如前面的公式中所示。将对剩余的超额积分收费，如 CPUSurplusCreditsCharged 指标表示。

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

最后，在实例终止时，将对由 CPUSurplusCreditBalance 跟踪的任何超额积分收费。如果实例从 unlimited 切换到 standard，则还会对任何剩余的 CPUSurplusCreditBalance 收费。

计算优化型实例

计算优化型实例是受益于高性能处理器的受计算限制的应用程序的理想选择。

C5 和 C5n 实例

这些实例非常适合以下用途：

- 批处理工作负载
- 媒体转码
- 高性能 Web 服务器
- 高性能计算 (HPC)

- 科学建模
- 专用游戏服务器和广告服务引擎
- Machine Learning 推理和其他计算密集型应用程序

裸机实例（如 `c5.metal`）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

C6g、C6gd 和 C6gn 实例

这些实例由 Amazon Graviton2 处理器提供支持，非常适合运行先进的计算密集型工作负载，例如：

- 高性能计算 (HPC)
- 批处理
- 广告服务
- 视频解码
- 游戏服务器
- 科学建模
- 分布式分析
- 基于 CPU 的机器学习推理

裸机实例（如 `c6g.metal`）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

C6i 和 C6id 实例

这些实例非常适合运行先进的计算密集型工作负载，例如：

- 高性能计算 (HPC)
- 批处理
- 广告服务
- 视频解码
- 分布式分析
- 高度可扩展的多人游戏

C6in 实例

这些实例非常适合计算密集型工作负载，例如：

- 分布式计算应用程序
- 网络虚拟设备
- 数据分析
- 高性能计算（HPC）
- 基于 CPU 的 AI/ML

有关更多信息，请参阅 Amazon EC2 C6i 实例。

Hpc6a 实例

这些实例非常适合运行高性能计算 (HPC) 工作负载，例如：

- 分子动力学
- 计算化学
- 计算流体动力学

- 天气预测
- 材料模拟
- 崩溃模拟
- 天体物理学

目录

- 硬件规格 (p. 307)
- 实例性能 (p. 312)
- 网络性能 (p. 312)
- Amazon EBS I/O 性能 (p. 319)
- 基于 SSD 的实例存储卷的 I/O 性能 (p. 319)
- 发布说明 (p. 320)

硬件规格

以下是计算优化型实例的硬件规格摘要。虚拟中央处理单元（vCPU）表示分配给虚拟机（VM）的物理 CPU 的一部分。对于 x86 实例，每个内核有两个 vCPU。对于 Graviton 实例，每个内核有一个 vCPU。

实例类型	默认 vCPU	内存（GiB）
c1.medium	2	1.70
c1.xlarge	8	7.00
c3.large	2	3.75
c3.xlarge	4	7.50
c3.2xlarge	8	15.00
c3.4xlarge	16	30.00
c3.8xlarge	32	60.00
c4.large	2	3.75
c4.xlarge	4	7.50
c4.2xlarge	8	15.00
c4.4xlarge	16	30.00
c4.8xlarge	36	60.00
c5.large	2	4.00
c5.xlarge	4	8.00
c5.2xlarge	8	16.00
c5.4xlarge	16	32.00
c5.9xlarge	36	72.00
c5.12xlarge	48	96.00
c5.18xlarge	72	144.00

实例类型	默认 vCPU	内存（GiB）
c5.24xlarge	96	192.00
c5.metal	96	192.00
c5a.large	2	4.00
c5a.xlarge	4	8.00
c5a.2xlarge	8	16.00
c5a.4xlarge	16	32.00
c5a.8xlarge	32	64.00
c5a.12xlarge	48	96.00
c5a.16xlarge	64	128.00
c5a.24xlarge	96	192.00
c5ad.large	2	4.00
c5ad.xlarge	4	8.00
c5ad.2xlarge	8	16.00
c5ad.4xlarge	16	32.00
c5ad.8xlarge	32	64.00
c5ad.12xlarge	48	96.00
c5ad.16xlarge	64	128.00
c5ad.24xlarge	96	192.00
c5d.large	2	4.00
c5d.xlarge	4	8.00
c5d.2xlarge	8	16.00
c5d.4xlarge	16	32.00
c5d.9xlarge	36	72.00
c5d.12xlarge	48	96.00
c5d.18xlarge	72	144.00
c5d.24xlarge	96	192.00
c5d.metal	96	192.00
c5n.large	2	5.25
c5n.xlarge	4	10.50
c5n.2xlarge	8	21.00
c5n.4xlarge	16	42.00

实例类型	默认 vCPU	内存（GiB）
c5n.9xlarge	36	96.00
c5n.18xlarge	72	192.00
c5n.metal	72	192.00
c6a.large	2	4.00
c6a.xlarge	4	8.00
c6a.2xlarge	8	16.00
c6a.4xlarge	16	32.00
c6a.8xlarge	32	64.00
c6a.12xlarge	48	96.00
c6a.16xlarge	64	128.00
c6a.24xlarge	96	192.00
c6a.32xlarge	128	256.00
c6a.48xlarge	192	384.00
c6a.metal	192	384.00
c6g.medium	1	2.00
c6g.large	2	4.00
c6g.xlarge	4	8.00
c6g.2xlarge	8	16.00
c6g.4xlarge	16	32.00
c6g.8xlarge	32	64.00
c6g.12xlarge	48	96.00
c6g.16xlarge	64	128.00
c6g.metal	64	128.00
c6gd.medium	1	2.00
c6gd.large	2	4.00
c6gd.xlarge	4	8.00
c6gd.2xlarge	8	16.00
c6gd.4xlarge	16	32.00
c6gd.8xlarge	32	64.00
c6gd.12xlarge	48	96.00
c6gd.16xlarge	64	128.00

实例类型	默认 vCPU	内存（GiB）
c6gd.metal	64	128.00
c6gn.medium	1	2.00
c6gn.large	2	4.00
c6gn.xlarge	4	8.00
c6gn.2xlarge	8	16.00
c6gn.4xlarge	16	32.00
c6gn.8xlarge	32	64.00
c6gn.12xlarge	48	96.00
c6gn.16xlarge	64	128.00
c6i.large	2	4.00
c6i.xlarge	4	8.00
c6i.2xlarge	8	16.00
c6i.4xlarge	16	32.00
c6i.8xlarge	32	64.00
c6i.12xlarge	48	96.00
c6i.16xlarge	64	128.00
c6i.24xlarge	96	192.00
c6i.32xlarge	128	256.00
c6i.metal	128	256.00
c6id.large	2	4.00
c6id.xlarge	4	8.00
c6id.2xlarge	8	16.00
c6id.4xlarge	16	32.00
c6id.8xlarge	32	64.00
c6id.12xlarge	48	96.00
c6id.16xlarge	64	128.00
c6id.24xlarge	96	192.00
c6id.32xlarge	128	256.00
c6id.metal	128	256.00
c6in.large	2	4.00
c6in.xlarge	4	8.00

实例类型	默认 vCPU	内存（GiB）
c6in.2xlarge	8	16.00
c6in.4xlarge	16	32.00
c6in.8xlarge	32	64.00
c6in.12xlarge	48	96.00
c6in.16xlarge	64	128.00
c6in.24xlarge	96	192.00
c6in.32xlarge	128	256.00
c6in.metal	128	256.00
c7g.medium	1	2.00
c7g.large	2	4.00
c7g.xlarge	4	8.00
c7g.2xlarge	8	16.00
c7g.4xlarge	16	32.00
c7g.8xlarge	32	64.00
c7g.12xlarge	48	96.00
c7g.16xlarge	64	128.00
c7g.metal	64	128.00
cc2.8xlarge	32	60.50
hpc6a.48xlarge	96	384.00

计算优化实例使用以下处理器。

Amazon Graviton 处理器

- Amazon Graviton2：C6g、C6gd、C6gn
- Amazon Graviton3：C7g

AMD 处理器

- 第二代 AMD EPYC 处理器（AMD EPYC 7R32）：C5a、C5ad
- 第三代 AMD EPYC 处理器（AMD EPYC 7R13）：C6a、Hpc6a

英特尔处理器

- 英特尔至强可扩展处理器（Haswell E5-2666 v3）：C4
- 英特尔至强可扩展处理器（Skylake 8124）：C5n
- 英特尔至强可扩展处理器（Skylake 8124M 或 Cascade Lake 8223CL）：更小的 C5 和 C5d
- 第二代英特尔至强可扩展处理器（Cascade Lake 8275CL）：更大的 C5 和 C5d

- 第三代英特尔至强可扩展处理器（Ice Lake 8375C）：C6i、C6id

有关更多信息，请参阅 Amazon EC2 实例类型。

实例性能

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。有些计算优化型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

有些计算优化型实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅您的 EC2 实例的处理器状态控制 (p. 707)。

网络性能

您可以为受支持的实例类型启用增强联网，以提供更低的延迟、更低的网络抖动和更高的每秒数据包数 (PPS) 性能。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。

以下是支持增强联网的计算优化型实例的网络性能摘要。

Note

标有 † 的实例类型具备基准带宽，并且可以通过网络输入/输出积分机制，尽可能将其基准带宽突增到基准以上。有关更多信息，请参阅实例网络带宽 (p. 1141)。

实例类型	网络性能	增强联网功能
c1.medium †	中	不支持
c1.xlarge †	高	不支持
c3.large †	中	不支持
c3.xlarge †	中	不支持
c3.2xlarge †	高	不支持
c3.4xlarge †	高	不支持
c3.8xlarge †	10Gb	不支持
c4.large †	中	不支持
c4.xlarge †	高	不支持
c4.2xlarge †	高	不支持
c4.4xlarge †	高	不支持
c4.8xlarge †	10Gb	不支持
c5.large †	高达 10Gb	ENA
c5.xlarge †	高达 10Gb	ENA
c5.2xlarge †	高达 10Gb	ENA
c5.4xlarge †	高达 10Gb	ENA

实例类型	网络性能	增强联网功能
c5.9xlarge	12Gb	ENA
c5.12xlarge	12Gb	ENA
c5.18xlarge	25Gb	ENA
c5.24xlarge	25Gb	ENA
c5.metal	25Gb	ENA
c5a.large †	高达 10Gb	ENA
c5a.xlarge †	高达 10Gb	ENA
c5a.2xlarge †	高达 10Gb	ENA
c5a.4xlarge †	高达 10Gb	ENA
c5a.8xlarge	10Gb	ENA
c5a.12xlarge	12Gb	ENA
c5a.16xlarge	20Gb	ENA
c5a.24xlarge	20Gb	ENA
c5ad.large †	高达 10Gb	ENA
c5ad.xlarge †	高达 10Gb	ENA
c5ad.2xlarge †	高达 10Gb	ENA
c5ad.4xlarge †	高达 10Gb	ENA
c5ad.8xlarge	10Gb	ENA
c5ad.12xlarge	12Gb	ENA
c5ad.16xlarge	20Gb	ENA
c5ad.24xlarge	20Gb	ENA
c5d.large †	高达 10Gb	ENA
c5d.xlarge †	高达 10Gb	ENA
c5d.2xlarge †	高达 10Gb	ENA
c5d.4xlarge †	高达 10Gb	ENA
c5d.9xlarge	12Gb	ENA
c5d.12xlarge	12Gb	ENA
c5d.18xlarge	25Gb	ENA
c5d.24xlarge	25Gb	ENA
c5d.metal	25Gb	ENA
c5n.large †	高达 25Gb	ENA

实例类型	网络性能	增强联网功能
c5n.xlarge †	高达 25Gb	ENA
c5n.2xlarge †	高达 25Gb	ENA
c5n.4xlarge †	高达 25Gb	ENA
c5n.9xlarge	50Gb	ENA | EFA
c5n.18xlarge	100Gb	ENA | EFA
c5n.metal	100Gb	ENA | EFA
c6a.large †	高达 12.5Gb	ENA
c6a.xlarge †	高达 12.5Gb	ENA
c6a.2xlarge †	高达 12.5Gb	ENA
c6a.4xlarge †	高达 12.5Gb	ENA
c6a.8xlarge	12.5Gb	ENA
c6a.12xlarge	18.75Gb	ENA
c6a.16xlarge	25Gb	ENA
c6a.24xlarge	37.5Gb	ENA
c6a.32xlarge	50Gb	ENA
c6a.48xlarge	50Gb	ENA | EFA
c6a.metal	50Gb	ENA | EFA
c6g.medium †	高达 10Gb	ENA
c6g.large †	高达 10Gb	ENA
c6g.xlarge †	高达 10Gb	ENA
c6g.2xlarge †	高达 10Gb	ENA
c6g.4xlarge †	高达 10Gb	ENA
c6g.8xlarge	12Gb	ENA
c6g.12xlarge	20Gb	ENA
c6g.16xlarge	25Gb	ENA
c6g.metal	25Gb	ENA
c6gd.medium †	高达 10Gb	ENA
c6gd.large †	高达 10Gb	ENA
c6gd.xlarge †	高达 10Gb	ENA
c6gd.2xlarge †	高达 10Gb	ENA
c6gd.4xlarge †	高达 10Gb	ENA

实例类型	网络性能	增强联网功能
c6gd.8xlarge	12Gb	ENA
c6gd.12xlarge	20Gb	ENA
c6gd.16xlarge	25Gb	ENA
c6gd.metal	25Gb	ENA
c6gn.medium †	高达 16Gb	ENA
c6gn.large †	高达 25Gb	ENA
c6gn.xlarge †	高达 25Gb	ENA
c6gn.2xlarge †	高达 25Gb	ENA
c6gn.4xlarge †	高达 25Gb	ENA
c6gn.8xlarge	50Gb	ENA
c6gn.12xlarge	75Gb	ENA
c6gn.16xlarge	100Gb	ENA | EFA
c6i.large †	高达 12.5Gb	ENA
c6i.xlarge †	高达 12.5Gb	ENA
c6i.2xlarge †	高达 12.5Gb	ENA
c6i.4xlarge †	高达 12.5Gb	ENA
c6i.8xlarge	12.5Gb	ENA
c6i.12xlarge	18.75Gb	ENA
c6i.16xlarge	25Gb	ENA
c6i.24xlarge	37.5Gb	ENA
c6i.32xlarge	50Gb	ENA | EFA
c6i.metal	50Gb	ENA | EFA
c6id.large †	高达 12.5Gb	ENA
c6id.xlarge †	高达 12.5Gb	ENA
c6id.2xlarge †	高达 12.5Gb	ENA
c6id.4xlarge †	高达 12.5Gb	ENA
c6id.8xlarge	12.5Gb	ENA
c6id.12xlarge	18.75Gb	ENA
c6id.16xlarge	25Gb	ENA
c6id.24xlarge	37.5Gb	ENA
c6id.32xlarge	50Gb	ENA | EFA

实例类型	网络性能	增强联网功能
c6id.metal	50Gb	ENA | EFA
c6in.large †	高达 25Gb	ENA
c6in.xlarge †	高达 30Gb	ENA
c6in.2xlarge †	高达 40Gb	ENA
c6in.4xlarge †	高达 50Gb	ENA
c6in.8xlarge	50Gb	ENA
c6in.12xlarge	75Gb	ENA
c6in.16xlarge	100Gb	ENA
c6in.24xlarge	150Gb	ENA
c6in.32xlarge	200Gb	ENA | EFA
c6in.metal	200Gb	ENA | EFA
c7g.medium †	高达 12.5Gb	ENA
c7g.large †	高达 12.5Gb	ENA
c7g.xlarge †	高达 12.5Gb	ENA
c7g.2xlarge †	高达 15Gb	ENA
c7g.4xlarge †	高达 15Gb	ENA
c7g.8xlarge	15Gb	ENA
c7g.12xlarge	22.5Gb	ENA
c7g.16xlarge	30Gb	ENA | EFA
c7g.metal	30Gb	ENA | EFA
hpc6a.48xlarge	100Gb	ENA | EFA

对于支持 200Gbps 的 32xlarge 和 metal 实例类型，实例上至少需要 2 个 ENI，并且每个 ENI 需要连接到不同的网卡，才能达到 200Gbps 的吞吐量。连接到网卡的每个 ENI 最大可达到 170Gbps。

下表显示了实例类型的基准带宽和突增带宽，这些实例类型通过网络输入/输出积分机制将其基准带宽突增到基准以上。

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
c1.medium	0.3	1.2
c1.xlarge	1.0	10.0
c3.large	0.5	1.2
c3.xlarge	0.7	10.0
c3.2xlarge	1.0	10.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
c3.4xlarge	2.0	10.0
c3.8xlarge	5.0	10.0
c4.large	0.625	1.2
c4.xlarge	1.25	2.8
c4.2xlarge	2.5	10.0
c4.4xlarge	5.0	10.0
c4.8xlarge	5.0	10.0
c5.large	0.75	10.0
c5.xlarge	1.25	10.0
c5.2xlarge	2.5	10.0
c5.4xlarge	5.0	10.0
c5a.large	0.75	10.0
c5a.xlarge	1.25	10.0
c5a.2xlarge	2.5	10.0
c5a.4xlarge	5.0	10.0
c5ad.large	0.75	10.0
c5ad.xlarge	1.25	10.0
c5ad.2xlarge	2.5	10.0
c5ad.4xlarge	5.0	10.0
c5d.large	0.75	10.0
c5d.xlarge	1.25	10.0
c5d.2xlarge	2.5	10.0
c5d.4xlarge	5.0	10.0
c5n.large	3.0	25.0
c5n.xlarge	5.0	25.0
c5n.2xlarge	10.0	25.0
c5n.4xlarge	15.0	25.0
c6a.large	0.781	12.5
c6a.xlarge	1.562	12.5
c6a.2xlarge	3.125	12.5
c6a.4xlarge	6.25	12.5

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
c6g.medium	0.5	10.0
c6g.large	0.75	10.0
c6g.xlarge	1.25	10.0
c6g.2xlarge	2.5	10.0
c6g.4xlarge	5.0	10.0
c6gd.medium	0.5	10.0
c6gd.large	0.75	10.0
c6gd.xlarge	1.25	10.0
c6gd.2xlarge	2.5	10.0
c6gd.4xlarge	5.0	10.0
c6gn.medium	1.6	16.0
c6gn.large	3.0	25.0
c6gn.xlarge	6.3	25.0
c6gn.2xlarge	12.5	25.0
c6gn.4xlarge	15.0	25.0
c6i.large	0.781	12.5
c6i.xlarge	1.562	12.5
c6i.2xlarge	3.125	12.5
c6i.4xlarge	6.25	12.5
c6id.large	0.781	12.5
c6id.xlarge	1.562	12.5
c6id.2xlarge	3.125	12.5
c6id.4xlarge	6.25	12.5
c6in.large	3.125	25.0
c6in.xlarge	6.25	30.0
c6in.2xlarge	12.5	40.0
c6in.4xlarge	25.0	50.0
c7g.medium	0.52	12.5
c7g.large	0.937	12.5
c7g.xlarge	1.876	12.5
c7g.2xlarge	3.75	15.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
c7g.4xlarge	7.5	15.0

Amazon EBS I/O 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 Amazon EBS 卷提供最佳性能。

有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

基于 SSD 的实例存储卷的 I/O 性能

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您最高可以获得下表所列的 IOPS（4096 字节的数据块大小）性能（在队列深度饱和时）。否则，您将获得较低的 IOPS 性能。

实例大小	100% 随机读取 IOPS	写入 IOPS
c5ad.large	16,283	7,105
c5ad.xlarge	32,566	14,211
c5ad.2xlarge	65,132	28,421
c5ad.4xlarge	130,263	56,842
c5ad.8xlarge	260,526	113,684
c5ad.12xlarge	412,500	180,000
c5ad.16xlarge	521,053	227,368
c5ad.24xlarge	825,000	360,000
c5d.large	20000	9,000
c5d.xlarge	40000	18000
c5d.2xlarge	80,000	37,000
c5d.4xlarge	175000	75000
c5d.9xlarge	350,000	170,000
c5d.12xlarge	700,000	340,000
c5d.18xlarge	700,000	340,000
c5d.24xlarge	1400000	680,000
c5d.metal	1400000	680,000
c6gd.medium	13438	5625
c6gd.large	26875	11250
c6gd.xlarge	53750	22500
c6gd.2xlarge	107500	45000

实例大小	100% 随机读取 IOPS	写入 IOPS
c6gd.4xlarge	215000	90000
c6gd.8xlarge	430000	180,000
c6gd.12xlarge	645000	270000
c6gd.16xlarge	860000	360,000
c6gd.metal	860000	360,000
c6id.large	33,542	16,771
c6id.xlarge	67,083	33,542
c6id.2xlarge	134,167	67,084
c6id.4xlarge	268,333	134,167
c6id.8xlarge	536,666	268,334
c6id.12xlarge	804,999	402,501
c6id.16xlarge	1,073,332	536,668
c6id.24xlarge	1,609,998	805,002
c6id.32xlarge	2,146,664	1,073,336
c6id.metal	2,146,664	1,073,336

随着您不断在您的实例的基于 SSD 的实例存储卷中填充数据，您可以达到的写入 IOPS 将不断减少。这是因为，SSD 控制器必须执行额外的工作，即查找可用空间、重写现有数据，以及擦除未使用的空间以使之可供重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为 实例提供的基于 SSD 的实例存储卷不会为超额配置预保留空白间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。

发布说明

- C4 实例和基于 Nitro 系统 (p. 246)构建的实例需要 64 位 EBS 支持的 HVM AMIs。它们具有高内存，需要 64 位操作系统才能利用这一容量。与内存增强型实例类型上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。此外，您必须使用 HVM AMI 才能利用增强联网功能。
- C7g 实例由最新一代 Amazon Graviton3 处理器提供支持。与第六代 Amazon 基于 Graviton2 的 C6g 实例相比，它们提供了多达 25% 的性能提升。C7g 实例是云中首个采用 DDR5 内存的实例，与 DDR4 内存相比，该实例提供了高 50% 的内存带宽，以便能够高速访问内存中的数据。
  - C7g 实例限制了高功率指令的总执行率，例如，实例中的内核之间的浮点数乘积累加。专注于其他工作负载细分的未来实例类型可能没有此限制

- 基于 Nitro 系统构建的实例具有以下要求：
  - 必须安装有 NVMe 驱动程序 (p. 1518)。
  - 必须安装有 Elastic Network Adapter (ENA) (p. 1143) 驱动程序。

  以下 Linux AMI 满足这些要求：
  - Amazon Linux 2
  - Amazon Linux AMI 2018.03
  - Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

    Note

    Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
  - Red Hat Enterprise Linux 7.4 或更高版本
  - SUSE Linux Enterprise Server 12 SP2 或更高版本
  - CentOS 7.4.1708 或更高版本
  - FreeBSD 11.1 或更高版本
  - Debian GNU/Linux 9 或更高版本
- 具有 Amazon Graviton 处理器的实例具有以下要求：
  - 使用适用于 64 位 Arm 架构的 AMI。
  - 支持通过带有 ACPI 表的 UEFI 进行引导，以及支持 ACPI 热插拔 PCI 设备。

  以下 AMI 满足这些要求：
  - Amazon Linux 2（64 位 Arm）
  - Ubuntu 16.04 或更高版本（64 位 Arm）
  - Red Hat Enterprise Linux 8.0 或更高版本（64 位 Arm）
  - SUSE Linux Enterprise Server 15 或更高版本（64 位 Arm）
  - Debian 10 或更高版本（64 位 Arm）
- 为了从 C6i 实例获得最佳性能，请确保它们的 ENA 驱动程序版本为 2.2.9 或更高版本。将早于 1.2 版本的 ENA 驱动程序用于这些实例会导致网络接口连接失败。以下 AMI 具备兼容的 ENA 驱动程序。
  - 内核版本为 4.14.186 的 Amazon Linux 2
  - 内核版本为 5.4.0-1025-aws 的 Ubuntu 20.04
  - 内核版本为 4.18.0-240.1.1.el8_3.ARCH 的 Red Hat Enterprise Linux 8.3
  - 内核版本为 5.3.18-24.15.1 的 SUSE Linux Enterprise Server 15 SP2
- 在 Nitro 系统实例上构建的实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。有关更多信息，请参阅Nitro 系统卷限制 (p. 1607)。
- 为了从 C6gn 实例获得最佳性能，请确保它们的 ENA 驱动程序版本为 2.2.9 或更高版本。将早于 1.2 版本的 ENA 驱动程序用于这些实例会导致网络接口连接失败。以下 AMI 具备兼容的 ENA 驱动程序。
  - 内核版本为 4.14.186 的 Amazon Linux 2
  - 内核版本为 5.4.0-1025-aws 的 Ubuntu 20.04
  - 内核版本为 4.18.0-240.1.1.el8_3.ARCH 的 Red Hat Enterprise Linux 8.3
  - 内核版本为 5.3.18-24.15.1 的 SUSE Linux Enterprise Server 15 SP2
- 要在 C6gn 实例上为所有 Linux 发行版启动 AMI，请使用最新版本的 AMI 并运行更新以获得 最新驱动程序。对于早期版本，从 GitHub 下载最新的驱动程序。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
```

```
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 在 Nitro 系统实例上构建的实例应安装了 acpid，以支持通过 API 请求执行干净关闭。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅 Amazon EC2 常见问题解答中的我可以在 Amazon EC2 中运行多少个实例？。

内存优化型实例

内存优化型实例旨在让处理内存中的大型数据集的工作负载实现快速性能。

R5、R5a、R5b 和 R5n 实例

这些实例非常适合以下用途：

- 高性能数据库，包括关系型数据库 MySQL 和 NoSQL（例如 MongoDB 数据库、Cassandra 数据库）。
- 提供键值型数据内存缓存功能的分布式 Web 级缓存存储，例如 Memcached 和 Redis。
- 使用用于商业智能的优化型数据存储格式与分析的内存数据库，例如 SAP HANA。
- 使用 Hadoop 和 Spark 集群对大型非结构化数据进行实时处理的应用程序
- 高性能计算 (HPC) 和 Electronic Design Automation (EDA) 应用程序。

裸机实例（如 `r5.metal`）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

R6a 实例

这些实例非常适合运行内存密集型工作负载，如下所示：

- 高性能数据库，例如关系型数据库和 NoSQL
- 分布式 Web 扩展内存中缓存，例如 Memcached 和 Redis
- 实时大数据分析，例如 Hadoop 和 Spark 集群

Hpc6id 实例

这些实例非常适合运行高性能计算 (HPC) 工作负载，例如：

- 地震和水库
- 崩溃模拟
- 有限元分析

R6g 和 R6gd 实例

这些实例由 Amazon Graviton2 处理器提供支持，非常适合运行内存密集型工作负载，例如：

- 开源数据库，例如 MySQL、MariaDB 和 PostgreSQL
- 内存缓存，例如 Memcached、Redis 和 KeyDB

裸机实例（如 `r6g.metal`）为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

R6i 和 R6id 实例

这些实例非常适合运行内存密集型工作负载，如下所示：

- 高性能数据库，例如关系型数据库和 NoSQL
- 内存数据库，例如 SAP HANA
- 分布式 Web 级内存缓存，例如 Memcached 和 Redis
- 实时大数据分析，例如 Hadoop 和 Spark 集群

R6in 和 R6idn 实例

这些实例非常适合网络密集型工作负载，例如：

- 高性能关系型数据库 MySQL 和 NoSQL。例如 MongoDB 数据库和 Cassandra 数据库
- 提供键值型数据内存缓存功能的分布式 Web 级缓存存储，例如 Memcached 和 Redis
- 使用用于商业智能的优化型数据存储格式与分析的内存数据库，例如 SAP HANA
- 金融服务的实时大数据分析，例如 Hadoop 和 Spark 集群

有关更多信息，请参阅 Amazon EC2 R6i 实例。

内存增强型 (u-*) 实例

这些实例为每个实例提供 3 TiB、6 TiB、9 TiB、12 TiB、18 TiB 和 24 TiB 内存。这些实例适合运行大型内存中数据库，包括 SAP HANA 内存中数据库的生产部署。

X1 实例

这些实例非常适合以下用途：

- 内存中数据库，如 SAP HANA，包含针对 Business Suite S/4HANA、Business Suite on HANA (SoH)、Business Warehouse on HANA (BW) 和 Data Mart Solutions on HANA 的 SAP 认证支持。有关更多信息，请参阅 Amazon 云上的 SAP HANA。
- 大数据处理引擎 (如 Apache Spark 或 Presto)。
- 高性能计算 (HPC) 应用程序。

X1e 实例

这些实例非常适合以下用途：

- 高性能数据库。
- 内存中数据库，例如 SAP HANA。有关更多信息，请参阅 Amazon 云上的 SAP HANA。
- 内存密集型企业应用程序。

X2gd 实例

这些实例非常适合以下用途：

- 内存中数据库，例如 Redis 和 Memcached。
- 关系数据库，例如 MySQL 和 PostGreSQL。
- Electronic Design Automation (EDA) 工作负载，例如物理验证和布局工具。
- 内存密集型工作负载，例如实时分析和实时缓存服务器。

X2idn、X2iedn 和 X2iezn 实例

这些实例非常适合以下用途：

- 内存中数据库，例如 Redis 和 Memcached。

- 关系数据库，例如 MySQL 和 PostGreSQL。
- Electronic Design Automation (EDA) 工作负载，例如物理验证和布局工具。
- 内存密集型工作负载，例如实时分析和实时缓存服务器。

X2idn 和 X2iedn 实例支持 io2 Block Express 卷。在启动过程中或启动之后，附至 X2idn 和 X2iedn 实例的所有 io2 卷会自动在 EBS Block Express 上运行。有关更多信息，请参阅 io2 Block Express 卷。

z1d 实例

这些实例提供较高的计算容量和较高的内存数量，非常适合以下用途：

- Electronic Design Automation (EDA)
- 关系数据库工作负载

z1d.metal 实例为应用程序提供对主机服务器的物理资源 (如处理器和内存) 的直接访问。

目录

- 硬件规格 (p. 324)
- 内存性能 (p. 331)
- 实例性能 (p. 332)
- 网络性能 (p. 332)
- Amazon EBS I/O 性能 (p. 342)
- 基于 SSD 的实例存储卷的 I/O 性能 (p. 342)
- 支持 个 vCPU (p. 345)
- 发布说明 (p. 345)

硬件规格

以下是内存优化型实例的硬件规格摘要。虚拟中央处理单元（vCPU）表示分配给虚拟机（VM）的物理 CPU 的一部分。对于 x86 实例，每个内核有两个 vCPU。对于 Graviton 实例，每个内核有一个 vCPU。

实例类型	默认 vCPU	内存（GiB）
cr1.8xlarge	32	243.76
hpc6id.32xlarge	64	1024.00
r3.large	2	15.00
r3.xlarge	4	30.50
r3.2xlarge	8	61.00
r3.4xlarge	16	122.00
r3.8xlarge	32	244.00
r4.large	2	15.25
r4.xlarge	4	30.50
r4.2xlarge	8	61.00
r4.4xlarge	16	122.00

实例类型	默认 vCPU	内存（GiB）
r4.8xlarge	32	244.00
r4.16xlarge	64	488.00
r5.large	2	16.00
r5.xlarge	4	32.00
r5.2xlarge	8	64.00
r5.4xlarge	16	128.00
r5.8xlarge	32	256.00
r5.12xlarge	48	384.00
r5.16xlarge	64	512.00
r5.24xlarge	96	768.00
r5.metal	96	768.00
r5a.large	2	16.00
r5a.xlarge	4	32.00
r5a.2xlarge	8	64.00
r5a.4xlarge	16	128.00
r5a.8xlarge	32	256.00
r5a.12xlarge	48	384.00
r5a.16xlarge	64	512.00
r5a.24xlarge	96	768.00
r5ad.large	2	16.00
r5ad.xlarge	4	32.00
r5ad.2xlarge	8	64.00
r5ad.4xlarge	16	128.00
r5ad.8xlarge	32	256.00
r5ad.12xlarge	48	384.00
r5ad.16xlarge	64	512.00
r5ad.24xlarge	96	768.00
r5b.large	2	16.00
r5b.xlarge	4	32.00
r5b.2xlarge	8	64.00
r5b.4xlarge	16	128.00

实例类型	默认 vCPU	内存（GiB）
r5b.8xlarge	32	256.00
r5b.12xlarge	48	384.00
r5b.16xlarge	64	512.00
r5b.24xlarge	96	768.00
r5b.metal	96	768.00
r5d.large	2	16.00
r5d.xlarge	4	32.00
r5d.2xlarge	8	64.00
r5d.4xlarge	16	128.00
r5d.8xlarge	32	256.00
r5d.12xlarge	48	384.00
r5d.16xlarge	64	512.00
r5d.24xlarge	96	768.00
r5d.metal	96	768.00
r5dn.large	2	16.00
r5dn.xlarge	4	32.00
r5dn.2xlarge	8	64.00
r5dn.4xlarge	16	128.00
r5dn.8xlarge	32	256.00
r5dn.12xlarge	48	384.00
r5dn.16xlarge	64	512.00
r5dn.24xlarge	96	768.00
r5dn.metal	96	768.00
r5n.large	2	16.00
r5n.xlarge	4	32.00
r5n.2xlarge	8	64.00
r5n.4xlarge	16	128.00
r5n.8xlarge	32	256.00
r5n.12xlarge	48	384.00
r5n.16xlarge	64	512.00
r5n.24xlarge	96	768.00

实例类型	默认 vCPU	内存（GiB）
r5n.metal	96	768.00
r6a.large	2	16.00
r6a.xlarge	4	32.00
r6g.2xlarge	8	64.00
r6a.4xlarge	16	128.00
r6a.8xlarge	32	256.00
r6a.12xlarge	48	384.00
r6a.16xlarge	64	512.00
r6a.24xlarge	96	768.00
r6a.32xlarge	128	1024.00
r6a.48xlarge	192	1536.00
r6a.metal	192	1536.00
r6g.medium	1	8.00
r6g.large	2	16.00
r6g.xlarge	4	32.00
r6g.2xlarge	8	64.00
r6g.4xlarge	16	128.00
r6g.8xlarge	32	256.00
r6g.12xlarge	48	384.00
r6g.16xlarge	64	512.00
r6g.metal	64	512.00
r6gd.medium	1	8.00
r6gd.large	2	16.00
r6gd.xlarge	4	32.00
r6gd.2xlarge	8	64.00
r6gd.4xlarge	16	128.00
r6gd.8xlarge	32	256.00
r6gd.12xlarge	48	384.00
r6gd.16xlarge	64	512.00
r6gd.metal	64	512.00
r6i.large	2	16.00

实例类型	默认 vCPU	内存（GiB）
r6i.xlarge	4	32.00
r6i.2xlarge	8	64.00
r6i.4xlarge	16	128.00
r6i.8xlarge	32	256.00
r6i.12xlarge	48	384.00
r6i.16xlarge	64	512.00
r6i.24xlarge	96	768.00
r6i.32xlarge	128	1024.00
r6i.metal	128	1024.00
r6idn.large	2	16.00
r6idn.xlarge	4	32.00
r6idn.2xlarge	8	64.00
r6idn.4xlarge	16	128.00
r6idn.8xlarge	32	256.00
r6idn.12xlarge	48	384.00
r6idn.16xlarge	64	512.00
r6idn.24xlarge	96	768.00
r6idn.32xlarge	128	1024.00
r6idn.metal	128	1024.00
r6in.large	2	16.00
r6in.xlarge	4	32.00
r6in.2xlarge	8	64.00
r6in.4xlarge	16	128.00
r6in.8xlarge	32	256.00
r6in.12xlarge	48	384.00
r6in.16xlarge	64	512.00
r6in.24xlarge	96	768.00
r6in.32xlarge	128	1024.00
r6in.metal	128	1024.00
r6id.large	2	16.00
r6id.xlarge	4	32.00

实例类型	默认 vCPU	内存（GiB）
r6gd.2xlarge	8	64.00
r6id.4xlarge	16	128.00
r6id.8xlarge	32	256.00
r6id.12xlarge	48	384.00
r6id.16xlarge	64	512.00
r6id.24xlarge	96	768.00
r6id.32xlarge	128	1024.00
r6id.metal	128	1024.00
r7g.medium	1	8.00
r7g.large	2	16.00
r7g.xlarge	4	32.00
r7g.2xlarge	8	64.00
r7g.4xlarge	16	128.00
r7g.8xlarge	32	256.00
r7g.12xlarge	48	384.00
r7g.16xlarge	64	512.00
r7g.metal	64	512.00
u-3tb1.56xlarge	224	3072.00
u-6tb1.56xlarge	224	6144.00
u-6tb1.112xlarge	448	6144.00
u-6tb1.metal	448	6144.00
u-9tb1.112xlarge	448	9216.00
u-9tb1.metal	448	9216.00
u-12tb1.112xlarge	448	12288.00
u-12tb1.metal	448	12288.00
u-18tb1.metal	448	18432.00
u-24tb1.metal	448	24576.00
x1.16xlarge	64	976.00
x1.32xlarge	128	1952.00
x2gd.medium	1	16.00
x2gd.large	2	32.00

实例类型	默认 vCPU	内存（GiB）
x2gd.xlarge	4	64.00
x2gd.2xlarge	8	128.00
x2gd.4xlarge	16	256.00
x2gd.8xlarge	32	512.00
x2gd.12xlarge	48	768.00
x2gd.16xlarge	64	1024.00
x2gd.metal	64	1024.00
x2idn.16xlarge	64	1024.00
x2idn.24xlarge	96	1536.00
x2idn.32xlarge	128	2048.00
x2idn.metal	128	2048.00
x2iedn.xlarge	4	128.00
x2iedn.2xlarge	8	256.00
x2iedn.4xlarge	16	512.00
x2iedn.8xlarge	32	1024.00
x2iedn.16xlarge	64	2048.00
x2iedn.24xlarge	96	3072.00
x2iedn.32xlarge	128	4096.00
x2iedn.metal	128	4096.00
x2iezn.2xlarge	8	256.00
x2iezn.4xlarge	16	512.00
x2iezn.6xlarge	24	768.00
x2iezn.8xlarge	32	1024.00
x2iezn.12xlarge	48	1536.00
x2iezn.metal	48	1536.00
x1e.xlarge	4	122.00
x1e.2xlarge	8	244.00
x1e.4xlarge	16	488.00
x1e.8xlarge	32	976.00
x1e.16xlarge	64	1952.00
x1e.32xlarge	128	3904.00

实例类型	默认 vCPU	内存（GiB）
z1d.large	2	16.00
z1d.xlarge	4	32.00
z1d.2xlarge	8	64.00
z1d.3xlarge	12	96.00
z1d.6xlarge	24	192.00
z1d.12xlarge	48	384.00
z1d.metal	48	384.00

* 每个逻辑处理器都是 224 个内核上的一个超线程。

内存优化的实例使用以下处理器。

Amazon Graviton 处理器

- Amazon Graviton2：R6g、R6gd、X2gd

AMD 处理器

- AMD EPYC 7000 系列处理器（AMD EPYC 7571）：R5a、R5ad
- 第三代 AMD EPYC 处理器 (AMD EPYC 7R13)：R6a

英特尔处理器

- 英特尔至强可扩展处理器（Haswell E7-8880 v3）：X1、X1e
- 英特尔至强可扩展处理器（Broadwell E5-2686 v4）：R4
- 英特尔至强可扩展处理器（Skylake 8151）：z1d
- 英特尔至强可扩展处理器（Skylake 8175M 或 Cascade Lake 8259CL）：R5、R5d
- 第二代英特尔至强可扩展处理器（Cascade Lake 8259CL）：R5b、R5n
- 第二代英特尔至强可扩展处理器（Cascade Lake 8252C）：X2iezn
- 第三代英特尔至强可扩展处理器（Ice Lake 8375C）：R6i、R6id、X2idn、X2iedn

有关更多信息，请参阅 Amazon EC2 实例类型。

内存性能

X1 实例包括英特尔可扩展内存缓冲区，从而提供了 300 GiB/s 的可持续内存读取带宽和 140 GiB/s 的可持续内存写入带宽。

有关可以为内存优化型实例启用多少 RAM 的更多信息，请参阅硬件规格 (p. 324)。

内存优化型实例拥有增强型内存，并且需要 64 位 HVM AMI 才能利用这一容量。与内存优化型实例上的半虚拟化 (PV) AMI 相比，HVM AMI 可提供卓越的性能。有关更多信息，请参阅 Linux AMI 虚拟化类型 (p. 106)。

实例性能

内存优化型实例通过最新的 Intel AES-NI 功能实现更高的加密性能，并支持高级矢量扩展 2 (Intel AVX2) 处理器指令，以将大多数整数命令扩展到 256 位。

一些内存优化型实例提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处于非活动状态时可以进入的睡眠级别，而 P 状态控制核心所需的性能 (通过 CPU 频率来测量)。有关更多信息，请参阅您的 EC2 实例的处理器状态控制 (p. 707)。

网络性能

您可以为受支持的实例类型启用增强联网，以提供更低的延迟、更低的网络抖动和更高的每秒数据包数 (PPS) 性能。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。

以下是支持增强联网的内存优化型实例的网络性能摘要。

> **Note**
>
> 标有 † 的实例类型具备基准带宽，并且可以通过网络输入/输出积分机制，尽可能将其基准带宽突增到基准以上。有关更多信息，请参阅实例网络带宽 (p. 1141)。

实例类型	网络性能	增强联网功能
hpc6id.32xlarge	200Gb	ENA | EFA
r3.large †	中	不支持
r3.xlarge †	中	不支持
r3.2xlarge †	高	不支持
r3.4xlarge †	高	不支持
r3.8xlarge †	10Gb	不支持
r4.large †	高达 10Gb	ENA
r4.xlarge †	高达 10Gb	ENA
r4.2xlarge †	高达 10Gb	ENA
r4.4xlarge †	高达 10Gb	ENA
r4.8xlarge	10Gb	ENA
r4.16xlarge	25Gb	ENA
r5.large †	高达 10Gb	ENA
r5.xlarge †	高达 10Gb	ENA
r5.2xlarge †	高达 10Gb	ENA
r5.4xlarge †	高达 10Gb	ENA
r5.8xlarge	10Gb	ENA
r5.12xlarge	12Gb	ENA
r5.16xlarge	20Gb	ENA

实例类型	网络性能	增强联网功能
r5.24xlarge	25Gb	ENA
r5.metal	25Gb	ENA
r5a.large †	高达 10Gb	ENA
r5a.xlarge †	高达 10Gb	ENA
r5a.2xlarge †	高达 10Gb	ENA
r5a.4xlarge †	高达 10Gb	ENA
r5a.8xlarge †	高达 10Gb	ENA
r5a.12xlarge	10Gb	ENA
r5a.16xlarge	12Gb	ENA
r5a.24xlarge	20Gb	ENA
r5ad.large †	高达 10Gb	ENA
r5ad.xlarge †	高达 10Gb	ENA
r5ad.2xlarge †	高达 10Gb	ENA
r5ad.4xlarge †	高达 10Gb	ENA
r5ad.8xlarge †	高达 10Gb	ENA
r5ad.12xlarge	10Gb	ENA
r5ad.16xlarge	12Gb	ENA
r5ad.24xlarge	20Gb	ENA
r5b.large †	高达 10Gb	ENA
r5b.xlarge †	高达 10Gb	ENA
r5b.2xlarge †	高达 10Gb	ENA
r5b.4xlarge †	高达 10Gb	ENA
r5b.8xlarge	10Gb	ENA
r5b.12xlarge	12Gb	ENA
r5b.16xlarge	20Gb	ENA
r5b.24xlarge	25Gb	ENA
r5b.metal	25Gb	ENA
r5d.large †	高达 10Gb	ENA
r5d.xlarge †	高达 10Gb	ENA
r5d.2xlarge †	高达 10Gb	ENA
r5d.4xlarge †	高达 10Gb	ENA

实例类型	网络性能	增强联网功能
r5d.8xlarge	10Gb	ENA
r5d.12xlarge	12Gb	ENA
r5d.16xlarge	20Gb	ENA
r5d.24xlarge	25Gb	ENA
r5d.metal	25Gb	ENA
r5dn.large †	高达 25Gb	ENA
r5dn.xlarge †	高达 25Gb	ENA
r5dn.2xlarge †	高达 25Gb	ENA
r5dn.4xlarge †	高达 25Gb	ENA
r5dn.8xlarge	25Gb	ENA
r5dn.12xlarge	50Gb	ENA
r5dn.16xlarge	75Gb	ENA
r5dn.24xlarge	100Gb	ENA | EFA
r5dn.metal	100Gb	ENA | EFA
r5n.large †	高达 25Gb	ENA
r5n.xlarge †	高达 25Gb	ENA
r5n.2xlarge †	高达 25Gb	ENA
r5n.4xlarge †	高达 25Gb	ENA
r5n.8xlarge	25Gb	ENA
r5n.12xlarge	50Gb	ENA
r5n.16xlarge	75Gb	ENA
r5n.24xlarge	100Gb	ENA | EFA
r5n.metal	100Gb	ENA | EFA
r6a.large †	高达 12.5Gb	ENA
r6a.xlarge †	高达 12.5Gb	ENA
r6a.2xlarge †	高达 12.5Gb	ENA
r6a.4xlarge †	高达 12.5Gb	ENA
r6a.8xlarge	12.5Gb	ENA
r6a.12xlarge	18.75Gb	ENA
r6a.16xlarge	25Gb	ENA
r6a.24xlarge	37.5Gb	ENA

实例类型	网络性能	增强联网功能
r6a.32xlarge	50Gb	ENA
r6a.48xlarge	50Gb	ENA | EFA
r6a.metal	50Gb	ENA | EFA
r6g.medium †	高达 10Gb	ENA
r6g.large †	高达 10Gb	ENA
r6g.xlarge †	高达 10Gb	ENA
r6g.2xlarge †	高达 10Gb	ENA
r6g.4xlarge †	高达 10Gb	ENA
r6g.8xlarge	12Gb	ENA
r6g.12xlarge	20Gb	ENA
r6g.16xlarge	25Gb	ENA
r6g.metal	25Gb	ENA
r6gd.medium †	高达 10Gb	ENA
r6gd.large †	高达 10Gb	ENA
r6gd.xlarge †	高达 10Gb	ENA
r6gd.2xlarge †	高达 10Gb	ENA
r6gd.4xlarge †	高达 10Gb	ENA
r6gd.8xlarge	12Gb	ENA
r6gd.12xlarge	20Gb	ENA
r6gd.16xlarge	25Gb	ENA
r6gd.metal	25Gb	ENA
r6i.large †	高达 12.5Gb	ENA
r6i.xlarge †	高达 12.5Gb	ENA
r6i.2xlarge †	高达 12.5Gb	ENA
r6i.4xlarge †	高达 12.5Gb	ENA
r6i.8xlarge	12.5Gb	ENA
r6i.12xlarge	18.75Gb	ENA
r6i.16xlarge	25Gb	ENA
r6i.24xlarge	37.5Gb	ENA
r6i.32xlarge	50Gb	ENA | EFA
r6i.metal	50Gb	ENA | EFA

实例类型	网络性能	增强联网功能
r6idn.large †	高达 25Gb	ENA
r6idn.xlarge †	高达 30Gb	ENA
r6idn.2xlarge †	高达 40Gb	ENA
r6idn.4xlarge †	高达 50Gb	ENA
r6idn.8xlarge	50Gb	ENA
r6idn.12xlarge	75Gb	ENA
r6idn.16xlarge	100Gb	ENA
r6idn.24xlarge	150Gb	ENA
r6idn.32xlarge	200Gb	ENA | EFA
r6idn.metal	200Gb	ENA | EFA
r6in.large †	高达 25Gb	ENA
r6in.xlarge †	高达 30Gb	ENA
r6in.2xlarge †	高达 40Gb	ENA
r6in.4xlarge †	高达 50Gb	ENA
r6in.8xlarge	50Gb	ENA
r6in.12xlarge	75Gb	ENA
r6in.16xlarge	100Gb	ENA
r6in.24xlarge	150Gb	ENA
r6in.32xlarge	200Gb	ENA | EFA
r6in.metal	200Gb	ENA | EFA
r6id.large †	高达 12.5Gb	ENA
r6id.xlarge †	高达 12.5Gb	ENA
r6id.2xlarge †	高达 12.5Gb	ENA
r6id.4xlarge †	高达 12.5Gb	ENA
r6id.8xlarge	12.5Gb	ENA
r6id.12xlarge	18.75Gb	ENA
r6id.16xlarge	25Gb	ENA
r6id.24xlarge	37.5Gb	ENA
r6id.32xlarge	50Gb	ENA | EFA
r6id.metal	50Gb	ENA | EFA
r7g.medium †	高达 12.5Gb	ENA

实例类型	网络性能	增强联网功能
r7g.large †	高达 12.5Gb	ENA
r7g.xlarge †	高达 12.5Gb	ENA
r7g.2xlarge †	高达 15Gb	ENA
r7g.4xlarge †	高达 15Gb	ENA
r7g.8xlarge	15Gb	ENA
r7g.12xlarge	22.5Gb	ENA
r7g.16xlarge	30Gb	ENA | EFA
r7g.metal	30Gb	ENA | EFA
u-3tb1.56xlarge	50Gb	ENA
u-6tb1.56xlarge	100Gb	ENA
u-6tb1.112xlarge	100Gb	ENA
u-6tb1.metal	100	ENA
u-9tb1.112xlarge	100Gb	ENA
u-9tb1.metal	100	ENA
u-12tb1.112xlarge	100Gb	ENA
u-12tb1.metal	100	ENA
u-18tb1.metal	100Gb	ENA
u-24tb1.metal	100Gb	ENA
x1.16xlarge	10Gb	ENA
x1.32xlarge	25Gb	ENA
x2gd.medium †	高达 10Gb	ENA
x2gd.large †	高达 10Gb	ENA
x2gd.xlarge †	高达 10Gb	ENA
x2gd.2xlarge †	高达 10Gb	ENA
x2gd.4xlarge †	高达 10Gb	ENA
x2gd.8xlarge	12Gb	ENA
x2gd.12xlarge	20Gb	ENA
x2gd.16xlarge	25Gb	ENA
x2gd.metal	25Gb	ENA
x2idn.16xlarge	50Gb	ENA
x2idn.24xlarge	75Gb	ENA

实例类型	网络性能	增强联网功能
x2idn.32xlarge	100Gb	ENA | EFA
x2idn.metal	100Gb	ENA | EFA
x2iedn.xlarge †	高达 25Gb	ENA
x2iedn.2xlarge †	高达 25Gb	ENA
x2iedn.4xlarge †	高达 25Gb	ENA
x2iedn.8xlarge	25Gb	ENA
x2iedn.16xlarge	50Gb	ENA
x2iedn.24xlarge	75Gb	ENA
x2iedn.32xlarge	100Gb	ENA | EFA
x2iedn.metal	100Gb	ENA | EFA
x2iezn.2xlarge †	高达 25Gb	ENA
x2iezn.4xlarge †	高达 25Gb	ENA
x2iezn.6xlarge	50Gb	ENA
x2iezn.8xlarge	75Gb	ENA
x2iezn.12xlarge	100Gb	ENA | EFA
x2iezn.metal	100Gb	ENA | EFA
x1e.xlarge †	高达 10Gb	ENA
x1e.2xlarge †	高达 10Gb	ENA
x1e.4xlarge †	高达 10Gb	ENA
x1e.8xlarge †	高达 10Gb	ENA
x1e.16xlarge	10Gb	ENA
x1e.32xlarge	25Gb	ENA
z1d.large †	高达 10Gb	ENA
z1d.xlarge †	高达 10Gb	ENA
z1d.2xlarge †	高达 10Gb	ENA
z1d.3xlarge †	高达 10Gb	ENA
z1d.6xlarge	12Gb	ENA
z1d.12xlarge	25Gb	ENA
z1d.metal	25Gb	ENA

对于支持 200Gbps 的 32xlarge 和 metal 实例类型，实例上至少需要 2 个 ENI，并且每个 ENI 需要连接到不同的网卡，才能达到 200Gbps 的吞吐量。连接到网卡的每个 ENI 最大可达到 170Gbps。

2020 年 3 月 12 日之后启动的 u-6tb1.metal、u-9tb1.metal 和 u-12tb1.metal 实例提供 100 Gbps 网络性能，而 2020 年 3 月 12 日之前启动的 u-6tb1.metal、u-9tb1.metal 和 u-12tb1.metal 实例可能仅提供 25 Gbps 网络性能。要确保在 2020 年 3 月 12 日之前启动的实例具有100 Gbps 网络性能，请与客户团队联系以免费升级实例。

下表显示了实例类型的基准带宽和突增带宽，这些实例类型通过网络输入/输出积分机制将其基准带宽突增到基准以上。

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
r3.large	0.5	1.2
r3.xlarge	0.7	2.8
r3.2xlarge	1.0	10.0
r3.4xlarge	2.0	10.0
r3.8xlarge	5.0	10.0
r4.large	0.75	10.0
r4.xlarge	1.25	10.0
r4.2xlarge	2.5	10.0
r4.4xlarge	5.0	10.0
r5.large	0.75	10.0
r5.xlarge	1.25	10.0
r5.2xlarge	2.5	10.0
r5.4xlarge	5.0	10.0
r5a.large	0.75	10.0
r5a.xlarge	1.25	10.0
r5a.2xlarge	2.5	10.0
r5a.4xlarge	5.0	10.0
r5a.8xlarge	7.5	10.0
r5ad.large	0.75	10.0
r5ad.xlarge	1.25	10.0
r5ad.2xlarge	2.5	10.0
r5ad.4xlarge	5.0	10.0
r5ad.8xlarge	7.5	10.0
r5b.large	0.75	10.0
r5b.xlarge	1.25	10.0
r5b.2xlarge	2.5	10.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
r5b.4xlarge	5.0	10.0
r5d.large	0.75	10.0
r5d.xlarge	1.25	10.0
r5d.2xlarge	2.5	10.0
r5d.4xlarge	5.0	10.0
r5dn.large	2.1	25.0
r5dn.xlarge	4.1	25.0
r5dn.2xlarge	8.125	25.0
r5dn.4xlarge	16.25	25.0
r5n.large	2.1	25.0
r5n.xlarge	4.1	25.0
r5n.2xlarge	8.125	25.0
r5n.4xlarge	16.25	25.0
r6a.large	0.781	12.5
r6a.xlarge	1.562	12.5
r6a.2xlarge	3.125	12.5
r6a.4xlarge	6.25	12.5
r6g.medium	0.5	10.0
r6g.large	0.75	10.0
r6g.xlarge	1.25	10.0
r6g.2xlarge	2.5	10.0
r6g.4xlarge	5.0	10.0
r6gd.medium	0.5	10.0
r6gd.large	0.75	10.0
r6gd.xlarge	1.25	10.0
r6gd.2xlarge	2.5	10.0
r6gd.4xlarge	5.0	10.0
r6i.large	0.781	12.5
r6i.xlarge	1.562	12.5
r6i.2xlarge	3.125	12.5
r6i.4xlarge	6.25	12.5

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
r6idn.large	3.125	25.0
r6idn.xlarge	6.25	30.0
r6idn.2xlarge	12.5	40.0
r6idn.4xlarge	25.0	50.0
r6in.large	3.125	25.0
r6in.xlarge	6.25	30.0
r6in.2xlarge	12.5	40.0
r6in.4xlarge	25.0	50.0
r6id.large	0.781	12.5
r6id.xlarge	1.562	12.5
r6id.2xlarge	3.125	12.5
r6id.4xlarge	6.25	12.5
r7g.medium	0.52	12.5
r7g.large	0.937	12.5
r7g.xlarge	1.876	12.5
r7g.2xlarge	3.75	15.0
r7g.4xlarge	7.5	15.0
x2gd.medium	0.5	10.0
x2gd.large	0.75	10.0
x2gd.xlarge	1.25	10.0
x2gd.2xlarge	2.5	10.0
x2gd.4xlarge	5.0	10.0
x2iedn.xlarge	1.875	25.0
x2iedn.2xlarge	5.0	25.0
x2iedn.4xlarge	12.5	25.0
x2iezn.2xlarge	12.5	25.0
x2iezn.4xlarge	15.0	25.0
x1e.xlarge	0.625	10.0
x1e.2xlarge	1.25	10.0
x1e.4xlarge	2.5	10.0
x1e.8xlarge	5.0	10.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
z1d.large	0.75	10.0
z1d.xlarge	1.25	10.0
z1d.2xlarge	2.5	10.0
z1d.3xlarge	5.0	10.0

Amazon EBS I/O 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 Amazon EBS 卷提供最佳性能。

有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

基于 SSD 的实例存储卷的 I/O 性能

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您最高可以获得下表所列的 IOPS（4096 字节的数据块大小）性能（在队列深度饱和时）。否则，您将获得较低的 IOPS 性能。

实例大小	100% 随机读取 IOPS	写入 IOPS
hpc6id.32xlarge	2,146,664	1,073,336
r5ad.large	30000	15000
r5ad.xlarge	59,000	29,000
r5ad.2xlarge	117,000	57,000
r5ad.4xlarge	234,000	114,000
r5ad.8xlarge	466666	233333
r5ad.12xlarge	700,000	340,000
r5ad.16xlarge	933333	466666
r5ad.24xlarge	1400000	680,000
r5d.large	30000	15000
r5d.xlarge	59,000	29,000
r5d.2xlarge	117,000	57,000
r5d.4xlarge	234,000	114,000
r5d.8xlarge	466666	233333
r5d.12xlarge	700,000	340,000
r5d.16xlarge	933333	466666
r5d.24xlarge	1400000	680,000
r5d.metal	1400000	680,000

实例大小	100% 随机读取 IOPS	写入 IOPS
r5dn.large	30000	15000
r5dn.xlarge	59,000	29,000
r5dn.2xlarge	117,000	57,000
r5dn.4xlarge	234,000	114,000
r5dn.8xlarge	466666	233333
r5dn.12xlarge	700,000	340,000
r5dn.16xlarge	933333	466666
r5dn.24xlarge	1400000	680,000
r5dn.metal	1400000	680,000
r6id.metal	3,219,995	1,610,005
r6gd.medium	13438	5625
r6gd.large	26875	11250
r6gd.xlarge	53750	22500
r6gd.2xlarge	107500	45000
r6gd.4xlarge	215000	90000
r6gd.8xlarge	430000	180,000
r6gd.12xlarge	645000	270000
r6gd.16xlarge	860000	360,000
r6gd.metal	860000	360,000
r6id.large	33,542	16,771
r6id.xlarge	67,083	33,542
r6id.2xlarge	134,167	67,084
r6id.4xlarge	268,333	134,167
r6id.8xlarge	536,666	268,334
r6id.12xlarge	804,999	402,501
r6id.16xlarge	1,073,332	536,668
r6id.24xlarge	1,609,998	805,002
r6id.32xlarge	2,146,664	1,073,336
r6id.metal	2,146,664	1,073,336
r6idn.large	33,542	16,771
r6idn.xlarge	67,083	33,542

实例大小	100% 随机读取 IOPS	写入 IOPS
r6idn.2xlarge	134,167	67,084
r6idn.4xlarge	268,333	134,167
r6idn.8xlarge	536,666	268,334
r6idn.12xlarge	804,999	402,501
r6idn.16xlarge	1,073,332	536,668
r6idn.24xlarge	1,609,998	805,002
r6idn.32xlarge	2,146,664	1,073,336
r6idn.metal	2,146,664	1,073,336
x2gd.medium	13438	5625
x2gd.large	26875	11250
x2gd.xlarge	53750	22500
x2gd.2xlarge	107500	45000
x2gd.4xlarge	215000	90000
x2gd.8xlarge	430000	180,000
x2gd.12xlarge	645000	270000
x2gd.16xlarge	860000	360,000
x2gd.metal	860000	360,000
x2idn.16xlarge	430000	180,000
x2idn.24xlarge	645000	270000
x2idn.32xlarge	860000	360,000
x2idn.metal	860000	360,000
x2iedn.xlarge	26875	11250
x2iedn.2xlarge	53750	22500
x2iedn.4xlarge	107500	45000
x2iedn.8xlarge	215000	90000
x2iedn.16xlarge	430000	180,000
x2iedn.24xlarge	645000	270000
x2iedn.32xlarge	860000	360,000
x2iedn.metal	860000	360,000
z1d.large	30000	15000
z1d.xlarge	59,000	29,000

实例大小	100% 随机读取 IOPS	写入 IOPS
z1d.2xlarge	117,000	57,000
z1d.3xlarge	175000	75000
z1d.6xlarge	350,000	170,000
z1d.12xlarge	700,000	340,000
z1d.metal	700,000	340,000

随着您不断在您的实例的基于 SSD 的实例存储卷中填充数据，您可以达到的写入 IOPS 将不断减少。这是因为，SSD 控制器必须执行额外的工作，即查找可用空间、重写现有数据，以及擦除未使用的空间以使之可供重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为 实例提供的基于 SSD 的实例存储卷不会为超额配置预保留空白间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。

支持 个 vCPU

内存优化型实例具有大量虚拟 vCPU，可能会在虚拟 vCPU 数量上限较低的操作系统上导致启动问题。我们强烈建议您在启动内存优化型实例时使用最新的 AMI。

以下 AMI 支持启动内存优化型实例：

- Amazon Linux 2 (HVM)
- Amazon Linux AMI 2016.03 (HVM) 或更高版本
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 SP1 (HVM)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 64 位
- Windows Server 2008 SP2 64 位

发布说明

- 基于 Nitro 系统构建的实例具有以下要求：
  - 必须安装有 NVMe 驱动程序 (p. 1518)。
  - 必须安装有 Elastic Network Adapter (ENA) (p. 1143) 驱动程序。

以下 Linux AMI 满足这些要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

  Note

  Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

- 具有 Amazon Graviton 处理器的实例具有以下要求：
  - 使用适用于 64 位 Arm 架构的 AMI。
  - 支持通过带有 ACPI 表的 UEFI 进行引导，以及支持 ACPI 热插拔 PCI 设备。

  以下 AMI 满足这些要求：
  - Amazon Linux 2（64 位 Arm）
  - Ubuntu 16.04 或更高版本（64 位 Arm）
  - Red Hat Enterprise Linux 8.0 或更高版本（64 位 Arm）
  - SUSE Linux Enterprise Server 15 或更高版本（64 位 Arm）
  - Debian 10 或更高版本（64 位 Arm）
- 为了从 R6i 实例获得最佳性能，请确保它们的 ENA 驱动程序版本为 2.2.9 或更高版本。将早于 1.2 版本的 ENA 驱动程序用于这些实例会导致网络接口连接失败。以下 AMI 具备兼容的 ENA 驱动程序。
  - 内核版本为 4.14.186 的 Amazon Linux 2
  - 内核版本为 5.4.0-1025-aws 的 Ubuntu 20.04
  - 内核版本为 4.18.0-240.1.1.el8_3.ARCH 的 Red Hat Enterprise Linux 8.3
  - 内核版本为 5.3.18-24.15.1 的 SUSE Linux Enterprise Server 15 SP2
- 在 Nitro 系统实例上构建的实例最多支持 28 个附加项，包括网络接口、EBS 卷和 NVMe 实例存储卷。有关更多信息，请参阅Nitro 系统卷限制 (p. 1607)。
- 在启动过程中或启动之后，附加到 C6a、C6in、C7g、M6a、M6in、M6idn、M7g、R5b、R6in、R6idn、R7g、Trn1、X2idn 和 X2iedn 实例的所有 `io2` 卷会在 EBS Block Express 上自动运行。有关更多信息，请参阅 io2 Block Express 卷。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 除了 `x1.16xlarge` 实例之外，您无法使用 Windows Server 2008 SP2 64 位 AMI 启动 X1 实例。
- 您无法使用 Windows Server 2008 SP2 64 位 AMI 启动 X1e 实例。
- 对于 Windows Server 2008 R2 64 位 AMI 的早期版本，您无法启动 `r4.large` 和 `r4.4xlarge` 实例。如果遇到此问题，请更新至该 AMI 的最新版本。

- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅 Amazon EC2 常见问题解答中的我可以在 Amazon EC2 中运行多少个实例？。

存储优化型实例

存储优化型实例适用于需要对本地存储上的极大型数据集进行高性能顺序读写访问的工作负载。它们经过了优化，可以向应用程序提供每秒上万次低延迟性随机 I/O 操作 (IOPS)。有关更多信息，包括所使用的技术，请参阅 Amazon EC2 Instance Type Details（Amazon EC2 实例类型详细信息）页面。

D2 实例

这些实例非常适合以下用途：

- 大规模并行处理 (MPP) 数据仓库
- MapReduce 和 Hadoop 分布式计算
- 日志或数据处理应用程序

D3 和 D3en 实例

这些实例提供了实例存储扩展，非常适合以下用途：

- 适用于 Hadoop 工作负载的分布式文件系统
- 文件存储工作负载，如 GPFC 和 BeeFS
- 适用于 HPC 工作负载的大型数据湖

H1 实例

这些实例非常适合以下用途：

- 数据密集型工作负载，例如，MapReduce 和分布式文件系统
- 需要顺序访问直接附加的实例存储上的大量数据的应用程序
- 需要以高吞吐量方式访问大量数据的应用程序

I3 和 I3en 实例

这些实例非常适合以下用途：

- 高频率联机事务处理 (OLTP) 系统
- 关系数据库
- NoSQL 数据库
- 内存中数据库 (例如，Redis) 的缓存
- 数据仓库应用程序
- 分布式文件系统

裸机实例为应用程序提供对主机服务器的物理资源（如处理器和内存）的直接访问。

I4i 实例

这些实例非常适合存在大量输入/输出的工作负载，这类工作负载需要使用本地存储上的中小型数据集（例如事务数据库和 NoSQL 数据库）。

Im4gn 实例

这些实例非常适合在低延迟下需要高随机输入/输出性能的工作负载，例如：

- 关系数据库
- NoSQL 数据库
- 搜索
- 分布式文件系统

Is4gen 实例

这些实例非常适合在低延迟下需要高随机输入/输出性能的工作负载，例如：

- NoSQL 数据库
- 索引
- 流式处理
- 缓存
- 热存储

目录

- 硬件规格 (p. 348)
- 实例性能 (p. 350)
- 网络性能 (p. 351)
- Amazon EBS I/O 性能 (p. 354)
- 基于 SSD 的实例存储卷的 I/O 性能 (p. 354)
- 支持 个 vCPU (p. 356)
- 发布说明 (p. 357)

硬件规格

以下是存储优化型实例的硬件规格摘要。虚拟中央处理单元（vCPU）表示分配给虚拟机（VM）的物理 CPU 的一部分。对于 x86 实例，每个内核有两个 vCPU。对于 Graviton 实例，每个内核有一个 vCPU。

实例类型	默认 vCPU	内存（GiB）
d2.xlarge	4	30.50
d2.2xlarge	8	61.00
d2.4xlarge	16	122.00
d2.8xlarge	36	244.00
d3.xlarge	4	32.00
d3.2xlarge	8	64.00
d3.4xlarge	16	128.00
d3.8xlarge	32	256.00
d3en.xlarge	4	16.00

实例类型	默认 vCPU	内存（GiB）
d3en.2xlarge	8	32.00
d3en.4xlarge	16	64.00
d3en.6xlarge	24	96.00
d3en.8xlarge	32	128.00
d3en.12xlarge	48	192.00
h1.2xlarge	8	32.00
h1.4xlarge	16	64.00
h1.8xlarge	32	128.00
h1.16xlarge	64	256.00
hs1.8xlarge	16	117.00
i2.xlarge	4	30.50
i2.2xlarge	8	61.00
i2.4xlarge	16	122.00
i2.8xlarge	32	244.00
i3.large	2	15.25
i3.xlarge	4	30.50
i3.2xlarge	8	61.00
i3.4xlarge	16	122.00
i3.8xlarge	32	244.00
i3.16xlarge	64	488.00
i3.metal	72	512.00
i3en.large	2	16.00
i3en.xlarge	4	32.00
i3en.2xlarge	8	64.00
i3en.3xlarge	12	96.00
i3en.6xlarge	24	192.00
i3en.12xlarge	48	384.00
i3en.24xlarge	96	768.00
i3en.metal	96	768.00
i4i.large	2	16.00
i4i.xlarge	4	32.00

实例类型	默认 vCPU	内存（GiB）
i4i.2xlarge	8	64.00
i4i.4xlarge	16	128.00
i4i.8xlarge	32	256.00
i4i.16xlarge	64	512.00
i4i.32xlarge	128	1024.00
i4i.metal	128	1024.00
im4gn.large	2	8.00
im4gn.xlarge	4	16.00
im4gn.2xlarge	8	32.00
im4gn.4xlarge	16	64.00
im4gn.8xlarge	32	128.00
im4gn.16xlarge	64	256.00
is4gen.medium	1	6.00
is4gen.large	2	12.00
is4gen.xlarge	4	24.00
is4gen.2xlarge	8	48.00
is4gen.4xlarge	16	96.00
is4gen.8xlarge	32	192.00

存储优化的实例使用以下处理器。

Amazon Graviton 处理器

- Amazon Graviton2：Im4gn、Is4gen

英特尔处理器

- 英特尔至强可扩展处理器（Haswell E5-2676 v3）：D2
- 英特尔至强可扩展处理器（Broadwell E5-2686 v4）：H1、I3
- 英特尔至强可扩展处理器（Skylake 8175M 或 Cascade Lake 8259CL）：I3en
- 第二代英特尔至强可扩展处理器（Cascade Lake 8259CL）：D3、D3en
- 第三代英特尔至强可扩展处理器（Ice Lake 8375C）：I4i

有关更多信息，请参阅 Amazon EC2 实例类型。

实例性能

要确保 Linux 上的实例实现最佳磁盘吞吐量性能，建议您使用最新版本的 Amazon Linux 2 或 Amazon Linux AMI。

对于具有 NVMe 实例存储卷的实例，您必须使用内核版本为 4.4 或更高版本的 Linux AMI。否则，您的实例将无法实现可用的最大 IOPS 性能。

如果使用可支持持久授予 (可显著提高磁盘吞吐量和可扩展性的 Xen 数据块环协议的扩展) 的 Linux 内核，D2 实例可提供最佳磁盘性能。有关持久授予的更多信息，请参阅 Xen 项目博客中的文章。

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。有些存储优化型实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

有些存储优化型实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅您的 EC2 实例的处理器状态控制 (p. 707)。

网络性能

您可以为受支持的实例类型启用增强联网，以提供更低的延迟、更低的网络抖动和更高的每秒数据包数 (PPS) 性能。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。

以下是支持增强联网的存储优化型实例的网络性能摘要。

Note

标有 † 的实例类型具备基准带宽，并且可以通过网络输入/输出积分机制，尽可能将其基准带宽突增到基准以上。有关更多信息，请参阅实例网络带宽 (p. 1141)。

实例类型	网络性能	增强联网功能
d2.xlarge †	中	不支持
d2.2xlarge †	高	不支持
d2.4xlarge †	高	不支持
d2.8xlarge †	10Gb	不支持
d3.xlarge †	高达 15Gb	ENA
d3.2xlarge †	高达 15Gb	ENA
d3.4xlarge †	高达 15Gb	ENA
d3.8xlarge	25Gb	ENA
d3en.xlarge †	高达 25Gb	ENA
d3en.2xlarge †	高达 25Gb	ENA
d3en.4xlarge	25Gb	ENA
d3en.6xlarge	40Gb	ENA
d3en.8xlarge	50Gb	ENA
d3en.12xlarge	75Gb	ENA
h1.2xlarge †	高达 10Gb	ENA
h1.4xlarge †	高达 10Gb	ENA
h1.8xlarge	10Gb	ENA

实例类型	网络性能	增强联网功能
h1.16xlarge	25Gb	ENA
i2.xlarge †	中	不支持
i2.2xlarge †	高	不支持
i2.4xlarge †	高	不支持
i2.8xlarge †	10Gb	不支持
i3.large †	高达 10Gb	ENA
i3.xlarge †	高达 10Gb	ENA
i3.2xlarge †	高达 10Gb	ENA
i3.4xlarge †	高达 10Gb	ENA
i3.8xlarge	10Gb	ENA
i3.16xlarge	25Gb	ENA
i3.metal	25Gb	ENA
i3en.large †	高达 25Gb	ENA
i3en.xlarge †	高达 25Gb	ENA
i3en.2xlarge †	高达 25Gb	ENA
i3en.3xlarge †	高达 25Gb	ENA
i3en.6xlarge	25Gb	ENA
i3en.12xlarge	50Gb	ENA | EFA
i3en.24xlarge	100Gb	ENA | EFA
i3en.metal	100Gb	ENA | EFA
i4i.large †	高达 10Gb	ENA
i4i.xlarge †	高达 10Gb	ENA
i4i.2xlarge †	高达 12Gb	ENA
i4i.4xlarge †	高达 25Gb	ENA
i4i.8xlarge	18.75Gb	ENA
i4i.16xlarge	37.5Gb	ENA
i4i.32xlarge	75Gb	ENA | EFA
i4i.metal	75Gb	ENA | EFA
im4gn.large †	高达 25Gb	ENA
im4gn.xlarge †	高达 25Gb	ENA
im4gn.2xlarge †	高达 25Gb	ENA

实例类型	网络性能	增强联网功能
im4gn.4xlarge	25Gb	ENA
im4gn.8xlarge	50Gb	ENA
im4gn.16xlarge	100Gb	ENA | EFA
is4gen.medium †	高达 25Gb	ENA
is4gen.large †	高达 25Gb	ENA
is4gen.xlarge †	高达 25Gb	ENA
is4gen.2xlarge †	高达 25Gb	ENA
is4gen.4xlarge	25Gb	ENA
is4gen.8xlarge	50Gb	ENA

下表显示了实例类型的基准带宽和突增带宽，这些实例类型通过网络输入/输出积分机制将其基准带宽突增到基准以上。

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
d2.xlarge	1.25	2.8
d2.2xlarge	2.5	10.0
d2.4xlarge	5.0	10.0
d2.8xlarge	5.0	10.0
d3.xlarge	3.0	15.0
d3.2xlarge	6.0	15.0
d3.4xlarge	12.5	15.0
d3en.xlarge	6.0	25.0
d3en.2xlarge	12.5	25.0
h1.2xlarge	2.5	10.0
h1.4xlarge	5.0	10.0
i2.xlarge	0.7	2.8
i2.2xlarge	1.0	10.0
i2.4xlarge	2.0	10.0
i2.8xlarge	5.0	10.0
i3.large	0.75	10.0
i3.xlarge	1.25	10.0
i3.2xlarge	2.5	10.0

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
i3.4xlarge	5.0	10.0
i3en.large	2.1	25.0
i3en.xlarge	4.2	25.0
i3en.2xlarge	8.4	25.0
i3en.3xlarge	12.5	25.0
i4i.large	0.781	10.0
i4i.xlarge	1.875	10.0
i4i.2xlarge	4.687	12.0
i4i.4xlarge	9.375	25.0
im4gn.large	3.125	25.0
im4gn.xlarge	6.25	25.0
im4gn.2xlarge	12.5	25.0
is4gen.medium	1.562	25.0
is4gen.large	3.125	25.0
is4gen.xlarge	6.25	25.0
is4gen.2xlarge	12.5	25.0

Amazon EBS I/O 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 Amazon EBS 卷提供最佳性能。

有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

基于 SSD 的实例存储卷的 I/O 性能

D2、D3 和 D3en 实例的主要数据存储是 HDD 实例存储卷。I3 和 I3en 实例的主要数据存储是非易失性存储规范 (NVMe) SSD 实例存储卷。

实例存储卷仅在实例生命周期内保留。当您停止、休眠或终止某个实例时，其实例存储卷中的应用程序和数据会被擦除。我们建议您定期备份或复制实例存储卷中的重要数据。有关更多信息，请参阅 Amazon EC2 实例存储 (p. 1579) 和 SSD 实例存储卷 (p. 1596)：

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您最高可以获得下表所列的 IOPS（4096 字节的数据块大小）性能（在队列深度饱和时）。否则，您将获得较低的 IOPS 性能。

实例大小	100% 随机读取 IOPS	写入 IOPS
i3.large	100,125	35000
i3.xlarge	206,250	70,000

实例大小	100% 随机读取 IOPS	写入 IOPS
i3.2xlarge	412,500	180,000
i3.4xlarge	825,000	360,000
i3.8xlarge	1650,000	720,000
i3.16xlarge	3,300,000	1400000
i3.metal	3,300,000	1400000
i3en.large	42,500	32,500
i3en.xlarge	85,000	65000
i3en.2xlarge	170,000	130,000
i3en.3xlarge	250,000	200,000
i3en.6xlarge	500,000	400,000
i3en.12xlarge	1000000	800,000
i3en.24xlarge	2,000,000	1,600,000
i3en.metal	2,000,000	1,600,000
i4i.large	50000	27,500
i4i.xlarge	100000	55,000
i4i.2xlarge	200,000	110,000
i4i.4xlarge	400,000	220,000
i4i.8xlarge	800,000	440,000
i4i.16xlarge	1,600,000	880,000
i4i.32xlarge	3,200,000	1,760,000
i4i.metal	3,200,000	1,760,000
im4gn.large	31,250	25000
im4gn.xlarge	62,000	50000
im4gn.2xlarge	125,000	100000
im4gn.4xlarge	250,000	200,000
im4gn.8xlarge	500,000	400,000
im4gn.16xlarge	1000000	800,000
is4gen.medium	31,250	25000
is4gen.large	62,000	50000
is4gen.xlarge	125,000	100000
is4gen.2xlarge	250,000	200,000

实例大小	100% 随机读取 IOPS	写入 IOPS
is4gen.4xlarge	500,000	400,000
is4gen.8xlarge	1000000	800,000

在填充基于 SSD 的实例存储卷时，您获得的 I/O 性能将会下降。这是因为，SSD 控制器必须执行额外的工作以查找可用的空间，重写现有的数据，以及擦除未使用的空间以进行重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为 实例提供的基于 SSD 的实例存储卷不会为超额配置预保留空白间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。

有关支持实例存储卷的所有实例类型的卷大小比较，请参阅 Available instance store volumes (p. 1581)（可用的实例存储卷）表。

支持 个 vCPU

d2.8xlarge 实例类型提供了 36 个 vCPU，在某些 vCPU 数量限制为 32 个的 Linux 操作系统中可能会导致启动问题。强烈建议您在启动 d2.8xlarge 实例时，使用最新的 AMI。

以下 Linux AMI 支持启动具有 36 个 vCPU 的 d2.8xlarge 实例：

- Amazon Linux 2 (HVM)
- Amazon Linux AMI 2018.03 (HVM)
- Ubuntu Server 14.04 LTS (HVM) 或更高版本
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 (HVM)

如果必须为您的应用程序使用其他 AMI，并且您的 d2.8xlarge 实例启动未成功完成 (例如，如果您的实例状态在启动过程中因 stopped 状态转换原因而更改为 Client.InstanceInitiatedShutdown)，则请修改您的实例 (如以下过程所述) 以支持 32 个以上的 vCPU，以便能够使用 d2.8xlarge 实例类型。

更新实例以支持 32 个以上的 vCPU

1. 通过选择除 d2.8xlarge 以外的任何其他 D2 实例类型来使用您的 AMI 启动 D2 实例。
2. 遵照特定于操作系统的说明，将内核更新到最新版本。例如，对于 RHEL 6，使用以下命令：

   ```
   sudo yum update -y kernel
   ```

3. 停止实例。
4. (可选) 从可用于启动其他任何您将来所需的 d2.8xlarge 实例的实例创建 AMI。
5. 将已停止实例的实例类型更改为 d2.8xlarge [依次选择 Actions（操作）、Instance settings（实例设置）、Change instance type（更改实例类型），然后按照说明进行操作]。

6. 启动实例。如果实例正确启动，则您已完成操作。如果实例仍未正确启动，请继续执行下一个步骤。
7. (可选) 如果实例仍未正确启动，则实例上的内核可能不支持 32 个以上的 vCPU。但是，如果您限制 vCPU 的数量，则可能可以启动实例。

   a. 将已停止实例的实例类型更改为 d2.8xlarge 之外的任何 D2 实例类型 [依次选择 Actions（操作）、Instance settings（实例设置）、Change instance type（更改实例类型），然后按照说明进行操作]。

   b. 遵照特定于操作系统的说明，将 maxcpus=32 选项添加到您的启动内核参数。例如，对于 RHEL 6，编辑 /boot/grub/menu.lst 文件，并将以下选项添加到最近处于活动状态的 kernel 条目：

```
default=0
timeout=1
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-504.3.3.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-504.3.3.el6.x86_64 maxcpus=32 console=ttyS0 ro
 root=UUID=9996863e-b964-47d3-a33b-3920974fdbd9 rd_NO_LUKS  KEYBOARDTYPE=pc
 KEYTABLE=us LANG=en_US.UTF-8 xen_blkfront.sda_is_xvda=1 console=ttyS0,115200n8
 console=tty0 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto rd_NO_LVM
 rd_NO_DM
initrd /boot/initramfs-2.6.32-504.3.3.el6.x86_64.img
```

   c. 停止实例。

   d. (可选) 从可用于启动其他任何您将来所需的 d2.8xlarge 实例的实例创建 AMI。

   e. 将已停止实例的实例类型更改为 d2.8xlarge [依次选择 Actions（操作）、Instance settings（实例设置）、Change instance type（更改实例类型），然后按照说明进行操作]。

   f. 启动实例。

发布说明

- 基于 Nitro 系统 (p. 246)构建的实例具有以下要求：
  - 必须安装有 NVMe 驱动程序 (p. 1518)。
  - 必须安装有 Elastic Network Adapter (ENA) (p. 1143) 驱动程序。

  以下 Linux AMI 满足这些要求：
  - Amazon Linux 2
  - Amazon Linux AMI 2018.03
  - Ubuntu 14.04 或更高版本（采用 linux-aws 内核）

    Note

    Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 linux-aws 内核）
  - Red Hat Enterprise Linux 7.4 或更高版本
  - SUSE Linux Enterprise Server 12 SP2 或更高版本
  - CentOS 7.4.1708 或更高版本
  - FreeBSD 11.1 或更高版本
  - Debian GNU/Linux 9 或更高版本
- 具有 Amazon Graviton 处理器的实例具有以下要求：
  - 使用适用于 64 位 Arm 架构的 AMI。
  - 支持通过带有 ACPI 表的 UEFI 进行引导，以及支持 ACPI 热插拔 PCI 设备。

  以下 AMI 满足这些要求：

  - Amazon Linux 2（64 位 Arm）
  - Ubuntu 16.04 或更高版本（64 位 Arm）
  - Red Hat Enterprise Linux 8.0 或更高版本（64 位 Arm）
  - SUSE Linux Enterprise Server 15 或更高版本（64 位 Arm）
  - Debian 10 或更高版本（64 位 Arm）
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 如果是 FreeBSD AMI，裸机实例需要近 1 小时才能启动，并且不能完成到本地 NVMe 存储的 I/O。解决方法是将下面的代码行添加到 `/boot/loader.conf` 并重启：

```
hw.nvme.per_cpu_io_queues="0"
```

- `d2.8xlarge` 实例类型具有 36 个 vCPU，在某些 vCPU 数量限制为 32 个的 Linux 操作系统中可能会导致启动问题。有关更多信息，请参阅支持 个 vCPU (p. 356)。
- `d3.8xlarge` 和`d3en.12xlarge` 实例最多支持三个挂载，包括根卷。如果在添加网络接口或 EBS 卷时超出挂载限制，则会导致实例出现挂载问题。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅 Amazon EC2 常见问题解答中的我可以在 Amazon EC2 中运行多少个实例？。

Linux 加速计算实例

加速计算实例使用硬件加速器或协处理器来执行一些功能，如浮点数计算、图形处理或数据模式匹配，比在 CPU 上运行的软件更有效。这些实例能在计算密集型工作负载上提供更高的并行度，以实现更高的吞吐量。

如果您需要高处理能力，您可以从使用加速计算实例中获益，这些实例可让您访问基于硬件的计算加速器，如图形处理单元 (GPU)、现场可编程门阵列 (FPGA) 或 Amazon Inferentia。

目录

- GPU 实例 (p. 359)
- 使用 Amazon Trainium 的实例 (p. 360)
- 包含 Amazon Inferentia 的实例 (p. 360)
- 包含 Habana 加速器的实例 (p. 361)
- 视频转码实例 (p. 361)
- FPGA 实例 (p. 361)
- 硬件规格 (p. 362)
- 实例性能 (p. 364)
- 网络性能 (p. 364)
- Amazon EBS I/O 性能 (p. 366)
- 基于 SSD 的实例存储卷的 I/O 性能 (p. 367)

- 发布说明 (p. 368)
- 在 Linux 实例上安装 NVIDIA 驱动程序 (p. 369)
- 在 Linux 实例上安装 AMD 驱动程序 (p. 387)
- 在 G4ad 上设置双 4K 显示器 (p. 391)
- 激活 NVIDIA GRID 虚拟应用程序 (p. 394)
- 优化 GPU 设置 (p. 395)

GPU 实例

基于 GPU 的实例能让您访问具有数千个计算内核的 NVIDIA GPU。您可以通过这些实例利用 CUDA 或开放计算语言 (OpenCL) 并行计算框架，为科学、工程和渲染应用程序加速。还可以将这些实例用于图形应用程序，包括游戏流式处理、3-D 应用流式处理和其他图形工作负载。

G5 实例

G5 实例使用 NVIDIA A10G GPU，为图形密集型应用程序（例如远程工作站、视频渲染和云游戏）和应用程序的深度学习模型（例如自然语言处理、计算机视觉和推荐引擎）提供高性能。这些实例配备多达 8 个 NVIDIA A10G GPU、第二代 AMD EPYC 处理器、高达 100Gbps 的网络带宽，以及高达 7.6TB 的本地 NVMe SSD 存储。

G5g 实例

G5g 实例使用 NVIDIA T4G GPU，为利用 OpenGL 和 Vulkan 等行业标准 API 的游戏流和渲染等图形密集型应用程序提供高性能。这些实例也适合为自然语言处理和计算机视觉等应用程序运行深度学习模型。这些实例最多配备 2 个 NVIDIA T4G Tensor Core GPU，Amazon Graviton2 处理器，以及高达 25Gbps 的网络带宽。

G4ad 和 G4dn 实例

G4ad 实例使用 AMD Radeon Pro V520 GPU 和第 2 代 AMD EPYC 处理器，非常适合使用 OpenGL、DirectX 和 Vulkan 等行业标准 API 的图形应用程序，例如远程图形工作站、游戏流和渲染。它们提供多达 4 个 AMD Radeon Pro V520 GPU、64 个 vCPU、25 Gbps 网络和 2.4 TB 本地基于 NVME 的 SSD 存储。

G4dn 实例使用 NVIDIA Tesla GPU，并为使用 CUDA 或机器学习框架的通用 GPU 计算以及使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。这些实例提供高带宽网络、强大的半精度和单精度浮点功能以及 INT8 和 INT4 精度。每个 GPU 具有 16 GiB GDDR6 内存，从而使 G4dn 实例非常适合机器学习推理、视频转码以及图形应用程序，例如，远程图形工作站和云中的游戏流。

G4dn 实例支持 NVIDIA GRID 虚拟工作站。有关更多信息，请参阅 NVIDIA Marketplace 产品。

G3 实例

这些实例使用 NVIDIA Tesla M60 GPU，为使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。G3 实例还提供 NVIDIA GRID 虚拟工作站功能 (如 4 个分辨率高达 4096x2160 的监视器) 以及 NVIDIA GRID 虚拟应用程序。G3 实例非常适合一些应用程序，例如，3D 可视化、图形密集型远程工作站、3D 渲染、视频编码、虚拟现实以及其他需要大量并行处理能力的服务器端图形工作负载。

G3 实例支持 NVIDIA GRID 虚拟工作站和 NVIDIA GRID 虚拟应用程序。要激活任一功能，请参阅激活 NVIDIA GRID 虚拟应用程序 (p. 394)。

G2 实例

这些实例使用 NVIDIA GRID K520 GPU，并为使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。NVIDIA GRID GPU 还支持 NVIDIA 的快速捕获和编码 API 操作。示例应用程序包括视频创建服务、3D 可视化、流图形密集型应用程序，以及其他服务器端图形工作负载。

P4d 实例

这些实例使用 NVIDIA A100 GPU，并为机器学习和 HPC 工作负载提供高性能平台。P4d 实例提供 400 Gbps 的聚合网络带宽吞吐量并支持 Elastic Fabric Adapter (EFA)。它们是首批提供多个网卡的 EC2 实例。

P4d 实例支持 NVDIA NVSwitch GPU 互连和 NVIDIA GPUDirect RDMA。

P4de 实例提供 NVIDIA 80GB-A100s GPU

P3 实例

这些实例使用 NVIDIA Tesla V100 GPU，可用于使用 CUDA 或 OpenCL 编程模型或通过机器学习框架进行的通用 GPU 计算。P3 实例提供了高带宽网络、强大的半精度\单精度\双精度浮点功能以及每 GPU 最高 32 GiB 内存，非常适合用于深度学习、计算流体动力学、计算金融、地震分析、分子建模、基因组学、渲染和其他服务器端 GPU 计算工作负载。Tesla V100 GPU 不支持图形模式。

P3 实例支持 NVIDIA NVLink 对等传输。有关更多信息，请参阅 NVIDIA NVLink。

P2 实例

P2 实例使用 NVIDIA Tesla GPU K80 和适用于使用 CUDA 和 OpenCL 编程模型的通用 GPU 计算设计。P2 实例提供了高带宽网络、强大的单双精度浮点功能以及每个 GPU 12 GiB 的内存，非常适合深度学习、图形数据库、高性能数据库、计算流体动力学、计算金融、地震分析、分子建模、基因组学、渲染和其他服务器端 GPU 计算工作负载。

P2 实例支持 NVIDIA GPUDirect 对等传输。有关更多信息，请参阅 NVIDIA GPUDirect。

使用 Amazon Trainium 的实例

由 Amazon Trainium 提供支持的 Amazon EC2 Trn1 实例专为高性能、经济实惠的深度学习训练而构建。您可以使用 Trn1 实例来训练在语音识别、推荐、欺诈检测以及图像和视频分类等各种应用程序中使用的自然语言处理、计算机视觉和推荐器模型。在流行的机器学习（ML）框架（如 PyTorch 和 TensorFlow）中使用您的现有工作流程。AmazonNeuron SDK 与这些框架无缝集成，因此您只需更改几行代码即可开始使用。

有关更多信息，请参阅 Amazon EC2 Trn1 实例。

包含 Amazon Inferentia 的实例

这些实例旨在利用 Amazon Inferentia 加速机器学习，它是 Amazon 提供的一款自定义 AI/ML 芯片，可提供高性能、低延迟的机器学习推理。这些实例经过优化，专用于部署各种应用领域的深度学习 (DL) 模型，例如自然语言处理、对象检测和分类、内容个性化和过滤以及语音识别。

您可以通过多种方式开始使用这些模型：

- 使用 SageMaker，这是一种完全托管的服务，是开始使用机器学习模型的最简单方法。有关更多信息，请参阅《Amazon SageMaker 开发人员指南》中的开始使用 SageMaker。
- 使用 Deep Learning AMI 启动 Inf1 实例。有关更多信息，请参阅 Amazon Deep Learning AMI 开发人员指南中的使用 DLAMI 的 Amazon Inferentia。
- 使用您自己的 AMI 启动 Inf1 实例并安装 Amazon Neuron 开发工具包，您可以利用此工具包为 Amazon Inferentia 编译、运行和分析深度学习模型。
- 结合使用 Inf1 实例和经过 Amazon ECS 优化的 AMI 启动容器实例。有关更多信息，请参阅 Amazon Elastic Container Service Developer Guide中的 Amazon Linux 2 (Inferentia) AMI。
- 创建包含运行 Inf1 实例的节点的 Amazon EKS 集群。有关更多信息，请参阅 Amazon EKS 用户指南中的 Inferentia 支持。

Inf1 实例

Inf1 实例采用 Amazon Inferentia 机器学习推理芯片。Inferentia 是为了在任何规模下实现高性价比的低延迟推理性能而开发的。

包含 Habana 加速器的实例

这些实例旨在加速深度学习模型 (DL) 培训工作负载。他们使用来自英特尔旗下公司 Habana Labs 的加速器。这些实例针对图像识别、目标检测和分类以及推荐系统等应用程序的 DL 模型进行了优化。

DL1 实例

DL1 实例使用 Habana Gaudi 加速器。每个加速器提供高达 400 Gbps 的聚合网络带宽以及 32 GB 的高带宽内存 (HBM)。DL1 实例旨在为培训深度学习模型提供高性能和成本效益。

您可以通过多种方式开始使用这些模型：

- 使用 Habana Deep Learning AMI 启动 DL1 实例。
- 使用您自己的 AMI 启动 DL1 实例并安装 Habana 驱动程序和 Habana SynapseAI SDK。
- 结合使用 DL1 实例和经过 Amazon ECS 优化的 AMI 启动容器实例。
- 创建包含运行 DL1 实例的节点的 Amazon EKS 集群。

视频转码实例

这些实例旨在加快视频转码工作负载，例如直播、视频会议和实时转码。

VT1 实例

VT1 实例采用 Xilinx Alveo U30 媒体加速器，专为实时视频转码工作负载而设计。这些实例提供多达 8 个 Xilinx Alveo U30 加速卡，提供高达 192 GB 的系统内存和高达 25 Gbps 的网络带宽。VT1 实例采用 H.264/AVC 和 H.265/HEVC 编解码器，支持高达 4K 超高清分辨率，适用于多流视频转码。

您可以通过多种方式开始使用这些模型：

- 使用 Amazon Web Services Marketplace 上的 Xilinx U30 AMI 启动 VT1 实例。
- 使用您自己的 AMI 启动 VT1 实例并安装 Xilinx U30 drivers and Xilinx Video SDK（Xilinx U30 驱动程序和 Xilinx 视频软件开发工具包）。
- 结合使用 VT1 实例和经过 Amazon ECS 优化的 AMI 启动容器实例。
- 创建包含运行 VT1 实例的节点的 Amazon EKS 集群。

FPGA 实例

基于 FPGA 的实例能让您访问具有数百万并行系统逻辑单元格的 FPGA。您可以通过基于 FPGA 的加速计算实例，利用定义自硬件加速来加速工作负载，例如基因组学、财务分析、实时视频处理、大数据分析和安全工作负载。您可以使用硬件描述语言 (如 Verilog 或 VHDL) 或使用更高级语言 (如 OpenCL 并行计算框架) 来开发这些加速。您可以开发自己的硬件加速代码或通过 Amazon Web Services Marketplace 购买硬件加速。

FPGA 开发人员 AMI 提供了用于开发、测试和构建 AFI 的工具。您可以在任何具有至少 32 GB 系统内存的 EC2 实例上使用 FPGA 开发人员 AMI (例如，C5、M4 和 R4 实例)。

有关更多信息，请参阅 Amazon FPGA 硬件开发人员工具包的文档。

F1 实例

F1 实例使用 Xilinx UltraScale+ VU9P FPGA 并且专用于加快计算密集型算法，例如不适合通用型 CPU 的数据流或高度并行操作。F1 实例中的每个 FPGA 包含大约 250 万个逻辑单元和大约 6800 个数字信号处理 (DSP) 引擎，连同 64 GiB 的本地 DDR ECC 保护内存一起，通过专用 PCIe Gen3 x16 连接与实例相连。F1 实例提供本地 NVMe SSD 卷。

开发人员可以使用 FPGA 开发人员 AMI 和 Amazon 硬件开发人员工具包来创建用于 F1 实例的自定义硬件加速。FPGA 人员开发 AMI 包括云中的用于全周期 FPGA 开发的开发工具。使用这些工具，开发人员可以创建和分享 Amazon FPGA 映像 (AFI)，这些映像可以加载到 F1 实例的 FPGA 上。

硬件规格

以下是加速计算实例的硬件规格摘要。虚拟中央处理单元（vCPU）表示分配给虚拟机（VM）的物理 CPU 的一部分。对于 x86 实例，每个内核有两个 vCPU。对于 Graviton 实例，每个内核有一个 vCPU。

实例类型	默认 vCPU	内存 (GiB)	加速器
dl1.24xlarge	96	768.00	8 个 GPU
f1.2xlarge	8	122.00	1 个 FPGA
f1.4xlarge	16	244.00	2 个 FPGA
f1.16xlarge	64	976.00	8 个 FPGA
g2.2xlarge	8	15.00	1 个 GPU
g2.8xlarge	32	60.00	4 个 GPU
g3.4xlarge	16	122.00	1 个 GPU
g3.8xlarge	32	244.00	2 个 GPU
g3.16xlarge	64	488.00	4 个 GPU
g4ad.xlarge	4	16.00	1 个 GPU
g4ad.2xlarge	8	32.00	1 个 GPU
g4ad.4xlarge	16	64.00	1 个 GPU
g4ad.8xlarge	32	128.00	2 个 GPU
g4ad.16xlarge	64	256.00	4 个 GPU
g4dn.xlarge	4	16.00	1 个 GPU
g4dn.2xlarge	8	32.00	1 个 GPU
g4dn.4xlarge	16	64.00	1 个 GPU
g4dn.8xlarge	32	128.00	1 个 GPU
g4dn.12xlarge	48	192.00	4 个 GPU
g4dn.16xlarge	64	256.00	1 个 GPU
g4dn.metal	96	384.00	8 个 GPU
g5.xlarge	4	16.00	1 个 GPU
g5.2xlarge	8	32.00	1 个 GPU
g5.4xlarge	16	64.00	1 个 GPU
g5.8xlarge	32	128.00	1 个 GPU
g5.12xlarge	48	192.00	4 个 GPU

实例类型	默认 vCPU	内存 (GiB)	加速器
g5.16xlarge	64	256.00	1 个 GPU
g5.24xlarge	96	384.00	4 个 GPU
g5.48xlarge	192	768.00	8 个 GPU
g5g.xlarge	4	8.00	1 个 GPU
g5g.2xlarge	8	16.00	1 个 GPU
g5g.4xlarge	16	32.00	1 个 GPU
g5g.8xlarge	32	64.00	1 个 GPU
g5g.16xlarge	64	128.00	2 个 GPU
g5g.metal	64	128.00	2 个 GPU
inf1.xlarge	4	8.00	1 个推理加速器
inf1.2xlarge	8	16.00	1 个推理加速器
inf1.6xlarge	24	48.00	4 个推理加速器
inf1.24xlarge	96	192.00	16 个推理加速器
p2.xlarge	4	61.00	1 个 GPU
p2.8xlarge	32	488.00	8 个 GPU
p2.16xlarge	64	732.00	16 个 GPU
p3.2xlarge	8	61.00	1 个 GPU
p3.8xlarge	32	244.00	4 个 GPU
p3.16xlarge	64	488.00	8 个 GPU
p3dn.24xlarge	96	768.00	8 个 GPU
p4d.24xlarge	96	1152.00	8 个 GPU
p4de.24xlarge	96	1152.00	8 个 GPU
trn1.2xlarge	8	32.00	
trn1.32xlarge	128	512.00	
vt1.3xlarge	12	24.00	
vt1.6xlarge	24	48.00	
vt1.24xlarge	96	192.00	

Note

Trn1 实例具有以下数量的 Trainium 加速器。

- `trn1.2xlarge` – 1
- `trn1.32xlarge` – 16

VT1 实例具有以下数量的 U30 加速器。

- vt1.3xlarge – 1
- vt1.6xlarge – 2
- vt1.24xlarge – 16

加速计算实例使用以下处理器。

Amazon Graviton 处理器

- Amazon Graviton2：G5g

AMD 处理器

- 第二代 AMD EPYC 处理器（AMD EPYC 7R32）：G4ad、G5

英特尔处理器

- 英特尔至强可扩展处理器 (Broadwell E5-2686 v4)：F1G3、P2、P3
- 英特尔至强可扩展处理器（Skylake 8175）：P3dn
- 第二代英特尔至强可扩展处理器（Cascade Lake P-8275CL）：DL1、P4d、P4de
- 第二代英特尔至强可扩展处理器（Cascade Lake P-8259CL）：VT1
- 第二代英特尔至强可扩展处理器（Cascade Lake P-8259L）：G4dn、Inf1

有关更多信息，请参阅 Amazon EC2 实例类型。

实例性能

您可以执行多个 GPU 设置优化，以实现实例的最佳性能。有关更多信息，请参阅优化 GPU 设置 (p. 395)。

通过 EBS 优化的实例，您可以消除 Amazon EBS I/O 与 实例的其他网络流量之间的争用，从而使 EBS 卷持续获得高性能。有些加速计算实例在默认情况下会进行 EBS 优化，这不会产生额外的费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

一些加速计算实例类型提供了在 Linux 上控制处理器 C 状态和 P 状态的功能。C 状态控制当核心处理非活动状态时可以进入的睡眠级别，而 P 状态控制核心的所需性能 (以 CPU 频率的形式)。有关更多信息，请参阅您的 EC2 实例的处理器状态控制 (p. 707)。

网络性能

您可以为受支持的实例类型启用增强联网，以提供更低的延迟、更低的网络抖动和更高的每秒数据包数 (PPS) 性能。大多数应用程序并非始终需要较高的网络性能，但较高的带宽有助于其发送或接收数据。有关更多信息，请参阅Linux 上的增强联网 (p. 1142)。

以下是支持增强联网的加速计算实例的网络性能摘要。

Note

标有 † 的实例类型具备基准带宽，并且可以通过网络输入/输出积分机制，尽可能将其基准带宽突增到基准以上。有关更多信息，请参阅实例网络带宽 (p. 1141)。

实例类型	网络性能	增强联网功能
dl1.24xlarge	4x100Gb	ENA | EFA

实例类型	网络性能	增强联网功能
g4ad.xlarge †	高达 10Gb	ENA
g4ad.2xlarge †	高达 10Gb	ENA
g4ad.4xlarge †	高达 10Gb	ENA
g4ad.8xlarge	15Gb	ENA
g4ad.16xlarge	25Gb	ENA
g4dn.xlarge †	高达 25Gb	ENA
g4dn.2xlarge †	高达 25Gb	ENA
g4dn.4xlarge †	高达 25Gb	ENA
g4dn.8xlarge	50Gb	ENA | EFA
g4dn.12xlarge	50Gb	ENA | EFA
g4dn.16xlarge	50Gb	ENA | EFA
g4dn.metal	100Gb	ENA | EFA
g5.xlarge †	高达 10Gb	ENA
g5.2xlarge †	高达 10Gb	ENA
g5.4xlarge †	高达 25Gb	ENA
g5.8xlarge	25Gb	ENA | EFA
g5.12xlarge	40Gb	ENA | EFA
g5.16xlarge	25Gb	ENA | EFA
g5.24xlarge	50Gb	ENA | EFA
g5.48xlarge	100Gb	ENA | EFA
g5g.xlarge †	高达 10Gb	ENA
g5g.2xlarge †	高达 10Gb	ENA
g5g.4xlarge †	高达 10Gb	ENA
g5g.8xlarge	12Gb	ENA
g5g.16xlarge	25Gb	ENA
g5g.metal	25Gb	ENA
inf1.xlarge †	高达 25Gb	ENA
inf1.2xlarge †	高达 25Gb	ENA
inf1.6xlarge	25Gb	ENA
inf1.24xlarge	100Gb	ENA | EFA
p3dn.24xlarge	100Gb	ENA | EFA

实例类型	网络性能	增强联网功能
p4d.24xlarge	4x100Gb	ENA | EFA
p4de.24xlarge	4x100Gb	ENA | EFA
trn1.2xlarge †	高达 12.5Gb	ENA
trn1.32xlarge	8x100Gb	ENA | EFA
vt1.3xlarge	3.12Gb	ENA
vt1.6xlarge	6.25Gb	ENA
vt1.24xlarge	25Gb	ENA | EFA

下表显示了实例类型的基准带宽和突增带宽，这些实例类型通过网络输入/输出积分机制将其基准带宽突增到基准以上。

实例类型	基准带宽 (Gbps)	突增带宽 (Gbps)
g4ad.xlarge	2.0	10.0
g4ad.2xlarge	4.167	10.0
g4ad.4xlarge	8.333	10.0
g4dn.xlarge	5.0	25.0
g4dn.2xlarge	10.0	25.0
g4dn.4xlarge	20.0	25.0
g5.xlarge	2.5	10.0
g5.2xlarge	5.0	10.0
g5.4xlarge	10.0	25.0
g5g.xlarge	1.25	10.0
g5g.2xlarge	2.5	10.0
g5g.4xlarge	5.0	10.0
inf1.xlarge	5.0	25.0
inf1.2xlarge	5.0	25.0
trn1.2xlarge	3.125	12.5

Amazon EBS I/O 性能

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 Amazon EBS 卷提供最佳性能。

有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

基于 SSD 的实例存储卷的 I/O 性能

如果您使用内核版本为 4.4 或更高版本的 Linux AMI 并使用可用于您的实例的、基于 SSD 的所有实例存储卷，则您最高可以获得下表所列的 IOPS（4096 字节的数据块大小）性能（在队列深度饱和时）。否则，您将获得较低的 IOPS 性能。

实例大小	100% 随机读取 IOPS	写入 IOPS
g4ad.xlarge	10417	8333
g4ad.2xlarge	20833	16667
g4ad.4xlarge	41667	33333
g4ad.8xlarge	83333	66667
g4ad.16xlarge	166666	133332
g4dn.xlarge	42500	32500
g4dn.2xlarge	42500	32500
g4dn.4xlarge	85000	65000
g4dn.8xlarge	250000	200000
g4dn.12xlarge	250000	200000
g4dn.16xlarge	250000	200000
g4dn.metal	500000	400000
g5.xlarge	40625	20313
g5.2xlarge	40625	20313
g5.4xlarge	125000	62500
g5.8xlarge	250000	125000
g5.12xlarge	312500	156250
g5.16xlarge	250000	125000
g5.24xlarge	312500	156250
g5.48xlarge	625000	312500
p3dn.24xlarge	700000	340000
p4d.24xlarge	2000000	1600000
p4de.24xlarge	2000000	1600000
trn1.2xlarge	107500	45000
trn1.32xlarge	1720000	720000

随着您不断在您的实例的基于 SSD 的实例存储卷中填充数据，您可以达到的写入 IOPS 将不断减少。这是因为，SSD 控制器必须执行额外的工作，即查找可用空间、重写现有数据，以及擦除未使用的空间以使之可供重写。这一垃圾回收过程将导致对 SSD 的内部写入放大影响，这以 SSD 写入操作数相对于用户写入操作数

的比率形式来表示。如果写入操作数并非 4096 字节的倍数，或不在 4096 字节这一边界上，则性能的降低会更明显。如果您写入的字节数较少或不在边界上，则 SSD 控制器必须读取周围的数据并在新位置存储结果。这种模式会大大增加写入放大的影响，加长延迟，并显著降低 I/O 性能。

SSD 控制器可以使用多种策略来减少写入放大的影响。其中的一个策略是在 SSD 实例存储中预订空间，以便控制器更高效地管理可用于写入操作的空间。这称为超额配置。为 实例提供的基于 SSD 的实例存储卷不会为超额配置预保留空白间。要减少写入放大问题造成的影响，建议您留出 10% 的卷空间不进行分区，以便 SSD 控制器可使用这部分空间来进行超额配置。虽然这会减少您可使用的存储空间，但可提高性能，即使磁盘容量快用完也是如此。

对于支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。

发布说明

- 您必须使用 HVM AMI 启动实例。
- 基于 Nitro 系统 (p. 246)构建的实例具有以下要求：
  - 必须安装有 NVMe 驱动程序 (p. 1518)。
  - 必须安装有 Elastic Network Adapter (ENA) (p. 1143) 驱动程序。

  以下 Linux AMI 满足这些要求：
  - Amazon Linux 2
  - Amazon Linux AMI 2018.03
  - Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

    Note

    Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
  - Red Hat Enterprise Linux 7.4 或更高版本
  - SUSE Linux Enterprise Server 12 SP2 或更高版本
  - CentOS 7.4.1708 或更高版本
  - FreeBSD 11.1 或更高版本
  - Debian GNU/Linux 9 或更高版本
- 除非安装了 NVIDIA 驱动程序，否则基于 GPU 的实例无法访问 GPU。有关更多信息，请参阅在 Linux 实例上安装 NVIDIA 驱动程序 (p. 369)。
- 启动裸机实例会启动基础服务器，包含验证所有硬件和固件组件。这意味着从实例进入运行状态直至在网络上可用需要超过 20 分钟的时间。
- 对裸机实例附加或分离 EBS 卷或辅助网络接口需要 PCIe 本机 hotplug 支持。Amazon Linux 2 和最新版本的 Amazon Linux AMI 支持 PCIe 本机 hotplug，但更早的版本不支持。必须启用以下 Linux 内核配置选项：

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 裸机实例使用基于 PCI 的串行设备而不是基于 I/O 端口的串行设备。上游 Linux 内核和最新 Amazon Linux AMI 支持此设备。裸机实例还提供一个 ACPI SPCR 表，使系统能够自动使用基于 PCI 的串行设备。最新 Windows AMI 自动使用基于 PCI 的串行设备。
- 每个区域仅限 100 个 AFI。
- 在一个区域中可以启动的实例总数存在限制，某些实例类型还存在其他限制。有关更多信息，请参阅 Amazon EC2 常见问题解答中的我可以在 Amazon EC2 中运行多少个实例？。

在 Linux 实例上安装 NVIDIA 驱动程序

已挂载 NVIDIA GPU 的实例（如 P3 或 G4dn 实例）必须安装相应的 NVIDIA 驱动程序。根据实例类型，您可以下载公有 NVIDIA 驱动程序、从仅对Amazon客户可用的 Amazon S3 下载驱动程序或者使用预安装了驱动程序的 AMI。

要在挂载 AMD GPU 的 Linux 实例（例如，G4ad 实例）上安装 AMD 驱动程序，则请参阅安装 AMD 驱动程序 (p. 387)。要在 Windows 实例上安装 NVIDIA 驱动程序，请参阅在 Windows 实例上安装 NVIDIA 驱动程序。

目录

- NVIDIA 驱动程序的类型 (p. 369)
- 按实例类型列出的可用驱动程序 (p. 369)
- 安装选项 (p. 370)
- 安装 CUDA 的附加版本 (p. 387)

NVIDIA 驱动程序的类型

以下是可与基于 GPU 的实例一起使用的 NVIDIA 驱动程序的主要类型。

Tesla 驱动程序

这些驱动程序主要用于将 GPU 用于计算任务的计算工作负载，例如适用于机器学习的并行浮点计算，以及适用于高性能计算应用的快速傅里叶变换。

GRID 驱动程序

这些驱动程序经过认证，可针对渲染 3D 模型或高分辨率视频等内容的专业可视化应用程序，提供最佳性能。您可以将 GRID 驱动程序配置为支持两种模式。Quadro 虚拟工作站的每个 GPU 可支持四个 4K 显示器。GRID vApps 提供 RDSH App 托管功能。

Gaming 驱动程序

这些驱动程序包含针对游戏的优化，并经常更新以提供性能增强。它们支持每个 GPU 单个 4K 显示器。

NVIDIA 控制面板

GRID 和游戏驱动程序支持 NVIDIA 控制面板。Tesla 驱动程序不支持此控制面板。

Tesla、GRID 和游戏驱动程序支持的 API

- OpenCL、OpenGL 和 Vulkan
- NVIDIA CUDA 和相关库（例如，cuDNN、TensorRT、nvJPEG 和 cuBLAS）
- 用于视频编码的 NVENC 和用于视频解码的 NVDEC

按实例类型列出的可用驱动程序

下表总结了各种 GPU 实例类型支持的 NVIDIA 驱动程序。

实例类型	Tesla 驱动程序	GRID 驱动程序	Gaming 驱动程序
G2	是	否	否

实例类型	Tesla 驱动程序	GRID 驱动程序	Gaming 驱动程序
G3	是	是	否
G4dn	是	是	是
G5	是	是	是
G5g	是[1]	否	否
P2	是	否	否
P3	是	是[2]	否
P4d	是	否	否
P4de	是	否	否

[1] 此 Tesla 驱动程序还支持特定于 ARM64 平台的优化图形应用程序

[2] 仅使用 Marketplace AMI

安装选项

使用以下选项之一获取 GPU 实例所需的 NVIDIA 驱动程序。

选项 1：安装了 NVIDIA 驱动程序的 AMI

Amazon 和 NVIDIA 随已安装的 NVIDIA 驱动程序提供了不同的 Amazon Machine Image (AMI)。

- 具备 Tesla 驱动程序的 Marketplace 产品
- 具备 GRID 驱动程序的 Marketplace 产品
- 具备 Gaming 驱动程序的 Marketplace 产品

要使用这些 AMI 之一更新已安装的驱动程序版本，您必须从实例中卸载 NVIDIA 软件包以避免版本冲突。使用此命令卸载 NVIDIA 软件包：

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Amazon 提供的 CUDA 工具包安装包对 NVIDIA 驱动程序有依赖性。卸载 NVIDIA 软件包也会删除 CUDA 工具包。必须在安装 NVIDIA 驱动程序之后重新安装 CUDA 工具包。

选项 2：公共 NVIDIA 驱动程序

Amazon 提供的选项附带了驱动程序所需的许可证。或者，您可以安装公共驱动程序并自带许可证。要安装公共驱动程序，请按照此处的说明从 NVIDIA 站点下载该驱动程序。

或者，您可以使用 Amazon 提供的选项而非公有驱动程序。要在 P3 实例上使用 GRID 驱动程序，请按照选项 1 (p. 370)中的说明使用 Amazon Web Services Marketplace AMI。要在 G5、G4dn 或 G3 实例上使用 GRID 驱动程序，请使用 Amazon Web Services Marketplace AMI（如选项 1 所述），或安装 Amazon 提供的 NVIDIA 驱动程序（如选项 3 (p. 371) 中所述）。

下载公共 NVIDIA 驱动程序

登录您的 Linux 实例并从 http://www.nvidia.com/Download/Find.aspx 下载适合实例类型的 64 位 NVIDIA 驱动程序。对于产品类型、产品系列和产品，请使用下表中的选项。

实例	产品类型	产品系列	产品
G2	GRID	GRID 系列	GRID K520
G3	Tesla	M-Class	M60
G4dn	Tesla	T 系列	T4
G5 [1]	Tesla	A 系列	A10
G5g [2]	Tesla	T 系列	NVIDIA T4G
P2	Tesla	E 系列	K80
P3	Tesla	V 系列	V100
P4d	Tesla	A 系列	A100
P4de	Tesla	A 系列	A100

[1] G5 实例需要驱动程序版本 470.00 或更高版本

[2] G5g 实例需要驱动程序版本 470.82.01 或更高版本。操作系统是 Linux aarch64

在 Linux 上安装 NVIDIA 驱动程序

有关安装和配置驱动程序的更多信息，请参阅 NVIDIA 驱动程序安装快速入门指南。

选项 3：GRID 驱动程序（G5、G4dn 和 G3 实例）

这些下载仅供 Amazon 客户使用。一旦开始下载，即表示您同意按照 NVIDIA GRID 云终端用户许可协议（EULA）中提及的 Amazon 解决方案的要求，仅将下载的软件用来开发 AMI，以用于 NVIDIA A10G、NVIDIA Tesla T4 或 NVIDIA Tesla M60 硬件。安装软件后，您将受 NVIDIA GRID 云最终用户许可协议的条款约束。有关适用于您操作系统的 NVIDIA GRID 驱动程序版本的信息，请参阅 NVIDIA 网站上的 NVIDIA® 虚拟 GPU（vGPU）软件文档。

先决条件

- 在 Linux 实例上安装 Amazon CLI 并配置默认凭证。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。
- 用户或角色必须具有包含 AmazonS3ReadOnlyAccess 策略的授予权限。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon 托管式策略：AmazonS3ReadOnlyAccess。
- G5 实例需要 GRID 13.1 或更高版本（或 GRID 12.4 或更高版本）。
- 要让 GRID 许可正常运行，G3 实例需要 Amazon 提供的 DNS 解析。
- IMDSv2 (p. 755) 仅在 14.0 或更高版本的 NVIDIA 驱动程序上受支持。

Amazon Linux 和 Amazon Linux 2

在实例上安装 NVIDIA GRID 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. 使用以下命令下载 GRID 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ . --region
 us-east-1 --no-sign-request
```

此存储桶中存储了多个版本的 GRID 驱动程序。您可以使用以下命令查看所有可用的版本。

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/  --region us-east-1
 --no-sign-request
```

7. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. 如下所示运行自安装脚本，安装您下载的 GRID 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Note

如果您使用的是具有 5.10 内核版本的 Amazon Linux 2，请使用以下命令安装 GRID 驱动程序。

```
[ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

9. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

10. 确认驱动程序正常运行。以下命令的响应列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. 如果您在 G4dn 或 G5g 实例上使用 14.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

12. （可选）根据您的用例，您可能会完成以下可选步骤。如果您不需要此功能，请不要完成这些步骤。

    a. 为了帮助利用高达 4K 分辨率的四个显示器，请设置高性能显示协议 NICE DCV。

b. NVIDIA Quadro 虚拟工作站模式默认处于启用状态。要为 RDSH 应用程序托管功能激活 GRID 虚拟应用程序，请完成激活 NVIDIA GRID 虚拟应用程序 (p. 394)中的 GRID 虚拟应用程序激活步骤。

CentOS 7 和 Red Hat Enterprise Linux 7

在实例上安装 NVIDIA GRID 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. 禁用 NVIDIA 显卡的 nouveau 开源驱动程序。

   a. 将 nouveau 添加到 `/etc/modprobe.d/blacklist.conf` 黑名单文件。复制下面的代码块并将其粘贴到终端中。

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. 编辑 `/etc/default/grub` 文件并添加以下行：

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. 重新生成 Grub 配置。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. 使用以下命令下载 GRID 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ . --region
 us-east-1 --no-sign-request
```

   此存储桶中存储了多个版本的 GRID 驱动程序。您可以使用以下命令查看所有可用的版本。

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/  --region us-east-1
 --no-sign-request
```

8. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. 如下所示运行自安装脚本，安装您下载的 GRID 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

10. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

11. 确认驱动程序正常运行。以下命令的响应列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. 如果您在 G4dn 或 G5g 实例上使用 14.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

13. （可选）根据您的用例，您可能会完成以下可选步骤。如果您不需要此功能，请不要完成这些步骤。

    a. 为了帮助利用高达 4K 分辨率的四个显示器，请设置高性能显示协议 NICE DCV。

    b. NVIDIA Quadro 虚拟工作站模式默认处于启用状态。要为 RDSH 应用程序托管功能激活 GRID 虚拟应用程序，请完成激活 NVIDIA GRID 虚拟应用程序 (p. 394)中的 GRID 虚拟应用程序激活步骤。

    c. 安装 GUI 桌面/工作站程序包。

```
[ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
```

CentOS Stream 8 和 Red Hat Enterprise Linux 8

在实例上安装 NVIDIA GRID 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. 使用以下命令下载 GRID 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ . --region
 us-east-1 --no-sign-request
```

此存储桶中存储了多个版本的 GRID 驱动程序。您可以使用以下命令查看所有可用的版本。

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/  --region us-east-1
 --no-sign-request
```

7. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. 如下所示运行自安装脚本，安装您下载的 GRID 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

9. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

10. 确认驱动程序正常运行。以下命令的响应列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. 如果您在 G4dn 或 G5g 实例上使用 14.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

12. （可选）根据您的用例，您可能会完成以下可选步骤。如果您不需要此功能，请不要完成这些步骤。

    a. 为了帮助利用高达 4K 分辨率的四个显示器，请设置高性能显示协议 NICE DCV。

    b. NVIDIA Quadro 虚拟工作站模式默认处于启用状态。要为 RDSH 应用程序托管功能激活 GRID 虚拟应用程序，请完成激活 NVIDIA GRID 虚拟应用程序 (p. 394)中的 GRID 虚拟应用程序激活步骤。

    c. 安装 GUI 工作站程序包。

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

在 Linux 实例上安装 NVIDIA GRID 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel kernel-
devel-$(uname -r)
```

6. 使用以下命令下载 GRID 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ . --region
 us-east-1 --no-sign-request
```

此存储桶中存储了多个版本的 GRID 驱动程序。您可以使用以下命令查看所有可用的版本。

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/  --region us-east-1
 --no-sign-request
```

7. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. 如下所示运行自安装脚本，安装您下载的 GRID 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

9. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

10. 确认驱动程序正常运行。以下命令的响应列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. 如果您在 G4dn 或 G5g 实例上使用 14.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

12. （可选）根据您的用例，您可能会完成以下可选步骤。如果您不需要此功能，请不要完成这些步骤。

    a. 为了帮助利用高达 4K 分辨率的四个显示器，请设置高性能显示协议 NICE DCV。

    b. NVIDIA Quadro 虚拟工作站模式默认处于启用状态。要为 RDSH 应用程序托管功能激活 GRID 虚拟应用程序，请完成激活 NVIDIA GRID 虚拟应用程序 (p. 394)中的 GRID 虚拟应用程序激活步骤。

Ubuntu 和 Debian

在实例上安装 NVIDIA GRID 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
$ sudo apt-get update -y
```

3. 升级 linux-aws 程序包以接收最新版本。

```
$ sudo apt-get upgrade -y linux-aws
```

4. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

5. 重启之后重新连接到实例。
6. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. 禁用 NVIDIA 显卡的 nouveau 开源驱动程序。

   a. 将 nouveau 添加到 /etc/modprobe.d/blacklist.conf 黑名单文件。复制下面的代码块并将其粘贴到终端中。

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. 编辑 /etc/default/grub 文件并添加以下行：

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. 重新生成 Grub 配置。

   ```
   $ sudo update-grub
   ```

8. 使用以下命令下载 GRID 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ . --region
 us-east-1 --no-sign-request
```

此存储桶中存储了多个版本的 GRID 驱动程序。您可以使用以下命令查看所有可用的版本。

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/  --region us-east-1
 --no-sign-request
```

9. 使用以下命令添加权限以运行驱动程序安装实用程序。

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. 如下所示运行自安装脚本，安装您下载的 GRID 驱动程序。例如：

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

11. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

12. 确认驱动程序正常运行。以下命令的响应列出已安装的 NVIDIA 驱动程序版本和有关 GPU 的详细信息。

```
[ec2-user ~]$ nvidia-smi -q | head
```

13. 如果您在 G4dn 或 G5g 实例上使用 14.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

14. （可选）根据您的用例，您可能会完成以下可选步骤。如果您不需要此功能，请不要完成这些步骤。

    a. 为了帮助利用高达 4K 分辨率的四个显示器，请设置高性能显示协议 NICE DCV。

    b. NVIDIA Quadro 虚拟工作站模式默认处于启用状态。要为 RDSH 应用程序托管功能激活 GRID 虚拟应用程序，请完成激活 NVIDIA GRID 虚拟应用程序 (p. 394)中的 GRID 虚拟应用程序激活步骤。

    c. 安装 GUI 桌面/工作站程序包。

```
[ec2-user ~]$ sudo apt-get install -y lightdm ubuntu-desktop
```

选项 4：NVIDIA Gaming 驱动程序（G5 和 G4dn 实例）

这些驱动程序仅供 Amazon 客户使用。下载驱动程序即表明您同意仅使用下载的软件开发用于 NVIDIA A10G 和 NVIDIA Tesla T4 硬件的 AMI。安装软件后，您将受 NVIDIA GRID 云最终用户许可协议的条款约束。

先决条件

- 在 Linux 实例上安装 Amazon CLI 并配置默认凭证。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。
- 用户或角色必须具有包含 AmazonS3ReadOnlyAccess 策略的授予权限。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon 托管式策略：AmazonS3ReadOnlyAccess。
- 要让 GRID 许可正常运行，G3 实例需要 Amazon 提供的 DNS 解析。
- IMDSv2 (p. 755) 仅在 495.x 或更高版本的 NVIDIA 驱动程序上受支持。

Amazon Linux 和 Amazon Linux 2

在实例上安装 NVIDIA Gaming 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

6. 使用以下命令下载 Gaming 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ . --region us-
east-1 --no-sign-request
```

此存储桶中存储了多个版本的游戏驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/ --region us-east-1 --no-
sign-request
```

7. 从下载的 `.zip` 归档中提取 Gaming 驱动程序安装实用程序。

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. 使用以下命令添加权限以运行驱动程序安装实用程序：

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. 使用以下命令运行安装程序：

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> 如果您使用的是具有 5.10 内核版本的 Amazon Linux 2，请使用以下命令安装 NVIDIA 游戏驱动程序。
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

10. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. 使用以下命令下载并重命名认证文件。
    - 对于 460.39 及更高版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
      gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
      ```

    - 对于 440.68 到 445.48 版本：

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- 对于早期版本：

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

13. 如果您在 G4dn 或 G5g 实例上使用 510.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

14. （可选）为了帮助利用高达 4K 分辨率的单个显示器，请设置高性能显示协议 NICE DCV。

CentOS 7 和 Red Hat Enterprise Linux 7

在实例上安装 NVIDIA Gaming 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. 禁用 NVIDIA 显卡的 nouveau 开源驱动程序。

   a. 将 nouveau 添加到 /etc/modprobe.d/blacklist.conf 黑名单文件。复制下面的代码块并将其粘贴到终端中。

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. 编辑 /etc/default/grub 文件并添加以下行：

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. 重新生成 Grub 配置。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. 使用以下命令下载 Gaming 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ . --region us-
east-1 --no-sign-request
```

此存储桶中存储了多个版本的游戏驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/ --region us-east-1 --no-
sign-request
```

8. 从下载的 .zip 归档中提取 Gaming 驱动程序安装实用程序。

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. 使用以下命令添加权限以运行驱动程序安装实用程序：

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. 使用以下命令运行安装程序：

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

11. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. 使用以下命令下载并重命名认证文件。
    - 对于 460.39 及更高版本：

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
```

    - 对于 440.68 到 445.48 版本：

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - 对于早期版本：

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-
gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

14. 如果您在 G4dn 或 G5g 实例上使用 510.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

15. （可选）为了帮助利用高达 4K 分辨率的单个显示器，请设置高性能显示协议 NICE DCV。如果您不需要此功能，请勿完成此步骤。

CentOS Stream 8 和 Red Hat Enterprise Linux 8

在实例上安装 NVIDIA Gaming 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
[ec2-user ~]$ sudo yum update -y
```

3. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. 使用以下命令下载 Gaming 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ . --region us-
east-1 --no-sign-request
```

此存储桶中存储了多个版本的游戏驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/ --region us-east-1 --no-
sign-request
```

7. 从下载的 `.zip` 归档中提取 Gaming 驱动程序安装实用程序。

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. 使用以下命令添加权限以运行驱动程序安装实用程序：

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. 使用以下命令运行安装程序：

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

10. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. 使用以下命令下载并重命名认证文件。
    - 对于 460.39 及更高版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
      ```

    - 对于 440.68 到 445.48 版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - 对于早期版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. 重启实例。

    ```
    [ec2-user ~]$ sudo reboot
    ```

13. 如果您在 G4dn 或 G5g 实例上使用 510.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

    ```
    sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

14. （可选）为了帮助利用高达 4K 分辨率的单个显示器，请设置高性能显示协议 NICE DCV。

Rocky Linux 8

在实例上安装 NVIDIA Gaming 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. 重启实例以加载最新内核版本。

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. 重启之后重新连接到实例。
5. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

   ```
   [ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-devel
    kernel-devel-$(uname -r)
   ```

6. 使用以下命令下载 Gaming 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ . --region us-east-1 --no-sign-request
```

此存储桶中存储了多个版本的游戏驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/ --region us-east-1 --no-sign-request
```

7. 从下载的 .zip 归档中提取 Gaming 驱动程序安装实用程序。

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. 使用以下命令添加权限以运行驱动程序安装实用程序：

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. 使用以下命令运行安装程序：

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

10. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. 使用以下命令下载并重命名认证文件。
    - 对于 460.39 及更高版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
      ```

    - 对于 440.68 到 445.48 版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - 对于早期版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

12. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

13. 如果您在 G4dn 或 G5g 实例上使用 510.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/
nvidia.conf
```

14. （可选）为了帮助利用高达 4K 分辨率的单个显示器，请设置高性能显示协议 NICE DCV。

Ubuntu 和 Debian

在实例上安装 NVIDIA Gaming 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。

```
$ sudo apt-get update -y
```

3. 升级 `linux-aws` 程序包以接收最新版本。

```
$ sudo apt-get upgrade -y linux-aws
```

4. 重启实例以加载最新内核版本。

```
[ec2-user ~]$ sudo reboot
```

5. 重启之后重新连接到实例。
6. 为您当前运行的内核版本安装 gcc 编译器和内核标头软件包。

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. 禁用 NVIDIA 显卡的 nouveau 开源驱动程序。

   a. 将 nouveau 添加到 `/etc/modprobe.d/blacklist.conf` 黑名单文件。复制下面的代码块并将其粘贴到终端中。

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. 编辑 `/etc/default/grub` 文件并添加以下行：

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. 重新生成 Grub 配置。

   ```
   $ sudo update-grub
   ```

8. 使用以下命令下载 Gaming 驱动程序安装实用程序：

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ . --region us-
east-1 --no-sign-request
```

此存储桶中存储了多个版本的游戏驱动程序。您可以使用以下命令查看所有可用的版本：

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/ --region us-east-1 --no-sign-request
```

9. 从下载的 .zip 归档中提取 Gaming 驱动程序安装实用程序。

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. 使用以下命令添加权限以运行驱动程序安装实用程序：

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. 使用以下命令运行安装程序：

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

系统提示时，接受许可协议并根据需要指定安装选项 (您可以接受默认选项)。

12. 使用以下命令创建所需的配置文件。

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. 使用以下命令下载并重命名认证文件。
    - 对于 460.39 及更高版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
      ```

    - 对于 440.68 到 445.48 版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - 对于早期版本：

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

14. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

15. 如果您在 G4dn 或 G5g 实例上使用 510.x 或更高版本的 NVIDIA 驱动程序，请使用以下命令禁用 GSP。有关为什么需要这样做的更多信息，请访问 NVIDIA 文档。

```
sudo touch /etc/modprobe.d/nvidia.conf
```

```
echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

16. （可选）为了帮助利用高达 4K 分辨率的单个显示器，请设置高性能显示协议 NICE DCV。如果您不需要此功能，请勿完成此步骤。

安装 CUDA 的附加版本

在您的实例上安装 NVIDIA 图形驱动程序后，您可以安装与图形驱动程序捆绑的版本以外的 CUDA 版本。以下过程演示如何在实例上配置多个版本的 CUDA。

安装 CUDA 工具包

1. 连接到 Linux 实例。
2. 打开 NVIDIA 网站，然后选择所需的 CUDA 版本。
3. 为您的实例上的操作系统选择架构、分发版和版本。对于安装程序类型，选择运行文件（本地）。
4. 按照说明下载安装脚本。
5. 将运行权限添加到您使用以下命令下载的安装脚本。

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. 按如下方式运行安装脚本以安装 CUDA 工具包并将 CUDA 版本号添加到工具包路径中。

```
[ec2-user ~]$ sudo downloaded_installer_file --silent --override --toolkit --samples --
toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-opengl-libs
```

7. （可选）按如下方式设置默认 CUDA 版本。

```
[ec2-user ~]$ ln -s /usr/local/cuda-version /usr/local/cuda
```

在 Linux 实例上安装 AMD 驱动程序

已挂载 AMD GPU 的实例（如 G4ad 实例）必须安装相应的 AMD 驱动程序。根据您的要求，您可以使用带有预装驱动程序的 AMI，也可以从 Amazon S3 下载驱动程序。

要在挂载 NVIDIA GPU 的实例（例如，G4dn 实例）上安装 NVIDIA 驱动程序，则请参阅安装 NVIDIA 驱动程序 (p. 369)。要在 Windows 实例上安装 AMD 驱动程序，请参阅在 Windows 实例上安装 AMD 驱动程序。

目录

- AMD Radeon Pro Software for Enterprise Driver (p. 387)
- 安装了 AMD 驱动程序的 AMI (p. 388)
- AMD 驱动程序下载 (p. 388)
- 设置交互式桌面 (p. 389)

AMD Radeon Pro Software for Enterprise Driver

The AMD Radeon Pro Software for Enterprise Driver 旨在为专业级图形使用案例提供支持。使用驱动程序，您可以将实例配置为每个 GPU 两个 4K 显示。

支持的 API

- OpenGL、OpenCL
- Vulkan
- AMD 高级媒体框架
- 视频加速 API

安装了 AMD 驱动程序的 AMI

Amazon 提供安装的 AMD 驱动程序随附的不同 Amazon 系统映像 (AMI)。打开使用 AMD 驱动程序的 Marketplace 产品。

AMD 驱动程序下载

如果您使用的不是安装了 AMD 驱动程序的 AMI，则可以下载 AMD 驱动程序并将其安装在您的实例上。

这些下载仅供 Amazon 客户使用。下载即表明您同意仅将下载的软件用于开发在 AMD Radeon Pro V520 硬件上使用的 AMIs。安装软件时，您需要遵循 AMD 软件最终用户许可协议的条款。

先决条件

- 在 Linux 实例上安装 Amazon CLI 并配置默认凭证。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。
- 用户或角色必须具有包含 AmazonS3ReadOnlyAccess 策略的授予权限。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 Amazon 托管式策略：AmazonS3ReadOnlyAccess。

在 Linux 实例上安装 AMD 驱动程序

1. 连接到 Linux 实例。安装 gcc 和 make（如果尚未安装）。
2. 更新软件包缓存并获取实例软件包更新。
   - 对于 Amazon Linux 2：

     ```
     $ sudo amazon-linux-extras install epel -y
     $ sudo yum update -y
     ```

   - 对于 Ubuntu：

     ```
     $ sudo dpkg --add-architecture i386
     $ sudo apt-get update -y && sudo apt upgrade -y
     ```

   - 对于 CentOS：

     ```
     $ sudo yum install epel-release -y
     $ sudo yum update -y
     ```

3. 重启实例。

   ```
   $ sudo reboot
   ```

4. 在实例重启后重新连接到实例。
5. 下载最新的 AMD 驱动程序。

   ```
   $ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
   ```

6. 解压文件。
   - 对于 Amazon Linux 2 和 CentOS：

     ```
     $ tar -xf amdgpu-pro-*rhel*.tar.xz
     ```

   - 对于 Ubuntu：

```
$ tar -xf amdgpu-pro*ubuntu*.xz
```

7. 切换到提取的驱动程序所在的文件夹。
8. 为驱动程序安装添加缺少的模块。

   - 对于 Amazon Linux 2 和 CentOS：

     跳过此步骤。
   - 对于 Ubuntu：

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
```

9. 运行自我安装脚本以安装完整的图形堆栈。

```
$ ./amdgpu-pro-install -y --opencl=pal,legacy
```

10. 重启实例。

```
$ sudo reboot
```

11. 确认驱动程序正常运行。

```
$ dmesg | grep amdgpu
```

该响应应当与以下内容相似：

```
Initialized amdgpu
```

设置交互式桌面

确认实例已安装 AMD GPU 驱动程序并且 amdgpu 正在使用中之后，您可以安装交互式桌面管理器。我们建议使用 MATE 桌面环境，以获得最佳兼容性和性能。

先决条件

打开文本编辑器并将以下内容另存为名为 xorg.conf 的文件。您的实例上需要此文件。

```
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
```

```
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection
Section "Monitor"
    Identifier     "Monitor0"
    VendorName     "Unknown"
    ModelName      "Unknown"
EndSection
Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
    Option         "DPMS" "Disable"
EndSection
Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Monitor0"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

在 Amazon Linux 2 上设置交互式桌面

1. 安装 EPEL 存储库。

```
$ sudo amazon-linux-extras install epel -y
```

2. 安装 MATE 桌面。

```
$ sudo amazon-linux-extras install mate-desktop1.x -y
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. 将 `xorg.conf` 文件复制到 `/etc/X11/xorg.conf`。
4. 重启实例。

```
$ sudo reboot
```

5. （可选）安装 NICE DCV 服务器以使用 NICE DCV 作为高性能显示协议，然后使用首选客户端连接到 NICE DCV 会话。

在 Ubuntu 上设置交互式桌面

1. 安装 MATE 桌面。

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
```

```
$ sudo apt purge ifupdown -y
```

2. 将 xorg.conf 文件复制到 /etc/X11/xorg.conf。
3. 重启实例。

```
$ sudo reboot
```

4. 为适当版本的 Ubuntu 安装 AMF 编码器。

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. （可选）安装 NICE DCV 服务器以使用 NICE DCV 作为高性能显示协议，然后使用首选客户端连接到 NICE DCV 会话。
6. DCV 安装完成后，授予 DCV 用户视频权限：

```
$ sudo usermod -aG video dcv
```

在 CentOS 上设置交互式桌面

1. 安装 EPEL 存储库。

```
$ sudo yum update -y
$ sudo yum install epel-release -y
```

2. 安装 MATE 桌面。

```
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. 将 xorg.conf 文件复制到 /etc/X11/xorg.conf。
4. 重启实例。

```
$ sudo reboot
```

5. （可选）安装 NICE DCV 服务器以使用 NICE DCV 作为高性能显示协议，然后使用首选客户端连接到 NICE DCV 会话。

在 G4ad 上设置双 4K 显示器

启动 G4ad 实例

1. 连接到您的 Linux 实例以获取相关 GPU 的 PCI 总线地址，以用作双 4K（2x4k）的目标：

```
lspci -vv | grep -i amd
```

您将获得与下内容类似的输出：

```
00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
 c3)
Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
```

2. 请注意，上述输出中的 PCI 总线地址为 00:1e.0。创建一个名为 /etc/modprobe.d/amdgpu.conf 的文件然后添加：

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. 按照此处 (p. 387)的说明在 Linux 上安装 AMD 驱动程序。如果您已经安装了 AMD GPU 驱动程序，则需要通过 dkms 重建 amdgpu 内核模块。
4. 使用下面的 xorg.conf 文件定义双（2x4K）屏幕拓扑并将文件保存到 `/etc/X11/xorg.conf`：

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
```

```
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. 按照设置交互式桌面中的说明设置 DCV。
6. 完成 DCV 设置后，重新启动。
7. 确认驱动程序运行正常：

```
dmesg | grep amdgpu
```

该响应应当与以下内容相似：

```
Initialized amdgpu
```

8. 您应会在 DISPLAY=:0 xrandr -q 的输出中看到您已连接了 2 个虚拟显示器：

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
```

```
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
 640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
 1600x1200  59.95
 1680x1050  60.00
 1400x1050  60.00
 1280x1024  59.95
 1440x900 59.99
 1280x960 59.99
 1280x854 59.95
 1280x800 59.96
 1280x720 59.97
 1152x768 59.95
 1024x768 60.00 59.95
 800x600  60.32 59.96 56.25
 848x480  60.00 59.94
 720x480  59.94
640x480  59.94 59.94
```

9. 连接到 DCV 后，将分辨率更改为 2x4K，确认 DCV 已经注册了双显示器支持。



激活 NVIDIA GRID 虚拟应用程序

要在 G3、G4dn 和 G5 实例上激活 GRID 虚拟应用程序（默认情况下启用 NVIDIA GRID 虚拟工作站），您必须在 `/etc/nvidia/gridd.conf` 文件为驱动程序定义产品类型。

激活 Linux 实例上的 GRID 虚拟应用程序

1. 从提供的模板文件创建 `/etc/nvidia/gridd.conf` 文件。

```
[ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

2. 在您常用的文本编辑器中打开 `/etc/nvidia/gridd.conf` 文件。
3. 找到 `FeatureType` 行，并将其设置为 `0`。然后，添加包含 `IgnoreSP=TRUE` 的行。

```
FeatureType=0
IgnoreSP=TRUE
```

4. 保存文件并退出。
5. 重启实例以接受新配置。

```
[ec2-user ~]$ sudo reboot
```

优化 GPU 设置

您可以执行多个 GPU 设置优化，以实现 NVIDIA GPU 实例 (p. 359)的最佳性能。对于其中一些实例类型，NVIDIA 驱动程序使用 autoboost 功能，该功能会改变 GPU 时钟速度。通过禁用 autoboost 并将 GPU 时钟速度设置为其最大频率，您可以始终获得 GPU 实例的最大性能。下面的程序可帮助您将 GPU 设置配置为永久，在需要时禁用 autoboost 功能，并将 GPU 时钟速度设置为其最大频率。

优化 GPU 设置

1. 将 GPU 设置配置为永久。该命令可能需要几分钟才能运行完毕。

```
[ec2-user ~]$ sudo nvidia-persistenced
```

2. [仅限 G2、G3 和 P2 实例] 禁用实例上所有 GPU 的 autoboost 功能。

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

3. 将所有 GPU 时钟速度设置为其最大频率。使用以下命令中指定的内存和图形时钟速度。

   有些版本的 NVIDIA 驱动程序不支持设置应用程序时钟速度，并会显示错误 "Setting applications clocks is not supported for GPU..."，您可以忽略该错误。

   - G3 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

   - G4dn 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
     ```

   - G5 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
     ```

   - P2 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,875
     ```

   - P3 和 P3dn 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 877,1530
     ```

   - P4d 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
     ```

   - P4de 实例：

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
     ```

查找 Amazon EC2 实例类型

您必须先选择要使用的实例类型，然后才能启动实例。您选择的实例类型可能取决于您的工作负载所需的资源，例如计算、内存或存储资源。确定几种可能适合您的工作负载的实例类型，并在测试环境中评估它们的性能可能很有帮助。没有方法可以替代衡量应用程序在负载下的性能。

如果您已在运行 EC2 实例，可以使用 Amazon Compute Optimizer 获取有关您应该用来提高性能、节省资金或两者兼顾的实例类型的建议。有关更多信息，请参阅the section called “获取建议” (p. 397)。

任务

- 使用控制台查找实例类型 (p. 396)
- 使用 Amazon CLI 查找实例类型 (p. 396)

使用控制台查找实例类型

您可以使用 Amazon EC2 控制台查找满足您的需求的实例类型。

使用控制台查找实例类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏，选择您在其中启动实例的区域。您可以选择向您提供的任何区域，无需理会您身处的位置。
3. 在导航窗格中，选择 Instance Types (实例类型)。
4. （可选）选择首选项（齿轮）图标以选择要显示的实例类型属性（例如 On-Demand Linux pricing (按需 Linux 定价)），然后选择 Confirm (确认)。或者，选择实例类型的名称以打开其详细信息页面，并查看通过控制台提供的所有属性。控制台不会显示通过 API 或命令行提供的所有属性。
5. 使用实例类型属性筛选显示的实例类型列表，以仅显示满足您的需求的实例类型。例如，您可以筛选以下属性：
   - Availability zones（可用区）– 可用区、本地区域或 Wavelength 区域的名称。有关更多信息，请参阅the section called “区域和可用区” (p. 1040)。
   - vCPUs 或 Cores（内核）– vCPU 或内核的数量。
   - Memory (GiB) [内存（GiB)] - 内存大小，以 GiB 为单位。
   - Network performance（网络性能）– 网络性能，以千兆为单位。
   - Local instance storage（本地实例存储）– 指示实例类型是否具有本地实例存储（`true` | `false`）。
6. （可选）要并排查看比较结果，请选中多个实例类型的复选框。比较结果显示在屏幕底部。
7. （可选）要将实例类型列表保存到逗号分隔值（.csv）文件以进一步查看，请依次选择 Actions（操作）、Download list CSV（下载列表 CSV）。该文件包括与您设置的筛选条件匹配的所有实例类型。
8. （可选）要使用符合您需求的实例类型启动实例，请选中该实例类型的复选框并依次选择 Actions（操作）、Launch instance（启动实例）。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

使用 Amazon CLI 查找实例类型

您可以在 Amazon EC2 中使用 Amazon CLI 命令以查找满足您的需求的实例类型。

使用 Amazon CLI 查找实例类型

1. 如果尚未安装，请安装 Amazon CLI。有关更多信息，请参阅 Amazon Command Line Interface 用户指南。
2. 使用 describe-instance-types 命令根据实例属性筛选实例类型。例如，您可以使用以下命令仅显示当前一代中具有 64 GiB（65536 MiB）的实例类型。

```
aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
 "Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].[InstanceType]"
 --output text | sort
```

3. 使用 describe-instance-type-offerings 命令筛选按位置（区域或区）提供的实例类型。例如，您可以使用以下命令以显示在指定的区中提供的实例类型。

```
aws ec2 describe-instance-type-offerings --location-type "availability-zone" --filters
 Name=location,Values=us-east-2a --region us-east-2 --query "InstanceTypeOfferings[*].
[InstanceType]" --output text | sort
```

4. 在找到满足您的需求的实例类型后，保存列表以便在启动实例时使用这些类型。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的启动实例。

获取实例类型建议

Amazon Compute Optimizer 提供了 Amazon EC2 实例建议，以帮助您提高性能和/或节省资金。您可以根据这些建议来决定是否移动到新的实例类型。

为了生成建议，Compute Optimizer 会分析现有实例规范和利用率指标。然后，利用已编译数据来建议哪些 Amazon EC2 实例类型能够最好地处理现有工作负载。建议随每小时实例定价一起返回。

本主题概述了如何通过 Amazon EC2 控制台查看建议。有关更多信息，请参阅 Amazon Compute Optimizer 用户指南。

> **Note**
>
> 要从 Compute Optimizer 中获取建议，您必须首先选择加入 Compute Optimizer。有关更多信息，请参阅 Amazon Compute Optimizer 用户指南中的 Amazon Compute Optimizer 入门。

目录

- 限制 (p. 397)
- 结果 (p. 397)
- 查看建议 (p. 398)
- 评估建议时的注意事项 (p. 399)
- 其他资源 (p. 399)

限制

Compute Optimizer 目前为 C、D、H、I、M、R、T、X 和 z 实例类型生成建议。Compute Optimizer 不会考虑其他实例类型。如果您使用的是其他实例类型，则不会在 Compute Optimizer 建议视图中列出它们。有关支持和不支持的实例类型的更多信息，请参阅《Amazon Compute Optimizer 用户指南》中的 Amazon EC2 实例要求。

结果

Compute Optimizer 将其对 EC2 实例的调查结果分类为：

- 预配置不足 – 当您的实例的至少一个规格（如 CPU、内存或网络）没有满足工作负载的性能要求时，将 EC2 实例视为预配置不足。预配置不足的 EC2 实例可能会导致应用程序性能较差。
- 过度预配置 – 当您的实例的至少一个规格（如 CPU、内存或网络）可缩小但仍能满足工作负载的性能要求时，并且没有任何规格处于预配置不足状态时，将 EC2 实例视为过度预配置。过度预配置的 EC2 实例可能会导致不必要的基础设施成本。

- 已优化 – 当您的实例的所有规格（如 CPU、内存和网络）满足工作负载的性能要求且实例未处于过度预配置状态时，将 EC2 实例视为已优化。已优化的 EC2 实例以最佳的性能和基础设施成本运行您的工作负载。对于已优化的实例，Compute Optimizer 有时可能会建议新一代实例类型。
- 无 – 没有对此实例的建议。如果您选择加入 Compute Optimizer 的时间少于 12 小时、实例的运行时间少于 30 小时，或者 Compute Optimizer 不支持实例类型，则可能会发生这种情况。有关更多信息，请参阅前一部分中的限制 (p. 397)。

查看建议

在选择加入 Compute Optimizer 后，您可以在 EC2 控制台中查看 Compute Optimizer 为 EC2 实例生成的结果。然后，您可以访问 Compute Optimizer 控制台来查看建议。如果您是最近选择加入的，EC2 控制台可能在长达 12 小时内不会反映调查结果。

通过 EC2 控制台查看对 EC2 实例的建议

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例，然后选择实例 ID。
3. 在实例摘要页面底部附近的 Amazon Compute Optimizer 横幅中，选择查看详细信息。

   实例将在 Compute Optimizer 中打开，在其中，将实例标记为 Current (当前) 实例。最多提供三个不同的实例类型建议，分别标记为 Option 1 (选项 1)、Option 2 (选项 2) 和 Option 3 (选项 3)。窗口的下半部分显示了当前实例的最新 CloudWatch 指标数据：CPU 利用率、内存利用率、网络输入和网络输出。
4. （可选）在 Compute Optimizer 控制台中，选择设置（  ）图标来更改表中的可见列，或查看当前和建议的实例类型的不同购买选项的公开定价信息。

   Note

   如果您购买了 Reserved Instance，您的个按需型实例可能会作为 Reserved Instance 进行计费。在更改当前实例类型之前，请首先评估对Reserved Instance使用率和覆盖率的影响。

确定是否要使用其中某个建议。决定是否要进行优化以便提高性能和/或减少成本。有关更多信息，请参阅 Amazon Compute Optimizer 用户指南中的查看资源建议。

通过 Compute Optimizer 控制台查看对所有区域中的所有 EC2 实例的建议

1. 打开 Compute Optimizer 控制台，网址为 https://console.aws.amazon.com/compute-optimizer/。
2. 选择 View recommendations for all EC2 instances (查看对所有 EC2 实例的建议)。
3. 您可以在建议页面上执行以下操作：

   a. 要将建议筛选为一个或多个 Amazon 区域，请在 Filter by one or more Regions（按一个或多个区域筛选）文本框中输入区域名称，或者在显示的下拉列表中选择一个或多个区域。

   b. 要查看其他账户中的资源建议，请选择 Account（账户），然后选择其他账户 ID。

      仅当您登录到组织的管理账户并选择加入组织内的所有成员账户时，此选项才可用。

   c. 要清除所选筛选器，请选择 Clear filters（清除筛选器）。

   d. 要更改为当前和建议的实例类型显示的购买选项，请选择设置（  ）图标，然后选择 On-Demand Instances（按需型实例）、Reserved Instances, standard 1-year no upfront（预留实例，标准 1 年期，无预付费用）或 Reserved Instances, standard 3-year no upfront（预留实例，标准 3 年期，无预付费用）。

   e. 要查看详细信息（例如，其他建议和利用率指标比较），请选择所需实例旁边列出的调查结果（Under-provisioned (预配置不足)、Over-provisioned (过度预配置) 或 Optimized (已优化)）。有关更多信息，请参阅 Amazon Compute Optimizer 用户指南中的查看资源详细信息。

评估建议时的注意事项

在更改实例类型之前，请考虑以下事项：

- 这些建议不会预测您的使用情况。建议基于您在最近 14 天时间段内的历史使用情况。请务必选择一种预计能够满足您的未来资源需求的实例类型。
- 关注图表指标以确定实际使用量是否低于实例容量。您还可以在 CloudWatch 中查看指标数据（平均值、峰值、百分比），以进一步评估 EC2 实例建议。例如，观察当天 CPU 百分比指标如何变化，以及是否有需要满足的峰值。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的查看可用指标。
- Compute Optimizer 可能会为可突增性能实例（即 T3、T3a 和 T2 实例）提供建议。如果您定期突增至基线之上，请确保您可以基于新实例类型的 vCPU 继续如此。有关更多信息，请参阅具爆发能力的实例的关键概念和定义 (p. 276)。
- 如果您购买了 Reserved Instance，您的个按需型实例可能会作为 Reserved Instance 进行计费。在更改当前实例类型之前，请首先评估对Reserved Instance使用率和覆盖率的影响。
- 尽可能考虑转换为较新一代实例。
- 在迁移到其他实例系列时，请确保当前实例类型和新实例类型在虚拟化、架构或网络类型等方面兼容。有关更多信息，请参阅更改实例类型的兼容性 (p. 402)。
- 最后，请考虑为每个建议提供的性能风险评级。性能风险指示您为了验证建议的实例类型是否满足工作负载的性能要求而可能需要执行的工作量。我们还建议在进行任何更改前后进行严格的负载和性能测试。

调整 EC2 实例大小时，还有其他注意事项。有关更多信息，请参阅更改实例类型 (p. 399)。

其他资源

有关更多信息：

- 实例类型 (p. 238)
- Amazon Compute Optimizer 用户指南

更改实例类型

随着您的需求变化，您可能会发现您的实例过度使用 (实例类型过小) 或利用不足 (实例类型过大)。如果是这种情况，您可以通过更改实例类型来调整实例的大小。例如，如果您 `t2.micro` 实例对于其工作负载来说太小，您可以通过将其更改为更大的 T2 实例类型来增加其大小，例如 `t2.large`。或者，您可以将其更改其它实例类型，如 `m5.large`。您可能还想将实例类型从上一代更改为最新一代以利用某些功能，例如 IPv6 支持。

如果您想要针对能够最好地处理现有工作负载的实例类型获得建议，则可以使用 Amazon Compute Optimizer。有关更多信息，请参阅获取实例类型建议 (p. 397)。

如果希望在不更改实例类型的情况下向实例添加额外的存储空间，请参阅 将 Amazon EBS 卷挂载到实例 (p. 1347)。

要遵循哪些说明？

对于更改实例类型，我们有不同的说明。应该使用哪些说明取决于实例的根卷，以及实例类型是否与实例的当前配置兼容。有关如何确定兼容性的信息，请参阅 更改实例类型的兼容性 (p. 402)。

使用下表确定需要遵守的说明。

根卷	兼容性	使用以下说明进行操作
EBS	兼容	更改现有的 EBS 支持实例的实例类型 (p. 400)

根卷	兼容性	使用以下说明进行操作
EBS	不兼容	通过启动新实例更改实例类型 (p. 401)
实例存储	不适用	更改实例存储支持的实例的实例类型 (p. 403)

兼容实例类型的注意事项

更改现有实例的实例类型时，请考虑以下事项：

- 您必须先停止由 Amazon EBS 支持的实例，然后才能更改其实例类型。当实例停止时，请确保您已计划停机时间。停止实例并更改其实例类型可能需要几分钟时间，重新启动实例所用的时间则由应用程序的启动脚本决定。有关更多信息，请参阅停止和启动您的实例 (p. 610)。
- 当您停止并启动实例时，我们会将该实例移动到新硬件。如果您的实例具有公有 IPv4 地址，则我们会释放该地址并向实例提供一个新的公有 IPv4 地址。如果您需要不会更改的公有 IPv4 地址，请使用弹性 IP 地址 (p. 1094)。
- 您不能更改已启用了休眠 (p. 616)的实例的实例类型。
- 您无法更改竞价型实例 (p. 471)的实例类型。
- 如果您的实例处于 Auto Scaling 组中，则 Amazon EC2 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。为防止出现此情况，您可以在更改实例类型时，为组暂停扩展流程。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的暂停和恢复 Auto Scaling 组的进程。
- 当您更改具有 NVMe 实例存储卷实例的实例类型时，更新后的实例可能会有更多实例存储卷，因为即使没有在 AMI 或实例块储存设备映射中指定，所有 NVMe 实例存储卷都可用。否则，已更新的实例通常具有您在启动原始实例时指定的相同实例存储卷数。

更改现有的 EBS 支持实例的实例类型

如果您想要的实例类型与实例的当前配置兼容，请按照以下说明来更改 EBS 支持的实例的实例类型。

更改由 Amazon EBS 支持的实例的实例类型

1. （可选）如果新实例类型需要现有实例上未安装的驱动程序，您必须先连接到您的实例并安装驱动程序。有关更多信息，请参阅更改实例类型的兼容性 (p. 402)。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择实例。
4. 选择所需实例，然后依次选择实例状态、停止实例。当系统提示您确认时，选择 Stop。停止实例可能需要几分钟时间。
5. 在实例处于选中状态时，依次选择操作、实例设置、更改实例类型。若实例状态不是 `stopped`，则此操作会显示为灰色。
6. 请在 Change instance type（更改实例类型）页面上执行以下操作：

   a. 对于 Instance type（实例类型），选择您所需的实例类型。

      如果列表中未包含该实例类型，则说明其与您的实例配置不兼容。请改为使用以下说明：通过启动新实例更改实例类型 (p. 401)。

   b. （可选）如果您选择的实例类型支持 EBS 优化，则选择 EBS-optimized（EBS 优化）以启用 EBS 优化，或取消选择 EBS-optimized（EBS 优化）以禁用 EBS 优化。如果您选择的实例类型默认情况下已经过 EBS 优化，则 EBS-optimized（EBS 优化）已选中，您无法取消选择。

   c. 选择 Apply（应用）以接受新设置。
7. 要启动实例，请选择该实例，然后依次选择 Instance state（实例状态）、Start instance（启动实例）。实例进入 `running` 状态可能需要几分钟时间。如果您的实例无法启动，请参阅 实例类型更改的问题排查 (p. 403)。

通过启动新实例更改实例类型

如果您的 EBS 支持的实例的当前配置与您所需的新实例类型不兼容，则无法更改原始实例的实例类型。您必须启动一个具有与您所需的新实例类型兼容的配置的新实例，并将应用程序迁移到新实例。例如，如果您从 PV AMI 启动了原始实例，但希望更改为仅受 HVM AMI 支持的当前一代实例类型，则需要从 HVM AMI 启动一个新的实例。有关如何确定兼容性的信息，请参阅 更改实例类型的兼容性 (p. 402)。

要将应用程序迁移到新实例，请执行以下操作：

- 备份原始实例上的数据。
- 启动一个具有与您所需的新实例类型兼容的配置的新实例，并将其附加至原始实例具有的所有 EBS 卷。
- 在您的新实例上安装应用程序和所有软件。
- 恢复所有数据。
- 如果您的原始实例具有弹性 IP 地址且您希望确保您的用户可不间断地继续使用新实例上的应用程序，那么必须将该弹性 IP 地址关联至新实例。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

如需为新的实例配置更改实例类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 备份需要保留的数据，如下所示：
   - 对于实例存储卷上的数据，请将这些数据备份到持久性存储中。
   - 对于 EBS 卷上的数据，请拍摄这些卷的快照 (p. 1372)或从实例中分离卷 (p. 1364)，以便您稍后可以将其附加到新的实例。
3. 在导航窗格中，选择实例。
4. 选择 Launch instances。配置实例时，执行以下操作：
   a. 选择支持您所需的实例类型的 AMI。请注意，当前一代的实例类型需要 HVM AMI。
   b. 选择所需的新实例类型。如果您所需的实例类型不可用，则说明其与您所选 AMI 的配置不兼容。
   c. 如果您正在使用弹性 IP 地址，请选择原始实例当前正在其中运行的 VPC。
   d. 如果您要允许相同的流量到达新实例，请选择与原始实例关联的安全组。
   e. 完成新实例的配置后，请完成以下步骤以选择密钥对并启动实例。实例进入 `running` 状态可能需要几分钟时间。
5. 如有需要，请将基于您创建的快照的所有新的 EBS 卷或您从原始实例中分离得到的所有 EBS 卷附加 (p. 1347)到新实例。
6. 在新实例上安装应用程序和所有必需软件。
7. 还原您在原始实例的实例存储卷中备份的所有数据。
8. 如果您正在使用弹性 IP 地址，请按如下所示将其分配给新实例：
   a. 在导航窗格中，选择 Elastic IPs。
   b. 选择与原始实例关联的弹性 IP 地址，然后依次选择操作、取消关联弹性 IP 地址。当系统提示进行确认时，选择取消关联。
   c. 在弹性 IP 地址仍处于选中状态的情况下，依次选择操作、关联弹性 IP 地址。
   d. 对于 Resource type (资源类型)，选择 Instance (实例)。
   e. 对于 Instance（实例），选择要将弹性 IP 地址关联到的实例。
   f. （可选）对于 Private IP address (私有 IP 地址)，请指定要将弹性 IP 地址关联到的私有 IP 地址。
   g. 选择 Associate。
9. (可选) 如果不再需要原始实例，您可以将其终止。选择实例，确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间），然后依次选择 Instance state（实例状态）、Terminate instance（终止实例）。

更改实例类型的兼容性

仅当实例的当前配置与您所需的实例类型兼容时，才能更改实例类型。如果您所需的实例类型与实例的当前配置不兼容，则您必须启动一个具有与新实例类型兼容的配置的新实例，并将应用程序迁移到新实例。

有关更改 Windows 实例类型的兼容性信息，请参阅《适用于 Windows 实例的用户指南》中的更改实例类型的兼容性。

可通过以下方式确定兼容性：

虚拟化类型

Linux AMI 使用两种虚拟化之一：半虚拟化 (PV) 或硬件虚拟机 (HVM)。如果是从 PV AMI 启动的实例，则您无法将其更改为仅限 HVM 的实例类型。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。要查看实例的虚拟化类型，请在 Amazon EC2 控制台中查看 Instances（实例）屏幕的详细信息窗格中的 Virtualization（虚拟化）值。

架构

AMI 特定于处理器的架构，因此您必须选择与当前实例类型具有相同处理器架构的实例类型。例如：

- 如果当前实例类型处理器是基于 Arm 架构的，则仅限于支持基于 Arm 架构的处理器的实例类型，例如 C6g 和 M6g。
- 只有以下实例类型支持 32 位 AMIs：`t2.nano`、`t2.micro`、`t2.small`、`t2.medium`、`c3.large`、`t1.micro`、`m1.small`、`m1.medium` 和 `c1.medium`。如需更改 32 位实例的实例类型，则仅限使用以下实例类型。

Network

较新的实例类型只能在 VPC 中启动。因此，您不能将 EC2-Classic 平台中的实例的实例类型更改为仅在 VPC 中可用的实例类型，除非您有非默认 VPC。要查看您的实例是否在 VPC 中，请在 Amazon EC2 控制台中查看 Instances (实例) 屏幕的详细信息窗格中的 VPC ID 值。有关更多信息，请参阅从 EC2-Classic 迁移到 VPC (p. 1211)。

网卡

有些实例类型支持多个网卡 (p. 1106)。您必须选择支持与当前实例类型相同数量的网卡的实例类型。

增强联网

支持增强联网 (p. 1142)的实例类型需要安装必要的驱动程序。例如，基于 Nitro 系统 (p. 246)的实例需要由 EBS 提供支持且安装有 Elastic Network Adapter (ENA) 驱动程序的 AMI。要将实例的实例类型从不支持增强联网的类型更改为支持增强联网的实例类型，必须根据需要在实例上安装 ENA 驱动程序 (p. 1143)或 ixgbevf 驱动程序 (p. 1158)。

> **Note**
>
> 在启用 ENA Express 的情况下调整实例大小时，新实例类型必须同时支持 ENA Express。有关支持 ENA Express 的实例类型列表，请参阅 ENA Express 支持的实例类型 (p. 1153)。要将实例类型从支持 ENA Express 更改为不支持 ENA Express，请确保在调整实例大小之前尚未启用 ENA Express。

NVMe

EBS 卷作为 NVMe 块存储设备在基于 Nitro 系统 (p. 246)构建的实例上公开。如果将实例类型不支持 NVMe 的实例的实例类型更改为支持 NVMe 的实例类型，您必须先在实例上安装 NVMe 驱动程序 (p. 1518)。此外，您在块储存设备映射中指定的设备的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。因此，要使用 `/etc/fstab` 在启动时挂载文件系统，必须使用 UUID/标签而非设备名称。

AMI

有关支持增强联网和 NVMe 的实例类型所需的 AMI 的信息，请参阅以下文档中的发行说明：

- 通用实例 (p. 252)
- 计算优化型实例 (p. 305)
- 内存优化型实例 (p. 322)
- 存储优化型实例 (p. 347)

实例类型更改的问题排查

使用以下信息可帮助您诊断和修复在更改实例类型时可能遇到的常见问题。

更改实例类型后，实例无法启动

可能的原因：未满足新实例类型的要求

如果您的实例未启动，则可能是新实例类型的某一要求未满足。有关更多信息，请参阅为什么我的 Linux 实例在更改其类型后无法启动？

可能的原因：AMI 不支持实例类型

若使用 EC2 控制台更改实例类型，则仅限所选 AMI 支持的实例类型可用。若使用 Amazon CLI 启动实例，则可以指定不兼容的 AMI 和实例类型。如果 AMI 和实例类型不兼容，则实例无法启动。有关更多信息，请参阅更改实例类型的兼容性 (p. 402)。

可能的原因：实例位于集群置放群组中

如果您的实例位于集群置放群组 (p. 1177)中，并且更改实例类型后实例无法启动，请尝试以下操作：

1. 停止集群置放群组中的所有实例。
2. 更改受影响的实例的实例类型。
3. 启动集群置放群组中的所有实例。

更改实例类型后，无法从互联网访问应用程序或网站

可能的原因：公有 IPv4 地址被释放

更改实例类型时，您必须先停止该实例。停止实例时，我们会释放公有 IPv4 地址并向该实例提供一个新的公有 IPv4 地址。

为了在实例停止和启动之间保留公有 IPv4 地址，我们建议您使用弹性 IP 地址，若您的实例处于运行中，则无需额外费用。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

更改实例存储支持的实例的实例类型

由实例存储支持的实例是具有实例存储根卷的实例。您无法更改具有实例存储根卷的实例的实例类型。相反，您必须从您的实例创建 AMI，并从此 AMI 启动新实例后选择您所需的实例类型，然后将应用程序迁移到新实例。请注意，您所需的实例类型必须与您创建的 AMI 兼容。有关如何确定兼容性的信息，请参阅 更改实例类型的兼容性 (p. 402)。

要将应用程序迁移到新实例，请执行以下操作：

- 备份原始实例上的数据。
- 从您的原始实例创建 AMI。
- 从此 AMI 中启动新实例并选择您所需的实例类型。
- 在新实例上安装应用程序。
- 如果您的原始实例具有弹性 IP 地址且您希望确保您的用户可不间断地继续使用新实例上的应用程序，那么必须将该弹性 IP 地址关联至新实例。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

如需更改实例存储支持的实例的实例类型

1. 备份需要保留的数据，如下所示：
   - 对于实例存储卷上的数据，请将这些数据备份到持久性存储中。
   - 对于 EBS 卷上的数据，请拍摄这些卷的快照 (p. 1372)或从实例中分离卷 (p. 1364)，以便您稍后可以将其附加到新的实例。
2. 通过满足先决条件并按照 创建由实例存储支持的 Linux AMI (p. 142) 中的过程执行，从实例创建 AMI。当您通过您的实例创建完 AMI 后，请返回到此过程。
3. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
4. 在导航窗格中，选择 AMIs。从筛选条件列表中，选择 Owned by me（我拥有的），然后选择您在步骤 2 中创建的镜像。请注意，AMI name（AMI 名称）是您在注册映像时指定的名称，而 Source（源）是您的 Amazon S3 存储桶。

   Note

   如果没有看到您在步骤 2 中创建的 AMI，请确保您已选择在其中创建了 AMI 的区域。
5. 选择 AMI 后，选择 Launch instance from image（从镜像启动实例）。配置实例时，执行以下操作：
   a. 选择所需的新实例类型。如果您所需的实例类型不可用，则说明其与您创建的 AMI 的配置不兼容。有关更多信息，请参阅更改实例类型的兼容性 (p. 402)。
   b. 如果您正在使用弹性 IP 地址，请选择原始实例当前正在其中运行的 VPC。
   c. 如果您要允许相同的流量到达新实例，请选择与原始实例关联的安全组。
   d. 完成新实例的配置后，请完成以下步骤以选择密钥对并启动实例。实例进入 `running` 状态可能需要几分钟时间。
6. 如有需要，请将基于您创建的快照的所有新的 EBS 卷或您从原始实例中分离得到的所有 EBS 卷附加 (p. 1347)到新实例。
7. 在新实例上安装应用程序和所有必需软件。
8. 如果您正在使用弹性 IP 地址，请按如下所示将其分配给新实例：
   a. 在导航窗格中，选择 Elastic IPs。
   b. 选择与原始实例关联的弹性 IP 地址，然后依次选择操作、取消关联弹性 IP 地址。当系统提示进行确认时，选择取消关联。
   c. 在弹性 IP 地址仍处于选中状态的情况下，依次选择操作、关联弹性 IP 地址。
   d. 对于 Resource type (资源类型)，选择 Instance (实例)。
   e. 对于 Instance（实例），选择要将弹性 IP 地址关联到的实例。
   f. （可选）对于 Private IP address (私有 IP 地址)，请指定要将弹性 IP 地址关联到的私有 IP 地址。
   g. 选择 Associate。
9. (可选) 如果不再需要原始实例，您可以将其终止。选择实例，确认您将要终止原始实例而不是新实例（例如，查看名称或启动时间），然后依次选择 Instance state（实例状态）、Terminate instance（终止实例）。

实例购买选项

Amazon EC2 提供了以下让您根据需求优化成本的购买选项：

- 按需型实例 – 按秒为启动的实例付费。
- 预留实例 – 通过承诺在 1 年或 3 年期限内提供一致的实例配置（包括实例类型和区域）来降低您的 Amazon EC2 成本。
- 竞价型实例 – 请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。

- 专用主机 – 为完全专用于运行您的实例的物理主机付费，让您现有的按插槽、按内核或按 VM 计费的软件许可证降低成本。
- 专用实例 – 为在单一租户硬件上运行的实例按小时付费。
- 预留容量 – 可在特定可用区中为 EC2 实例预留容量，持续时间不限。

如果您需要预留容量，请为特定可用区购买预留实例或预留容量。如果能灵活控制应用程序的运行时间并且您的应用程序可以中断，竞价型实例就是经济实惠之选。专用主机或专用实例可以通过使用现有服务器端绑定软件许可证来满足合规性要求和降低成本。有关更多信息，请参阅 Amazon EC2 定价。

目录

- 确定实例生命周期 (p. 405)
- 按需型实例 (p. 406)
- Reserved Instances (p. 408)
- Scheduled Reserved Instances (p. 447)
- Spot Instances (p. 448)
- Dedicated Hosts (p. 504)
- Dedicated Instances (p. 533)
- On-Demand Capacity Reservations (p. 538)

确定实例生命周期

实例的生命周在运行时开始，在停止时结束。您所选择的购买选项将影响实例的生命周期。例如，一个按需型实例将在您启动它时运行并在您终止它时结束。只要具有可用的容量，并且您的最高价高于 Spot 价格，竞价型实例就会运行。

使用以下任一方法来确定实例的生命周期。

使用控制台确定实例的生命周期

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 在详细信息选项卡中的实例详细信息下，找到生命周期。如果值为 `spot`，表示实例是竞价型实例。如果值为 `normal`，表示实例是按需型实例或预留实例。
5. 在详细信息选项卡中的主机和置放群组下，找到租期。如果值为 `host`，表示实例正在 专用主机 上运行。如果值为 `dedicated`，表示实例是 专用实例。

使用Amazon CLI来确定实例的生命周期。

使用以下描述实例口令：

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

如果实例正在专用主机上运行，那么输出内容包含以下信息：

```
"Tenancy": "host"
```

如果实例为专用实例，那么输出内容包含以下信息：

```
"Tenancy": "dedicated"
```

如果实例为竞价型实例，那么输出内容包含以下信息：

```
"InstanceLifecycle": "spot"
```

否则，输出不包含 `InstanceLifecycle`。

按需型实例

使用按需型实例，您按秒为计算容量支付费用，无需长期订阅。您可以完全控制其生命周期 — 您确定何时发布、停止、休眠、启动、重启或终止它。

购买按需型实例没有长期承诺。您只需要为处于 `running` 状态的按需型实例的秒数付费，最少 60 秒。运行中的个按需型实例的每秒价格是固定的，上列出了此价格。

我们建议您为短期的不规则且不能中断的应用程序使用按需型实例。

目录

- 使用 按需型实例 (p. 406)
- 个按需型实例限制 (p. 406)
    - 监控 个按需型实例 限制和使用情况 (p. 407)
    - 计算所需的 vCPU 数量 (p. 407)
    - 请求提高限制 (p. 408)
- 查询按需型实例的价格 (p. 408)

使用 按需型实例

您可以通过以下方式使用按需型实例：

- 启动实例 (p. 574)
- 连接到您的 Linux 实例 (p. 644)
- 停止和启动您的实例 (p. 610)
- 休眠 Linux 按需型实例 (p. 616)
- 重启实例 (p. 631)
- 实例指令引退 (p. 632)
- 终止实例 (p. 634)
- 恢复实例 (p. 640)
- 配置您的 Amazon Linux 实例 (p. 699)
- 识别 EC2 Linux 实例 (p. 808)

如果您是 Amazon EC2 的新用户，请参阅如何开始使用 Amazon EC2 (p. 1)。

个按需型实例限制

每个区域的每个 Amazon 账户运行的按需型实例数具有一定的限制。按需实例限制是根据运行的按需实例使用的虚拟中央处理器 (vCPU) 数进行管理的，而不论实例类型如何。

按需型实例具有以下限制：

- 正在运行的按需 DL 实例
- 正在运行的按需 F 实例
- 正在运行的按需 G 和 VT 实例

- 正在运行按需内存增强型实例
- 正在运行的按需型 HPC 实例
- 正在运行的按需 Inf 实例
- 正在运行的按需 P 实例
- 正在运行的按需标准（A、C、D、H、I、M、R、T、Z）实例
- 正在运行的按需型 Trn 实例
- 正在运行的按需 X 实例

每种限制指定了一个或多个实例系列的 vCPU 限制。有关不同实例系列、实例代和大小的信息，请参阅 Amazon EC2 实例类型。

只要 vCPU 数不超过您的账户限制，您就可以启动满足您不断变化的应用程序需求的任意实例类型组合。例如，对于 256 个 vCPU 的标准实例限制，您可以启动 32 个 `m5.2xlarge` 实例 (32 x 8 vCPU) 或 16 个 `c5.4xlarge` 实例 (16 x 16 vCPU)。有关更多信息，请参阅 EC2 个按需实例限制。

任务

- 监控 个按需型实例 限制和使用情况 (p. 407)
- 计算所需的 vCPU 数量 (p. 407)
- 请求提高限制 (p. 408)

监控 个按需型实例 限制和使用情况

您可以使用以下方法查看和管理按需型实例限制。

使用 Amazon EC2 控制台查看当前限制

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择一个区域。
3. 从导航窗格中，选择 Limits。
4. 从第一个筛选条件中选择正在运行的实例。当前限制列会显示账户中每种按需型实例类型的最大 vCPU 数量。

使用 Amazon Trusted Advisor 控制台查看当前限制

打开 Amazon Trusted Advisor 控制台中的服务限制页面。

配置 CloudWatch 告警

使用 Amazon CloudWatch 指标集成，您可以根据限制监控 EC2 使用情况。您还可以配置警报以警告即将达到限制。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的可视化服务配额并设置告警。

计算所需的 vCPU 数量

您可以使用 vCPU 限制计算器来确定应用程序需要的 vCPU 数。

使用计算器时，请注意：计算器假定您已达到当前限制。您为实例计数输入的值是在当前限制允许的数量之外您需要启动的实例数量。该计算器将您的当前限制添加到实例计数以获得新的限制。

您可以查看和使用以下控件和信息：

- 实例类型 – 您添加到 vCPU 限制计算器的实例类型。
- 实例计数 – 您需要的所选实例类型的实例数。
- vCPU 计数 – 与实例计数对应的 vCPU 数。

- 当前限制 – 实例类型所属的限制类型的当前限制。该限制应用到相同限制类型的所有实例类型。例如，在前面的屏幕截图中，m5.2xlarge 和 c5.4xlarge 的当前限制为 2016 个 vCPU，这是属于所有标准实例限制的所有实例类型的限制。
- 新限制 – 新限制以 vCPU 数量为单位，通过将 vCPU 计数与当前限制相加来计算。
- X – 选择 X 可删除行。
- 添加实例类型 – 选择添加实例类型可将其他实例类型添加到计算器。
- 限制计算 – 显示当前限制、所需 vCPU 以及限制类型的新限制。
  - 实例限制名称 – 您选择的实例类型的限制类型。
  - 当前限制 – 限制类型的当前限制。
  - 所需 vCPU – 与您在实例计数中指定的实例数对应的 vCPU 数。对于所有标准实例限制类型，需要的 vCPU 数通过将此限制类型的所有实例类型的 vCPU 计数相加得到。
  - 新限制 – 新限制通过将当前限制与所需 vCPU 相加得到。
  - 选项 – 选择请求提高限制可请求提高对应限制类型的限制。

计算所需 vCPU 数

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择一个区域。
3. 从左侧导航器，选择限制。
4. 选择计算 vCPU 限制。
5. 选择添加实例类型，选择所需实例类型，然后指定所需实例数。要添加更多实例类型，请再次选择添加实例类型。
6. 查看限制计算窗格，了解指定实例所需的新限制。
7. 使用完计算器后，您可以选择 Request on-demand limit increase（请求提高按需限制）或 Close（关闭）。

请求提高限制

即使 Amazon EC2 会根据您的使用情况自动增加按需型实例限制，您也可以在必要时请求提高限制。例如，如果您打算启动超过当前限制允许数量的实例，可以使用上一部分介绍的限制计算器或使用 Amazon EC2 Service Quotas (p. 1678) 所述的方法之一。

查询按需型实例的价格

可以使用价目表服务 API 或 Amazon 价目表 API 查询按需型实例的价格。有关更多信息，请参阅 Amazon Billing 用户指南中的使用Amazon价目表 API。

Reserved Instances

相比按需型实例定价，预留实例可大幅节约您的 Amazon EC2 成本。预留实例不是物理实例，而是对账户中使用的按需型实例所应用的账单折扣。这些按需型实例必须与特定属性（例如实例类型和区域）匹配才能享受账单折扣。

Note

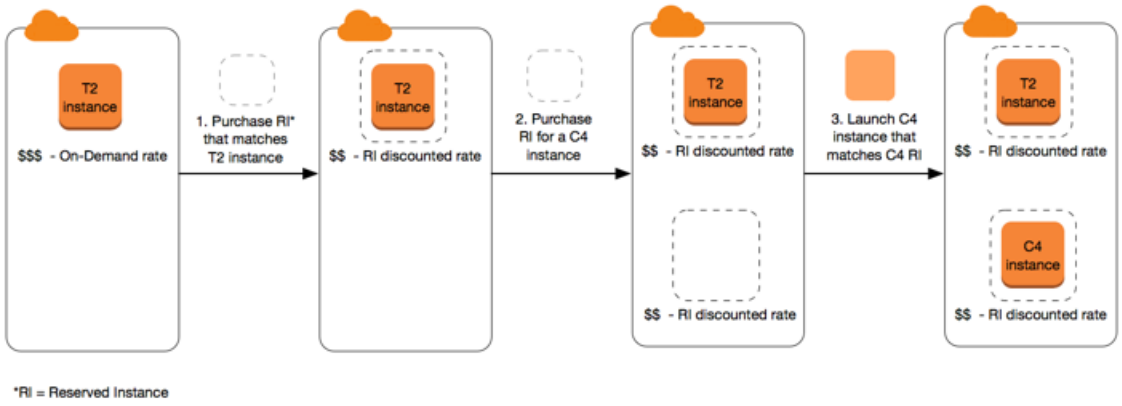
预留实例主题

- Reserved Instance概述 (p. 409)
- 决定Reserved Instance定价的关键变量 (p. 409)
- 区域和可用区预留实例（范围） (p. 410)
- 预留实例的类型（提供的类别） (p. 411)

- 如何应用预留实例 (p. 412)
- 使用您的 预留实例 (p. 417)
- 如何计费 (p. 418)
- 购买预留实例 (p. 422)
- 在预留实例 Marketplace 中销售 (p. 429)
- 修改 预留实例 (p. 434)
- 交换 可转换预留实例 (p. 441)
- 预留实例限额 (p. 445)

Reserved Instance概述

下图是购买和使用预留实例的基本概述。



在此场景中，您的账户中有一个正在运行的个按需型实例 (T2)，当前您按照按需费率支付。您购买了一个与您正在运行的实例的属性相匹配的Reserved Instance，账单优势立即体现。接下来，您为 C4 实例购买一个 Reserved Instance。您的账户中没有任何正在运行的实例与此Reserved Instance的属性相匹配。在最后的步骤中，您启动了一个与 C4 Reserved Instance的属性相匹配的实例，账单优势立即体现。

决定Reserved Instance定价的关键变量

Reserved Instance 定价由以下关键变量决定。

实例属性

预留实例有四个决定其价格的实例属性。

- 实例类型：例如，`m4.large`。这由实例系列（例如，`m4`）和实例大小（例如，`large`）组成。
- 区域：购买Reserved Instance的区域。
- 租赁：您的实例在共享 (默认) 还是单租户 (专用) 硬件上运行。有关更多信息，请参阅Dedicated Instances (p. 533)。
- 平台：操作系统；例如，Windows 或 Linux/Unix。有关更多信息，请参阅选择平台 (p. 422)。

期限承诺

您可以承诺购买一年或三年的 Reserved Instance，三年承诺可以获得更大的折扣。

- 一年：一年定义为 31536000 秒（365 天）。
- 三年：三年定义为 94608000 秒 (1095 天)。

预留实例不会自动续订；当它们过期时，可以继续使用 EC2 实例而不会中断，但要支付按需费率。在上面的示例中，当涵盖 T2 和 C4 实例的 预留实例 过期后，将改为以按需费率支付，直至终止这些实例或者购买与实例属性相匹配的新 预留实例。

Important

购买Reserved Instance后，您将不能取消您的购买。但是，如果您需要更改，则可以修改 (p. 434)、交换 (p. 441)或出售 (p. 429)您的 Reserved Instance。

付款选项

针对 预留实例 可使用以下付款选项：

- 预付全费：所有款项于期限开始时支付，无论使用了多少小时数，剩余期限不会再产生其他任何费用或额外按小时计算的费用。
- 预付部分费用：必须预付部分费用，无论是否使用了 Reserved Instance，期限内剩余的小时数都将按照打折小时费率计费。
- 无预付费用：无论是否使用 Reserved Instance，您都将按照期限内的小时数，采用打折小时费率进行付费。无需预付款。

Note

在整个预留期限内，“无预付费用”预留实例需要根据合同义务每月支付费用。因此，账户需要具有成功的账单历史记录才能购买“无预付”预留实例。

一般而言，通过为 预留实例 支付选较高的预付款，可以节省更多成本。您也可以在预留实例 Marketplace 中找到由第三方卖家以短期低价提供的预留实例。有关更多信息，请参阅在预留实例 Marketplace 中销售 (p. 429)。

优惠类别

在计算需求发生变化时，您可以根据产品类别修改或交换 Reserved Instance。

- 标准：这些提供最大力度的折扣，但只可以修改。标准 预留实例 无法交换。
- 可转换：这些相较于标准 预留实例 提供较低的折扣，但可以与具有不同实例属性的可转换 Reserved Instance 进行交换。可转换 预留实例 也可修改。

有关更多信息，请参阅预留实例的类型（提供的类别）(p. 411)。

Important

购买Reserved Instance后，您将不能取消您的购买。但是，如果您需要更改，则可以修改 (p. 434)、交换 (p. 441)或出售 (p. 429)您的 Reserved Instance。

有关更多信息，请参阅。

区域和可用区预留实例（范围）

当您购买 Reserved Instance 时，可决定 Reserved Instance 的范围。范围可以是区域或可用区。

- 区域：当您购买某个区域的 Reserved Instance，该实例称为区域性 Reserved Instance。
- 可用区：当您购买特定可用区的 Reserved Instance 时，该实例称为可用区 Reserved Instance。

范围不影响价格。您为区域或可用区 Reserved Instance 支付相同的价格。有关 Reserved Instance 定价的更多信息，请参阅决定Reserved Instance定价的关键变量 (p. 409)和Amazon EC2 预留实例定价。

有关如何指定预留实例范围的更多信息，请参阅 RI 属性，特别是可用区小点。

区域性或可用区预留实例之间的差异

下表重点介绍了区域性 预留实例 和可用区 预留实例 之间的一些主要区别：

	区域性预留实例	可用区预留实例
是否能够预留容量	区域性Reserved Instance无法预留容量。	可用区Reserved Instance可在指定可用区中预留容量。
可用区灵活性	Reserved Instance 折扣适用于指定区域的任何可用区中的实例使用。	无可用区灵活性 — Reserved Instance 折扣仅适用于指定可用区中的实例使用。
实例大小灵活性	Reserved Instance 折扣适用于实例系列中的实例使用，无论实例大小如何。 只在具有默认租期的 Amazon Linux/Unix 预留实例 上受支持。有关更多信息，请参阅实例大小灵活性由标准化因子决定 (p. 413)。	无实例大小灵活性 — Reserved Instance 折扣仅适用于指定实例类型和大小的实例使用。
排队购买	您可以排队购买区域预留实例。	您不能将可用区预留实例的购买排队。

有关更多信息以及示例，请参阅 如何应用预留实例 (p. 412)。

预留实例的类型（提供的类别）

Reserved Instance 的产品类别是标准或可转换。标准 Reserved Instance 提供的折扣比可转换 Reserved Instance 更多，但是您无法交换标准 Reserved Instance。您可以交换可转换 预留实例。您可以修改标准版和可转换 预留实例。

Reserved Instance 的配置包括单个实例类型、平台、范围和租期。在计算需求发生变化时，您可以修改或交换 Reserved Instance。

标准和可转换 预留实例 的差异

下面是标准和可转换 预留实例 之间的差别。

	标准Reserved Instance	Convertible Reserved Instance
修改 预留实例	有些属性可以修改。有关更多信息，请参阅修改 预留实例 (p. 434)。	有些属性可以修改。有关更多信息，请参阅修改 预留实例 (p. 434)。
交换预留实例	无法交换。	在期限内可以与具有新属性（包括实例系列、实例类型、平台、范围或租期）的其他 可转换预留实例 进行交换。有关更多信息，请参阅交换 可转换预留实例 (p. 441)。
在预留实例 Marketplace 中销售	可以在预留实例 Marketplace 中销售。	无法在预留实例 Marketplace 中销售。

	标准Reserved Instance	Convertible Reserved Instance
在预留实例 Marketplace 中购买	可以在预留实例 Marketplace 中购买。	无法在预留实例 Marketplace 中购买。

如何应用预留实例

预留实例不是物理实例，而是对账户中正在运行的按需型实例所应用的账单折扣。这些按需型实例必须与预留实例的特定规格匹配，才能享受账单折扣。

如果您购买了预留实例并且已经有正在运行的按需型实例与预留实例的规范匹配，则账单折扣将立即自动应用。您不必重启您的实例。若没有符合条件的正在运行的按需型实例，则请启动与您的预留实例具有相同规格的按需型实例。有关更多信息，请参阅使用您的 预留实例 (p. 417)。

预留实例的优惠类别（标准或可转换）不会影响账单折扣的应用方式。

主题

- 如何应用可用区预留实例 (p. 412)
- 如何应用区域性预留实例 (p. 412)
- 实例大小灵活性 (p. 412)
- 应用预留实例的示例 (p. 415)

如何应用可用区预留实例

为特定可用区中的预留容量而购买的预留实例称为地区性预留实例。

- 预留实例折扣适用于该可用区中匹配的实例使用。
- 正在运行的实例的属性 (租期、平台、可用区、实例类型和实例大小) 必须与预留实例的属性匹配。

例如，如果购买可用区 us-east-1a 中的两个 `c4.xlarge` 默认租期 Linux/Unix 标准预留实例，则可用区 us-east-1a 中最多两个正在运行的 `c4.xlarge` 默认租赁 Linux/Unix 实例可享受预留实例折扣。

如何应用区域性预留实例

为区域购买的预留实例称为区域性预留实例，可提供可用区和实例大小的灵活性。

- Reserved Instance 折扣适用于该区域的任何可用区中的实例使用。
- 预留实例折扣适用于实例系列中的实例使用，无论实例大小如何，这称为实例大小灵活性 (p. 412)。

实例大小灵活性

使用实例大小灵活性，预留实例折扣适用于实例系列中的实例使用。预留实例基于标准化因子应用于实例系列中各种规模的实例（从最小到最大）。有关如何应用预留实例折扣的示例，请参阅 场景 2：使用标准化因素在单个账户中使用预留实例 (p. 416)。

限制

实例大小灵活性仅适用于区域预留实例。

实例大小灵活性不适用于以下 预留实例：

- 针对特定可用区购买的 预留实例（可用区 预留实例）

- 使用专用租赁的预留实例
- 适用于 Windows Server、装有 SQL Standard 的 Windows Server、装有 SQL Server Enterprise 的 Windows Server、装有 SQL Server Web 的 Windows Server、RHEL 和 SUSE Linux Enterprise Server 的 预留实例
- G4ad、G4dn、G5、G5g 和 Inf1 实例的预留实例

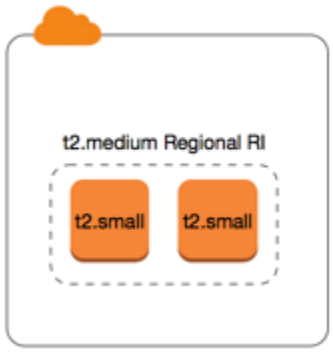
实例大小灵活性由标准化因子决定

实例大小灵活性取决于实例大小的标准化因子。根据预留的实例大小，区域中的任何可用区中的相同实例系列的运行实例将享受全部或部分折扣。必须匹配的属性仅为实例系列、租期和平台。

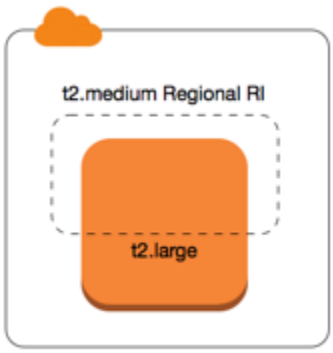
下表列出了实例系列中的各种大小以及相应的标准化因子。这种比例用于将 预留实例 的折扣费率应用于实例系列的标准化使用。

实例大小	标准化因子
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
56xlarge	448
112xlarge	896

例如，`t2.medium` 实例具有标准化因子 2。如果您在 US East (N. Virginia) 中购买了 `t2.medium` 默认租期 Amazon Linux/Unix Reserved Instance，并且您的账户在该区域中有两个正在运行的 `t2.small` 实例，则账单优势应用于全部两个实例。



或者，如果您的账户在 US East (N. Virginia) 区域有一个 `t2.large` 实例，则账单优势应用到 50% 的实例使用。



在修改预留实例时，标准化因子也适用。有关更多信息，请参阅修改 预留实例 (p. 434)。

裸机实例的标准化因子

实例大小灵活性也适用于实例系列中的裸机实例。如果您具有区域性 Amazon Linux/Unix 预留实例 并对裸机实例使用共享租期，则可以获得在相同实例系列中节省 Reserved Instance 的好处。反过来也是如此：如果您具有区域性 Amazon Linux/Unix 预留实例 并对与裸机实例相同的系列中的实例使用共享租期，则可以获得在裸机实例中节省 Reserved Instance 的好处。

`metal` 实例大小的标准化因子不是单一的。裸机实例的标准化因子与同一实例系列中的等效虚拟化实例大小相同。例如，`i3.metal` 实例与 `i3.16xlarge` 实例具有相同的标准化因子。

实例大小	标准化因子
`a1.metal`	32
`m5zn.metal` | `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144
`c5.metal` | `c5d.metal` | `i3en.metal` | `m5.metal` | `m5d.metal` | `m5dn.metal` | `m5n.metal` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r5dn.metal` | `r5n.metal`	192
`u-*.metal`	896

例如，i3.metal 实例的标准化因子为 128。如果您购买 US East (N. Virginia) 中的 i3.metal 默认租期 Amazon Linux/Unix Reserved Instance，则可以获得如下的账单优惠：

- 如果您在该区域的账户中有一个正在运行的 i3.16xlarge，则账单优惠全部应用于 i3.16xlarge 实例（i3.16xlarge 标准化因子 = 128）。
- 或者，如果您在该区域的账户中有两个正在运行的 i3.8xlarge 实例，则账单优惠全部应用于这两个 i3.8xlarge 实例（i3.8xlarge 标准化因子 = 64）。
- 或者，如果您在该区域的账户中有四个正在运行的 i3.4xlarge 实例，则账单优惠全部应用于所有四个 i3.4xlarge 实例（i3.4xlarge 标准化因子 = 32）。

反之亦然。例如，如果您购买 US East (N. Virginia) 中的两个 i3.8xlarge 默认租期 Amazon Linux/Unix 预留实例，并且您在该区域中有一个正在运行的 i3.metal 实例，则账单优惠全部应用于 i3.metal 实例。

应用预留实例的示例

以下方案涵盖了各种应用预留实例的方式。

- 方案 1：单个账户中的预留实例 (p. 415)
- 场景 2：使用标准化因素在单个账户中使用预留实例 (p. 416)
- 场景 3：关联账户中的区域性预留实例 (p. 416)
- 场景 4：关联账户中的可用区预留实例 (p. 417)

方案 1：单个账户中的预留实例

您在账户 A 中运行以下按需型实例：

- 4 x m3.large Linux，可用区 us-east-1a 中的默认租期实例
- 2 x m4.xlarge Amazon Linux，可用区 us-east-1b 中的默认租期实例
- 1 x c4.xlarge Amazon Linux，可用区 us-east-1c 中的默认租期实例

您在账户 A 中购买以下预留实例：

- 4 x m3.large，可用区 us-east-1a 中的默认租期 预留实例（容量为预留）
- 4 x m4.large Amazon Linux，区域 us-east-1 中的默认租期 预留实例
- 1 x c4.large Amazon Linux，区域 us-east-1 中的默认租期 预留实例

Reserved Instance优惠以下面方式应用：

- 四个 m3.large 地区性 预留实例 的折扣和容量预留将由四个 m3.large 实例使用，因为它们之间的属性（实例大小、区域、平台、租期）相匹配。
- m4.large 区域性 预留实例 具备可用区和实例大小灵活性，因为它们是带默认租期的区域性 Amazon Linux 预留实例。

  m4.large 等效于 4 个标准化单位/小时。

  您已购买四个 m4.large 区域性 预留实例，它们加起来等效于 16 个标准化单位/小时 (4x4)。账户 A 具有两个正在运行的 m4.xlarge 实例，等效于 16 个标准化单位/小时 (2x8)。这种情况下，四个 m4.large 区域性预留实例可享受使用两个 m4.xlarge 实例的全部成本优势。
- us-east-1 中的 c4.large 区域 Reserved Instance 提供了可用区和实例大小灵活性，因为它是带默认租期的区域 Amazon Linux Reserved Instance，并且将应用于 c4.xlarge 实例。c4.large 实例等效于 4 个标准化单位/小时，c4.xlarge 等效于 8 个标准化单位/小时。

  在这种情况下，c4.large 区域 Reserved Instance 提供了针对 c4.xlarge 用量的部分优势。这是因为 c4.large Reserved Instance 等效于 4 个标准化单位/小时的用量，而 c4.xlarge 实例需要 8 个标准

化单位/小时。因此，c4.large Reserved Instance 账单折扣应用于 50% 的 c4.xlarge 用量。剩余的 c4.xlarge 用量按照按需费率收费。

场景 2：使用标准化因素在单个账户中使用预留实例

您在账户 A 中运行以下按需型实例：

- 2 x m3.xlarge Amazon Linux，可用区 us-east-1a 中的默认租期实例
- 2 x m3.large Amazon Linux，可用区 us-east-1b 中的默认租期实例

您在账户 A 中购买以下预留实例：

- 1 x m3.2xlarge Amazon Linux，区域 us-east-1 中的默认租期预留实例

Reserved Instance优惠以下面方式应用：

- us-east-1 中的 m3.2xlarge 区域预留实例提供了可用区和实例大小灵活性，因为它是带默认租期的区域 Amazon Linux 预留实例。它首先适用于 m3.large 实例，然后适用于 m3.xlarge 实例，因为它根据标准化因子应用于实例系列中从最小到最大的实例大小。

  m3.large 实例等效于 4 个标准化单位/小时。

  m3.xlarge 实例等效于 8 个标准化单位/小时。

  m3.2xlarge 实例等效于 16 个标准化单位/小时。

  该益处应用如下：

  m3.2xlarge 区域性预留实例为 2 x m3.large 使用提供充分的益处，因为这些实例加起来占 8 个标准化单位/小时。这会使 8 个标准化单位/小时适用于 m3.xlarge 实例。

  对于剩余 8 个标准化单位/小时，m3.2xlarge 区域性预留实例为 1 x m3.xlarge 使用提供充分益处，因为每个 m3.xlarge 实例等效于 8 个标准化单位/小时。剩余的 m3.xlarge 用量按照按需费率收费。

场景 3：关联账户中的区域性预留实例

预留实例首先供购买它们的账户使用，然后供组织中符合条件的任何其他账户使用。有关更多信息，请参阅预留实例和整合账单 (p. 420)。对于具备大小灵活性的区域性预留实例，这种优势适用于实例系列中各种规模的实例 (从最小到最大)。

您在账户 A (购买账户) 中运行以下按需型实例：

- 2 x m4.xlarge Linux，可用区 us-east-1a 中的默认租期实例
- 1 x m4.2xlarge Linux，可用区 us-east-1b 中的默认租期实例
- 2 x c4.xlarge Linux，可用区 us-east-1a 中的默认租期实例
- 1 x c4.2xlarge Linux，可用区 us-east-1b 中的默认租期实例

另一个客户在账户 B（链接账户）中运行以下 按需型实例：

- 2 x m4.xlarge Linux，可用区 us-east-1a 中的默认租期实例

您在账户 A 中购买以下区域性预留实例：

- 4 x m4.xlarge Linux，区域 us-east-1 中的默认租期 预留实例

- 2 x c4.xlarge Linux，区域 us-east-1 中的默认租期 预留实例

区域Reserved Instance优惠以下面方式应用：

- 四个 m4.xlarge 预留实例 的折扣将由两个 m4.xlarge 实例和账户 A（购买账户）中的单个 m4.2xlarge 实例使用。所有三个实例均与这些属性相匹配（实例系列、区域、平台和租期）。折扣将首先应用于购买账户（账户 A）中的实例，即使账户 B（链接账户）具有两个也匹配 预留实例 的 m4.xlarge。由于 预留实例 是区域性 预留实例，因此没有容量预留。
- 两个 c4.xlarge 预留实例 的折扣适用于两个 c4.xlarge，因为它们比 c4.2xlarge 实例小。由于 预留实例 是区域性 预留实例，因此没有容量预留。

场景 4：关联账户中的可用区预留实例

通常，某个账户拥有的预留实例首先供该账户自用。不过，如果组织的其他账户中有适用于特定可用区、符合条件的未使用 预留实例（地区性 预留实例），这些实例将先于账户拥有的区域性 预留实例 应用于账户。这样做是为了确保实现最大Reserved Instance使用率和较低的费用。出于记账目的，组织中的所有账户将被视为一个账户。以下示例可能有助于您理解。

您在账户 A (购买账户) 中运行以下个按需型实例：

- 1 x m4.xlarge Linux，可用区 us-east-1a 中的默认租期实例

某个客户在关联账户 B 中运行了以下个按需型实例：

- 1 x m4.xlarge Linux，可用区 us-east-1b 中的默认租期实例

您在账户 A 中购买以下区域性预留实例：

- 1 x m4.xlarge Linux，区域 us-east-1 中的默认租期 Reserved Instance

客户还在关联账户 C 中购买了以下区预留实例：

- 1 x m4.xlarge Linux，可用区 us-east-1a 中的默认租期 预留实例

Reserved Instance优惠以下面方式应用：

- 账户 C 拥有的 m4.xlarge 地区性 Reserved Instance 的折扣应用于账户 A 中的 m4.xlarge 用量。
- 账户 A 拥有的 m4.xlarge 区域性 Reserved Instance 的折扣应用于账户 B 中的 m4.xlarge 用量。
- 如果账户 A 拥有的区域性 Reserved Instance 先应用于账户 A 中的用量，则账户 C 拥有的地区性 Reserved Instance 将保持未使用状态，而账户 B 中的用量将按照按需费率收费。

有关更多信息，请参阅 Billing and Cost Management 报告中的 预留实例。

使用您的 预留实例

预留实例 将自动应用于正在运行的 按需型实例（前提匹配规范）。如果正在运行的 按需型实例 都与 Reserved Instance 的规范不匹配，则不会使用 Reserved Instance，直到您启动具有指定规范的实例。

如果您要启动按需型实例以利用预留实例的账单收益，请确保您在配置按需型实例时指定了以下信息：

平台

您必须指定与您预留实例的平台（产品说明）相匹配的 Amazon Machine Image (AMI)。例如，如果您为预留实例指定 Linux/UNIX，则可以从 Amazon Linux AMI 或 Ubuntu AMI 启动实例。

实例类型

如果您购买了可用区预留实例，则必须指定与您的预留实例相同的实例类型，例如：t3.large。有关更多信息，请参阅如何应用可用区预留实例 (p. 412)。

如果您购买了区域性预留实例，则必须指定与预留实例的实例类型相同的实例系列中的实例类型。例如，如果您为预留实例指定 t3.xlarge 作为实例类型，则您必须从 T3 系列启动实例，但可指定其为任意大小，例如 t3.medium。有关更多信息，请参阅如何应用区域性预留实例 (p. 412)。

可用区：

如果您为特定可用区购买了可用区预留实例，则必须在相同的可用区中启动实例。

如果您购买了区域性预留实例，则可以在任何您为该预留实例指定的区域的可用区中启动实例。

租赁

实例的租赁必须与预留实例的租赁匹配；例如 dedicated 或 shared。有关更多信息，请参阅Dedicated Instances (p. 533)。

有关如何将预留实例应用于正在运行的按需型实例的示例，请参阅 如何应用预留实例 (p. 412)。有关更多信息，请参阅为什么我的 Amazon EC2 预留实例没有以我期望的方式应用于我的 Amazon 账单？

您可以使用多种方法来启动使用您的预留实例折扣的按需型实例。有关不同启动方法的信息，请参阅 启动实例 (p. 574)。您也可以使用 Amazon EC2 Auto Scaling 来启动实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。

如何计费

与按需定价不同，所有预留实例都提供折扣。使用预留实例时，无论实际使用情况如何，都需要为整个期限付费。您可以根据为 Reserved Instance 指定的付款选项 (p. 410)，为 Reserved Instance 选择预付、部分预付或按月付费。

预留实例过期后，需要根据按需费率支付 EC2 实例使用费用。您最早可以提前三年排队购买 Reserved Instance。这样可以帮助您确保获得不中断的服务。有关更多信息，请参阅排队购买 (p. 423)。

AmazonFree Tier（免费套餐）可供新 Amazon 账户使用。如果您正在用 AmazonFree Tier（免费套餐）运行 Amazon EC2 实例，然后购买了一个预留实例，那么将按照标准定价指南付费。有关信息，请参阅 AmazonFree Tier（免费套餐）。

目录

- 使用情况计费 (p. 418)
- 查看您的账单 (p. 419)
- 预留实例和整合账单 (p. 420)
- Reserved Instance折扣定价套餐 (p. 420)

使用情况计费

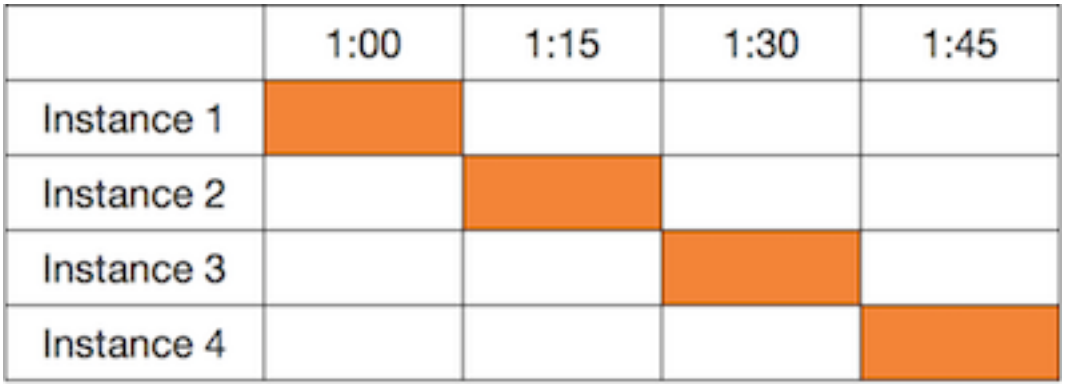
在选择的预留实例期限内，无论实例是否运行，预留实例均按小时计费。每时钟小时从标准 24 小时制的整点（该小时经过了零分零秒）开始。例如，1:00:00 到 1:59:59 是一个时钟小时。有关实例状态的更多信息，请参阅 实例生命周期 (p. 570)。

Reserved Instance账单优势适用于按秒收费的运行实例。每秒计费适用于使用开源 Linux 发行版的实例，例如 Amazon Linux 和 Ubuntu。每小时计费用于商业 Linux 发行版，例如 Red Hat Enterprise Linux 和 SUSE Linux Enterprise Server。

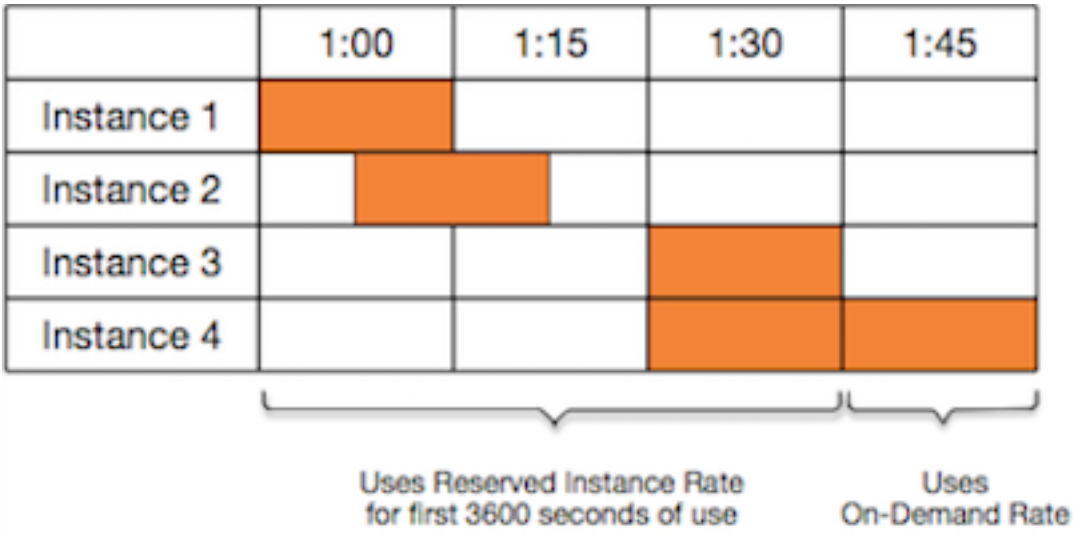
Reserved Instance账单优势适用于每小时最多 3600 秒 (一小时) 的实例使用。您可同时运行多个实例，但每小时只能获得总计 3600 秒的Reserved Instance折扣优惠；每小时超出 3600 秒的实例使用将根据按需费率计费。

例如，如果您购买了一个 m4.xlarge Reserved Instance，同时运行 4 个 m4.xlarge 实例 1 小时，则一个实例将按 1 小时的Reserved Instance使用收费，其他三个实例将按 3 小时的按需使用收费。

但是，如果您购买一个 m4.xlarge Reserved Instance，在同一小时内运行 4 个 m4.xlarge 实例各 15 分钟（900 秒），那么实例的总运行时间为 1 小时，这将产生 1 小时的Reserved Instance使用和 0 小时的按需使用。



如果多个合格实例同时运行，Reserved Instance账单优势将在一小时内（最多 3600 秒）同时适用于所有实例；在该时间后，根据按需费率收取费用。



使用 Billing and Cost Management 控制台上的 Cost Explorer (成本管理器) 可以分析运行 按需实例 所节省的成本。预留实例 常见问题包括标价计算的示例。

如果您关闭 Amazon 账户，则您资源的按需计费会停止。不过，如果账户中有任何预留实例，则会继续收到这些实例的账单，直至实例过期。

查看您的账单

您可通过查看 Amazon Billing and Cost Management 控制台来了解您的账户的费用情况。

- 控制面板显示了您的账户的花费汇总。
- 在 Bills (账单) 页面的 Details (详细信息) 下，展开 Elastic Compute Cloud 部分及区域，以了解有关您的预留实例 的账单信息。

您可以在线查看费用，也可以下载 CSV 文件。

您还可以使用Amazon成本和使用情况报告来跟踪您的预留实例使用情况。有关更多信息，请参阅 Amazon Billing 用户指南中的“成本和使用情况报告”下的预留实例。

预留实例和整合账单

如果购买者账户是在一个整合账单付款人账户之下计费的一组账户中的其中之一，则可以共享预留实例定价优惠。每月将在付款人账户中汇总所有成员账户的实例使用量。这通常对具有不同职能团队或团体的公司很有用；然后，将应用正常的Reserved Instance逻辑来计算账单。有关更多信息，请参阅 Amazon Organizations 的整合账单。

如果您关闭购买预留实例的账户，会继续向付款人账户收取预留实例的费用，直到预留实例过期为止。已关闭的账户永久删除后，成员账户不再享受预留实例账单折扣。

Reserved Instance折扣定价套餐

如果您的账户有资格获得折扣定价套餐，那么自您取得该资格时起，您在该套餐等级内购买的Reserved Instance的预付费和实例使用费均自动享受折扣。要取得折扣资格，在该区域内的 预留实例 的标价必须达到 500000 美元或更高。

以下规则适用：

- 定价套餐和相关折扣仅适用于购买 Amazon EC2 标准 预留实例。
- 定价套餐不适用于面向带 SQL Server Standard、SQL Server Web 和 SQL Server Enterprise 的 Windows 的 预留实例。
- 定价套餐不适用于面向带 SQL Server Standard、SQL Server Web 和 SQL Server Enterprise 的 Linux 的预留实例。
- 定价套餐折扣仅适用于通过 Amazon 进行的购买。这些折扣不适用于第三方预留实例购买。
- 折扣定价套餐当前不适用于可转换预留实例购买。

主题

- 计算 Reserved Instance 定价折扣 (p. 420)
- 以折扣套餐价格购买 (p. 421)
- 跨越定价套餐 (p. 421)
- 定价套餐的整合账单 (p. 422)

计算 Reserved Instance 定价折扣

通过计算在区域中的所有 预留实例 的标价，可以确定账户所适用的定价套餐。将每个预留的每小时费用乘以期限的总小时数，再加上购买时的未打折预付价格（也称为固定价格）。因为价目表值基于未打折 (公开) 定价，是否有资格获得批量折扣或者购买预留实例后是否降价均不影响价目表值。

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

例如，对于一年期部分预付 `t2.small` Reserved Instance，假定预付价格是 60.00 美元，每小时费率为 0.007 美元。这将提供 121.32 美元的标价。

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

使用 Amazon EC2 控制台查看 预留实例 的固定价格

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Reserved Instances。
3. 要显示 Upfront price (预付价格) 列，请选择右上角的设置图标 ()，开启 Upfront price (预付价格)，然后选择 Confirm (确认)。

Old console

使用 Amazon EC2 控制台查看 预留实例 的固定价格

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 要显示 Upfront Price (预付价格) 列，请选择右上角的设置图标 ()，选择 Upfront Price (预付价格)，然后选择 Close (关闭)。

使用命令行查看 预留实例 的固定价格

- describe-reserved-instances (Amazon CLI)
- Get-EC2ReservedInstance (Amazon Tools for Windows PowerShell)
- DescribeReservedInstances (Amazon EC2 API)

以折扣套餐价格购买

购买 预留实例 时，Amazon EC2 自动将所有折扣应用于所购产品处于折扣定价套餐范围内的部分。您无需执行任何其他操作，而且可以使用任何 Amazon EC2 工具购买 预留实例。有关更多信息，请参阅购买预留实例 (p. 422)。

在某区域的活动 预留实例 的标价达到某一折扣定价套餐范围后，以后在该区域购买任何 预留实例 都将按打折费率计费。如果在某区域的 预留实例 单项购买额超过折扣套餐阈值，则该项购买超出价格阈值的部分将按打折费率计费。有关在购买过程中创建的临时 Reserved Instance ID 的更多信息，请参阅跨越定价套餐 (p. 421)。

如果标价降至低于折扣定价套餐价格点（例如，如果部分 预留实例 到期），之后在该区域购买 预留实例 将不享受折扣。不过，原来在折扣定价套餐范围内购买的所有预留实例将继续享受折扣。

购买预留实例时，可能出现以下四种情况之一：

- 没有折扣 — 您在某区域内的购买仍然低于折扣阈值。
- 部分折扣 — 您在某区域内的购买跨越了第一折扣套餐的阈值。没有折扣将应用于一个或多个预留，而折扣费率将应用于剩余的预留。
- 全部折扣 — 您在某区域内的购买全部在一个折扣套餐之内并且获得了相应的折扣。
- 两种折扣率 — 您在某区域内的购买从较低折扣套餐跨入较高的折扣套餐。您将按两种费率付费：一个或多个预留采用较低的折扣费率，剩余的预留采用较高的折扣费率。

跨越定价套餐

如果您的购买跨入某个折扣定价套餐范围，您将看到该项购买有多个条目：一个条目显示购买中将按常规价格收费的部分，另一个条目显示购买中将按适用的打折费率收费的部分。

Reserved Instance 服务会生成多个 Reserved Instance ID，因为您的购买从未打折套餐跨入到打折套餐，或从一个打折套餐跨入到另一个打折套餐。套餐中的每组预留都有一个 ID。因此，由购买 CLI 命令或 API 操作返回的 ID 不同于新预留实例的实际 ID。

定价套餐的整合账单

整合账单账户汇总了某个区域内所有成员账户的标价。当整合账单账户的所有活动 预留实例 的标价达到折扣定价套餐时，整合账单账户的任何账户成员在此后购买任何 预留实例 都将享受打折费率（前提是整合账单账户的标价始终高于折扣定价套餐阈值）。有关更多信息，请参阅预留实例和整合账单 (p. 420)。

购买预留实例

要购买预留实例，请从Amazon和第三方卖家搜索预留实例产品，调整搜索参数，直至您找到与您的目标完全相符的对象。

在搜索要购买的预留实例时，您将收到一个关于退还产品的成本报价。当您继续购买时，Amazon 将自动对购买价格设定一个限定价格。预留实例的总成本不会超过报价金额。

如果价格由于任何原因上升或变动，将不会完成购买。如果在购买之时有与您的选择类似的低价位产品，Amazon 将为您提供价格更低的产品。

在确认购买之前，请检查您计划购买的Reserved Instance的详细信息，并确保所有参数都是准确的。在您购买预留实例之后（无论是从预留实例 Marketplace 中的第三方卖家购买还是从 Amazon 购买），将无法取消您的购买。

> Note
>
> 要购买和修改预留实例，请确保您的用户具有相应的权限，例如描述可用区的能力。有关更多信息，请参阅使用 Amazon CLI 或Amazon开发工具包的示例策略和在 Amazon EC2 控制台中工作的示例策略。

主题

- 选择平台 (p. 422)
- 排队购买 (p. 423)
- 购买标准 预留实例 (p. 423)
- 购买 可转换预留实例 (p. 425)
- 从预留实例 Marketplace 中购买 (p. 427)
- 查看您的 预留实例 (p. 428)
- 取消已排队的购买 (p. 428)
- 续订 Reserved Instance (p. 429)

选择平台

Amazon EC2 支持以下适用于 预留实例 的 Linux 平台：

- Linux/UNIX
- 含有 SQL Server Standard 的 Linux
- 含有 SQL Server Web 的 Linux
- 含有 SQL Server Enterprise 的 Linux
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux with HA

您购买 Reserved Instance 时，必须选择面向代表您的实例的操作系统的平台 的产品。

- 对于 SUSE Linux 和 RHEL 发行版，您必须选择适用于这些特定平台（即 SUSE Linux 或 Red Hat Enterprise Linux 平台）的服务产品。
- 对于所有其他 Linux 分配 (包括 Ubuntu)，选择面向 Linux/UNIX 平台的服务产品。

- 如果您使用现有的 RHEL 订阅，则必须选择适用于 Linux/UNIX 平台而不是 Red Hat Enterprise Linux 平台的服务产品。

  Important

  如果您计划购买预留实例以应用于从 Amazon Web Services Marketplace AMI 启动的按需型实例，请首先检查 AMI 的 `PlatformDetails` 字段。`PlatformDetails` 字段指示要购买的Reserved Instance。AMI 的平台详细信息必须与预留实例的平台匹配，否则预留实例将不会应用于个按需型实例。有关如何查看 AMI 平台详细信息的信息，请参阅 了解 AMI 账单信息 (p. 204)。

有关所支持的 Windows 平台的信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的选择平台。

排队购买

默认情况下，当您购买时 Reserved Instance，购买立即完成。或者，您也可以排队预约在将来的某个日期和时间购买。例如，您可以排队预约在现有 Reserved Instance 到期的时间购买。这样可以帮助您确保获得不中断的服务。

您可以排队购买区域 预留实例，但不能排队购买其他卖家的区域 预留实例 或 预留实例。您最早可以提前三年排队购买。在指定日期和时间，将使用默认支付方式进行购买。支付成功后，将体现账单优势。

您可以在 Amazon EC2 控制台中查看已排队的购买。已排队的购买的状态为已排队。在指定时间之前，您随时可以取消已排队的购买。有关详细信息，请参阅 取消已排队的购买 (p. 428)。

购买标准 预留实例

您可以购买特定可用区中的标准预留实例从而获得容量预留。或者，您也可以放弃容量预留并购买区域性标准Reserved Instance。

New console

使用控制台购买标准 预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances (预留实例)，然后选择 Purchase 预留实例 (购买 预留实例)。
3. 对于 Offering class (服务类别)，选择 Standard (标准) 以显示标准 预留实例。
4. 要购买容量预留，请在购买屏幕的右上角开启 Only show offerings that reserve capacity (只显示预留容量的产品)。开启此设置后，Availability Zone (可用区) 字段将会出现。

   要购买区域 Reserved Instance，请关闭此设置。关闭此设置后，Availability Zone (可用区) 字段将会消失。
5. 根据需要选择其他配置，然后选择 Search (搜索)。
6. 对于您要购买的每个 Reserved Instance，输入所需数量，然后选择 Add to cart (添加到购物车)。

   要从预留实例市场购买标准预留实例，请在搜索结果的 Seller (卖家) 列中查找 3rd party (第三方)。Term 列会显示非标准期限。有关更多信息，请参阅从预留实例 Marketplace 中购买 (p. 427)。
7. 要查看已选择的 预留实例 的汇总，请选择 View cart (查看购物车)。
8. 如果 Order on (订购时间) 为 Now (现在)，则在您选择 Order all (全部订购) 后，购买将立即完成。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。购买已排队，一直到选定日期 UTC 00:00 之前。
9. 要完成订单，请选择 Order all (全部订购)。

   如果在下订单时有与您的选择类似的低价位产品，Amazon 将为您提供价格更低的产品。

10. 选择 Close。

    您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 `Payment-pending` 变为 `Active`。当 Reserved Instance 的状态为 `Active` 时即可使用。

    Note

    如果状态转为 `Retired`，Amazon 可能未收到您的付款。

Old console

使用控制台购买标准 预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances (预留实例)，然后选择 Purchase 预留实例 (购买 预留实例)。
3. 对于 Offering Class (产品类别)，选择 Standard (标准) 以显示标准 预留实例。
4. 要购买容量预留，请选择购买屏幕右上角中的 Only show offerings that reserve capacity。要购买区域性Reserved Instance，请保留复选框未选中。
5. 根据需要选择其他配置并选择 搜索。

   要从预留实例市场购买标准预留实例，请在搜索结果的 Seller (卖家) 列中查找 3rd Party (第三方)。Term 列会显示非标准期限。
6. 对于您要购买的每个 Reserved Instance，输入数量，然后选择 Add to Cart (添加到购物车)。
7. 要查看已选择的 预留实例 的汇总，请选择 View Cart (查看购物车)。
8. 如果 Order On (订购日期) 为 Now (现在)，则会立即完成购买。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。购买已排队，一直到选定日期 UTC 00:00 之前。
9. 要完成订单，请选择 Order (订单)。

   如果在下订单时有与您的选择类似的低价位产品，Amazon 将为您提供价格更低的产品。
10. 选择 Close。

    您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 `payment-pending` 变为 `active`。当 Reserved Instance 的状态为 `active` 时即可使用。

    Note

    如果状态转为 `retired`，Amazon 可能未收到您的付款。

使用 Amazon CLI 控制台购买标准预留实例

1. 使用 describe-reserved-instances-offerings 命令查找可用 预留实例。为 `standard` 参数指定 `--offering-class` 以仅返回标准 预留实例。可以应用更多参数来缩小结果范围。例如，如果仅希望为 `t2.large` 购买具有默认租期的一年期区域性 `Linux/UNIX` Reserved Instance：

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

   要仅在预留实例 Marketplace 上查找预留实例，请使用 `marketplace` 筛选条件并在请求中不指定持续时间，因为期限可能会短于 1 年期或 3 年期。

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

当您找到符合需求的 Reserved Instance 时，请记下产品 ID。例如：

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. 使用 purchase-reserved-instances-offering 命令购买您的 Reserved Instance。您必须指定在上一步中获取的Reserved Instance产品 ID，并且必须为预留指定实例数量。

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

默认情况下，会立即完成购买。或者，若要排队购买，请在之前的调用中增加以下参数。

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. 使用 describe-reserved-instances 命令获取您的 Reserved Instance 的状态。

```
aws ec2 describe-reserved-instances
```

或者，使用以下 Amazon Tools for Windows PowerShell 命令：

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

购买完成后，如果已有正在运行的与 Reserved Instance 规范匹配的实例，账单优势将立即体现。您不必重启您的实例。如果您没有合适的运行实例，请启动实例并确保符合您为Reserved Instance指定的相同标准。有关更多信息，请参阅使用您的 预留实例 (p. 417)。

有关如何将 预留实例 应用于正在运行的实例的示例，请参阅如何应用预留实例 (p. 412)。

购买 可转换预留实例

您可以购买特定可用区中的可转换预留实例从而获得容量预留。或者，您也可以放弃容量预留并购买区域性可转换预留实例。

New console

使用控制台购买 可转换预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances (预留实例)，然后选择 Purchase 预留实例 (购买 预留实例)。
3. 对于 Offering class (服务类别)，选择 Convertible (可转换) 以显示 可转换预留实例。
4. 要购买容量预留，请在购买屏幕的右上角开启 Only show offerings that reserve capacity (只显示预留容量的产品)。开启此设置后，Availability Zone (可用区) 字段将会出现。

要购买区域 Reserved Instance，请关闭此设置。关闭此设置后，Availability Zone (可用区) 字段将会消失。

5. 根据需要选择其他配置并选择 搜索。
6. 对于您要购买的每个 可转换预留实例，输入数量，然后选择 Add to cart (添加到购物车)。
7. 要查看您的选择的摘要，请选择 View cart (查看购物车)。
8. 如果 Order on (订购时间) 为 Now (现在)，则在您选择 Order all (全部订购) 后，购买将立即完成。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。购买已排队，一直到选定日期 UTC 00:00 之前。
9. 要完成订单，请选择 Order all (全部订购)。

   如果在下订单时有与您的选择类似的低价位产品，Amazon 将为您提供价格更低的产品。
10. 选择 Close。

    您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 `Payment-pending` 变为 `Active`。当 Reserved Instance 的状态为 `Active` 时即可使用。

    Note

    如果状态转为 `Retired`，Amazon 可能未收到您的付款。

Old console

使用控制台购买 可转换预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances (预留实例)，然后选择 Purchase 预留实例 (购买 预留实例)。
3. 对于 Offering Class (产品类别)，选择 Convertible (可转换) 以显示 可转换预留实例。
4. 要购买容量预留，请选择购买屏幕右上角中的 Only show offerings that reserve capacity。要购买区域性Reserved Instance，请保留复选框未选中。
5. 根据需要选择其他配置并选择 搜索。
6. 对于您要购买的每个 可转换预留实例，输入数量，然后选择 Add to Cart (添加到购物车)。
7. 要查看您的选择的摘要，请选择 View cart (查看购物车)。
8. 如果 Order On (订购日期) 为 Now (现在)，则会立即完成购买。要排队购买，请选择 Now (现在) 并选择一个日期。您可以为购物车中每个符合条件的产品选择不同的日期。购买已排队，一直到选定日期 UTC 00:00 之前。
9. 要完成订单，请选择 Order (订单)。

   如果在下订单时有与您的选择类似的低价位产品，Amazon 将为您提供价格更低的产品。
10. 选择 Close。

    您的订单状态将在 State (状态) 列中列出。当您的订单完成时，State (状态) 值将从 `payment-pending` 变为 `active`。当 Reserved Instance 的状态为 `active` 时即可使用。

    Note

    如果状态转为 `retired`，Amazon 可能未收到您的付款。

使用 Amazon CLI 购买可转换预留实例

1. 使用 describe-reserved-instances-offerings 命令查找可用 预留实例。为 `convertible` 参数指定 `--offering-class` 以仅返回 可转换预留实例。可以应用更多参数来缩小结果范围；例如，如果仅希望为 `t2.large` 购买具有默认租期的区域性 `Linux/UNIX` Reserved Instance：

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

当您找到符合需求的 Reserved Instance 时，请记下产品 ID。例如：

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. 使用 purchase-reserved-instances-offering 命令购买您的 Reserved Instance。您必须指定在上一步中获取的Reserved Instance产品 ID，并且必须为预留指定实例数量。

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

默认情况下，会立即完成购买。或者，若要排队购买，请在之前的调用中增加以下参数。

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. 使用 describe-reserved-instances 命令获取您的 Reserved Instance 的状态。

```
aws ec2 describe-reserved-instances
```

或者，使用以下 Amazon Tools for Windows PowerShell 命令：

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

如果已经有与Reserved Instance的规格匹配的运行实例，则将立即体现账单收益。您不必重启您的实例。如果您没有合适的运行实例，请启动实例并确保符合您为Reserved Instance指定的相同标准。有关更多信息，请参阅使用您的 预留实例 (p. 417)。

有关如何将 预留实例 应用于正在运行的实例的示例，请参阅如何应用预留实例 (p. 412)。

从预留实例 Marketplace 中购买

您可以从预留实例 Marketplace 向不再需要其预留实例的第三方卖家购买预留实例。您可以使用 Amazon EC2 控制台或命令行工具执行此操作。该过程类似于从Amazon购买预留实例。有关更多信息，请参阅购买标准 预留实例 (p. 423)。

在预留实例 Marketplace 中购买的预留实例与直接从 Amazon 购买的预留实例有一些区别：

- 有效期 – 从第三方卖方购买的预留实例具有的剩余期限短于完整标准期限。从 Amazon 获得的完整标准期限为一年或三年。
- 预付价格 – 第三方预留实例可以不同的预付价格出售。使用费或周期性费用与最初从Amazon购买预留实例时设定的费用一致。
- 预留实例类型 – 只能从预留实例市场购买 Amazon EC2 标准预留实例。可转换预留实例、Amazon RDS 和 Amazon ElastiCache 预留实例不能在预留实例 Marketplace 上购买。

有关您的基本信息将与卖方进行共享，如您的邮政编码和国家/地区信息。

此信息使卖方能够计算他们必须向政府缴纳并且采用支付报告形式提供的任何必需的交易税 (如销售税或增值税)。在极少数情况下，Amazon 可能必须向卖方提供您的电子邮件地址，这样卖方才能就与销售相关的问题 (例如税务问题) 与您联系。

出于相似的原因，Amazon 将在买方的购货发票上共享卖方的法律实体名称。如果您出于税务或相关原因需要关于卖方的额外信息，请联系 Amazon Web Services Support。

查看您的 预留实例

您可以使用 Amazon EC2 控制台或命令行工具查看已购买的 预留实例。

在控制台中查看您的预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 此时将列出已排队、活动和已停用的 预留实例。State 列显示状态。
4. 如果您是预留实例市场中的卖家，My Listings (我的列表) 选项卡会显示预留实例市场 (p. 429)中列出的预留的状态。有关更多信息，请参阅Reserved Instance列表状态 (p. 433)。

使用命令行查看预留实例

- describe-reserved-instances (Amazon CLI)
- Get-EC2ReservedInstance (Tools for Windows PowerShell)

取消已排队的购买

您最早可以提前三年排队购买。在指定时间之前，您随时可以取消已排队的购买。

New console

取消已排队的购买

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择一个或多个 预留实例。
4. 依次选择 Actions (操作)、Delete queued Reserved Instances (删除已排队的预留实例)。
5. 提示进行确认时，选择 Delete (删除)，然后选择 Close (关闭)。

Old console

取消已排队的购买

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择一个或多个 预留实例。
4. 依次选择 Actions (操作)、Delete Queued Reserved Instances (删除已排队的预留实例)。
5. 当系统提示进行确认时，选择 Yes, Delete。

使用命令行取消排队的购买

- delete-queued-reserved-instances (Amazon CLI)

- Remove-EC2QueuedReservedInstance (Tools for Windows PowerShell)

续订 Reserved Instance

您可以在 Reserved Instance 按计划过期之前续订它。续订 Reserved Instance 将对购买 Reserved Instance（具有相同配置）进行排队，直到当前 Reserved Instance 过期。

New console

使用排队的购买续订预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择要续订的预留实例。
4. 依次选择 Actions (操作)、Renew Reserved Instances (续订预留实例)。
5. 要完成订单，请选择 Order all (全部订购)，然后选择 Close (关闭)。

Old console

使用排队的购买续订预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择要续订的预留实例。
4. 依次选择 Actions (操作)、Renew Reserved Instances (续订预留实例)。
5. 要完成订单，请选择 Order (订单)。

在预留实例 Marketplace 中销售

预留实例 Marketplace 是一个支持销售第三方和 Amazon 客户的未使用标准预留实例的平台，这些实例的有效期时间和定价选项各不相同。例如，在将实例移到新Amazon区域中、更改为新实例类型、项目结束但期限仍未到期、业务需求变化或者具有不需要的容量时，您可能希望出售预留实例。

只要在预留实例 Marketplace 中列出预留实例，便可供潜在的买方找到。所有预留实例将根据剩余期限及小时价格进行分组。

为满足买方的请求，Amazon首先出售指定分组中预付价格最低的预留实例。然后，Amazon再出售下一个最低价格的预留实例，直到买方的整个订单完成为止。Amazon随后处理这些交易，并将预留实例的所有权转移给买方。

在您的Reserved Instance出售之前，它将归您所有。出售之后，您便放弃了容量预留和打折的周期性费用。如果继续使用您的实例，Amazon将从您的预留实例出售的时间开始以按需价格向您收费。

在预留实例 Marketplace 上销售未使用的预留实例必须满足特定资格条件。

有关在预留实例 Marketplace 上购买预留实例的更多信息，请参阅 从预留实例 Marketplace 中购买 (p. 427)。

目录

- 限制和局限性 (p. 430)
- 注册成为卖家 (p. 430)
- 银行支付账户 (p. 431)

- 税务信息 (p. 431)
- 您的 预留实例 的价格 (p. 431)
- 列出您的 预留实例 (p. 432)
- Reserved Instance列表状态 (p. 433)
- 列表的生命周期 (p. 433)
- 在Reserved Instance出售后 (p. 434)
- 收款 (p. 434)
- 与买方共享的信息 (p. 434)

限制和局限性

您必须先注册为预留实例 Marketplace 中的卖家，然后才能出售未使用的预留实例。有关信息，请参阅 注册成为卖家 (p. 430)。

以下限制在出售预留实例时适用：

- 仅 Amazon EC2 标准预留实例可在预留实例 Marketplace 出售。Amazon EC2 可转换预留实例不能出售。其他Amazon服务（例如 Amazon RDS 和 Amazon ElastiCache）的预留实例无法销售。
- 标准Reserved Instance的剩余期限必须至少为一个月。
- 您不能在默认禁用的区域中销售标准 Reserved Instance。
- 您不能在中国区域（北京和宁夏）中销售标准Reserved Instance。
- 预留实例 Marketplace 中允许的最低价格为 0.00 USD。
- 只要实例在账户中处于激活状态至少 30 天，您就可以在预留实例市场中销售“无预付费用”“预付部分费用”或“预付全部费用”的预留实例。此外，如果预留实例上有预付款，则只能在 Amazon 收到预付款之后将其出售。
- 您无法在预留实例 Marketplace 中直接修改您的列示内容。然而，您可通过先取消它然后再用新参数创建另一个实例出售清单来改变您的实例出售清单。有关信息，请参阅 您的 预留实例 的价格 (p. 431)。您也可以在列出预留实例时对其进行修改。有关信息，请参阅 修改 预留实例 (p. 434)。
- 您无法通过控制台出售区域预留实例。要在市场中列出区域预留实例，您必须首先将范围修改为区域。
- Amazon会向您收取您在预留实例市场中出售的每个标准预留实例的总预付价格 12% 的服务费。预付价格是卖方对标准Reserved Instance收取的费用。
- 当您注册为卖家时，您指定的银行必须有一个美国地址。有关更多信息，请参阅 Amazon Web Services Marketplace 销售指南中的对付费商品的其他卖家要求。
- Amazon Internet Services Private Limited (AISPL) 客户即使拥有美国银行账户也不能在预留实例 Marketplace 中销售预留实例。有关更多信息，请参阅 Amazon 账户和 AISPL 账户之间有何区别？

注册成为卖家

> **Note**
>
> 只有 Amazon Web Services 账户根用户 才可以将账户注册为卖家。

要在预留实例 Marketplace 中销售，您必须先注册为卖家。在注册过程中，您应提供以下信息：

- 银行信息 –Amazon为了支付您出售预留实例时收取的资金，必须获得您的银行信息。您指定的银行必须有一个美国地址。有关更多信息，请参阅银行支付账户 (p. 431)。
- 税务信息 — 所有卖方都需要完成税务信息审查以确定任何必要的税务报告义务。有关更多信息，请参阅税务信息 (p. 431)。

在 Amazon 收到您已完成的卖家注册后，您会收到对您的注册进行确认并告知您可以开始在预留实例 Marketplace 中出售实例的电子邮件。

银行支付账户

为了支付您出售预留实例时收取的资金，Amazon必须获得您的银行信息。您指定的银行必须有一个美国地址。有关更多信息，请参阅 Amazon Web Services Marketplace 销售指南中的对付费商品的其他卖家要求。

注册付款的默认银行账户

1. 打开预留实例市场卖家注册页面并使用您的 Amazon 凭证登录。
2. 在 Manage Bank Account 页面上，提供有关您的收款行的以下信息：
   - 银行账户持有人姓名
   - 路由号码
   - 账号
   - 银行账户类型

   Note

   如果您正在使用一个公司银行账户，则系统将提示您通过传真 (1-206-765-3424) 发送关于该银行账户的信息。

注册后，将提供的银行账户设置为默认账户，等待银行进行验证。验证新的银行账户可能需要两周时间，在此期间，您无法收到付款。对于已建立的账户，付款的完成通常需要两天左右的时间。

更改付款的默认银行账户

1. 在预留实例市场卖家注册页面上，使用您注册时所用的账户登录。
2. 在 Manage Bank Account 页面上，根据需要添加新的银行账户或修改默认银行账户。

税务信息

出售预留实例可能需要交纳交易税，例如销售税或增值税。您应与您的企业的税务、法律、财务或会计部门沟通，以确定是否适用于基于交易的税种。您负责向相关税务机构收集并交纳基于交易的税款。

作为卖家注册的一部分，您必须在卖家注册门户中完成税务审查。此审查将收集税务信息并填充 IRS 表 W-9、W-8BEN 或 W-8BEN-E，后者用于确定任何必要的税务报告义务。

您在税务审查中输入的税务信息可能不同，具体取决于您是作为个人还是企业运营，以及您是否为美国人，您的企业是否为美国实体。当您填写税务资料时，请记住以下事项：

- Amazon 提供的信息 (包括本主题中的信息) 不构成税务、法律或其他专业建议。查明 IRS 报告要求将如何影响您的企业，或者如果您有其他问题，请联系您的税务、法律或其他专业顾问。
- 为了尽可能高效地满足 IRS 报告要求，在会见过程中回答所有的问题并输入所有要求的信息。
- 检查您的回答。避免拼写错误或输入了不正确的税务识别号，它们会导致纳税申报表格无效。

根据您的税务审查响应和 IRS 报告阈值，Amazon 可能对表格 1099-K 归档。 Amazon 会在您的账户达到阈值级别的那一年的后一年的 1 月 31 日或之前通过电子邮件发送表格 1099-K 的副本。例如，如果您的账户在 2018 年达到阈值，则将在 2019 年 1 月 31 日或之前通过电子邮件发送您的表 1099-K。

有关 IRS 要求和表 1099-K 的更多信息，请参阅 IRS 网站。

您的 预留实例 的价格

预付费用是您可为正在出售的Reserved Instance指定的唯一费用。预付费用是买方在购买Reserved Instance时支付的一次性费用。

要注意以下重要限制：

- 对于预留实例，您最多可以销售 50,000 USD。要提高此限制，请填写 EC2 Reserved Instance 销售表。
- 您最多可以销售 5,000 个预留实例。要提高此限制，请填写 EC2 Reserved Instance 销售表。
- 最低价格为 0 美元。预留实例 Marketplace 中允许的最低价格为 0.00 USD。

您无法直接修改您的实例出售清单。然而，您可通过先取消它然后再用新参数创建另一个实例出售清单来改变您的实例出售清单。

只要清单处于 `active` 状态，您就可以随时将其取消。您无法取消已经匹配或正在为销售进行处理的实例出售清单。如果您的实例出售清单中的某些实例已匹配且您取消了实例出售清单，则仅剩余的未匹配的实例将从实例出售清单中删除。

因为预留实例的价值随时间的推移而降低，所以，默认情况下，Amazon可设定以同样的变化量逐月降低的价格。但是，您可根据预留实例出售的时间设置不同的预付价格。

例如，如果您的 Reserved Instance 剩余期限为九个月，您可以指定客户如需购买这个剩余九个月的 Reserved Instance，您愿意接受的价格。您还可以分别设置剩余期限为五个月、一个月的价格。

列出您的 预留实例

注册卖家可以选择销售一个或多个预留实例。您可以选择在一次列出中销售所有实例，或分成多个部分销售。此外，您可以列出任意实例类型、平台和范围配置的预留实例。

控制台将确定建议的价格。它会检查与您的 Reserved Instance 匹配的产品，并与价格最低的产品匹配。否则，它会根据剩余时间的 Reserved Instance 成本计算建议价格。如果计算出的价值小于 1.01 美元，则建议的价格为 1.01 美元。

如果您取消出售清单，且出售清单的一部分已经售出，则取消不会在已售出的部分生效。仅实例出售清单中未售出的部分在预留实例 Marketplace 中将不再可用。

使用 Amazon Web Services Management Console 在预留实例 Marketplace 中列出预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择要列出的预留实例，然后依次选择操作、销售预留实例。
4. 在 Configure Your Reserved Instance Listing (配置您的预留实例列表) 页面上，在相关列中设置要出售的实例数并为剩余期限设定预付价格。单击 Months Remaining 列旁边的箭头，了解您的预留的价值是如何随着剩余期限的变化而变化的。
5. 如果您是高级用户且想对定价进行自定义，那么您可为后续月输入一个不同的值。要返回默认的线性价格降低，请选择 Reset。
6. 当您完成列表配置后，请选择 Continue (继续)。
7. 在 Confirm Your Reserved Instance Listing (确认您的预留实例列表) 页面上确认您的列表详细信息；如果对此类信息感到满意，请选择 List Reserved Instance (列出预留实例)。

在控制台中查看您的实例出售清单

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 选择您已列出的Reserved Instance，然后选择页面底部附近的我的列表选项卡。

使用 Amazon CLI 管理预留实例 Marketplace 中的预留实例

1. 使用 describe-reserved-instances 命令获取 预留实例 的列表。

2. 记录要列出的 Reserved Instance 的 ID 并调用 create-reserved-instances-listing。您必须指定Reserved Instance的 ID、实例数以及价格表。
3. 要查看列表，请使用 describe-reserved-instances-listings 命令。
4. 要取消列表，请使用 cancel-reserved-instances-listings 命令。

Reserved Instance列表状态

预留实例 页面的 My Listings (我的列表) 选项卡上的 Listing State (列表状态) 显示了列表的当前状态：

Listing State (列表状态) 显示的信息与您在预留实例市场中的列表的状态有关。它与 Reserved Instances (预留实例) 页面中的 State (状态) 列显示的状态信息不同。此 State 信息是关于您的预留的。

- active (已激活) — 列表可供购买。
- canceled (已取消) –列表已取消，并且在预留实例市场中不再可供购买。
- closed (已关闭) — Reserved Instance 未列出。Reserved Instance 可能因列表已完成销售而处于 `closed` 状态。

列表的生命周期

当实例出售清单中的所有实例都匹配且售出时，My Listings 选项卡将指示 Total instance count 匹配 Sold 下方列出的计数。此外，实例出售清单中没有 Available 实例，并且其 Status 为 `closed`。

当列表中只有一部分售出时，Amazon将停用列表中的预留实例并创建与剩余预留实例数量相等的预留实例。因此，实例出售清单 ID 及其代表的实例出售清单 (现在具有较少的待售预留) 仍处于激活状态。

将以此方式处理此列表中任何未来预留实例销售。当列表中的所有预留实例售出后，Amazon将列表标记为 `closed`。

例如，您创建一个列表数量为 5 的列表：预留实例 listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample。

Reserved Instance 控制台页中的 My Listings 选项卡将按以下所示显示实例出售清单：

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 0
- 可用 = 5
- 状态 = 已激活

某个买家购买了其中两个预留，这使得三个预留的计数依然可供销售。由于此部分销售，Amazon 创建了一个实例计数为 3 的新预留，以表示剩下的三个预留依然可供销售。

这是您的实例出售清单在 My Listings 选项卡中的显示方式：

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- 总预留计数= 5
- 已售 = 2
- 可用 = 3
- 状态 = 已激活

如果您取消您的出售清单，且出售清单的一部分已经售出，取消不会在已售出的部分生效。仅实例出售清单中未售出的部分在预留实例 Marketplace 中将不再可用。

在Reserved Instance出售后

当您的预留实例售出后，Amazon会向您发送一条电子邮件通知。每天如有任何类型的活动，您会收到一封电子邮件通知，其中包含当天的所有活动。活动可能包括您创建或销售列表，或者 Amazon 向您的账户发送资金。

在控制台中跟踪Reserved Instance列表的状态

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航页面中，选择预留实例。
3. 选择我的列表选项卡。

   My Listings 选项卡包含 Listing State 值，还包含期限信息、标价以及实例出售清单中可用、等待、售出和取消的实例数量明细。

您也可以使用 describe-reserved-instances-listings 命令，借助合适的筛选条件来获取您的预留实例出售清单信息。

收款

Amazon从买方收到资金后，会向已售预留实例的注册所有者账户发送一封电子邮件。

Amazon 将自动清算所 (ACH) 电汇发送至您的指定银行账户。通常，此电汇在您的Reserved Instance已售出后的一天到三天内发生。支付每天只发生一次。在发放资金后，您将收到包含支付报告的电子邮件。请记住，在 Amazon 从您的银行收到确认信息后，您才能收到付款。这可能需要长达两周的时间。

在查看 预留实例 时，仍会显示已销售的 Reserved Instance。

预留实例的现金付款通过电汇转账直接进入您的银行账户。Amazon 向您收取您在预留实例 Marketplace 中出售的每个预留实例的总预付价格 12% 的服务费。

与买方共享的信息

当您在预留实例 Marketplace 中出售时，Amazon 将按照美国的规章在买方声明上分享您的公司法律名称。此外，如果买家因发票或其他税务相关的原因需要联系您而致电 Amazon Web Services Support，那么 Amazon 可能需要向买家提供您的电子邮件地址，这样买家就能与您直接联系。

出于同样的原因，买方的邮政编码和国家/地区信息将在支付报告中提供给卖方。作为卖家，您可能需要在汇给政府任何必要的交易税 (例如销售税和增值税) 时附带此信息。

Amazon 不能提供税务建议，但如果您的税务专家确定您另外需要特定的信息，请联系 Amazon Web Services Support。

修改 预留实例

当需求改变时，可以修改标准或可转换预留实例并继续利用账单优势。您可以修改可用区、实例大小（在相同的实例系列和世代中），以及预留实例的范围等属性。

> **Note**
>
> 您还可以将可转换预留实例交换为具有不同配置的其他可转换预留实例。有关更多信息，请参阅交换 可转换预留实例 (p. 441)。

可以修改全部或部分预留实例。可以将原始 预留实例 分为两个或更多新的 预留实例。例如，如果您在 `us-east-1a` 中有 10 个实例的预留，并决定将其中 5 个实例移至 `us-east-1b`，则修改请求会生成两个新的预留实例 - 一个用于 `us-east-1a` 中的 5 个实例，另一个用于 `us-east-1b` 中的 5 个实例。

还可以将两个或更多 预留实例 合并 成单个 Reserved Instance。例如，如果有四个 `t2.small` 均为 预留实例，则可以将其合并以创建单个 `t2.large` Reserved Instance。有关更多信息，请参阅对于修改实例大小的支持 (p. 436)。

修改之后，预留实例的定价权益仅适用于与新参数匹配的实例。例如，如果您更改预留的可用区，则容量预留和定价优势自动应用到在新可用区中使用的实例。除非您的账户有其他适用的预留，否则将按照按需费率对不再符合新参数的实例收费。

如果您的修改请求成功：

- 修改的预留会立即生效，并且定价优惠将于进行修改请求时这一小时的开始应用于新实例。例如，如果您在晚上 9:15 成功修改了预留，则定价优惠将在晚上 9:00 转移到新实例。您可以使用 describe-reserved-instances 命令，获取修改后的预留实例的生效日期。
- 原始预留将停用。其结束日期是新预留的开始日期，而新预留的结束日期与原始Reserved Instance的结束日期相同。如果您修改一个剩余期限为 16 个月的三年期预留，则修改后得到的预留是为期 16 个月的预留，其结束日期与原始预留相同。
- 已修改的预留将列出 0 美元固定价格，而不是原始预留的固定价格。
- 已修改的预留实例的固定价格不影响您的账户的折扣定价套餐计算，后者基于原始预留的固定价格。

如果修改请求失败，预留实例会保持其原始配置，并立即对其他修改请求可用。

修改不会产生任何费用，因此您不会收到任何新账单或发票。

您可以根据自己的需要随时修改预留，但是不能在提交之后更改或取消挂起的修改请求。修改成功完成后，如果需要，您可以提交另一个修改请求，以回滚您所做的任何更改。

目录

- 修改的要求和限制 (p. 435)
- 对于修改实例大小的支持 (p. 436)
- 提交修改请求 (p. 439)
- 修改请求故障排除 (p. 441)

修改的要求和限制

您可以按如下方式修改这些属性。

可修改的属性	支持的平台	限制和注意事项
在相同区域内更改可用区	Linux 和 Windows	-
将范围从可用区更改到区域以及反之	Linux 和 Windows	可用区预留实例的范围限定为可用区，并在该可用区中预留容量。如果您将范围从可用区更改为区域（即从可用区范围到区域性），则会失去容量预留优势。 区域性预留实例的范围限定为区域。预留实例折扣适用于在该区域任何可用区中运行的实例。此外，预留实例折扣适用于所选实例系列中所有大小的实例用量。如果您将范围从区域更改为可用区（即从区域性到可用区范围），则会失去可用区灵活性和实例大小灵活性（如果适用）。 有关更多信息，请参阅如何应用预留实例 (p. 412)。

可修改的属性	支持的平台	限制和注意事项
更改相同实例系列和世代中的实例大小	仅限 Linux/UNIX 实例大小灵活性不适用于其他平台上的 预留实例，这些平台包括含有 SQL Server Standard 的 Linux、含有 SQL Server Web 的 Linux、含有 SQL Server Enterprise 的 Linux、Red Hat Enterprise Linux、SUSE Linux、Windows、含有 SQL Standard 的 Windows、含有 SQL Server Enterprise 的 Windows 和含有 SQL Server Web 的 Windows。	预留必须使用默认租赁。某些实例系列不受支持，因为没有其他大小可用。有关更多信息，请参阅 中的对于修改实例大小的支持 (p. 436)。
将网络 从 EC2-Classic 更改为 Amazon VPC，反之亦然	Linux 和 Windows	网络平台在您的 Amazon 账户中必须可用。如果您的 Amazon 账户是在 2013 年 12 月 4 日之后创建的，则它不支持 EC2-Classic。

要求

Amazon EC2 处理您的修改请求的前提是，对于您的新配置（如果适用），有足够的容量，同时满足以下条件：

- 在您购买 Reserved Instance 时或在此之前，无法对其进行修改
- Reserved Instance 必须是活动的
- 不能有待处理的修改请求
- 预留实例未列在预留实例 Marketplace 中
- 原始预留的实例大小占用空间必须与新配置匹配。有关更多信息，请参阅对于修改实例大小的支持 (p. 436)。
- 原始 预留实例 要么全部是标准 预留实例，要么全部是 可转换预留实例，不能每种类型都有一些
- 原始预留实例如果是标准预留实例，则必须在相同的时间过期
- 预留实例不是 G4 实例。

对于修改实例大小的支持

在满足以下要求时可以修改Reserved Instance的实例大小。

要求

- 平台是 Linux/UNIX。
- 您必须在相同 实例系列 (p. 238)（用字母表示，例如 T）和 世代 (p. 238)（用数字指示，例如 2）中选择其他实例大小。

  例如，您可以将预留实例从 `t2.small` 修改为 `t2.large`，因为它们属于同一 T2 系列和世代。但您不能将预留实例从 T2 修改为 M2 或从 T2 修改为 T3，因为在这两个示例中，目标实例系列和世代与原始预留实例不同。
- 您不能修改以下实例的预留实例的实例大小，因为以下每个实例都仅有一个大小：
  - `cc2.8xlarge`
  - `cr1.8xlarge`

  - `hs1.8xlarge`
  - `t1.micro`
- 您不能修改以下 实例系列、世代和属性 (p. 238) 组合的预留实例的实例大小：
  - G4ad
  - G4dn
  - G5
  - G5g
  - Inf1
- 原始和新 Reserved Instance 必须具有相同的实例大小占用空间。

目录

- 实例大小占用空间 (p. 437)
- 裸机实例的标准化因子 (p. 439)

实例大小占用空间

每个Reserved Instance都有实例大小占用空间，该空间由预留中实例大小的标准化因子和实例数量决定。修改 Reserved Instance 中的实例大小时，新配置的占用空间必须与原始配置相匹配，否则不会处理修改请求。

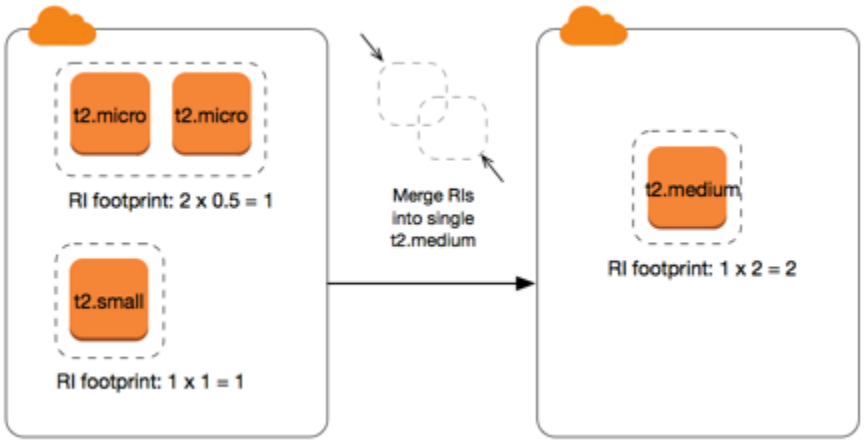
要计算Reserved Instance的实例占用空间大小，请将实例数量乘以标准化因子。在 Amazon EC2 控制台中，标准化因子用单位数来度量。下表描述了一个实例系列中实例大小的标准化因子。例如，`t2.medium` 的标准化因子为 2，因此 4 个 `t2.medium` 实例的预留具有 8 个单位的占用空间。

实例大小	标准化因子
nano	0.25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128

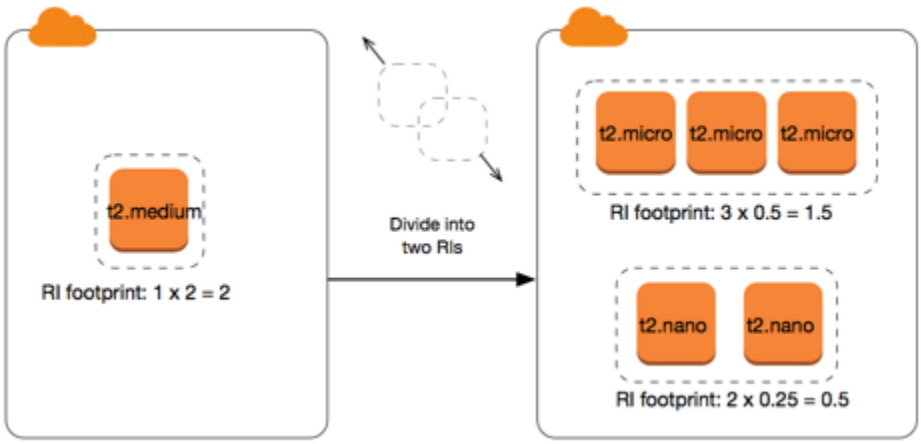
实例大小	标准化因子
18xlarge	144
24xlarge	192
32xlarge	256
56xlarge	448
112xlarge	896

只要预留的实例大小占用空间保持不变，您就可以将预留分配给相同实例系列中的不同实例大小。例如，您可以将 1 个 t2.large（1 个 4 单位）实例的预留划分为 4 个 t2.small（4 个 1 单位）实例。同样，您可以将 4 个 t2.small 实例的预留合并为 1 个 t2.large 实例。但是，您不能将两个 t2.small 实例的预留更改为一个 t2.large 实例，因为新预留的占用空间（4 个单位）大于原始预留的占用空间（2 个单位）。

在以下示例中，您有 1 个具有 2 个 t2.micro 实例（1 个单位）的预留和 1 个具有 1 个 t2.small 实例（1 个单位）的预留。如果您将这些预留合并到具有 1 个 t2.medium 实例（2 个单位）的单个预留中，则新预留的占用空间等于合并预留的占用空间。



您还可以修改预留以将其拆分为多个预留。在以下示例中，您有 1 个具有 t2.medium 实例（2 个单位）的预留。您可以将该预留划分为两个预留，其中之一具有 2 个 t2.nano 实例（.5 个单位），另一个具有 3 个 t2.micro 实例（1.5 个单位）。



裸机实例的标准化因子

您可以使用相同实例系列中的其他大小，通过 metal 实例修改预留。同样，您可以使用相同实例系列中的 metal 大小，通过裸机实例以外的实例修改预留。通常，裸机实例的大小与相同实例系列中可用的最大实例大小相同。例如，i3.metal 实例的大小与 i3.16xlarge 实例的大小相同，因此它们具有相同的标准化因子。

下表描述了具有裸机实例的实例系列中裸机实例大小的标准化因子。metal 实例的标准化因子取决于实例系列，与其他实例大小不同。

实例大小	标准化因子
a1.metal	32
m5zn.metal | z1d.metal	96
c6g.metal | c6gd.metal | i3.metal | m6g.metal | m6gd.metal | r6g.metal | r6gd.metal | x2gd.metal	128
c5n.metal	144
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
u-*.metal	896

例如，i3.metal 实例的标准化因子为 128。如果您购买 i3.metal 默认租期 Amazon Linux/Unix Reserved Instance，则可以按照如下方式划分预留：

- i3.16xlarge 的大小与 i3.metal 实例的大小相同，因此其标准化因子为 128 (128/1)。一个 i3.metal 实例的预留可以修改到一个 i3.16xlarge 实例中。
- i3.8xlarge 的大小是 i3.metal 实例大小的一半，因此其标准化因子为 64 (128/2)。一个 i3.metal 实例的预留可以划分到两个 i3.8xlarge 实例中。
- i3.4xlarge 的大小是 i3.metal 实例大小的四分之一，因此其标准化因子为 32 (128/4)。一个 i3.metal 实例的预留可以划分到四个 i3.4xlarge 实例中。

提交修改请求

在修改预留实例之前，请确保已阅读适用的限制 (p. 435)。在您修改实例大小之前，请计算所要修改的原始预留的总实例大小占用空间 (p. 436)，并确保该值与新配置的总实例大小占用空间相匹配。

New console

使用Amazon Web Services Management Console修改预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 Reserved Instances (预留实例) 页面上，选择一个或多个要修改的预留实例，然后依次选择 Actions (操作) 和 Modify Reserved Instances (修改预留实例)。

   Note

   如果 预留实例 不处于活动状态或无法修改，则 Modify 预留实例 (修改预留实例) 处于禁用状态。
3. 修改表中的第一个条目显示选定 预留实例 的属性，而且其下方至少有一个目标配置。Units 列显示总实例大小占用空间。单击各个新配置的 Add 以添加。根据需要修改每个配置的属性。

- Scope (范围)：选择配置是应用于可用区还是整个区域。
- Availability Zone：选择所需的可用区。不适用于区域性预留实例。
- Instance type (实例类型)：选择所需的实例类型。组合配置必须等于原始配置的实例大小占用空间。
- Count (数量)：指定实例数。要将预留实例拆分为多个配置，请减少数量，选择 Add (添加)，然后为其他配置指定数量。例如，如果单个配置的数量为 10，则可以将其数量更改为 6，并添加数量为 4 的配置。此过程在激活新的预留实例后会停用原始的Reserved Instance。

4. 选择 Continue (继续)。
5. 指定好目标配置之后，要确认您的修改选择，请选择 Submit modifications (提交修改)。
6. 您可以在 预留实例 屏幕中通过查看 State (状态) 列来确定修改请求的状态。有以下可能状态。

   - active (活动)（等待修改）— 原始预留实例的转换状态
   - 停用（等待修改）— 创建新预留实例时原始预留实例的转换状态。
   - 停用 — 已成功修改和替换预留实例
   - 活动 — 以下选项之一：
     - 从成功的修改请求创建的新预留实例
     - 修改请求失败后的原始预留实例

Old console

使用Amazon Web Services Management Console修改预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 Reserved Instances (预留实例) 页面上，选择一个或多个要修改的预留实例，然后依次选择 Actions (操作) 和 Modify Reserved Instances (修改预留实例)。

   Note

   如果 预留实例 不处于活动状态或无法修改，则 Modify 预留实例 (修改预留实例) 处于禁用状态。

3. 修改表中的第一个条目显示选定预留实例的属性，下方至少有一个目标配置。Units 列显示总实例大小占用空间。单击各个新配置的 Add 以添加。根据需要修改各配置的属性，然后选择继续：

   - Scope (范围)：选择配置是应用于可用区还是整个区域。
   - Availability Zone：选择所需的可用区。不适用于区域性预留实例。
   - Instance type (实例类型)：选择所需的实例类型。组合配置必须等于原始配置的实例大小占用空间。
   - Count (数量)：指定实例数。要将预留实例拆分为多个配置，请减少数量，选择 Add (添加)，然后为其他配置指定数量。例如，如果单个配置的数量为 10，则可以将其数量更改为 6，并添加数量为 4 的配置。此过程在激活新的预留实例后会停用原始的Reserved Instance。

4. 指定好目标配置之后，要确认您的修改选择，请选择 Submit modifications (提交修改)。
5. 您可以在 预留实例 屏幕中通过查看 State (状态) 列来确定修改请求的状态。有以下可能状态。

   - active (活动)（等待修改）— 原始预留实例的转换状态
   - 停用（等待修改）— 创建新预留实例时原始预留实例的转换状态。
   - 停用 — 已成功修改和替换预留实例
   - 活动 — 以下选项之一：
     - 从成功的修改请求创建的新预留实例
     - 修改请求失败后的原始预留实例

使用命令行修改预留实例

1. 要修改预留实例，可以使用以下命令之一：
   - modify-reserved-instances (Amazon CLI)
   - Edit-EC2ReservedInstance (Amazon Tools for Windows PowerShell)
2. 要获取修改请求（`processing`、`fulfilled` 或 `failed`）的状态，请使用以下命令之一：
   - describe-reserved-instances-modifications (Amazon CLI)
   - Get-EC2ReservedInstancesModification (Amazon Tools for Windows PowerShell)

修改请求故障排除

如果您请求的目标配置设置是唯一的，则您会收到正在处理该请求的消息。此时，Amazon EC2 仅确定了修改请求的参数有效。在处理过程中，您的修改请求仍然可能因无可用容量而失败。

在某些情况下，您可能会收到一个指示修改请求未完成或失败的消息而不是确认。使用此类消息中的信息作为重新提交另一个更改请求的起点。提交请求前，请确保您已阅读适用的限制 (p. 435)。

并非所有选择的预留实例都可以进行修改处理

Amazon EC2 会确定并列出无法修改的 预留实例。如果收到与此类似的消息，请转到 Amazon EC2 控制台中的 Reserved Instances (预留实例) 页面，查看 预留实例 的信息。

处理修改请求时出错

您提交了一个或多个预留实例进行修改，但无法处理您的任何请求。根据您修改的预留数量，您可以获取不同版本的消息。

Amazon EC2 会显示无法处理请求的原因。举例来说，您可能已经为想要修改的 预留实例 的一个或更多子集指定了相同的目标配置（可用区和平台的组合）。尝试重新提交修改请求，但确保预留的实例详细信息是匹配的，并确保修改的所有子集的目标配置是唯一的。

交换 可转换预留实例

您可以将一个或多个 可转换预留实例 与具有不同配置的其他 可转换预留实例（包括实例系列、操作系统和租期）进行交换。执行交换的次数没有限制，前提是新的可转换预留实例的值等于或高于要交换的可转换预留实例的值。

在交换可转换预留实例时，您当前预留的实例数与新可转换预留实例的配置的实例数（其涵盖的值相等或更高）进行交换。Amazon EC2 计算您可以通过交换获得的预留实例数量。

您不能交换标准 预留实例，但可对其进行修改。有关更多信息，请参阅修改 预留实例 (p. 434)。

目录

- 交换可转换预留实例的要求 (p. 441)
- 计算 可转换预留实例 交换 (p. 442)
- 合并 可转换预留实例 (p. 443)
- 交换部分 可转换预留实例 (p. 443)
- 提出交换请求 (p. 444)

交换可转换预留实例的要求

如果满足以下条件，Amazon EC2 将处理您的交换请求。您可转换预留实例必须：

- 处于活动状态
- 没有以前等待处理的交换请求
- 距离到期至少还剩 24 小时

以下规则适用：

- 可转换预留实例只能与当前由Amazon提供的其他可转换预留实例交换。
- 可转换预留实例 与特定区域关联，在预留期限内是固定的。您不能将 可转换预留实例 与其他区域中的 可转换预留实例 进行交换。
- 一次只能将一个或多个 可转换预留实例 与一个 可转换预留实例 交换。
- 要交换部分 可转换预留实例，您可以修改它以将其拆分为两个或更多预留，然后将一个或多个预留与新 可转换预留实例 交换。有关更多信息，请参阅交换部分 可转换预留实例 (p. 443)。有关修改 预留实例 的更多信息，请参阅修改 预留实例 (p. 434)。
- 预付全费的 可转换预留实例 可用来交换预付部分费用的 可转换预留实例，反之亦然。

  Note

  如果交换所需的总预付款（调整费用）少于 0.00 USD，Amazon会自动向您提供可转换预留实例中可确保调整费用大于等于 0.00 USD 的实例数。

  Note

  如果新可转换预留实例的总价值（预付价格 + 每小时价格 * 剩余小时数）少于交换的可转换预留实例的总价值，Amazon会自动向您提供可转换预留实例中可确保总价值大于等于交换的可转换预留实例的总价值的实例数。
- 要享受更优惠的定价，您可以将无预付费用的 可转换预留实例 交换为预付全费或预付部分费用的 可转换预留实例。
- 不能将预付全费和预付部分费用的 可转换预留实例 交换为无预付费用的 可转换预留实例。
- 仅当新 可转换预留实例 的每小时价格大于等于交换的 可转换预留实例 的每小时价格时，才能将一个无预付费用的 可转换预留实例 交换为另一个无预付费用的 可转换预留实例。

  Note

  如果新可转换预留实例的总价值（预付价格 + 每小时价格 * 剩余小时数）少于交换的可转换预留实例的总价值，Amazon会自动向您提供可转换预留实例中可确保总价值大于等于交换的可转换预留实例的总价值的实例数。
- 如果交换到期日期不同的多个 可转换预留实例，则新 可转换预留实例 的到期日期是将来最晚的日期。
- 如果您交换了单个 可转换预留实例，则它必须与新 可转换预留实例 具有相同的期限（1 年或 3 年）。如果合并期限不同的多个 可转换预留实例，则新 可转换预留实例 期限为 3 年。有关更多信息，请参阅合并可转换预留实例 (p. 443)。
- 当 Amazon EC2 交换可转换预留实例时，它会停用相关的预留，并将结束日期传输到新预留。交换后，Amazon EC2 会将旧预留的结束日期和新预留的开始日期设置为等于交换日期。例如，如果您交换一个剩余期限为 16 个月的三年期预留，则新预留是为期 16 个月的预留，其结束日期与您交换的可转换预留实例相同。

计算 可转换预留实例 交换

交换可转换预留实例是免费的。但是，您可能需要支付调整费用，即您拥有的原始 可转换预留实例 与通过交换收到的新 可转换预留实例 之间差额的按比例预付费用。

每个可转换预留实例都具有标价。此价目表值与您想要的可转换预留实例的价目表值比较，用于确定您可通过交换收到的实例预留数。

例如：您有 1 个 35 美金标价的可转换预留实例，您希望交换为标价为 10 美金的全新实例类型。

```
$35/$10 = 3.5
```

您可以将 可转换预留实例 交换为三个 10 美元的 可转换预留实例。无法购买半预留；因此必须购买额外的可转换预留实例才能涵盖剩余部分：

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved Instance
```

第四个可转换预留实例与其他三个具有相同的结束日期。如果要交换部分或全部预付可转换预留实例，则需要支付第四个预留的调整费用。如果 可转换预留实例 的剩余预付费用为 500 USD，新预留通常按比例分摊为 600 USD，则需要支付 100 USD。

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of original
 reservations = $100 difference
```

合并 可转换预留实例

如果合并两个或更多 可转换预留实例，则新 可转换预留实例 的期限必须与原始 可转换预留实例 的期限相同，或者与原始 可转换预留实例 中的最高期限相同。新可转换预留实例的到期日期是未来有效时间最长的到期日期。

例如，您的账户中有以下可转换预留实例：

Reserved Instance ID	租期	到期日期
aaaa1111	1 年	2018-12-31
bbbb2222	1 年	2018-07-31
cccc3333	3 年	2018-06-30
dddd4444	3 年	2019-12-31

- 您可以合并 aaaa1111 和 bbbb2222 并将它们与 1 年期 可转换预留实例 交换。您无法将它们与 3 年期可转换预留实例交换。新可转换预留实例的到期日期为 2018-12-31。
- 您可以合并 bbbb2222 和 cccc3333 并将它们与 3 年期 可转换预留实例 交换。您无法将它们与 1 年期可转换预留实例交换。新可转换预留实例的到期日期为 2018-07-31。
- 您可以合并 cccc3333 和 dddd4444 并将它们与 3 年期 可转换预留实例 交换。您无法将它们与 1 年期可转换预留实例交换。新可转换预留实例的到期日期为 2019-12-31。

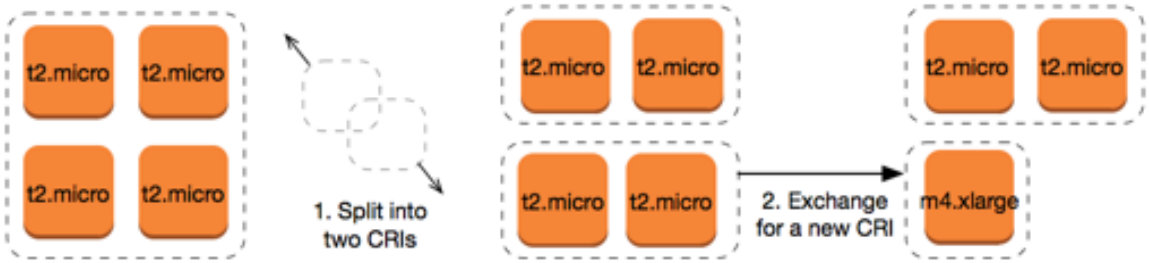
交换部分 可转换预留实例

您可以使用修改过程将 可转换预留实例 拆分为较小的预留，然后将一个或多个新预留与新 可转换预留实例交换。以下示例演示了如何执行此操作。

Example 示例：包含多个实例的可转换预留实例

在本示例中，您有一个在预留中有四个实例的 t2.micro 可转换预留实例。将两个 t2.micro 实例与一个 m4.xlarge 实例交换：

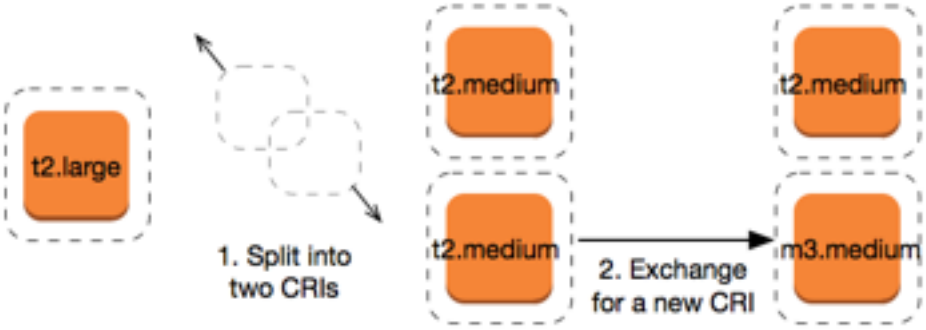
1. 修改 t2.micro 可转换预留实例，方法为将其拆分为两个 t2.micro 可转换预留实例，每一个都包含两个实例。
2. 将其中一个新 t2.micro 可转换预留实例 与一个 m4.xlarge 可转换预留实例 交换。



Example 示例：包含单个实例的可转换预留实例

在本示例中，您拥有一个 t2.large 可转换预留实例。将其更改为一个较小的 t2.medium 实例和一个 m3.medium 实例：

1. 修改 t2.large 可转换预留实例，方法为将其拆分为两个 t2.medium 可转换预留实例。单个 t2.large 实例具有两个 t2.medium 实例相同的实例大小占用空间。
2. 将其中一个新 t2.medium 可转换预留实例 与一个 m3.medium 可转换预留实例 交换。



有关更多信息，请参阅 对于修改实例大小的支持 (p. 436) 和 提出交换请求 (p. 444)：

提出交换请求

您可以使用 Amazon EC2 控制台或命令行工具来交换 可转换预留实例。

使用控制台交换 可转换预留实例

您可以搜索可转换预留实例产品并从提供的选项中选择新配置。

New console

使用 Amazon EC2 控制台交换 可转换预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Reserved Instances (预留实例)，选择要交换的 可转换预留实例，然后依次选择 Actions (操作) 和 Exchange Reserved Instance (交换预留实例)。
3. 选择所需配置的属性，然后选择 Find offering (查找产品)。
4. 选择一个新的 可转换预留实例。在屏幕底部，您可以查看通过交换收到的 预留实例 数和任何额外费用。
5. 当您选择了符合需求的 可转换预留实例 时，请选择 Review (审核)。
6. 选择 Exchange (交换)，然后选择 Close (关闭)。

Old console

使用 Amazon EC2 控制台交换 可转换预留实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Reserved Instances (预留实例)，选择要交换的 可转换预留实例，然后依次选择 Actions (操作) 和 Exchange Reserved Instance (交换预留实例)。
3. 选择所需配置的属性，然后选择 Find Offering (查找产品)。
4. 选择一个新的 可转换预留实例。Instance Count (实例数量) 列显示通过交换收到的 预留实例 数。当您选择了符合要求的 可转换预留实例 时，请选择 Exchange (交换)。

已交换的 预留实例 将停用，Amazon EC2 控制台中将显示新的 预留实例。此过程可能需要几分钟才能传播。

使用命令行界面交换 可转换预留实例

要交换 可转换预留实例，请首先查找符合您的要求的新 可转换预留实例：

- describe-reserved-instances-offerings (Amazon CLI)
- Get-EC2ReservedInstancesOffering (Tools for Windows PowerShell)

获取交换的报价，这包括通过交换获得的预留实例数以及交换的调整费用：

- get-reserved-instances-exchange-quote (Amazon CLI)
- GetEC2-ReservedInstancesExchangeQuote (Tools for Windows PowerShell)

最后，执行交换：

- accept-reserved-instances-exchange-quote (Amazon CLI)
- Confirm-EC2ReservedInstancesExchangeQuote (Tools for Windows PowerShell)

预留实例限额

您可以每月购买新的预留实例。您每月可购买的新预留实例数由每月配额决定，如下所示：

配额描述	默认配额
新的区域性 (p. 412)预留实例	每个区域每月 20 个
新的可用区 (p. 412)预留实例	每个可用区每月 20 个

例如，在带有三个可用区的区域中，默认配额为每月 80 个新预留实例，计算方法如下：

- 该区域有 20 个区域预留实例
- 加 60 个可用区预留实例（三个可用区各有 20 个）

查看您已购买的预留实例数量

您购买的预留实例数量通过 Instance count（实例计数）字段（控制台）或 `InstanceCount` 参数（Amazon CLI）表示。当您购买新的预留实例时，配额会根据实例总数进行衡量。例如，如果您购买了实例数量为 10 的单个预留实例配置，则计入配额的购买数量为 10，而不是 1。

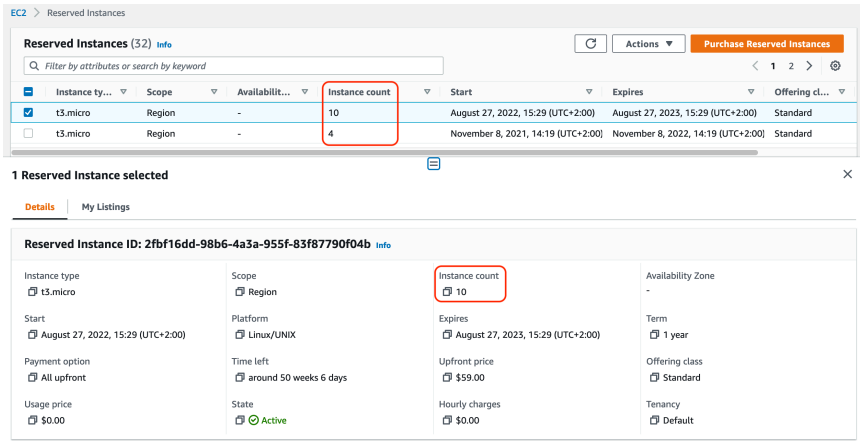
您可以使用 Amazon EC2 或 Amazon CLI 查看已购买的预留实例数量。

Console

查看您已购买的预留实例数量

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Reserved Instances。
3. 从表中选择预留实例配置，然后查看 Instance count（实例计数）字段。

   在下列屏幕截图中，选定的行表示 t3.micro 实例类型的单个预留实例配置。表视图中的 Instance count（实例计数）列和详细信息视图中的 Instance count（实例计数）字段（在屏幕截图中划出）表示此配置有 10 个预留实例。



Amazon CLI

查看您已购买的预留实例数量

使用 describe-reserved-instances CLI 命令并指定预留实例配置的 ID。

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
    --output table
```

输出示例 – InstanceCount 字段表示此配置有 10 个预留实例。

```
-------------------------------------------------------------------
|                   DescribeReservedInstances                     |
+-----------------------------------------------------------------+
||                      ReservedInstances                        ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  2fbf16dd-98b6-4a3a-955f-83f87790f04b  ||
||  Scope               |  Region                                ||
```

```
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                      RecurringCharges                        |||
||+----------------------------------+--------------------------+||
|||  Amount                          |  0.0                     |||
|||  Frequency                       |  Hourly                  |||
||+----------------------------------+--------------------------+||
```

注意事项

区域性预留实例账单折扣适用于正在运行的按需型实例。默认按需型实例 限制为 20。购买区域性预留实例时，不能超出正在运行的按需型实例限制。例如，如果您已有 20 个正在运行的按需型实例，并且购买了 20 个区域性预留实例，则使用 20 个区域性预留实例将折扣应用于 20 个正在运行的按需型实例。即使您购买了更多的区域性预留实例，也无法启动更多的实例，因为已达到按需型实例限制。

在购买区域性预留实例 之前，请确保 个按需型实例 限制匹配或超出您打算拥有的区域性预留实例 的数量。如果需要，请确保在购买更多区域性 预留实例 之前，请求增加 个按需实例 限制。

可用区预留实例（为特定可用区域购买的预留实例）提供容量预留以及折扣。购买地区性 预留实例 时，可以超出 正在运行的 个按需实例 限制。例如，如果您已有 20 个正在运行的 按需型实例，并且购买了 20 个地区性 预留实例，则可以启动另外的 20 个 按需型实例，以区配地区性 预留实例 为您提供总共 40 个正在运行的实例的规范。

查看您的预留实例配额并请求增加配额

Amazon EC2 控制台提供了配额信息。您也可以请求增加配额。有关更多信息，请参阅 查看您的当前限制 (p. 1678) 和 请求提高 (p. 1679)：

Scheduled Reserved Instances

利用计划的预留实例，可以以一年为期限购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的预留容量。完成购买后，实例可在您指定的时间窗口内启动。

> **Important**
>
> 您目前无法购买计划预留实例。Amazon没有任何容量可用于计划预留实例，也没有任何计划在未来使用。要预留容量，请改用 On-Demand Capacity Reservations (p. 538)。为了获得折扣费率，请使用 Savings Plans。

Spot Instances

竞价型实例是一种使用备用 EC2 容量的实例，以低于按需价格提供。由于竞价型实例允许您以极低的折扣请求未使用的 EC2 实例，这可能会显著降低您的 Amazon EC2 成本。竞价型实例的每小时价格称为 Spot 价格。每个可用区中的每种实例类型的 Spot 价格是由 Amazon EC2 设置的，并根据竞价型实例的长期供求趋势逐步调整。您的竞价型实例在容量可用时运行。

如果能灵活控制应用程序的运行时间并且应用程序可以中断，竞价型实例就是经济实惠之选。例如，竞价型实例非常适合数据分析、批处理作业、后台处理和可选的任务。有关更多信息，请参阅 Amazon EC2 Spot 实例。

有关 EC2 实例不同购买选项的比较，请参阅 实例购买选项 (p. 404)。

主题

- 概念 (p. 448)
- 如何开始 (p. 449)
- 相关服务 (p. 449)
- 定价和节省 (p. 450)

概念

在开始使用竞价型实例之前，应该熟悉以下概念：

- Spot 容量池 – 一组具有相同实例类型（如 `m5.large`）和可用区的未使用 EC2 实例。
- Spot 价格 – Spot 实例的当前每小时价格。
- Spot 实例请求 – 请求 Spot 实例。当有容量可用时，Amazon EC2 将满足您的请求。Spot 实例请求是一次性或者持续性请求。在与请求关联的竞价型实例中断之后，Amazon EC2 会自动重新提交持续性竞价型实例请求。
- EC2 实例再平衡建议 – Amazon EC2 发出实例再平衡建议信号，以通知您竞价型实例处于中断高风险。此信号使您有机会在现有或新的竞价型实例间主动再平衡工作负载，而无需等待两分钟的竞价型实例中断通知。
- 竞价型实例中断 – 如果 Amazon EC2 需要回收容量，Amazon EC2 会将您的竞价型实例停止、停止或休眠。Amazon EC2 将提供竞价型实例中断通知，这会在实例中断之前为其提供两分钟的警告。

竞价型实例与按需型实例的主要区别

下表列出了竞价型实例与按需型实例 (p. 406)之间的主要区别。

	竞价型实例	On-Demand Instances
启动时间	只有竞价型实例请求处于活动状态并且有可用容量时才能立即启动。	只有发出手动启动请求并且有可用容量时才能立即启动。
可用容量	如果没有可用容量，则竞价型实例请求会继续自动发起启动请求，直到有可用容量为止。	如果在发出启动请求时没有可用容量，您会收到容量不足错误 (ICE)。
每小时价格	竞价型实例的每小时价格根据长期的供需情况而有所调整。	按需型实例的每小时价格是静态的。
再平衡建议	当实例处于较高的中断风险时，Amazon EC2 为正在运行的竞价型实例发出信号。	您可以决定何时中断个按需型实例（停止、休眠或终止）。

	竞价型实例	On-Demand Instances
实例中断	您可以停止和启动由 Amazon EBS 支持的竞价型实例。此外，如果容量不再可用，Amazon EC2 可能会中断 (p. 484)单个竞价型实例。	您可以决定何时中断个按需型实例（停止、休眠或终止）。

如何开始

您需要做的第一件事是为使用 Amazon EC2 进行设置。在启动竞价型实例之前，若拥有启动按需型实例的经验也会有所帮助。

设置和运行

- 设置以使用 Amazon EC2 (p. 5)
- 教程：Amazon EC2 Linux 实例入门 (p. 9)

Spot 基础知识

- 竞价型实例的工作原理 (p. 453)

使用竞价型实例

- 创建竞价型实例请求 (p. 460)
- 获取请求状态信息 (p. 478)
- 竞价型实例中断 (p. 484)

相关服务

您可以直接使用 Amazon EC2 预置竞价型实例。也可以使用 Amazon 中的其他服务预置竞价型实例。有关更多信息，请参阅以下文档。

Amazon EC2 Auto Scaling 和竞价型实例

> 您可以创建启动模板或配置，以便 Amazon EC2 Auto Scaling 可以启动竞价型实例。有关更多信息，请参阅为具有容错要求且灵活的应用程序请求 Spot 实例和 Amazon EC2 Auto Scaling 用户指南 中的包含多种实例类型和购买选项的 Auto Scaling 组。

Amazon EMR 和竞价型实例

> 有时候，在 Amazon EMR 集群中运行竞价型实例会非常有帮助。有关更多信息，请参阅 Amazon EMR 管理指南中的竞价型实例https://docs.amazonaws.cn/emr/latest/ManagementGuide/emr-instance-purchasing-options.html#emr-spot-instances和什么时候应该使用竞价型实例。

Amazon CloudFormation 模板

> 借助 Amazon CloudFormation，您可以使用 JSON 格式的模板创建和管理 Amazon 资源集合。有关更多信息，请参阅 EC2竞价型实例更新 – Auto Scaling 和 CloudFormation 集成。

Amazon SDK for Java

> 可以使用 Java 编程语言来管理竞价型实例。有关更多信息，请参阅教程：Amazon EC2 Spot 实例 和教程：高级 Amazon EC2 Spot 请求管理。

Amazon SDK for .NET

> 可以使用 .NET 编程环境来管理竞价型实例。有关更多信息，请参阅教程：Amazon EC2 竞价型实例。

定价和节省

您可以为竞价型实例支付 Spot 价格，该价格由 Amazon EC2 设置，并根据竞价型实例的长期供求趋势逐步进行调整。您的竞价型实例将持续运行，直到您将其终止、容量不再可用或您的 Amazon EC2 Auto Scaling 组在横向缩减期间将其终止为止。

如果您或 Amazon EC2 中断正在运行的竞价型实例，您将按使用的秒数或整个小时付费，或者您不收取任何费用，具体取决于所使用的操作系统以及竞价型实例的中断方。有关更多信息，请参阅中断的竞价型实例的计费 (p. 493)。

查看价格

要查看各个 Amazon Web Services 区域和实例类型的当前最低竞价型实例价格（每 5 分钟更新一次），请参阅 Amazon EC2 竞价型实例定价 页面。

要查看过去三个月的 Spot 价格历史记录，请使用 Amazon EC2 控制台或 describe-spot-price-history 命令 (Amazon CLI)。有关更多信息，请参阅竞价型实例定价历史记录 (p. 454)。

我们将可用区独立地映射到每个 Amazon Web Services 账户的代码。因此，不同账户的相同可用区代码 (如 `us-west-2a`) 可能会返回不同的结果。

查看节省

您可以查看使用单个 竞价型实例集 (p. 871) 或所有竞价型实例时通过使用竞价型实例所节省的成本。您可以查看过去一小时或过去三天的节省，还可以查看每 vCPU 小时和每内存 (GiB) 小时的平均费用。节省是估算的，因为未算入您使用期间的计费调整，所以可能与实际的节省有所差异。有关查看节省信息的更多信息，请参阅通过购买竞价型实例实现节省 (p. 455)。

查看账单

您的账单提供了服务使用量的详细信息。有关更多信息，请参阅 Amazon Billing 用户指南中的查看您的账单。

EC2 Spot 的最佳实践

Amazon EC2 竞价型实例是 Amazon Web Services 云 中的备用 EC2 计算容量，与按需型实例价格相比，这种实例最高可以为您节省 90% 的成本。按需型实例和竞价型实例之间的唯一区别是，当 Amazon EC2 再次需要使用容量时，Amazon EC2 可以中断竞价型实例并提前两分钟发出通知。

竞价型实例建议用于无状态、容错且灵活的应用程序。例如，竞价型实例非常适合大数据、容器化工作负载、CI/CD、无状态 Web 服务器、高性能计算 (HPC) 和渲染工作负载。

在运行时，竞价型实例与按需型实例完全相同。不过，Spot 不能保证您可以将运行的实例保持足够长的时间以完成工作负载。Spot 也不能保证您可以立即使用查找的实例，或者不能保证您始终可以获得请求的总容量。此外，竞价型实例中断和容量可能会随着时间的推移而发生变化，因为竞价型实例可用性根据供需关系而发生变化，过去的性能并不能保证将来的结果。

竞价型实例不适用于不灵活、有状态、非容错或在实例节点之间紧密耦合的工作负载。对于不能容忍目标容量偶尔不完全可用的工作负载，也不建议使用该实例。我们强烈警告您不要在这些工作负载中使用竞价型实例或尝试故障转移到按需型实例以处理中断。

无论您是经验丰富的 Spot 用户还是竞价型实例新用户，如果您当前遇到竞价型实例中断或可用性问题，我们建议您按照以下最佳实践以获得使用 Spot 服务的最佳体验。

Spot 最佳实践

- 准备各个实例以处理中断 (p. 451)
- 灵活地选择实例类型和可用区 (p. 451)
- 使用 EC2 Auto Scaling 组或 Spot 实例集管理总容量 (p. 451)
- 使用价格和容量优化分配策略 (p. 451)

- 使用主动容量再平衡 (p. 451)
- 使用集成的 Amazon 服务以管理竞价型实例 (p. 452)
- 使用哪种竞价型请求方法最好？ (p. 452)

准备各个实例以处理中断

正常处理竞价型实例中断的最佳方法是，设计应用程序以提供容错能力。为此，您可以利用 EC2 实例再平衡建议和竞价型实例中断通知。

EC2 实例再平衡建议是一个新信号，可在竞价型实例处于较高的中断风险时通知您。该信号使您有机会在两分钟的竞价型实例中断通知之前主动管理竞价型实例。您可以决定将工作负载再平衡到不处于较高中断风险的新的或现有的竞价型实例。通过使用 Auto Scaling 组和 Spot 实例集中的容量再平衡功能，我们使您可以轻松地使用这个新信号。有关更多信息，请参阅使用主动容量再平衡 (p. 451)。

竞价型实例中断通知是在 Amazon EC2 中断竞价型实例之前的两分钟发出的警告。如果工作负载为“时间灵活型”负载，您可以将竞价型实例配置为在中断时停止或休眠，而不是终止。Amazon EC2 在中断时使竞价型实例自动停止或休眠，并在我们具有可用容量时自动恢复这些实例。

我们建议您在 Amazon EventBridge 中创建一个规则以捕获再平衡建议和中断通知，然后触发工作负载进度的检查点或正常处理中断。有关更多信息，请参阅监控再平衡建议信号 (p. 481)。有关指导您如何创建和使用事件规则的详细示例，请参阅利用 Amazon EC2 Spot 实例中断通知。

有关更多信息，请参阅EC2 实例再平衡建议 (p. 480) 和 竞价型实例中断 (p. 484)。

灵活地选择实例类型和可用区

竞价型容量池是具有相同实例类型（如 `m5.large`）和可用区（如 us-east-1a）的未使用 EC2 实例的集合。您应该灵活地选择请求哪些实例类型，以及可以在哪些可用区中部署工作负载。这为 Spot 提供了更好的机会以查找和分配所需数量的计算容量。例如，如果您希望使用 c4、m5 和 m4 系列中的大型实例，则不要仅请求 `c5.large`。

根据您的特定需求，您可以评估可灵活地选择哪些实例类型以满足您的计算要求。如果可以纵向扩展工作负载，您应该在请求中包括更大的实例类型（更多的 vCPU 和内存）。如果您只能横向扩展，您应该包括较旧一代的实例类型，因为按需客户很少需要使用它们。

一条很好的经验法则是，对于每种工作负载，灵活地在至少 10 种实例类型之间进行选择。此外，还要确保所有可用区配置为在 VPC 中使用，并为工作负载选择了这些可用区。

使用 EC2 Auto Scaling 组或 Spot 实例集管理总容量

Spot 允许您考虑总容量（包括 vCPU、内存、存储或网络吞吐量），而不是考虑单个实例。通过使用 Auto Scaling 组和 Spot 实例集，您可以启动和维持目标容量，自动请求资源以替换任何中断或手动终止的资源。在配置 Auto Scaling 组或 Spot 实例集时，您仅需要根据应用程序需求指定实例类型和目标容量。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的 Auto Scaling 组和本用户指南中的创建 Spot 队列请求 (p. 900)。

使用价格和容量优化分配策略

Auto Scaling 组中的分配策略可以帮助您预置目标容量，而无需手动查找具有备用容量的 Spot 容量池。我们建议使用 `price-capacity-optimized` 策略，因为该策略自动从可用性最佳的竞价型容量池中预置实例，同时也具有最低价格。您也可以在 Spot 实例集中利用 `price-capacity-optimized` 分配策略。由于竞价型实例容量来自于具有最佳容量的池，因此，这会降低回收竞价型实例的可能性。有关分配策略的更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的 Spot 实例和本用户指南中的当工作负载拥有较高中断成本时 (p. 873)。

使用主动容量再平衡

容量再平衡功能可在运行中的竞价型实例收到两分钟的竞价型实例中断通知之前，主动使用新的竞价型实例扩展您的队列，从而帮助您维护工作负载的可用性。启用容量再平衡后，Auto Scaling 或竞价型实例集将尝

试主动替换已收到再平衡建议的竞价型实例，从而使您有机会将工作负载再平衡到不处于较高中断风险的新竞价型实例。

容量再平衡补充了价格容量优化分配策略（旨在帮助找到最佳备用容量）和混合实例策略（旨在通过在多个可用区中运行的多个实例类型上部署实例来提高可用性）。

有关更多信息，请参阅容量再平衡 (p. 888)。

使用集成的 Amazon 服务以管理竞价型实例

其他 Amazon 服务与 Spot 集成在一起以降低总体计算成本，而无需管理各个实例或队列。我们建议您针对适用的工作负载考虑以下解决方案：Amazon EMR、Amazon Elastic Container Service、Amazon Batch、Amazon Elastic Kubernetes Service、Amazon SageMaker、Amazon Elastic Beanstalk 和 Amazon GameLift。要了解这些服务的 Spot 最佳实践的更多信息，请参阅 Amazon EC2 竞价型实例 Workshops 网站。

使用哪种竞价型请求方法最好？

使用下表确定在请求竞价型实例时使用哪个 API。

API	何时使用？	使用案例	我应该使用这个 API 吗？
CreateAutoScalingGroup	• 您需要多个采用单一配置或混合配置的实例。 • 您希望通过可配置的 API 自动执行生命周期管理。	创建一个 Auto Scaling 组，以管理实例的生命周期，同时保持所需的实例数量。支持在指定的最小和最大限值之间的水平扩展（添加更多实例）。	是
CreateFleet	• 您需要多个采用单一配置或混合配置的实例。 • 您希望自行管理实例生命周期。 • 如果不需要弹性伸缩，我们建议您使用 `instant` 类型的实例集。	在单个请求中创建一个由按需型实例和竞价型实例组成的实例集，并具有多个因实例类型、AMI、可用区或子网而异的启动规范。竞价型实例分配策略默认为每单位 `lowest-price`，但您可以将其更改为 `price-capacity-optimized`、`capacity-optimized` 或 `diversified`。	是 - 如果不需要弹性伸缩，则在 `instant` 模式下
RunInstances	• 您已经在使用 RunInstances API 启动按需型实例，而且只想通过更改单个参数来更改为启动竞价型实例。 • 您不需要多个实例类型不同的实例。	使用 AMI 和一个实例类型启动指定数量的实例。	否 - 因为 RunInstances 不允许在单个请求中混合多个实例类型
RequestSpotFleet	• 我们强烈反对使用 RequestSpotFleet API，因为它是不具有计划投资的旧式 API。	请勿使用。RequestSpotFleet 是不具有计划投资的旧式 API。	否

API	何时使用？	使用案例	我应该使用这个 API 吗？
	• 如果想要管理实例生命周期，请使用 CreateFleet API。 • 如果不想管理实例生命周期，请使用 CreateAutoScalingGroup API。		
RequestSpotInstances	• 我们强烈反对使用 RequestSpotInstances API，因为它是不具有计划投资的旧式 API。	请勿使用。RequestSpotInstances 是不具有计划投资的旧式 API。	否

竞价型实例的工作原理

要启动 Spot 实例，您可以创建 Spot 实例请求，或者 Amazon EC2 代表您创建 Spot 实例请求。竞价型实例在满足竞价型实例请求时启动。

您可以使用多种不同的服务启动竞价型实例。有关更多信息，请参阅 Amazon EC2 Spot 实例入门。在本用户指南中，我们介绍了以下使用 EC2 启动竞价型实例的方法：

- 您可以使用 Amazon EC2 控制台中的启动实例向导 (p. 575)或 run-instances Amazon CLI 命令创建竞价型实例请求。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。
- 您可以创建 EC2 实例集，在其中指定所需数量的竞价型实例。Amazon EC2 代表您为 EC2 实例集中指定的每个竞价型实例创建一个竞价型实例请求。有关更多信息，请参阅创建 EC2 队列 (p. 860)。
- 您可以创建竞价型实例集请求，在其中指定所需数量的竞价型实例。Amazon EC2 代表您为竞价型实例集中指定的每个竞价型实例创建一个竞价型实例请求。有关更多信息，请参阅创建 Spot 队列请求 (p. 900)。

如果有可用容量，则您的竞价型实例将启动。

您的 Spot 实例会一直运行，直到您停止或终止它，或者 Amazon EC2 中断它（称为 Spot 实例中断）。

当您使用竞价型实例时，您必须为中断做好准备。在竞价型实例需求增加或供应减少时，Amazon EC2 可能会中断您的竞价型实例。在 Amazon EC2 中断竞价型实例时，将提供竞价型实例中断通知，这会在 Amazon EC2 终止该实例之前为其提供两分钟的警告。无法为竞价型实例启用终止保护。有关更多信息，请参阅竞价型实例中断 (p. 484)。

您可以停止、启动、重启或终止由 Amazon EBS 支持的竞价型实例。Spot 服务可以在中断 Spot实例时可使实例停止、终止或休眠。

目录

- 在启动组中启动竞价型实例 (p. 453)
- 在可用区组中启动竞价型实例 (p. 454)
- 在 VPC 中启动竞价型实例 (p. 454)

在启动组中启动竞价型实例

在竞价型实例请求中指定启动组，可以通知 Amazon EC2 只有在可以全部启动一组竞价型实例时才启动该组。此外，如果 Spot 服务必须终止启动组中的某个实例，它必须终止所有实例。不过，如果由您终止启动组中的一个或多个实例，Amazon EC2 不会终止该启动组中的剩余实例。

尽管此选项有用处，但是添加此约束会减少完成竞价型实例请求的几率并且增加竞价型实例被终止的几率。例如，启动组包括多个可用区中的实例。如果其中一个可用区中的容量减少且不再可用，则 Amazon EC2 会终止启动组的所有实例。

如果您创建了另一个成功的竞价型实例请求并指定与之前成功请求相同（现有）的启动组，则新实例将添加到该启动组中。以后，在该启动组的一个实例终止时，启动组中的所有实例均会终止，这包括第一次请求和第二次请求启动的实例。

在可用区组中启动竞价型实例

在竞价型实例请求中指定可用区组，可以通知 Amazon EC2 在同一可用区中启动一组竞价型实例。Amazon EC2 无需同时中断可用区组中的所有实例。如果 Amazon EC2 必须中断可用区组中的某个实例，剩余的实例仍保持运行。

虽然此选项非常有用，但添加此约束会减少完成您的竞价型实例请求的几率。

如果您指定了可用区组，但未在竞价型实例请求中指定可用区，则具体结果将取决于您所指定的网络。

默认 VPC

Amazon EC2 使用指定子网的可用区。如果您未指定子网，它会为您选择一个可用区及其默认子网，但不一定是价格最低的可用区。如果您删除了可用区的默认子网，则必须指定其他子网。

非默认 VPC

Amazon EC2 使用指定子网的可用区。

在 VPC 中启动竞价型实例

按照为按需型实例指定子网的相同方法，为您的竞价型实例指定子网。

- [默认 VPC] 如果希望在特定的低价格可用区中启动您的竞价型实例，您必须在竞价型实例请求中指定对应的子网。如果您没有指定子网，则 Amazon EC2 将为您选择一个子网，而该子网的可用区中的 Spot 价格不一定是最低的。
- [非默认 VPC] 您必须为您的竞价型实例指定子网。

竞价型实例定价历史记录

竞价型实例的价格由 Amazon EC2 设置，并根据竞价型实例容量的长期供求趋势逐步调整。

当您的 Spot 请求得到满足时，您的竞价型实例将以当前 Spot 价格启动，并且不超过按需价格。您可以查看最近 90 天的 Spot 价格历史记录，并按照实例类型、操作系统和可用区筛选。

查看当前 Spot 价格

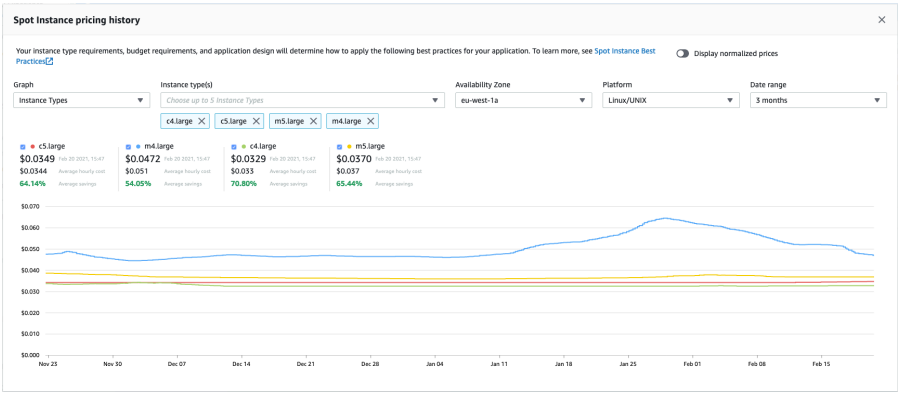
要查看当前 Spot 实例价格，请参阅 Amazon EC2 Spot 实例定价。

查看 Spot 价格历史记录（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择定价历史记录。
4. 对于 Graph (图表)，选择按 Availability Zones (可用区) 或 Instance Types (实例类型) 来比较价格历史记录。
   - 如果选择 Availability Zones（可用区），则选择 Instance type（实例类型）、操作系统 [Platform（平台）] 以及要查看价格历史记录的 Date range（日期范围）。

- 如果选择 Instance Types（实例类型），则最多选择五个 Instance type（实例类型）、Availability Zone（可用区）、操作系统 [Platform（平台）] 以及要查看价格历史记录的 Date range（日期范围）。

以下屏幕截图显示了不同实例类型的价格比较。



5. 将指针移动到图形上并悬停，可显示选定日期范围内的特定时间的价格。价格显示在图表上方的信息块中。顶行中显示的价格显示了特定日期的价格。第二行中显示的价格显示了选定日期范围内的平均价格。
6. 要显示每个 vCPU 的价格，请开启 Display normalized prices (显示标准化价格)。要显示实例类型的价格，请关闭 Display normalized prices (显示标准化价格)。

使用命令行查看 Spot 价格历史记录

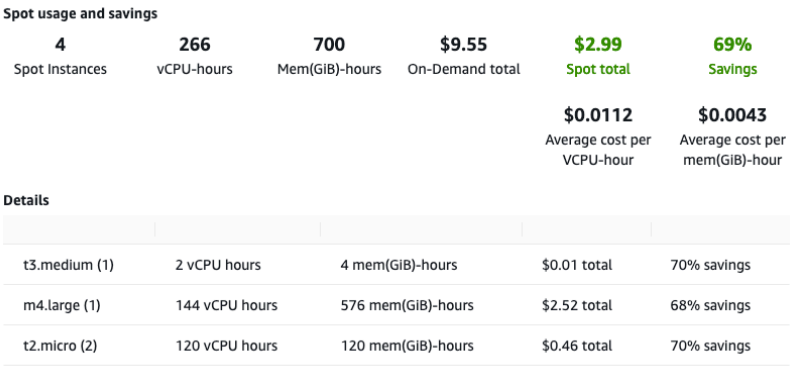
您可以使用以下任一命令。有关更多信息，请参阅访问 Amazon EC2 (p. 3)。

- describe-spot-price-history (Amazon CLI)
- Get-EC2SpotPriceHistory (Amazon Tools for Windows PowerShell)

通过购买竞价型实例实现节省

您可以在每个队列级别或针对所有正在运行的竞价型实例，查看竞价型实例的用量和节省信息。在每个队列级别，用量和节省信息包括该队列启动和终止的所有实例。您可以查看过去一小时或过去三天的此信息。

来自 Savings (节省成本) 部分的以下屏幕截图显示了 Spot 实例集的 Spot 用量和节省信息。



您可查看以下用量和节省信息：

- Spot Instances (Spot 实例) – Spot 实例集启动和终止的 Spot 实例数量。在查看节省摘要时，该数字表示您的所有正在运行的竞价型实例。
- vCPU-hours (vCPU 小时数) – 在所选时间范围内所有 Spot 实例 使用的 vCPU 小时数。
- Mem(GiB)-hours (内存 (GiB) 小时数) – 在所选时间范围内所有 Spot 实例 使用的 GiB 小时数。
- On-Demand total (按需总额) – 您在将这些实例作为 按需实例 启动后，在所选时间范围内支付的总额。
- Spot total (Spot 总额) – 您在所选时间范围内支付的总额。
- Savings (节省) – 您通过未支付按需价格而节省的百分比。
- Average cost per vCPU-hour (每 vCPU 小时的平均费用) – 在所选时间范围内所有 Spot 实例 使用 vCPU 的平均小时费用，其计算方式如下：每 vCPU 小时的平均费用 = Spot 总额 / vCPU 小时数。
- Average cost per mem(GiB)-hour (每内存 (GiB) 小时的平均费用) – 在所选时间范围内所有 Spot 实例 使用 GiB 的平均小时费用，其计算方式如下：每内存 (GiB) 小时的平均费用 = Spot 总额 / 内存 (GiB) 小时数。
- Details (详细信息) 表 – 构成 Spot 实例集的各种实例类型（每个实例类型的实例数括在圆括号中）。在查看节省摘要时，这些数字涵盖了您的所有正在运行的竞价型实例。

节省信息只能使用 Amazon EC2 控制台查看。

查看 Spot 实例的节省信息（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择 Spot 队列请求的 ID，然后滚动到 Savings (节省成本) 部分。

   或者，选中 Spot 队列请求 ID 旁的复选框，然后选择 Savings (节省成本) 选项卡。
4. 默认情况下，该页面显示过去三天的用量和节省信息。您可以选择 last hour (过去一小时) 或 last three days (过去三天)。对于不到一小时之前启动的 Spot 队列，该页面显示这一小时的预计节省。

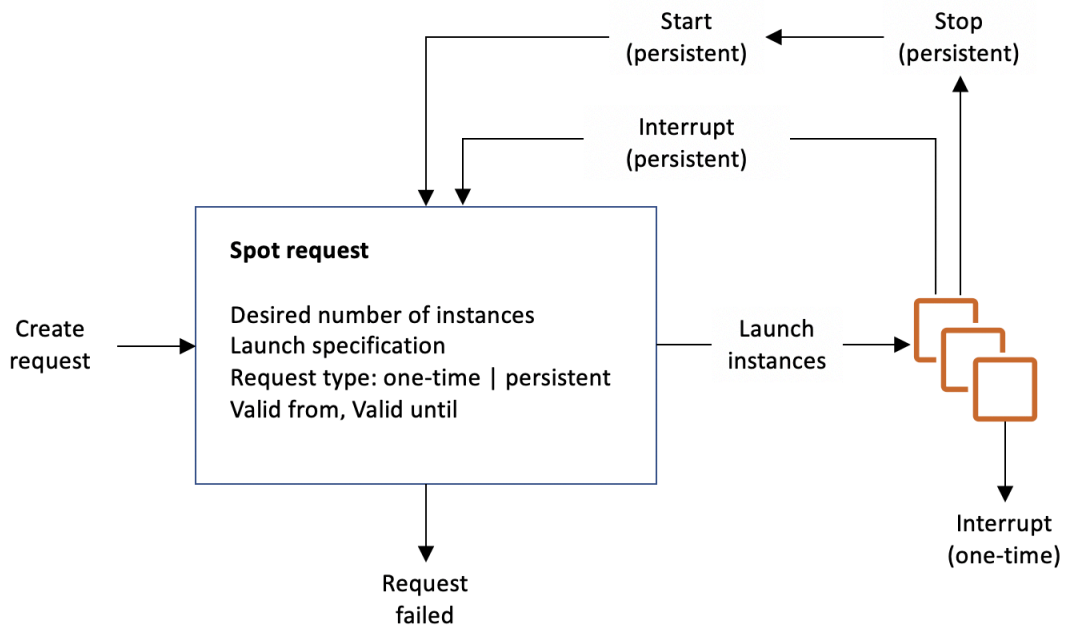
查看所有正在运行的竞价型实例的节省信息（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择 Savings Summary (节省成本摘要)。

使用竞价型实例

要使用竞价型实例，您需要创建竞价型实例请求，其中包括所需实例数量、实例类型以及可用区。当有容量可用时，Amazon EC2 将立即满足您的请求。否则，Amazon EC2 将等待直至可以完成您的请求，或者直至您取消请求。

以下演示了竞价型实例请求的运行方式。请注意，请求类型（一次性或持久性）确定在 Amazon EC2 中断竞价型实例时或者在您停止竞价型实例时是否重新打开请求。如果请求是持久性请求，则在中断竞价型实例之后将重新打开请求。如果请求是持久性的，并且您停止了竞价型实例，则请求仅在您启动竞价型实例后打开。



目录

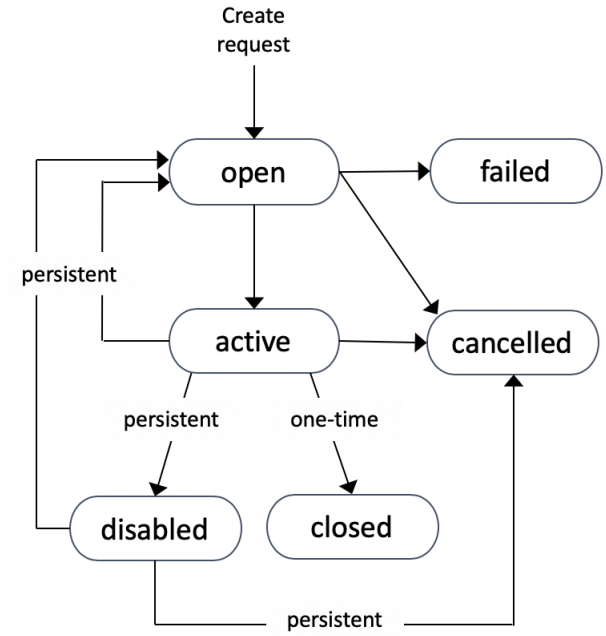
- 竞价型实例请求状态 (p. 457)
- 指定竞价型实例的租期 (p. 458)
- 竞价型实例请求的服务相关角色 (p. 458)
- 创建竞价型实例请求 (p. 460)
- 查找正在运行的竞价型实例 (p. 464)
- 标记竞价型实例请求 (p. 465)
- 取消竞价型实例请求 (p. 470)
- 停止竞价型实例 (p. 471)
- 启动竞价型实例 (p. 471)
- 终止竞价型实例 (p. 472)
- 竞价型实例请求示例启动规范 (p. 473)

竞价型实例请求状态

竞价型实例请求可以处于以下某种状态：

- `open` – 请求正在等待执行。
- `active` – 请求已执行并有关联的竞价型实例。
- `failed` – 请求的一个或多个参数错误。
- `closed` – 竞价型实例被中断或终止。
- `disabled` – 您停止了竞价型实例。
- `cancelled` – 您取消了请求或请求已过期。

以下显示了请求状态之间的转换。请注意，转换取决于请求类型 (一次性还是持久性)。



一次性竞价型实例请求在 Amazon EC2 启动竞价型实例、请求过期前或者您取消请求前保持有效。当没有容量可用时，将终止您的竞价型实例并关闭竞价型实例请求。

持久性竞价型实例请求在过期或您取消它之前保持有效，即使该请求已完成也如此。当没有容量可用时，您的竞价型实例将会中断。在您的实例中断后，在再次具有可用的容量时，将会启动竞价型实例（如果已停止）或将其恢复（如果已休眠）。您可以停止竞价型实例，然后在有容量可用是重新启动实例。如果竞价型实例终止（无论竞价型实例处于停止状态还是正在运行状态），则会重新打开竞价型实例请求，并且 Amazon EC2 启动一个新的竞价型实例。有关更多信息，请参阅停止竞价型实例 (p. 471)、启动竞价型实例 (p. 471)和终止竞价型实例 (p. 472)。

您可以跟踪竞价型实例请求的状态以及通过该状态启动的竞价型实例的状态。有关更多信息，请参阅Spot 请求状态 (p. 474)。

指定竞价型实例的租期

您可以在单租户硬件上运行竞价型实例。专用竞价型实例与属于其他 Amazon 账户的实例物理隔离。有关更多信息，请参阅Dedicated Instances (p. 533)和 Amazon EC2 专用实例产品页面。

要运行专用竞价型实例，请执行以下操作之一：

- 在创建竞价型实例请求时，请指定租期 `dedicated`。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。
- 在 VPC 中请求实例租期为 `dedicated` 的竞价型实例。有关更多信息，请参阅创建有专用实例租赁的 VPC (p. 536)。如果您在 VPC 中请求实例租期为 `dedicated` 的竞价型实例，则无法请求租期为 `default` 的竞价型实例。

所有实例系列都支持除 T 实例外的专用竞价型实例。对于每个受支持的实例系列，只有最大的实例或设备支持专用竞价型实例。

竞价型实例请求的服务相关角色

Amazon EC2 使用服务相关角色获取代表您调用其他Amazon服务所需的权限。服务相关角色是一种独特类型的 IAM 角色，它与Amazon服务直接相关。服务相关角色提供了一种将权限委托给 Amazon 服务的安全方

式，因为只有相关服务才能担任服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的使用服务相关角色。

Amazon EC2 使用名为 Amazon Web Services ServiceRoleForEC2Spot 的服务相关角色代表您启动和管理 Spot 实例。

Amazon Web Services ServiceRoleForEC2Spot 授予的权限

Amazon EC2 使用 Amazon Web Services ServiceRoleForEC2Spot 完成以下操作：

- `ec2:DescribeInstances` – 描述竞价型实例
- `ec2:StopInstances` – 停止竞价型实例
- `ec2:StartInstances` – 启动竞价型实例

创建服务相关角色

在大多数情况下，无需手动创建服务相关角色。Amazon EC2 在您首次使用控制台请求 Spot 实例时创建 Amazon Web Services ServiceRoleForEC2Spot 服务相关角色。

如果在 2017 年 10 月之前具有活动Spot 实例请求（此时 Amazon EC2 开始支持该服务相关角色），则 Amazon EC2 在您的Amazon账户中创建 Amazon Web Services ServiceRoleForEC2Spot 角色。有关更多信息，请参阅IAM 用户指南中的我的账户中出现新角色。

如果您使用 Amazon CLI 或 API 来请求竞价型实例，则必须确保此角色存在。

要使用控制台创建 Amazon Web Services ServiceRoleForEC2Spot

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色）。
3. 选择创建角色。
4. 在 Select type of trusted entity (选择受信任实体的类型) 页面上，依次选择 EC2、EC2 - Spot Instances (EC2 - Spot 实例) 和 Next: Permissions (下一步: 权限)。
5. 在下一页上，选择 Next:Review（下一步：审核）。
6. 在 Review (审核) 页面上，选择 Create role (创建角色)。

要使用 Amazon CLI 创建 Amazon Web Services ServiceRoleForEC2Spot

如下所示使用 create-service-linked-role 命令。

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

如果您不再需要使用 Spot 实例，我们建议您删除 Amazon Web Services ServiceRoleForEC2Spot 角色。从账户中删除该角色后，如果您请求竞价型实例，Amazon EC2 将再次创建该角色。

授予对用于加密的 AMI 和 EBS 快照的客户托管密钥的访问权限

如果为 Spot 实例指定加密的 AMI (p. 196) 或加密的 Amazon EBS 快照 (p. 1504)，并且您使用客户托管密钥进行加密，则必须为 Amazon Web Services ServiceRoleForEC2Spot 角色授予使用客户托管密钥的权限，以便 Amazon EC2 可以代表您启动 Spot 实例。为此，您必须在客户托管密钥中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用授权和在 Amazon KMS 中使用密钥策略。

为 Amazon Web Services ServiceRoleForEC2Spot 角色授予使用客户托管密钥的权限

- 使用 create-grant 命令在客户托管密钥中添加授权，并指定授予权限的委托人（Amazon Web Services ServiceRoleForEC2Spot 服务相关角色），以执行授权允许的操作。客户托管密钥由 `key-id` 参数和客户托管密钥的 ARN 指定。委托人是由 `grantee-principal` 参数和 Amazon Web Services ServiceRoleForEC2Spot 服务相关角色的 ARN 指定的。

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

创建竞价型实例请求

您可以使用 Amazon EC2 控制台中的启动实例向导 (p. 575)或 run-instances Amazon CLI 命令以与启动按需型实例相同的方式请求竞价型实例。建议使用此方法的原因如下：

- 您已经在使用启动实例向导 (p. 575)或 run-instances 命令启动按需型实例，而且只想通过更改单个参数来更改为启动竞价型实例。
- 您不需要多个实例类型不同的实例。

通常不建议使用此方法来启动竞价型实例，因为您无法指定多种实例类型，也无法在同一请求中启动竞价型实例和按需型实例。有关启动竞价型实例的首选方法（包括启动实例集，其中包含具有多种实例类型的竞价型实例和按需型实例类型），请参阅 使用哪种竞价型请求方法最好？ (p. 452)

如果您一次请求了多个竞价型实例，Amazon EC2 将创建单独的竞价型实例，这样您可以分别跟踪各个请求的状态。有关跟踪竞价型实例请求的更多信息，请参阅 Spot 请求状态 (p. 474)。

New console

使用启动实例向导创建竞价型实例请求

步骤 1-9 与启动按需型实例时使用的步骤相同。在步骤 10 中，您配置竞价型实例请求。

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，选择一个区域。
3. 从 Amazon EC2 控制台控制面板中，选择启动实例。
4. （可选）在Name and tags（名称和标签）下，您可以为实例命名，并为竞价型实例请求、实例、卷和弹性图形添加标签。有关标签的信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

   a. 对于 Name（名称），为您的实例输入一个描述性名称。

      实例名称是一个标签，其中密钥为 Name（名称），而值为您指定的名称。如果您没有指定名称，则可以通过其 ID 标识实例，该 ID 将在您启动实例时自动生成。

   b. 要为竞价型实例请求、实例、卷和弹性图形添加标签，请选择 Add additional tags（添加其他标签）。选择 Add tag（添加标签），然后输入密钥和值，然后选择要标记的资源类型。为每个要添加的其它标签选择 Add tag（添加标签）。
5. 在 Application and OS Images（Amazon Machine Image）（应用程序和操作系统镜像（Amazon Machine Image））下，为您的实例选择操作系统（OS），然后选择 AMI。有关更多信息，请参阅应用程序和操作系统镜像 (Amazon Machine Image) (p. 577)。
6. 在 Instance type（实例类型）下，请选择符合您对实例硬件配置和大小要求的实例类型。有关更多信息，请参阅实例类型 (p. 578)。

7. 在 Key pair（login）（密钥对（登录））下，选择一个现有密钥对，或选择 Create new key pair（创建新密钥对）来新建一个密钥对。有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

   Important

   如果您选择 Proceed without key pair (Not recommended)（在没有密钥对的情况下继续（不推荐））选项，则将无法连接到此实例，除非您选择配置为允许用户以其它方式登录的 AMI。

8. 在 Network settings（网络设置）下，使用默认设置，或选择 Edit（编辑）根据需要配置网络设置。

   安全组构成了网络设置的一部分，并为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。

   有关更多信息，请参阅Network settings (网络设置) (p. 579)。

9. 您选择的 AMI 包含一个或多个存储卷，包括根设备卷。在 Configure storage（配置存储）下，您可以选择 Add new volume（添加新卷）来指定要附加到实例的其他卷。有关更多信息，请参阅配置存储 (p. 580)。

10. 在 Advanced details（高级详细信息）下，按如下方式配置竞价型实例请求：

    a. 在 Purchasing option（购买选项）下，选择 Request Spot Instances（请求竞价型实例）复选框。

    b. 您可以保留竞价型实例请求的默认配置，也可以选择（位于右侧的） Customize（自定义）为竞价型实例请求指定自定义设置。

       选择 Customize（自定义）后，将显示以下字段。

       i. Maximum price（最高价）：您可以以 Spot 价格请求竞价型实例，上限为按需价格，也可以指定您愿意支付的最高金额。

          Warning

          如果您指定了某个最高价，则实例被中断的频率将比您选择 No maximum price（无最高价）时更高。

          - No maximum price（无最高价）：您的竞价型实例将以当前的 Spot 价格启动。价格永远不会超过按需价格。（建议）
          - Set your maximum price (per instance/hour)（设置最高价（每实例/小时））：您可以指定愿意支付的最高金额。
            - 如果您指定的最高价低于 Spot 价格，则不会启动您的竞价型实例。
            - 如果您指定的最高价高于当前 Spot 价格，则您的竞价型实例将按当前 Spot 价格启动和计费。竞价型实例运行后，如果 Spot 价格上涨到超过您的最高价格，Amazon EC2 将中断您的竞价型实例。
            - 无论您指定哪种最高价，都将始终按当前的 Spot 价格向您收取费用。

          要查看 Spot 价格趋势，请参阅 竞价型实例定价历史记录 (p. 454)。

       ii. Request type（请求类型）：您选择的竞价型实例请求类型决定了竞价型实例中断时会发生什么。

          - One-time（一次性）：Amazon EC2 为您的竞价型实例发出一次性请求。如果您的竞价型实例被中断，不会重新提交请求。
          - Persistent request（持久性请求）：Amazon EC2 对您的竞价型实例发出持久请求。如果您的竞价型实例中断，则将重新提交请求以补充中断的竞价型实例。

          如果您未指定值，则默认值为一次性请求。

iii. Valid to（有效截止时间）：持久性竞价型实例请求的到期日期。

一次性请求不支持此字段。一次性请求在请求中的所有实例启动或者您取消请求前保持有效。

- No request expiry date（没有请求到期日期）：请求在您将其取消之前保持有效。
- Set your request expiry date（设置请求到期日期）：持久性请求将保持活动状态，直到您指定的日期或取消该请求为止。

iv. Interruption behavior（中断行为）：您选择的行为决定了竞价型实例中断时会发生什么。

- 对于持久性请求，有效值为 Stop（停止）和 Hibernate（休眠）。实例停止后，将收取 EBS 卷存储费用。
- 对于一次性请求，只有 Terminate（终止）有效。

如果您未指定值，则默认值为 Terminate（终止），这对持久性竞价型实例请求无效。如果您保持默认设置并尝试启动持久性竞价型实例请求，则会收到错误消息。

有关更多信息，请参阅中断行为 (p. 485)。

v. Block duration (minutes) [区块持续时间（分钟）]

Note

不再支持具有定义持续时间（也称作竞价型限制）的竞价型实例。

11. 在存储库的 Summary（摘要）面板，对于 Number of instances（实例数量），输入要启动的实例数量。

Note

Amazon EC2 为每个竞价型实例创建一个单独的请求。

12. 在 Summary（摘要）面板，查看实例的详细信息并进行必要的更改。在提交竞价型实例请求后，您无法更改该请求的参数。您可以在 Summary（摘要）面板选择启动实例向导中某部分的链接以直接导航到该部分。有关更多信息，请参阅摘要 (p. 582)。
13. 当您准备好启动您的实例时，请选择 Launch instance（启动实例）。

如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

Old console

使用启动实例向导创建竞价型实例请求

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，选择一个区域。
3. 从 Amazon EC2 控制台控制面板中，选择 Launch Instance。
4. 在选择一个 Amazon Machine Image (AMI) 页上，选择一个 AMI。有关更多信息，请参阅步骤 1：选择 Amazon Machine Image (AMI) (p. 584)。
5. 在 Choose an Instance Type（选择实例类型）页上，选择要启动的实例的硬件配置和大小，然后选择 Next: Configure Instance Details（下一步：配置实例详细信息）。有关更多信息，请参阅步骤 2：选择实例类型 (p. 585)。
6. 在配置实例详细信息页上，按如下方式配置 Spot 实例请求：

- Number of instances (实例的数量)：输入要启动的实例的数量。

Note

Amazon EC2 为每个竞价型实例创建一个单独的请求。

- （可选）为帮助确保保持正确数量的实例来处理应用程序，您可选择 Launch into Auto Scaling Group (启动至 Auto Scaling 组) 以创建启动配置和 Auto Scaling 组。Auto Scaling 将根据您的规格来扩展组中的实例数。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。
- Purchasing option (购买选项)：选择 Request Spot instances (请求 Spot 实例) 以启动 Spot 实例。选择此选项后，将显示以下字段。
- 当前价格：为选定的实例类型显示每个可用区中的当前 Spot 价格。
- （可选）最高价：您可以将此字段留空，也可以指定您愿意支付的最高金额。

  Warning

  如果您指定了某个最高价，则实例被中断的频率将比您将此字段留空时更高。

  - 如果您指定的最高价低于 Spot 价格，则不会启动您的竞价型实例。
  - 如果您指定的最高价高于当前 Spot 价格，则您的竞价型实例将按当前 Spot 价格启动和计费。竞价型实例运行后，如果 Spot 价格上涨到超过您的最高价格，Amazon EC2 将中断您的竞价型实例。
  - 无论您指定哪种最高价，都将始终按当前的 Spot 价格向您收取费用。
  - 如果您将此字段留空，您将支付当前 Spot 价格。
- Persistent request (持久性请求)：如果您的 Spot 实例已中断，请选择 Persistent request (持久性请求) 以重新提交 Spot 实例请求。
- Interruption behavior (中断行为)：默认情况下，在 Spot 实例中断后，Spot 服务会将它终止。如果选择 Persistent request (持久性请求)，则可以指定 Spot 服务在 Spot 实例中断后将它停止或休眠。有关更多信息，请参阅中断行为 (p. 485)。
- （可选）请求有效截止时间：选择 Edit (编辑) 可指定 Spot 实例请求的过期时间。

有关配置竞价型实例的更多信息，请参阅 步骤 3：配置实例详细信息 (p. 585)。

7. 您选择的 AMI 包含一个或多个存储卷，包括根设备卷。在添加存储页面上，您可以选择添加新卷来指定要附加到实例的其他卷。有关更多信息，请参阅步骤 4：添加存储 (p. 587)。
8. 在 Add Tags 页面上，通过提供键和值组合来指定标签 (p. 1664)。有关更多信息，请参阅步骤 5：添加标签 (p. 587)。
9. 在 Configure Security Group (配置安全组) 页面上，使用安全组为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。所有其他的流量将被忽略。(有关安全组的更多信息，请参阅 适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。) 选择或创建安全组，然后选择审核和启动。有关更多信息，请参阅步骤 6：配置安全组 (p. 588)。
10. 在 Review Instance Launch 页面上，检查您的实例的详细信息，然后选择相应的 Edit 链接进行任何必要更改。如果准备就绪，请选择 Launch。有关更多信息，请参阅步骤 7：查看实例启动并选择密钥对 (p. 588)。
11. 在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，您可以选择现有密钥对，也可以创建新的密钥对。例如，选择选择现有密钥对，然后选择您在进行设置时创建的密钥对。有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

    Important

    如果您选择 Proceed without key pair 选项，则将无法连接到此实例，除非您选择配置为允许用户以其他方式登录的 AMI。
12. 要启动您的实例，请选中确认复选框，然后选择 Launch Instances。

    如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

Amazon CLI

使用 run-instances 创建竞价型实例请求

使用 run-instances 命令并在 `--instance-market-options` 参数中指定 Spot 实例选项。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

以下是要在 JSON 文件中为 `--instance-market-options` 指定的数据结构。您还可以指定 `ValidUntil` 和 `InstanceInterruptionBehavior`。如果未在数据结构中指定字段，则将使用默认值。

以下示例将创建一个 `persistent` 请求。

```
{
  "MarketType": "spot",
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

使用 request-spot-instances 创建竞价型实例请求

> **Note**
>
> 我们强烈反对使用 request-spot-instances 命令来请求竞价型实例，因为它是不具有计划投资的旧式 API。有关更多信息，请参阅 使用哪种竞价型请求方法最好？ (p. 452)

使用 request-spot-instances 命令可创建一次性请求。

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

使用 request-spot-instances 命令可创建持久性请求。

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

有关要用于这些命令的启动规范文件的示例，请参阅竞价型实例请求示例启动规范 (p. 473)。如果您从竞价型请求控制台下载启动规范文件，必须改为使用 request-spot-fleet 命令（竞价型请求控制台使用竞价型实例集指定竞价型实例请求）。

查找正在运行的竞价型实例

当有容量可用时，Amazon EC2 会启动竞价型实例。竞价型实例将一直运行，直到该实例中断，或者您自行终止该实例。

查找正在运行的竞价型实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。您可以同时查看竞价型实例请求和竞价型实例集请求。如果 Spot 实例请求已执行，那么 Capacity (容量) 就是 Spot 实例的 ID。对于 Spot 实例集，Capacity (容量) 表示已执行的请求容量。要查看 Spot 实例集中的实例的 ID，请选择扩展箭头，或者选择队列，然后选择 Instances (实例)。

   Note

   对于由竞价型实例集创建的竞价型实例请求，不会立即为这些请求添加用于指示它们所属的竞价型实例的系统标签，并且这些请求在一段时间内可能会独立于竞价型实例请求显示。

   或者，在导航窗格中，选择 Instances。在右上角，选择设置图标 ()，然后在属性列下选择实例生命周期。对于每个实例，实例生命周期为 `normal`、`spot` 或 `scheduled`。

查找正在运行的竞价型实例（Amazon CLI）

要枚举您的 Spot 实例，请结合使用 describe-spot-instance-requests 命令和 `--query` 选项。

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

下面是示例输出：

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

或者，您可结合使用 describe-instances 命令和 `--filters` 选项来枚举您的 Spot 实例。

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

要描述单个 Spot 实例，请使用带 `--spot-instance-request-ids` 选项的 describe-spot-instance-requests 命令。

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-08b93456
```

标记竞价型实例请求

要对您的竞价型实例请求进行分类和管理，您可使用自定义元数据标记它们。您可以在创建竞价型实例请求时或之后为其分配标签。您可以使用 Amazon EC2 控制台或命令行工具分配标签。

在标记竞价型实例请求时，不会自动标记由竞价型实例请求启动的实例和卷。您需要明确标记由竞价型实例请求启动的实例和卷。您可以在启动期间或之后为竞价型实例和卷分配标签。

有关标签的工作原理的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

目录

- 先决条件 (p. 466)
- 标记新的竞价型实例请求 (p. 467)
- 标记现有竞价型实例请求 (p. 468)
- 查看竞价型实例请求标记 (p. 468)

先决条件

授予用户标记资源的权限。有关 IAM policies 和示例策略的更多信息，请参阅示例：标记资源 (p. 1261)。

您创建的 IAM policy 由您用于创建竞价型实例请求的方法决定。

- 如果您使用启动实例向导或 `run-instances` 请求 Spot 实例，请参阅To grant a user the permission to tag resources when using the launch instance wizard or run-instances。
- 如果您使用 `request-spot-instances` 命令请求竞价型实例，请参阅 To grant a user the permission to tag resources when using request-spot-instances。

在使用启动实例向导或 run-instances 时向用户授予资源标记权限

创建包含以下内容的 IAM policy：

- `ec2:RunInstances` 操作。这将授予用户授予启动实例的权限。
- 对于 `Resource`，请指定 `spot-instances-request`。这允许用户创建竞价型实例请求，以请求竞价型实例。
- `ec2:CreateTags` 操作。这将授予用户创建标签的权限。
- 对于 `Resource`，请指定 `*`。这将允许用户标记在实例启动期间创建的所有资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Note

当您使用 RunInstances 操作创建竞价型实例请求并在创建时标记竞价型实例请求时，您需要了解 Amazon EC2 如何在 RunInstances 语句中评估 `spot-instances-request` 资源。在 IAM policy 中评估 `spot-instances-request` 资源，如下所示：

- 如果您在创建时未标记竞价型实例请求，则 Amazon EC2 不会在 RunInstances 语句中评估 `spot-instances-request` 资源。
- 如果您在创建时标记竞价型实例请求，则 Amazon EC2 会在 RunInstances 语句中评估 `spot-instances-request` 资源。

因此，对于 `spot-instances-request` 资源，以下规则适用于 IAM policy：

- 如果您使用 RunInstances 创建竞价型实例请求，并且您不打算在创建时标记竞价型实例请求，则无需明确允许 `spot-instances-request` 资源；调用将成功。
- 如果您使用 RunInstances 创建竞价型实例请求并打算在创建时标记竞价型实例请求，则必须在 RunInstances 允许语句中包含 `spot-instances-request` 资源，否则调用将失败。
- 如果您使用 RunInstances 创建竞价型实例请求并打算在创建时标记竞价型实例请求，则必须在 CreateTags 允许语句中指定 `spot-instances-request` 资源或包括 * 通配符，否则调用将失败。

有关示例 IAM policy（包括竞价型实例请求不支持的策略），请参阅 使用竞价型实例 (p. 1256)。

在使用 request-spot-instances 时向用户授予资源标记权限

创建包含以下内容的 IAM policy：

- `ec2:RequestSpotInstances` 操作。这将授予用户创建竞价型实例请求的权限。
- `ec2:CreateTags` 操作。这将授予用户创建标签的权限。
- 对于 `Resource`，请指定 `spot-instances-request`。这将允许用户仅标记竞价型实例请求。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

标记新的竞价型实例请求

使用控制台标记新的竞价型实例请求

1. 按照创建竞价型实例请求 (p. 460)过程操作。
2. 要添加标签，请在添加标签页上，选择添加标签，然后输入标签的键和值。为每个附加标签选择添加其他标签。

   对于每个标签，您可以使用相同标签来标记竞价型实例请求、竞价型实例和卷。要标记所有这三个项，请确保已选定 Instances (实例)、Volumes (卷)和 Spot Instance Requests (Spot 实例请求)。要仅标记其中的一个或两个项，请确保已选定要标记的资源，并清除其他资源。

3. 填写必填字段以创建 Spot 实例请求，然后选择 Launch (启动)。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。

使用 Amazon CLI 标记新的竞价型实例请求

要在创建时标记竞价型实例请求请求，请按以下方式配置竞价型实例请求配置：

- 使用 `--tag-specification` 参数指定竞价型实例请求的标签。
- 对于 `ResourceType`，请指定 `spot-instances-request`。如果指定其他值，则竞价型实例请求将失败。
- 对于 `Tags`，请指定键值对。您可以指定多个键值对。

在以下示例中，使用两个标签来标记竞价型实例请求：键=环境，值=生产；键=成本中心，值=123。

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

标记现有竞价型实例请求

使用控制台标记现有的竞价型实例请求

创建竞价型实例请求后，您可以使用控制台向竞价型实例请求添加标签。

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，请选择 Spot Requests。
2. 选择您的竞价型实例请求。
3. 选择 Tags (标签) 选项卡，然后选择 Create Tag (创建标签)。

使用控制台标记现有的竞价型实例

在竞价型实例请求启动竞价型实例后，您可以使用控制台向实例添加标签。有关更多信息，请参阅在单个资源上添加和删除标签 (p. 1670)。

使用 Amazon CLI 标记现有的竞价型实例请求或竞价型实例

使用 create-tags 命令标记现有的资源。在以下示例中，使用以下标签标记现有竞价型实例请求和竞价型实例：键=目的，值=测试。

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

查看竞价型实例请求标记

使用控制台查看竞价型实例请求标签

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，请选择 Spot Requests。
2. 选择您的 Spot 实例请求并选择 Tags (标签) 选项卡。

描述竞价型实例请求标记

使用 describe-tags 命令可查看指定资源的标签。在以下示例中，您将描述指定请求的标签。

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sir-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sir-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-instances-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sir-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-instances-request",
            "Value": "Another value"
        }
    ]
}
```

您还可以通过描述竞价型实例请求来查看竞价型实例请求的标签。

使用 describe-spot-instance-requests 命令可查看指定的 Spot 实例请求的配置，其中包括为请求指定的任何标签。

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotInstanceRequests": [
        {
            "CreateTime": "2020-06-24T14:22:11+00:00",
            "InstanceId": "i-1234567890EXAMPLE",
            "LaunchSpecification": {
                "SecurityGroups": [
                    {
                        "GroupName": "launch-wizard-6",
                        "GroupId": "sg-1234567890EXAMPLE"
                    }
                ],
                "BlockDeviceMappings": [
                    {
                        "DeviceName": "/dev/xvda",
                        "Ebs": {
                            "DeleteOnTermination": true,
                            "VolumeSize": 8,
                            "VolumeType": "gp2"
                        }
                    }
                ],
                "ImageId": "ami-1234567890EXAMPLE",
                "InstanceType": "t2.micro",
                "KeyName": "my-key-pair",
                "NetworkInterfaces": [
                    {
                        "DeleteOnTermination": true,
                        "DeviceIndex": 0,
                        "SubnetId": "subnet-11122233"
```

```
                    }
                ],
                "Placement": {
                    "AvailabilityZone": "eu-west-1c",
                    "Tenancy": "default"
                },
                "Monitoring": {
                    "Enabled": false
                }
            },
            "LaunchedAvailabilityZone": "eu-west-1c",
            "ProductDescription": "Linux/UNIX",
            "SpotInstanceRequestId": "sir-1234567890EXAMPLE",
            "SpotPrice": "0.012600",
            "State": "active",
            "Status": {
                "Code": "fulfilled",
                "Message": "Your spot request is fulfilled.",
                "UpdateTime": "2020-06-25T18:30:21+00:00"
            },
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ],
            "Type": "one-time",
            "InstanceInterruptionBehavior": "terminate"
        }
    ]
}
```


取消竞价型实例请求

如果您不再需要竞价型实例请求，您可以将其取消。您只能取消 open、active 或 disabled 的竞价型实例请求。

- 当您的请求未执行，且实例没有启动时，您的竞价型实例请求处于 open 状态。
- 当您的请求完成且竞价型实例因此已启动时，您的竞价型实例请求处于 active 状态。
- 当您停止竞价型实例时，您的竞价型实例请求处于 disabled 状态。

如果您的竞价型实例请求处于 active 状态，且关联的竞价型实例正在运行，那么取消请求不会终止该实例。有关终止竞价型实例的更多信息，请参阅 终止竞价型实例 (p. 472)。

取消竞价型实例请求（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Spot Requests (Spot 请求)，然后选择 Spot 请求。
3. 依次选择操作和取消请求。
4. (可选) 如果不再使用关联的竞价型实例，可以将其终止。在取消竞价请求对话框中，选择终止实例，然后选择确认。

取消 Spot 实例请求 (Amazon CLI)

- 使用 cancel-spot-instance-requests 命令可取消指定的 Spot 实例请求。

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

停止竞价型实例

如果您现在不需要竞价型实例，但希望在以后重启它们且不会丢失 Amazon EBS 卷中保留的数据，您可以停止它们。停止竞价型实例的步骤与停止按需型实例的步骤类似。

Note

在停止竞价型实例后，您可以修改其部分实例属性，但不能修改实例类型。
我们不会对已停止的竞价型实例收费，也不会收取数据传输费，但我们会对所有 Amazon EBS 卷的存储收费。

限制

- 只有当竞价型实例是从 `persistent` 竞价型实例请求启动时，您才能停止竞价型实例。
- 如果关联的竞价型实例请求被取消，则无法停止竞价型实例。当竞价型实例请求被取消后，您只能终止竞价型实例。
- 如果竞价型实例是某个队列或启动组或可用区组的一部分，则无法停止它。

Console

停止竞价型实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择 Spot 实例。
3. 依次选择实例状态、停止实例。
4. 当系统提示您确认时，选择 Stop。

Amazon CLI

停止竞价型实例（Amazon CLI）

- 使用 stop-instances 命令手动停止一个或多个 Spot 实例。

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

启动竞价型实例

您可以启动以前停止的竞价型实例。启动竞价型实例的步骤与启动按需型实例的步骤类似。

先决条件

您只能在以下情况下启动竞价型实例：

- 您手动停止了竞价型实例。
- 竞价型实例是 EBS 支持的实例。
- 竞价型实例容量可用。
- Spot 价格低于您的最高价格。

限制

- 如果竞价型实例是某个队列或启动组或可用区组的一部分，则无法启动它。

Console

启动竞价型实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择 Spot 实例。
3. 依次选择实例状态、启动实例。

Amazon CLI

启动竞价型实例（Amazon CLI）

- 使用 start-instances 命令手动启动一个或多个 Spot 实例。

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

终止竞价型实例

如果您终止的运行中或已停止竞价型实例是由持久性竞价型实例请求启动的，则竞价型实例请求会转换为 open 状态，这样就可以启动新的竞价型实例。要确保没有启动新的竞价型实例，您必须首先取消该竞价型实例请求。

如果您取消含有正在运行的竞价型实例的 active 竞价型实例请求，则正在运行的竞价型实例不会自动终止；您必须手动终止该竞价型实例。

如果您取消含有已停止的竞价型实例的 disabled 竞价型实例请求，则 Amazon EC2 Spot 服务将自动终止已停止的竞价型实例。取消竞价型实例请求与 Spot 服务终止竞价型实例之间可能存在短暂的滞后。

有关取消 Spot 实例请求的信息，请参阅取消竞价型实例请求 (p. 470)。

Console

使用控制台手动终止竞价型实例

1. 在终止实例前，请确认您是否会丢失任何数据，方法是确认您的 Amazon EBS 卷是否会在终止时被删除，以及您是否已将所需数据从实例存储卷复制到持久性存储，例如 Amazon EBS 或 Amazon S3。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择实例。
4. 要确认实例是否是 Spot 实例，请检查 Instance lifecycle (实例生命周期) 列中是否显示 spot。
5. 选择相应实例，然后依次选择 Instance state (实例状态)、Terminate instance (终止实例)。
6. 当系统提示您确认时，选择终止。

Amazon CLI

使用 Amazon CLI 手动终止竞价型实例

- 使用 terminate-instances 命令可手动终止 Spot 实例。

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

竞价型实例请求示例启动规范

以下示例显示了可与 request-spot-instances 命令结合使用来创建 Spot 实例请求的启动配置。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。

> **Note**
>
> 我们强烈反对使用 request-spot-instances 命令来请求竞价型实例，因为它是不具有计划投资的旧式 API。有关更多信息，请参阅 使用哪种竞价型请求方法最好？ (p. 452)

示例

- 示例 1：启动竞价型实例 (p. 473)
- 示例 2：在指定的可用区中启动竞价型实例 (p. 473)
- 示例 3：在指定的子网中启动竞价型实例 (p. 473)
- 示例 4：启动专用竞价型实例 (p. 474)

示例 1：启动竞价型实例

以下示例不包含可用区或子网。Amazon EC2 会为您选择可用区。Amazon EC2 会在所选可用区的默认子网中启动实例。

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

示例 2：在指定的可用区中启动竞价型实例

以下示例包括一个可用区。Amazon EC2 会在指定可用区的默认子网中启动实例。

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

示例 3：在指定的子网中启动竞价型实例

以下示例包括子网。Amazon EC2 会在指定子网中启动实例。如果 VPC 是一个非默认 VPC，则默认情况下，该实例不会收到公有 IPv4 地址。

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

要将公有 IPv4 地址分配给非默认 VPC 中的实例，请指定 `AssociatePublicIpAddress` 字段，如以下示例所示。指定网络接口时，您必须包含使用网络接口 (而不是使用之前的代码块中所示的 `SubnetId` 和 `SecurityGroupIds` 字段) 的子网 ID 和安全组 ID。

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

示例 4：启动专用竞价型实例

以下示例请求租期为 `dedicated` 的竞价型实例。专用竞价型实例必须在 VPC 中启动。

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Spot 请求状态

要帮助跟踪您的竞价型实例请求和规划您对竞价型实例的使用，请使用 Amazon EC2 提供的请求状态。例如，请求状态可以提供尚未完成 Spot 请求的原因，或者列出妨碍完成 Spot 请求的限制。

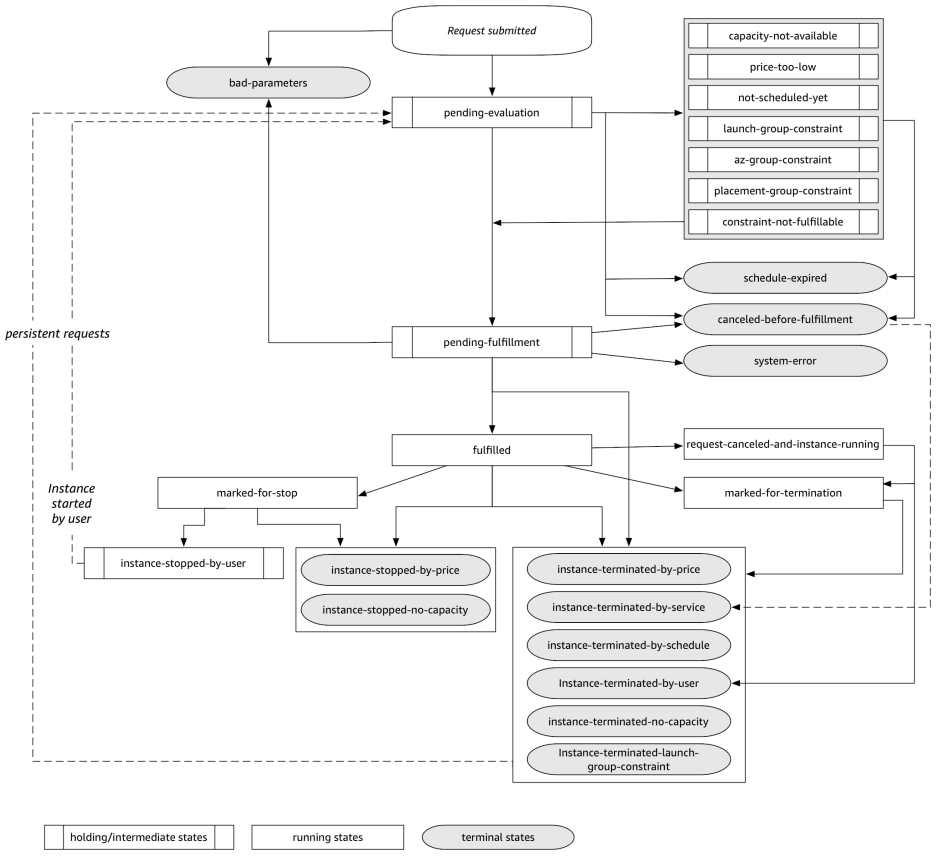
在此过程（也称为 Spot 请求生命周期）中的每一步，都有特定事件确定连续的请求状态。

目录

- Spot 请求的生命周期 (p. 475)
- 获取请求状态信息 (p. 478)
- Spot 请求状态代码 (p. 478)
- EC2 竞价型实例请求履行事件 (p. 480)

Spot 请求的生命周期

以下图表显示您的 Spot 请求在其整个生命周期 (从提交到终止) 所遵循的路径。每个步骤用节点表示，每个节点状态代码描述您的 Spot 请求和竞价型实例的状态。



待评估

当您创建竞价型实例请求之后，除非一个或多个请求参数无效（`bad-parameters`），否则该请求就会进入 `pending-evaluation` 状态。

状态代码	请求状态	实例状态
`pending-evaluation`	`open`	不适用
`bad-parameters`	`closed`	不适用

备用

如果一个或多个请求限制有效但目前无法满足，或者如果没有足够的容量，那么请求将进入暂挂状态，等待满足限制。请求选项影响请求完成的可能性。例如，如果没有容量可用，您的请求将会保持暂挂状态，直到有容量可用为止。如果您指定了可用区组，则该请求将保持为暂挂状态，直至满足可用区的限制。

如果其中一个可用区中断，则可能会影响其他可用区中可用于竞价型实例请求的备用 EC2 容量。

状态代码	请求状态	实例状态
`capacity-not-available`	`open`	不适用

状态代码	请求状态	实例状态
price-too-low	open	不适用
not-scheduled-yet	open	不适用
launch-group-constraint	open	不适用
az-group-constraint	open	不适用
placement-group-constraint	open	不适用
constraint-not-fulfillable	open	不适用

等待评估/最终执行

如果您创建的请求仅在特定时段内有效，但该时段在您的请求到达等待执行阶段之前过期，则您的竞价型实例请求可能会进入 terminal 状态。如果您取消请求，或者出现系统错误，请求也可能会进入该状态。

状态代码	请求状态	实例状态
schedule-expired	cancelled	不适用
canceled-before-fulfillment [1]	cancelled	不适用
bad-parameters	failed	不适用
system-error	closed	不适用

[1] 如果您取消请求。

等待履行

如果满足指定的限制（如有），您的 Spot 请求将会进入 pending-fulfillment 状态。

此时，Amazon EC2 已经准备好为您预置您请求的实例。如果该过程在此时停止，则可能是因为用户在启动竞价型实例之前取消了请求。也可能是因为出现了意外的系统错误。

状态代码	请求状态	实例状态
pending-fulfillment	open	不适用

已完成

当您的竞价型实例的所有规范都得到满足时，您的竞价型实例就会执行。Amazon EC2 会启动竞价型实例，这可能需要几分钟的时间。如果竞价型实例在中断时休眠或停止，它将保持该状态，直到可以再次完成该请求或取消该请求。

状态代码	请求状态	实例状态
fulfilled	active	pending → running
fulfilled	active	stopped → running

如果您停止竞价型实例，则 Spot 请求将进入 marked-for-stop 或 instance-stopped-by-user 状态，直到竞价型实例可以重新启动或者取消了请求。

状态代码	请求状态	实例状态
marked-for-stop	active	stopping
instance-stopped-by-user [1]	disabled 或 cancelled [2]	stopped

[1] 如果您停止实例或从实例运行 shutdown 命令，则竞价型实例将进入 instance-stopped-by-user 状态。停止实例后，您可以重新启动它。重新启动时，竞价型实例请求将返回 pending-evaluation 状态，然后 Amazon EC2 在满足约束时启动一个新的竞价型实例。

[2] 如果您停止竞价型实例但不取消请求，则 Spot 请求状态为 disabled。如果您的竞价型实例已停止并且请求已过期，则请求状态为 cancelled。

执行的最终

只要实例类型具有可用的容量，并且您未终止竞价型实例，这些实例就会继续运行。如果 Amazon EC2 必须终止竞价型实例，竞价型请求将会进入终止状态。如果取消 Spot 请求或终止竞价型实例，请求也将进入终止状态。

状态代码	请求状态	实例状态
request-canceled-and-instance-running	cancelled	running
marked-for-stop	active	running
marked-for-termination	active	running
instance-stopped-by-price	disabled	stopped
instance-stopped-by-user	disabled	stopped
instance-stopped-no-capacity	disabled	stopped
instance-terminated-by-price	closed（一次性），open（持久性）	terminated
instance-terminated-by-schedule	closed	terminated
instance-terminated-by-service	cancelled	terminated
instance-terminated-by-user	closed 或 cancelled [1]	terminated
instance-terminated-no-capacity	closed（一次性），open（持久性）	running †
instance-terminated-no-capacity	closed（一次性），open（持久性）	terminated

状态代码	请求状态	实例状态
instance-terminated-launch-group-constraint	closed（一次性），open（持久性）	terminated

[1] 如果您终止实例但未取消请求，则请求状态为 closed。如果您终止实例并取消请求，则请求状态为 cancelled。即使您在取消实例请求之前终止了竞价型实例，Amazon EC2 检测您的竞价型实例已终止的过程可能会有延迟。在这种情况下，请求状态可能是 closed 或 cancelled。

† Amazon EC2 中断竞价型实例时（如果其需要恢复容量且该实例配置为在中断时终止），状态将立即设置为 instance-terminated-no-capacity（如果未设置为 marked-for-termination）。但是，实例会保持 2 分钟 running 状态，以反映实例收到竞价型实例中断通知的 2 分钟时间段。2 分钟后，实例状态设置为 terminated。

持久性请求：

当您的竞价型实例终止（由您或由 Amazon EC2）时，如果 Spot 请求为持久性请求，则该请求返回 pending-evaluation 状态，并且在满足约束时，Amazon EC2 可以启动新的竞价型实例。

获取请求状态信息

您可以使用 Amazon Web Services Management Console或命令行工具获取请求状态信息。

获取请求状态信息（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests (Spot 请求)，然后选择所需的 Spot 请求。
3. 要检查状态，请在 Description (描述) 选项卡上检查 Status (状态) 字段。

使用命令行获取请求状态信息

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-spot-instance-requests (Amazon CLI)
- Get-EC2SpotInstanceRequest (Amazon Tools for Windows PowerShell)

Spot 请求状态代码

Spot 请求状态信息包含状态代码、更新时间以及状态消息。这些信息帮助您确定如何处理 Spot 请求。

下面是 Spot 请求状态代码：

az-group-constraint

Amazon EC2 无法在同一可用区中启动您请求的所有实例。

bad-parameters

您的 Spot 请求的一个或多个参数无效 (例如，您指定的 AMI 不存在)。状态消息指示哪个参数无效。

canceled-before-fulfillment

在完成前，用户取消了竞价请求。

capacity-not-available

您请求的实例没有足够的容量可用。

`constraint-not-fulfillable`

由于一个或多个限制无效 (例如，可用区不存在)，Spot 请求无法完成。状态消息指示哪个限制无效。

`fulfilled`

Spot 请求处于 `active` 状态，Amazon EC2 正在启动您的 Spot 实例。

`instance-stopped-by-price`

您的实例已停止，因为 Spot 价格超出了您的最高价格。

`instance-stopped-by-user`

由于用户停止了实例或从实例运行了 shutdown 命令，您的实例已停止。

`instance-stopped-no-capacity`

由于 EC2 容量管理需要，您的实例已停止。

`instance-terminated-by-price`

您的实例已终止，因为 Spot 价格超出了您的最高价格。如果您的请求是持久性的，该过程将重新开始，因此，您的请求将等待进行评估。

`instance-terminated-by-schedule`

您的竞价型实例在其计划持续时间结束时终止。

`instance-terminated-by-service`

您的实例从停止状态终止。

`instance-terminated-by-user` 或者 `spot-instance-terminated-by-user`**

您终止了已完成的竞价型实例，因此，请求状态为（`closed`除非这是持久性请求），实例状态为 `terminated`。

`instance-terminated-launch-group-constraint`

您的启动组中的一个或多个实例已终止，因此不再满足启动组的限制。

`instance-terminated-no-capacity`

由于标准容量管理流程，您的实例已终止。

`launch-group-constraint`

Amazon EC2 无法同时启动您请求的所有实例。启动组内的所有实例都一起启动和终止。

`limit-exceeded`

超过了 EBS 卷数量或总卷存储的限制。有关这些限制以及如何请求提高限制的更多信息，请参阅Amazon Web Services General Reference中的 Amazon EBS 限制。

`marked-for-stop`

竞价型实例被标记为停止。

`marked-for-termination`

竞价型实例被标记为终止。

`not-scheduled-yet`

您的 Spot 请求在指定日期之前不会被评估。

`pending-evaluation`

当您提交竞价型实例请求之后，该请求会进入 `pending-evaluation` 状态，同时系统会评估您的请求中的参数。

`pending-fulfillment`

Amazon EC2 正尝试预置竞价型实例。

`placement-group-constraint`

因为竞价型实例目前不能添加到置放群组中，因此尚无法完成 Spot 请求。

`price-too-low`

由于您的最高价低于 Spot 价格，无法完成请求。在这种情况下，不会启动任何实例，并且您的请求保持 open 状态。

`request-canceled-and-instance-running`

在竞价型实例仍在运行时，您取消了 Spot 请求。请求为 `cancelled`，但是，实例保持为 `running`。

`schedule-expired`

由于没有在指定日期前完成，Spot 请求已过期。

`system-error`

出现意外系统错误。如果这是反复出现的问题，请联系 Amazon Web Services Support 以获取帮助。

EC2 竞价型实例请求履行事件

当竞价型实例请求履行后，Amazon EC2 会向 Amazon EventBridge 发送一个 EC2 竞价型实例请求履行事件。您可以创建一条规则，以在此事件发生时执行操作，例如调用某个 Lambda 函数或通知某个 Amazon SNS 主题。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

有关更多信息，请参阅 Amazon EventBridge 用户指南。

EC2 实例再平衡建议

EC2 实例再平衡建议是一个信号，可在竞价型实例处于较高的中断风险时通知您。信号可能比该两分钟的 Spot 实例中断通知 (p. 490)更早到达，从而让您有机会主动管理 Spot 实例。您可以决定将工作负载再平衡到不处于较高中断风险的新的或现有的竞价型实例。

Amazon EC2 并不总能在两分钟的竞价型实例中断通知之前发送再平衡建议信号。因此，再平衡建议信号可能会随两分钟的中断通知一起到达。

再平衡建议是作为 CloudWatch 事件以及竞价型实例上的实例元数据 (p. 754)中的项目提供的。尽最大努力发出事件。

Note

再平衡建议仅支持 2020 年 11 月 5 日 00:00 UTC 之后推出的竞价型实例。

主题

- 您可以采取的再平衡操作 (p. 481)
- 监控再平衡建议信号 (p. 481)
- 使用再平衡建议信号的服务 (p. 484)

您可以采取的再平衡操作

以下是您可以采取的一些可能的再平衡操作：

正常关闭

当您收到竞价型实例的再平衡建议信号时，您可以启动实例关闭过程，其中可能包括确保在停止进程之前完成它们。例如，您可以将系统或应用程序日志上传到 Amazon Simple Storage Service (Amazon S3)、关闭 Amazon SQS 工作程序或从域名系统 (DNS) 中完成注销。您还可以将工作保存在外部存储器中，稍后再恢复工作。

防止计划新工作

当您收到竞价型实例的再平衡建议信号时，您可以阻止在实例上计划新工作，同时继续使用实例直到计划的工作完成。

主动启动新的替换实例

您可以配置 Auto Scaling 组、EC2 实例集或竞价型实例集，以在系统发出再平衡建议信号时自动启动替换竞价型实例集。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 Amazon EC2 Auto Scaling 容量再平衡以及本用户指南中适用于 EC2 实例集 的 容量再平衡 (p. 849) 和适用于 Spot 实例集的 容量再平衡 (p. 888)。

监控再平衡建议信号

您可以监控再平衡建议信号，以便在发出该信号时，可以执行上一节中指定的操作。再平衡建议信号作为发送到 Amazon EventBridge（以前称为 Amazon CloudWatch Events）的事件和竞价型实例上的实例元数据提供。

监控再平衡建议信号：

- 使用 Amazon EventBridge (p. 481)
- 使用实例元数据 (p. 483)

使用 Amazon EventBridge

当发出竞价型实例的再平衡建议信号时，该信号的事件将被发送到 Amazon EventBridge。如果 EventBridge 检测到与规则中定义的模式匹配的事件模式，则 EventBridge 调用规则中指定的一个或多个目标。

以下是再平衡建议信号的示例事件。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

下列字段构成规则中定义的事件模式：

`"detail-type": "EC2 Instance Rebalance Recommendation"`

确定该事件是再平衡建议事件

`"source": "aws.ec2"`

识别来自 Amazon EC2 的事件

创建 EventBridge 规则

当事件模式与规则匹配时，您可以编写 EventBridge 规则并自动执行要采取的操作。

下面的示例可创建 EventBridge 规则，以便在 Amazon EC2 每次发出再平衡建议信号时发送电子邮件、短信或移动推送通知。信号作为 `EC2 Instance Rebalance Recommendation` 事件发出，这将触发规则定义的操作。

创建 EventBridge 规则之前，您必须为电子邮件、短信或移动推送通知创建 Amazon SNS 主题。

要为再平衡建议事件创建 EventBridge 规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于定义规则详细信息，请执行以下操作：
   a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

      规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
   b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。
   c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。
   d. 选择 Next（下一步）。
4. 对于 Build event pattern（构建事件模式），执行以下操作：
   a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。
   b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 `EC2 Instance Rebalance Recommendation` 事件，然后选择 Save（保存）。

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

      要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

      i. 要使用模板创建事件模式，请执行以下操作：

         A. 选择 Event pattern form（事件模式表）。

B. 对于 Event source（事件源），选择 Amazon services（服务）。
C. 对于 Amazon 服务，选择 EC2 竞价型实例集。
D. 对于 Event type（事件类型），选择 EC2 Instance Rebalance Recommendation（EC2 实例再平衡建议）。
E. 要自定义模板，请选择 Edit pattern（编辑模式），然后进行更改以匹配示例事件模式。

ii. （可选）要指定自定义事件模式，请执行以下操作：

A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。
B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。

c. 选择 Next（下一步）。

5. 对于 Select target(s)（选择目标），请执行以下操作：

a. 对于 Target types（目标类型），选择 Amazon service（服务）。
b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。
c. 对于 Topic（主题），选择现有主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。
d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。
e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。
7. 对于 Review and create（查看与创建），执行以下操作：

a. 查看规则的详细信息并根据需要对其进行修改。
b. 选择 Create rule（创建规则）。

有关更多信息，请参阅 Amazon EventBridge 用户指南中的为Amazon服务创建规则和事件模式

使用实例元数据

实例元数据类别 `events/recommendations/rebalance` 提供为 Spot 实例发出再平衡建议信号的大致时间 (UTC)。

我们建议您每 5 秒检查一次再平衡建议信号，这样您就不会错过对再平衡建议采取行动的机会。

如果竞价型实例收到再平衡建议，则信号发出的时间将显示在实例元数据中。您可以按如下方式检索信号发出的时间。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

以下是示例输出，表示为竞价型实例发出的再平衡建议信号时间 (UTC)。

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

如果尚未为实例发出信号，则 `events/recommendations/rebalance` 不存在，您将在尝试检索该信号时收到 HTTP 404 错误。

使用再平衡建议信号的服务

Amazon EC2 Auto Scaling、EC2 实例集和竞价型实例集使用再平衡建议信号让您可以轻松地在运行中的实例收到两分钟的竞价型实例中断通知之前，主动使用新的竞价型实例扩展您的队列，从而帮助您维护工作负载的可用性。您可以让这些服务监控和主动响应影响您的竞价型实例可用性的更改。有关更多信息，请参阅下列内容：

- Amazon EC2 Auto Scaling 用户指南中的 Amazon EC2 Auto Scaling 容量再平衡
- 容量再平衡 (p. 849)本用户指南中 EC2 队列 主题中的
- 本用户指南中 Spot 实例集主题中的 容量再平衡 (p. 888)

竞价型实例中断

您可以在空闲的 EC2 容量上启动竞价型实例，以便在 Amazon EC2 需要收回这些容量时，就返还实例获得大幅折扣。我们将 Amazon EC2 回收 Spot 实例的情况称为 Spot 实例中断。

当 Amazon EC2 中断竞价型实例时，它会终止、停止或休眠实例，具体取决于您在创建竞价型请求时指定的内容。

对竞价型实例的需求可能因时间不同而有显著的差异，竞价型实例 的可用性也会因为有多少未使用 EC2 实例可用而差别巨大。竞价型实例可能会中断。

在 EC2 实例集或 Spot 实例集中指定的按需型实例不能中断。

目录

- 中断原因 (p. 484)
- 中断行为 (p. 485)
- 停止中断的竞价型实例 (p. 485)
- 休眠中断的竞价型实例 (p. 486)
- 终止中断的竞价型实例 (p. 488)
- 准备中断 (p. 488)
- 启动竞价型实例中断 (p. 489)
- 竞价型实例中断通知 (p. 490)
- 查找中断的竞价型实例 (p. 492)
- 确定 Amazon EC2 是否终止了竞价型实例 (p. 493)
- 中断的竞价型实例的计费 (p. 493)

中断原因

下面列出了 Amazon EC2 中断您的竞价型实例的可能原因：

容量

Amazon EC2 可以在需要收回时中断 Spot 实例。EC2 回收您的实例主要是为了重新调整容量用途，但也可能出于其他原因，如主机维护或硬件停用。

价格

Spot 价格高于您的最高价格。

您可以在竞价型请求中指定最高价格。但如果您指定了某个最高价，则实例被中断的频率将比您未指定时更高。

约束

如果您的竞价型请求包含约束（如启动组或可用区组），则当不再满足约束时，这些竞价型实例将成组终止。

您可以在 Spot Instance Advisor（Spot 实例顾问）中查看实例类型的历史中断率。

中断行为

您可以指定 Amazon EC2 在中断竞价型实例时必须执行以下操作之一：

- 停止中断的竞价型实例 (p. 485)
- 休眠中断的竞价型实例 (p. 486)
- 终止中断的竞价型实例 (p. 488)（这是默认行为）

指定中断行为

您可以在创建 Spot 请求时指定中断行为。如果未指定中断行为，则默认情况是 Amazon EC2 在中断竞价型实例时终止它们。

指定中断行为的方式根据您请求竞价型实例的方式会有所不同。

- 如果您使用启动实例向导 (p. 575)请求竞价型实例，则可以按如下方式指定中断行为：从 Request type（请求类型）中，选中 Persistent（持久性）（新控制台）或选中 Persistent request（持久性请求）复选框（旧控制台），然后从 Interruption behavior（中断行为）中，选择中断行为。
- 如果您使用 Spot 控制台 (p. 900) 请求 Spot 实例，则可以按如下方式指定中断行为：选中保持目标容量复选框，然后从中断行为中选择中断行为。
- 如果您在启动模板 (p. 590)中配置竞价型实例，则可以按如下方式指定中断行为：在启动模板中，展开 Advanced details（高级详细信息），然后选择 Request 竞价型实例（请求）复选框。选择 自定义，然后从中断行为中选择中断行为。
- 如果您在使用 create-fleet CLI 时在请求配置中对竞价型实例进行配置，则可以按如下方式指定中断行为：对于 `InstanceInterruptionBehavior`，请指定中断行为。
- 如果您在使用 request-spot-fleet CLI 时在请求配置中对竞价型实例进行配置，则可以按如下方式指定中断行为：对于 `InstanceInterruptionBehavior`，请指定中断行为。
- 如果您使用 request-spot-instances CLI 配置竞价型实例，则可以按如下方式指定中断行为：对于 `--instance-interruption-behavior`，请指定中断行为。

停止中断的竞价型实例

您可以指定 Amazon EC2 在竞价型实例中断时将其停止。有关更多信息，请参阅指定中断行为 (p. 485)。

注意事项

- 只有 Amazon EC2 才能重新启动已停止的竞价型实例。
- 对于由 `persistent` 竞价型实例请求启动的竞价型实例：Amazon EC2 会在容量在同一可用区中可用且适用于已停止的实例的同一实例类型（必须使用相同的启动规范）时重新启动已停止的实例。
- 对于类型为 `maintain` 的 EC2 集群或竞价型实例集启动的竞价型实例：竞价型实例中断后，Amazon EC2 启动替代实例以维持目标容量。Amazon EC2 基于指定的分配策略（`lowestPrice`、`diversified` 或 `InstancePoolsToUseCount`）查找最优竞价型容量池；它不会使用早期已停止的实例确定池的优先级。稍后，如果分配策略产生了包含早期已停止的实例的池，则 Amazon EC2 会重新启动已停止的实例以满足目标容量。

例如，考虑使用 lowestPrice 分配策略的 Spot 实例集。初始启动时，c3.large 池满足启动规范的 lowestPrice 条件。稍后，当中断 c3.large 实例时，Amazon EC2 会停止实例并从符合 lowestPrice 策略的其他池中补充容量。此时，该池正好是一个 c4.large 池，并且 Amazon EC2 会启动 c4.large 实例以满足目标容量。同样，Spot 实例集下次可以移动到 c5.large 池。在这些转换的每个转换中，Amazon EC2 不会使用早期已停止的实例确定池的优先级，但会仅在指定的分配策略上确定优先级。lowestPrice 策略可以返回到包含早期已停止的实例的池。例如，如果实例在 c5.large 池中被中断且 lowestPrice 策略将其返回到 c3.large 或 c4.large 池，则早期已停止的实例会重新启动以满足目标容量。

- 在停止竞价型实例后，您可以修改其部分实例属性，但不能修改实例类型。如果您分离或删除一个 EBS 卷，则在启动竞价型实例时不会附加该卷。如果您分离根卷并且 Amazon EC2 尝试启动竞价型实例，则该实例将无法启动，Amazon EC2 将终止已停止的实例。
- 当竞价型实例停止时，您可以将其终止。
- 如果取消竞价型实例请求、EC2 机群或竞价型实例集，Amazon EC2 将终止任何停止的关联竞价型实例。
- 在中断的竞价型实例停止后，您只需为保留的 EBS 卷付费。对于 EC2 实例集和 Spot 实例集，如果具有很多停止的实例，则可能会超出您的账户的 EBS 卷数限制。有关竞价型实例中断时如何收费的更多信息，请参阅 中断的竞价型实例的计费 (p. 493)。
- 确保您熟知停止实例的影响。有关实例停止可能会发生情况的更多信息，请参阅 重启、停止、休眠和终止之间的区别 (p. 573)。

先决条件

要停止已中断的竞价型实例，必须满足以下先决条件：

竞价型请求类型

竞价型实例请求类型 – 必须为 persistent。您不能在竞价型实例请求中指定启动组。

EC2 机群或竞价型实例集请求类型 – 必须为 maintain。

根卷类型

必须是 EBS 卷，而不是实例存储卷。

休眠中断的竞价型实例

您可以指定 Amazon EC2 在竞价型实例中断时将其休眠。有关更多信息，请参阅指定中断行为 (p. 485)。

当 Amazon EC2 休眠竞价型实例时，会出现以下情况：

- 在实例从 Amazon EC2 收到信号时，该代理将提示操作系统休眠。如果未安装该代理，或底层操作系统不支持休眠，或者没有足够的卷空间以保存实例内存，休眠将失败并且 Amazon EC2 停止该实例。
- 实例内存 (RAM) 保留在根卷上。
- 将会保留实例的 EBS 卷和私有 IP 地址。
- 不会保留实例存储卷和公有 IP 地址（非弹性 IP 地址）。

有关将按需实例休眠的信息，请参阅休眠 Linux 按需型实例 (p. 616)。

注意事项

- 只有 Amazon EC2 才能让竞价型实例休眠。您无法手动让竞价型实例休眠。
- 只有 Amazon EC2 才能恢复休眠的竞价型实例。您无法手动恢复休眠的竞价型实例。
- 当有容量可用时，Amazon EC2 会恢复实例。
- 当 Amazon EC2 休眠竞价型实例时，休眠立即开始。您将收到一条中断通知，但不会在竞价型实例中断之前留出两分钟的时间。

- 在实例进行休眠过程中，实例运行状况检查可能会失败。
- 在休眠过程完成时，实例状态为 `stopped`。
- 在实例休眠时，仅向您收取 EBS 卷费用。对于 EC2 实例集和 Spot 实例集，如果具有很多休眠的实例，则可能会超出您的账户的 EBS 卷数限制。
- 确保您熟知休眠实例的影响。有关实例休眠可能会发生情况的更多信息，请参阅 重启、停止、休眠和终止之间的区别 (p. 573)。

先决条件

要使竞价型实例休眠，必须满足以下先决条件：

竞价型请求类型

竞价型实例请求类型 – 必须为 `persistent`。您不能在竞价型实例请求中指定启动组。

EC2 机群或竞价型实例集请求类型 – 必须为 `maintain`。

支持的 Linux AMI

以下支持 AMI 包含休眠代理。要使用以下 AMI 的早期版本，您必须安装休眠代理 (p. 488)。

- Amazon Linux 2 2019.08.29 或更高版本
- Amazon Linux AMI 2017.09.1 或更高版本
- Ubuntu Xenial 16.04 20171121 或更高版本 [1]

[1] 要使用早期版本的 Ubuntu Xenial AMI，它必须具有由 Amazon 调优的高于 4.4.0-1041 的 Ubuntu 内核版本（`linux-aws`）。

有关支持的 Windows AMI 的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的先决条件。

启动休眠代理

我们建议您使用用户数据在实例启动时启动该代理。或者，您也可以手动启动该代理。有关更多信息，请参阅在启动时启动休眠代理 (p. 488)。

支持的实例系列

C3、C4、C5、M4、M5、R3、R4

实例 RAM 大小

必须小于 100GB。

根卷类型

必须是 EBS 卷，而不是实例存储卷。

EBS 根卷大小

必须足够大以在休眠期间存储实例内存 (RAM)。

EBS 根卷加密 – 推荐但不是竞价型实例休眠的先决条件

我们强烈建议您将加密的 EBS 卷作为根卷，因为在休眠期间实例内存存储在根卷上。这确保在卷上静态存储数据以及在实例和卷之间移动数据时，将加密内存 (RAM) 内容。

可以使用以下三个选项之一，以确保根卷是加密的 EBS 卷：

- EBS encryption by default（EBS 原定设置加密）- 您可以启用 EBS 原定设置加密，以确保对在您的 Amazon 账户中创建的所有新 EBS 卷进行加密。这样，您就可以为实例启用休眠，而无需在实例启动时指定加密意图。有关更多信息，请参阅默认加密 (p. 1507)。

- EBS "single-step" encryption（EBS“单步”加密）- 您可以从未加密的 AMI 中启动 EBS 支持的加密 EC2 实例，并且还可以同时启用休眠。有关更多信息，请参阅将加密与 EBS 支持的 AMI 结合使用 (p. 196)。
- Encrypted AMI（加密的 AMI）- 您可以使用加密的 AMI 启动实例以启用 EBS 加密。如果 AMI 没有加密的根快照，则可以将其复制到新的 AMI 并请求加密。有关更多信息，请参阅 在复制过程中将未加密映像加密 (p. 200) 和 复制 AMI (p. 174)。

在您的 Linux AMI 上安装休眠代理

您必须在您的 AMI 上安装休眠代理，除非您计划使用已包含该代理的 AMI。

以下说明介绍了如何在 Linux AMI 上安装休眠代理。有关在 Windows AMI 上安装休眠代理的说明，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的在您的 Windows AMI 上安装休眠代理。

要在 Amazon Linux AMI 上安装休眠代理

1. 确认您的内核支持休眠，并在必要时更新内核。

```
sudo yum update kernel
```

2. 如果您的 AMI 不包含该代理，请安装该代理。

```
sudo yum update; sudo yum install hibagent
```

要在 Ubuntu AMI 上安装休眠代理

如果您的 AMI 不包含该代理，请安装该代理。休眠代理仅在 Ubuntu 16.04 或更高版本上可用。

```
sudo apt-get install hibagent
```

在启动时启动休眠代理

休眠代理必须在实例启动时运行，无论该代理是包含在您的 AMI 中，还是您自行安装的。

以下说明介绍了如何在 Linux 实例上启动休眠代理。有关在 Windows AMI 上启动休眠代理的说明，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的在启动时启动休眠代理。

在竞价型实例上启动休眠代理

按照以下步骤使用您的首选启动方法 (p. 574)请求一个竞价型实例，然后将以下内容添加到用户数据中。

```
#!/bin/bash
/usr/bin/enable-ec2-spot-hibernation
```

终止中断的竞价型实例

当 Amazon EC2 中断竞价型实例时，默认情况下会终止该实例，除非您指定了其他中断行为，例如停止或休眠。有关更多信息，请参阅指定中断行为 (p. 485)。

准备中断

对竞价型实例的需求可能因时间不同而有显著的差异，竞价型实例 的可用性也会因为有多少未使用 EC2 实例可用而差别巨大。竞价型实例可能会中断。因此，必须确保应用程序针对竞价型实例中断做好准备。

我们建议您遵循以下最佳实践，以便您为竞价型实例中断做好准备。

- 使用 Auto Scaling 组创建竞价型请求。如果您的竞价型实例被中断，Auto Scaling 组将自动启动替换实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的具有多个实例类型和购买选项的自动扩缩组。
- 使用包含所需软件配置的 Amazon Machine Image (AMI)，确保您的实例在请求完成时随时可以启动。您还可以使用用户数据在启动时运行命令。
- 停止或终止实例后，实例存储卷上的数据将丢失。将实例存储卷上的所有重要数据备份到持久性存储，例如 Amazon S3、Amazon EBS 或 Amazon DynamoDB。
- 在不会受竞价型实例终止影响的位置例行存储重要数据。例如，您可以使用 Amazon S3、Amazon EBS 或 DynamoDB。
- 将工作拆分为小的任务 (使用网格、Hadoop 或基于队列的架构) 或者使用检查点，以便您经常保存工作。
- 当实例处于较高的中断风险时，Amazon EC2 会向竞价型实例发出再平衡建议信号。您可以依靠再平衡建议来主动管理竞价型实例中断，而无需等待两分钟的竞价型实例中断通知。有关更多信息，请参阅EC2 实例再平衡建议 (p. 480)。
- 使用两分钟的竞价型实例中断通知监控您的竞价型实例的状态。有关更多信息，请参阅竞价型实例中断通知 (p. 490)。
- 虽然我们尽一切努力尽快提供这些警告，但您的竞价型实例可能会在我们提供此警告之前被中断。测试您的应用程序，确保它很好地处理了意外的实例终止，即使您正在监控再平衡建议信号和中断通知。您可以使用按需型实例来运行应用程序，然后自行终止该按需型实例，以便确认这一点。
- 使用 Amazon Fault Injection Simulator 运行受控的故障注入实验，以测试在竞价型实例中断时应用程序如何响应。有关更多信息，请参阅 Amazon Fault Injection Simulator 用户指南中的教程，使用 Amazon FIS 测试竞价型实例中断。

启动竞价型实例中断

您可以在 Amazon EC2 控制台中选择一个竞价型实例并启动中断，从而测试竞价型实例上的应用程序将如何处理中断。当您启动竞价型实例中断时，Amazon EC2 会向您发送通知，提示您的竞价型实例将在两分钟后中断，然后 Amazon EC2 将在两分钟后中断该竞价型实例。

执行竞价型实例中断的底层服务是 Amazon Fault Injection Simulator（Amazon FIS）。有关 Amazon FIS 的信息，请参阅 Amazon Fault Injection Simulator。

> **Note**
>
> 中断行为包括 `terminate`、`stop` 和 `hibernate`。如果您将中断行为设置为 `hibernate`，则当您启动竞价型实例中断时，将会立即开始休眠过程。

除亚太地区（雅加达）、亚太地区（大阪）、中国（北京）、中国（宁夏）和中东地区（阿联酋）外，所有 Amazon Web Services 区域均支持启动竞价型实例中断。

主题

- 启动竞价型实例中断 (p. 489)
- 验证竞价型实例中断 (p. 490)

启动竞价型实例中断

您可以使用 EC2 控制台快速启动竞价型实例中断。要进行更高级的实验来测试竞价型实例中断情况，您可以使用 Amazon FIS 控制台创建自己的实验。

使用 EC2 控制台启动竞价型实例中断

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests（竞价型实例请求）。
3. 选择一个竞价型实例请求，然后依次选择 Actions（操作）、Initiate interruption（启动中断）。

Note

目前不支持选择竞价型实例集请求来一次启动中断实例集中的所有竞价型实例；您必须单独选择实例集中的每个竞价型实例请求。此外，您同样不能选择多个竞价型实例请求来启动一个中断；一次只能为一个竞价型实例启动一个中断。

4. 在 Initiate Spot Instance interruption（启动竞价型实例中断）对话框的 Service access（服务访问权限）下，您可以使用默认角色，也可以选择一个现有的角色。要选择角色，请选择 Use an existing service role（使用现有的服务角色），然后对于 Service role name（服务角色名称），选择要使用的角色。
5. 准备好启动竞价型实例中断后，选择 Initiate interruption（启动中断）。

使用 Amazon FIS 控制台创建更高级的实验来测试竞价型实例中断

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests（竞价型实例请求）。
3. 依次选择 Actions（操作）、Create advanced experiments（创建高级实验）。

   Amazon FIS 控制台将打开。有关更多信息，请参阅《Amazon Fault Injection Simulator 用户指南》中的 教程，使用 Amazon FIS 测试竞价型实例中断。

验证竞价型实例中断

启动中断后，将会发生以下情况：

- 竞价型实例收到一个 实例再平衡建议 (p. 480)。
- 在 Amazon EC2 中断实例之前两分钟发出 竞价型实例中断通知 (p. 490)。
- 两分钟后，竞价型实例将会中断。
- 已被 Amazon FIS 停止的竞价型实例将在您将其重新启动之前一直处于停止状态。

验证实例在您启动中断后是否已中断

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航窗格中，在单独的浏览器选项卡或窗口中打开 Spot Requests（竞价型实例请求）和 Instances（实例）。
3. 对于 Spot Requests（竞价型实例请求），选择该竞价型实例请求。初始状态为 `fulfilled`。实例中断后，状态会根据中断行为出现以下变化：
   - `terminate` – 状态变为 `instance-terminated-by-experiment`。
   - `stop` – 实例的状态首先变为 `marked-for-stop-by-experiment`，然后变为 `instance-stopped-by-experiment`。
4. 对于 Instances（实例），选择该竞价型实例。初始状态为 `Running`。在收到竞价型实例中断通知后两分钟，状态会根据中断行为出现以下变化：
   - `stop` – 实例的状态首先变为 `Stopping`，然后变为 `Stopped`。
   - `terminate` – 实例的状态首先变为 `Shutting-down`，然后变为 `Terminated`。

竞价型实例中断通知

竞价型实例中断通知是在 Amazon EC2 停止或终止竞价型实例之前的两分钟发出的警告。如果您将休眠指定为中断行为，则会收到中断通知，但由于休眠过程立即开始，因此您不会提前两分钟收到警告。

正常处理竞价型实例中断的最佳方法是，设计应用程序以提供容错能力。为此，您可以利用竞价型实例中断通知。我们建议您每 5 秒检查一次这些中断通知。

中断通知是作为 CloudWatch 事件以及 Spot 实例上的实例元数据 (p. 754)中的项目提供的。将尽最大努力发出中断通知。

EC2 Spot Instance interruption notice

当 Amazon EC2 将要中断竞价型实例时，它在实际中断之前的两分钟发出一个事件（休眠除外，此时会收到中断通知，但不会提前两分钟，因为休眠是立即开始的）。Amazon CloudWatch Events 可以检测该事件。有关 CloudWatch Events 的更多信息，请参阅 Amazon CloudWatch Events 用户指南。有关指导您如何创建和使用事件规则的详细示例，请参阅利用 Amazon EC2 Spot 实例中断通知。

以下是竞价型实例中断事件的示例。`instance-action` 的可能值为 `hibernate`、`stop` 或 `terminate`。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

instance-action

如果竞价型实例标记为由 Amazon EC2 停止或终止，将在您的实例元数据 (p. 754)中包含 `instance-action` 项。如果没有，则不显示。您可以按如下方式检索 `instance-action`。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/spot/instance-action
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/spot/instance-action
```

`instance-action` 项目指定操作及其大致执行时间 (采用 UTC 格式)。

以下示例输出指示将停止此实例的时间。

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

以下示例输出指示将终止此实例的时间。

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

如果 Amazon EC2 没有准备停止或终止该实例，或者如果您自己终止了该实例，则实例元数据中不存在 `instance-action`，并且在尝试检索它时出现 HTTP 404 错误。

termination-time

为向后兼容而保留此项目；您应改为使用 `instance-action`。

如果竞价型实例标记为由 Amazon EC2 终止，则您的实例元数据中将显示 `termination-time` 项目。如果没有，则不显示。您可以按如下方式检索 `termination-time`。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo terminated; fi
```

IMDSv1

```
[ec2-user ~]$ if curl -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo terminated; fi
```

`termination-time` 项目指定实例将收到关闭信号的大致时间（用 UTC 表示）。下面是示例输出。

```
2015-01-05T18:02:00Z
```

如果 Amazon EC2 未准备终止实例，或者如果您自己终止了竞价型实例，则 `termination-time` 项目或者不存在于实例元数据中（这样您会收到 HTTP 404 错误），或者包含并非时间值的值。

如果 Amazon EC2 无法终止实例，请求状态将设置为 `fulfilled`。`termination-time` 值会将实例元数据保持原始大致时间（现已成为过去时间）。

查找中断的竞价型实例

在控制台中，实例窗格显示所有实例，包括 Spot 实例。您可以从 Instance lifecycle (实例生命周期) 列中的 `spot` 值识别 Spot 实例。实例状态列指示实例处于 `pending`、`running`、`stopping`、`stopped`、`shutting-down` 还是 `terminated` 状态。对于休眠的竞价型实例，实例状态为 `stopped`。

查找中断的竞价型实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。在右上角，选择设置图标 ()，然后在属性列下选择实例生命周期。对于 Spot 实例，实例生命周期为 `spot`。

   或者，在导航窗格中，选择 Spot Requests (Spot 请求)。您可以同时查看竞价型实例请求和竞价型实例集请求。要查看实例的 ID，请选择 Spot 实例请求或 Spot 实例集请求，然后选择 Instances (实例) 选项卡。选择实例 ID 以在实例窗格中显示实例。
3. 对于每个 Spot 实例，您可以在 Instance State (实例状态) 列中查看其状态。

查找中断的竞价型实例（Amazon CLI）

您可以使用带 `--filters` 参数的 describe-instances 命令列出中断的 Spot 实例。要仅在输出中列出实例 ID，请包括 `--query` 参数。

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-name,Values=terminated,stopped \
```

```
    --query "Reservations[*].Instances[*].InstanceId"
```

确定 Amazon EC2 是否终止了竞价型实例

如果竞价型实例终止，您可以使用 CloudTrail 查看 Amazon EC2 是否终止了竞价型实例。在 Amazon CloudTrail 中，事件名称 `BidEvictedEvent` 表示 Amazon EC2 终止了竞价型实例。

查看 CloudTrail 中的 BidEvictedEvent 事件

1. 访问 https://console.aws.amazon.com/cloudtrail/，打开 CloudTrail 控制台。
2. 在导航窗格中，选择事件历史记录。
3. 在筛选器下拉列表中，选择 Event name (事件名称)，然后在右侧的过滤器字段中输入 BidEvictedEvent。
4. 选择结果列表中的 BidEvictedEvent，以查看其详细信息。在 Event record (事件记录) 下，您可以找到实例 ID。

有关使用 CloudTrail 的更多信息，请参阅使用 Amazon CloudTrail 记录 Amazon EC2 和 Amazon EBS API 调用 (p. 1037)。

中断的竞价型实例的计费

当竞价型实例被中断时，将向您收取实例和 EBS 卷使用的费用，如下所示。

实例使用情况

谁中断了竞价型实例	操作系统	在第一个小时内中断	在第一个小时后的任一小时内中断
如果您停止或终止 Spot 实例	Windows 和 Linux（不包括 RHEL 和 SUSE）	按使用的秒数收费	按使用的秒数收费
	RHEL 和 SUSE	按完整小时收费（即使您的使用时间是部分小时也是如此）	按使用的完整小时数收费，对于中断的部分完整小时，按完整小时收费
如果 Amazon EC2 中断竞价型实例	Windows 和 Linux（不包括 RHEL 和 SUSE）	免费	按使用的秒数收费
	RHEL 和 SUSE	免费	按使用的完整小时数收费，对于中断的部分小时，不收费

EBS 卷使用情况

在中断的竞价型实例停止后，您只需为保留的 EBS 卷付费。

对于 EC2 实例集和 Spot 实例集，如果具有很多停止的实例，则可能会超出您的账户的 EBS 卷数限制。

竞价放置分数

竞价放置分数功能可以根据您的竞价容量需求推荐一个Amazon区域或可用区。竞价型容量会发生波动，所以您无法确保始终获得所需的容量。竞价放置分数表示竞价请求在某个区域或可用区中获得成功的可能性。

Note

在中国（北京）或中国（宁夏）区域使用竞价放置分数功能时，Amazon EC2 只会返回该区域的分数，或者该区域中发出调用的每个可用区的分数。

Note

竞价放置分数不能提供在可用容量或中断风险方面的任何保证。竞价放置分数仅可作为建议使用。

优点

您可以使用竞价放置分数功能完成以下操作：

- 根据需要将竞价型计算容量重新定位和扩展到不同区域，以应对当前区域内的容量需求增加或可用容量减少。
- 确定在其中运行单个可用区工作负载的最佳可用区。
- 模拟未来的竞价型容量需求，以便您可以选择一个最佳区域来扩展基于竞价的工作负载。
- 确定实例类型的最佳组合以满足竞价容量需求。

主题

- 成本 (p. 494)
- 竞价放置分数的工作原理 (p. 494)
- 限制 (p. 496)
- 所需的 IAM 权限 (p. 496)
- 计算竞价放置分数 (p. 497)
- 示例配置 (p. 501)

成本

使用竞价放置分数功能不会收取任何额外费用。

竞价放置分数的工作原理

在使用竞价放置分数功能时，您先指定竞价型实例的计算要求，然后 Amazon EC2 会返回竞价请求可能成功的区域的分数或可用区。每个区域或可用区的评分范围为 1 到 10，其中 10 表示竞价请求的成功性较高，1 则表示竞价请求的成功性较低。

请按照以下步骤使用竞价放置分数功能：

- 步骤 1：指定竞价需求 (p. 494)
- 步骤 2：筛选竞价放置分数响应 (p. 495)
- 步骤 3：审查建议 (p. 495)
- 步骤 4：采纳建议 (p. 495)

步骤 1：指定竞价需求

首先，请指定所需的目标竞价容量和计算要求，如下所示：

1. 指定目标竞价容量，也可以选择目标容量单位。

您可以根据实例数或 vCPU 数，或者根据以 MiB 为单位的内存量来指定所需的目标竞价容量。若根据 vCPU 数或内存量来指定目标容量，则必须将目标容量单位指定为 `vcpu` 或 `memory-mib`。否则即默认为实例数。

若根据 vCPU 数或内存量指定目标容量，则您可以在计算总容量时使用这些单位。例如，若要混合使用不同大小的实例，则可以将目标容量指定为 vCPU 的总数。然后竞价放置分数功能会根据 vCPU 数来考虑请求中的每种实例类型，并计算 vCPU 总数，而不是在合计目标容量时计算实例总数。

例如，假设您指定的总目标容量为 30 个 vCPU，并且您的实例类型列表中包括 c5.xlarge（4 个 vCPU）、m5.2xlarge（8 个 vCPU）和 r5.large（2 个 vCPU）。若要实现总计 30 个 vCPU，则您可以获得 2 个 c5.xlarge（2*4 vCPU）、2 个 m5.2xlarge（2*8 个 vCPU）和 3 个 r5.large（3*2 个 vCPU）的组成。

2. 指定实例类型或实例属性。

   您可以指定所用的实例类型，也可以指定计算要求所需的实例属性，然后由 Amazon EC2 来确定具有这些属性的实例类型。这称为基于属性的实例类型选择。

   您无法在同一竞价放置分数请求中同时指定实例类型和实例属性。

   如果您指定实例类型，则必须至少指定三种不同的实例类型，否则 Amazon EC2 将返回较低的竞价放置分数。同样，如果您指定实例属性，则其必须解析为至少三种不同的实例类型。

有关指定竞价需求的不同方法的示例，请参阅 示例配置 (p. 501)。

步骤 2：筛选竞价放置分数响应

Amazon EC2 会计算区域或区域内每个可用区的竞价放置分数，并返回您的竞价请求可能成功的区域或可用区的分数。默认为返回区域的分数。如果您计划在单个可用区中启动所有竞价容量，那么请求一个已评分的可用区列表会非常有帮助。

步骤 3：审查建议

每个区域或可用区的竞价放置分数是根据目标容量、实例类型的组成、历史和当前竞价使用趋势以及请求的时间来计算的。由于竞价容量不断波动，因此在不同时间计算同一竞价放置分数请求时，可能会产生不同的分数。

区域和可用区的评分范围为 1 至 10。分数为 10 表示您的竞价请求具有较高的成功性（但不能保证）。分数为 1 则表示您的竞价请求几乎没有成功的可能。即使是不同的区域或可用区，也可能会返回相同的分数。

如果返回的分数较低，则您可以编辑计算要求并重新计算分数。您还可以在一天中的不同时间为同一个计算要求请求竞价放置分数建议。

步骤 4：采纳建议

只有在竞价请求具有与竞价放置分数配置（目标容量、目标容量单位和实例类型或实例属性）完全相同的配置时，竞价放置分数才是相关的，并且被配置为使用 `capacity-optimized` 分配策略。否则，获得可用竞价型容量的可能性将与分数不一致。

尽管竞价放置分数可作为指导，但无法保证完全或部分满足您的竞价请求，所以您可以使用以下信息来获得最佳结果：

- 使用相同的配置 – 仅当 Auto Scaling 组、EC2 机群或竞价型实例集中的竞价请求配置（目标容量、目标容量单位、实例类型或实例属性）与您为了获取竞价放置分数而输入的配置相同时，竞价放置分数才是相关的。

  如果您在竞价放置分数请求中使用了基于属性的实例类型选择，就可以使用基于属性的实例类型选择来配置 Auto Scaling 组、EC2 机群或竞价型实例集。有关更多信息，请参阅创建具有关于所用实例类型的一组要求的 Auto Scaling 组、EC2 机群的基于属性的实例类型选择 (p. 836) 和 竞价型实例集的基于属性的实例类型选择 (p. 874)。

Note

如果您根据 vCPU 数或内存量指定了目标容量，并且在竞价放置分数配置中指定了实例类型，那么请注意，您当前无法在 Auto Scaling 组、EC2 机群或竞价型实例集中创建此配置。相反，您必须使用 `WeightedCapacity` 参数来手动设置实例权重。

- 使用 **`capacity-optimized`** 分配策略 – 任何分数都假定您的实例集请求将被配置为使用所有可用区（用于跨区域请求容量）或单个可用区（若在一个可用区中请求容量）和用于成功请求竞价容量的 `capacity-optimized` 竞价型分配策略。如果您使用其它分配策略，例如 `lowest-price`，则获得竞价容量的可能性会与分数不一致。
- 立即根据分数采取行动 – 竞价放置分数建议反映了请求时的可用竞价容量，由于竞价容量会发生波动，所以在不同时间计算相同的配置可能会得到不同的分数。尽管 10 分意味着竞价型容量请求具有较高的成功性，但不能保证成功，所以为了获得最佳效果，我们建议您立即根据分数采取行动。我们还建议您在每次尝试请求容量时都获取新的分数。

限制

- 目标容量限制 – 您的竞价放置分数目标容量限制取决于您最近的竞价用量，并同时考虑潜在的使用量增长。如果您最近没有产生竞价用量，那么我们会为您提供一个较低的默认限制，这个默认限制与您的竞价请求限制一致。
- 请求配置限制 – 如果我们检测到与竞价放置分数功能的预期用途无关的模式，则我们可以限制 24 小时内的新请求配置的数量。如果达到限制，则可以重试曾使用过的请求配置，但在下一个 24 小时期间之前，您无法指定新的请求配置。
- 实例类型的最小数量 – 如果您指定实例类型，则必须指定至少三种不同的实例类型，否则 Amazon EC2 将返回较低的竞价放置分数。同样，如果您指定实例属性，则其必须解析为至少三种不同的实例类型。如果实例类型的名称不同，则被视为不同的实例类型。例如，m5.8xlarge、m5a.8xlarge 和 m5.12xlarge 都会被视作不同的实例类型。

所需的 IAM 权限

默认情况下，IAM 身份（用户、角色或组）不具备使用竞价放置分数功能的权限。如需允许 IAM 身份使用竞价放置分数功能，则您必须创建一个 IAM policy，以授予其使用 `ec2:GetSpotPlacementScores` EC2 API 操作的权限。然后，将策略附加到需要此权限的 IAM 身份。

以下为授予使用 `ec2:GetSpotPlacementScores` EC2 API 操作权限的 IAM policy 的示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

有关编辑 IAM policy 的信息，请参阅 IAM 用户指南中的编辑 IAM policy。

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：

- 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
- （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

计算竞价放置分数

您可以使用 Amazon EC2 控制台或 Amazon CLI 来计算竞价放置分数。

主题

- 通过指定实例属性来计算竞价放置分数（控制台）(p. 497)
- 通过指定实例类型来计算竞价放置分数（控制台）(p. 497)
- 计算竞价放置分数 (Amazon CLI) (p. 498)

通过指定实例属性来计算竞价放置分数（控制台）

如需通过指定实例属性来计算竞价放置分数

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 从顶部导航栏中，选择要在其中评估竞价放置分数的区域。
3. 选择 Spot placement score（竞价放置分数）。
4. 选择 Enter requirements（输入要求）。
5. 对于 Target capacity（目标容量），请根据 instances（实例）或 vCPUs (vCPU) 的数量或者根据 memory (MiB)（内存 (MiB)）的数量来输入所需的容量。
6. 对于 Instance type requirements（实例类型要求），如需指定您的计算要求并使 Amazon EC2 识别符合这些要求的最佳实例类型，请选择 Specify instance attributes that match your compute requirements（指定符合计算要求的实例属性）。
7. 对于 vCPU，输入所需的最小和最大 vCPU 数。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。
8. 对于 Memory (GiB)（内存 (GiB)），输入所需的最小和最大内存量。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。
9. 对于 CPU architecture（CPU 架构），选择所需的实例架构。
10. （可选）对于 Additional instance attributes（其它实例属性），您可以选择指定一个或多个属性以更详细地表达计算要求。每个额外属性都会进一步增加对您的请求的限制。您可以省略其它属性；如果省略，则使用默认值。有关每个属性及其默认值的描述，请参阅 Amazon EC2 命令行参考中的 get-spot-placement-scores。
11. （可选）要查看具有指定属性的实例类型，请展开 Preview matching instance types（预览匹配的实例类型）。要排除在安置性评量中使用的实例类型，请选择实例，然后选择 Exclude selected instance types（排除选定的实例类型）。
12. 选择 Load placement scores（加载放置分数），并审查结果。
13. （可选）要在显示的区域中显示可用区的竞价放置分数，请选择 Provide placement scores per Availability Zone（提供每个可用区的放置分数）复选框。如果您希望在单个可用区中启动所有竞价容量，那么一个已评分的可用区列表会非常有帮助。
14. （可选）如需编辑计算要求并获得新的放置分数，请选择 Edit（编辑）以进行必要的调整，然后选择 Calculate placement scores（计算放置分数）。

通过指定实例类型来计算竞价放置分数（控制台）

如需通过指定实例类型来计算竞价放置分数

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 从顶部导航栏中，选择要在其中评估竞价放置分数的区域。

3. 选择 Spot placement score（竞价放置分数）。
4. 选择 Enter requirements（输入要求）。
5. 对于 Target capacity（目标容量），请根据 instances（实例）或 vCPUs (vCPU) 的数量或者根据 memory (MiB)（内存 (MiB)）的数量来输入所需的容量。
6. 对于 Instance type requirements（实例类型要求），如需指定要使用的实例类型，请选择 Manually select instance types（手动选择实例类型）。
7. 选择 Select instance types（选择实例类型），选择要使用的实例类型，然后选择 Select（选择）。如需快速查找实例类型，您可以使用筛选条件来按不同属性筛选实例类型。
8. 选择 Load placement scores（加载放置分数），并审查结果。
9. （可选）要在显示的区域中显示可用区的竞价放置分数，请选择 Provide placement scores per Availability Zone（提供每个可用区的放置分数）复选框。如果您希望在单个可用区中启动所有竞价容量，那么一个已评分的可用区列表会非常有帮助。
10. （可选）如需编辑实例类型列表并获得新的放置分数，请选择 Edit（编辑）以进行必要的调整，然后选择 Calculate placement scores（计算放置分数）。

计算竞价放置分数 (Amazon CLI)

如需计算竞价放置分数

1. （可选）如需生成所有可以指定为竞价放置分数配置参数，请使用 get-spot-placement-scores 命令和 `--generate-cli-skeleton` 参数。

```
aws ec2 get-spot-placement-scores \
    --region cn-north-1 \
    --generate-cli-skeleton
```

预期输出

```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
```

```
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 使用上一步的输出创建 JSON 配置文件，然后按如下方式进行配置：

   a. 对于 `TargetCapacity`（目标容量），请根据 instances（实例）或 vCPUs (vCPU) 的数量或者根据 memory (MiB)（内存 (MiB)）的数量来输入所需的容量。

   b. 对于 `TargetCapacityUnitType`，请输入目标容量的单位。如果省略此参数，则默认为 `units`。

      有效值：`units`（转换为实例数）| `vcpu` | `memory-mib`

c. 对于 SingleAvailabilityZone（单个可用区），请指定 true 以获得返回已评分的可用区列表的响应。如果您希望在单个可用区中启动所有竞价容量，那么一个已评分的可用区列表会非常有帮助。如果省略此参数，则默认为 false，然后响应会返回已评分的区域。

d. （可选）对于 RegionNames，请指定要用作筛选条件的区域。此处必须指定区域代码，例如 cn-north-1。

使用区域筛选条件后，响应将仅返回您指定的区域。若将 SingleAvailabilityZone 指定为 true，则响应仅返回指定区域中的可用区。

e. 配置中可以包括 InstanceTypes（实例类型）或 InstanceRequirements（实例要求），但两者不可同时包含于同一配置中。

在 JSON 配置中指定以下之一：

- 如需指定实例类型列表，请指定 InstanceTypes 参数中的实例类型。指定至少三种不同的实例类型。若只指定了一种或两种实例类型，则竞价放置分数将返回一个较低的分数。有关实例类型的列表，请参阅 Amazon EC2 实例类型。
- 如需指定实例属性以便 Amazon EC2 识别与这些属性匹配的实例类型，请指定位于 InstanceRequirements（实例要求）结构中的属性。

  必须提供 VCpuCount、MemoryMiB 和 CpuManufacturers 的值。您可以省略其它属性；如果省略，则使用默认值。有关每个属性及其默认值的描述，请参阅 Amazon EC2 命令行参考中的 get-spot-placement-scores。

有关示例配置，请参阅 示例配置 (p. 501)。

3. 若要获取您在 JSON 文件中指定的要求的竞价放置分数，请使用 get-spot-placement-scores 命令，然后使用 --cli-input-json 参数为 JSON 文件指定名称和路径。

```
aws ec2 get-spot-placement-scores \
    --region cn-north-1 \
    --cli-input-json file://file_name.json
```

如果 SingleAvailabilityZone 被设置为 false 或省略（省略即默认为 false）时的输出示例 – 返回已评分的区域

```
{
    "SpotPlacementScores": [
        {
            "Region": "cn-north-1",
            "Score": 9
        }
    ]
}
```

如果 SingleAvailabilityZone 被设置为 true 时的输出示例 – 返回可用区的评分列表

```
{
    "SpotPlacementScores": [
        {
            "Region": "cn-north-1",
            "AvailabilityZoneId": "cnn1-az2",
            "Score": 9
        },
        {
            "Region": "cn-north-1",
            "AvailabilityZoneId": "cnn1-az4",
            "Score": 9
        },
```

```
        {
            "Region": "cn-north-1",
            "AvailabilityZoneId": "cnn1-az1",
            "Score": 9
        }
    ]
}
```

示例配置

使用 Amazon CLI，您可以使用以下示例配置。

示例配置

- 示例：指定实例类型和目标容量 (p. 501)
- 示例：根据内存指定实例类型和目标容量 (p. 501)
- 示例：为基于属性的实例类型选择指定属性 (p. 501)
- 示例：为基于属性的实例类型选择指定属性并返回可用区的评分列表 (p. 502)

示例：指定实例类型和目标容量

以下示例配置指定了三种不同的实例类型和 500 个竞价型实例的目标竞价容量。

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

示例：根据内存指定实例类型和目标容量

以下示例配置指定了三种不同的实例类型和 500000MiB 内存的目标竞价容量，其中要启动的竞价型实例数必须能够提供总计 500000MiB 的内存。

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

示例：为基于属性的实例类型选择指定属性

以下示例配置是针对基于属性的实例类型选择而进行的配置，以及该示例配置的文本说明。

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
```

```
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

InstanceRequirementsWithMetadata

要使用基于属性的实例类型选择，您必须在配置中包括 InstanceRequirementsWithMetadata 结构，并为竞价型实例指定所需的属性。

在上述示例中，指定了以下必要实例属性：

- ArchitectureTypes – 实例类型的架构类型必须为 arm64。
- VirtualizationTypes – 实例类型的虚拟化类型必须为 hvm。
- VCpuCount – 实例类型的 vCPU 数量必须最少为 1 个，最多为 12 个。
- MemoryMiB – 实例类型的最小内存必须为 512MiB。若省略 Max 参数，则表示没有最大限制。

请注意，您可以指定其它几个可选属性。有关属性列表，请参阅 Amazon EC2 命令行参考中的 get-spot-placement-scores。

TargetCapacityUnitType

TargetCapacityUnitType 参数为目标容量指定单位。在该示例中，目标容量是 5000，目标容量单位类型是 vcpu，它们共同指定了所需的 5000 个 vCPU 目标容量，其中要启动的竞价型实例数必须能够提供总计 5000 个 vCPU。

示例：为基于属性的实例类型选择指定属性并返回可用区的评分列表

以下示例配置是针对基于属性的实例类型选择而进行的配置。若指定 "SingleAvailabilityZone": true，则响应将返回已评分的可用区列表。

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

竞价型实例限制

每个区域的每个Amazon账户运行的和请求的 Spot 实例数具有一定的限制。Spot 实例限制根据您为完成未处理的 Spot 实例请求而正在使用或将使用的运行中 Spot 实例所用的虚拟中央处理器 (vCPU) 数量进行管理。

如果您终止竞价型实例但不取消竞价型实例请求，则请求将计入您的竞价型实例 vCPU 限制，直到 Amazon EC2 检测到竞价型实例终止并关闭请求。

有七种竞价型实例限制：

- 所有标准（A、C、D、H、I、M、R、T、Z）竞价型实例请求
- 所有 DL 竞价型实例请求
- 所有 F 竞价型实例请求
- 所有 G 和 VT 竞价型实例请求
- 所有 Inf 竞价型实例请求
- 所有 P 竞价型实例请求
- 所有 X 竞价型实例请求

每种限制指定了一个或多个实例系列的 vCPU 限制。有关不同实例系列、实例代和大小的信息，请参阅 Amazon EC2 实例类型。

对于 vCPU 限制，您可以按照满足您不断变化的应用程序需求的任意实例类型组合所要启动的 vCPU 数来使用限制。例如，假设您的所有标准 Spot 实例请求限制是 256 个 vCPU，您可以请求 32 个 `m5.2xlarge` Spot 实例 (32 x 8 vCPU) 或 16 个 `c5.4xlarge` Spot 实例 (16 x 16 vCPU)，或者总共有 256 个 vCPU 的任意标准 Spot 实例类型和大小的组合。

主题

- 监控竞价型实例限制和使用情况 (p. 503)
- 请求提高竞价型实例限制 (p. 503)

监控竞价型实例限制和使用情况

您可以使用以下方法查看和管理您的竞价型实例限制：

- Amazon EC2 控制台中的“限制”页面

有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）

使用 Amazon CloudWatch 指标集成，您可以根据限制监控 EC2 使用情况。您还可以配置警报以警告即将达到限制。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的可视化服务配额并设置告警。

请求提高竞价型实例限制

即使 Amazon EC2 会根据您的使用情况自动增加限制，您也可以在必要时请求提高竞价型实例限制。例如，如果您打算启动超过当前限制允许数量的竞价型实例，则可以请求提高限制。如果您提交 Spot 实例请求并收到错误 `Max spot instance count exceeded`，则也可以请求提高限制。

请求提高竞价型实例限制

1. 在位于 https://console.aws.amazon.com/support/home#/case/create 的 Support Center 控制台打开创建案例、提高服务限制表单。
2. 对于 Limit type (限制类型)，选择 EC2 Spot Instances (EC2 Spot 实例)。
3. 对于区域，选择所需的区域。
4. 对于 Primary instance type (主实例类型)，选择要请求提高其限制的 Spot 实例限制。
5. 对于新限制值，请输入要同时运行的 vCPU 总数。要确定所需的 vCPU 总数，请参阅 Amazon EC2 实例类型，以查找每种实例类型的 vCPU 数量。
6. （条件）您必须为每个竞价型实例限制创建单独的限制请求。要请求增加另一个 Spot 实例限制，请选择 Add another request (添加另一个请求)，然后重复此过程中的步骤 4 和 5。

7. 对于使用案例描述，请输入您的使用案例，然后选择提交。

有关查看限制和请求提高限制的更多信息，请参阅 Amazon EC2 Service Quotas (p. 1678)。

具爆发能力的实例

T 实例类型是可突增性能实例 (p. 274)。如果您使用可突增性能的实例类型启动竞价型实例，并计划立即短时间使用可突增性能的竞价型实例，且没有空闲时间来累积 CPU 积分，建议您以标准模式 (p. 288)启动实例，以避免支付更高的费用。如果您以无限模式 (p. 282)启动可突增性能的 Spot 实例并立即突增 CPU，您将会为突增花费超额积分。如果使用实例的时间很短，使得实例没有时间积累 CPU 积分来支付超额积分，则您将在终止实例时为超额积分付费。

仅当实例的运行时间较长，足以积累进行突增的 CPU 积分时，针对可突增性能的竞价型实例的无限模式才适用。否则，支付剩余积分会使可突增性能的竞价型实例比使用其他实例更加昂贵。有关更多信息，请参阅何时使用无限模式与固定 CPU (p. 283)。

以标准模式 (p. 288)配置的 T2 实例可获得启动积分 (p. 289)。T2 实例是唯一可获得启动积分的可突增性能实例。通过提供足够的计算资源来配置实例，启动积分旨在为 T2 实例提供有成效的初始启动体验。不允许重复启动 T2 实例以访问新的启动积分。如果您需要持续的 CPU，您可以赚取积分（通过空转一段时间），将无限模式 (p. 282)用于 T2 Spot 实例，或将实例类型和专用 CPU 一起使用。

Dedicated Hosts

Amazon EC2 专用主机是指 EC2 实例容量完全转供您专用的物理服务器。专用主机允许您使用按插槽、按内核或按虚拟机授权的现有软件许可证，包括 Windows Server、Microsoft SQL Server、SUSE 和 Linux Enterprise Server。

有关更多信息，请参阅专用主机。

目录

- 专用主机与专用实例的区别 (p. 504)
- 自带许可 (p. 505)
- 专用主机实例容量 (p. 505)
- 专属主机上的可突发 T3 实例 (p. 506)
- 专用主机 限制 (p. 507)
- 定价和计费 (p. 507)
- 使用 专用主机 (p. 508)
- 主机恢复 (p. 524)
- 主机维护 (p. 528)
- 跟踪配置更改 (p. 532)

专用主机与专用实例的区别

专用主机和专用实例均可用于在专供您使用的物理服务器上启动 Amazon EC2 实例。

专用实例与专属主机上的实例在性能、安全性或物理特性方面没有区别。但是，这两者之间也存在一些差异。下表重点介绍专用主机和专用实例之间的一些重要区别：

	Dedicated Host	Dedicated Instance
计费	按主机计费	按实例计费

	Dedicated Host	Dedicated Instance
套接字、内核和主机 ID 的可见性	提供套接字数和物理内核数的可见性	无可见性
主机和实例关联	允许您在一段时间内将您的实例一致地部署到同一物理服务器	不支持
定向实例置放	提供额外可见性以及对在物理服务器上放置实例的方式的控制	不支持
自动实例恢复	支持。有关更多信息，请参阅主机恢复 (p. 524)。	支持
自带许可 (BYOL)	支持	不支持
容量预留	不支持	支持

自带许可

专用主机允许使用现有的按插槽、按内核或按虚拟机软件的许可证。如果自带许可，您有责任管理自己的许可证。不过，Amazon EC2 具有一些帮助您保持许可证合规性的功能，例如实例关联和定向置放。

要将您自己的卷许可的计算机镜像引入到 Amazon EC2 中，需要执行以下常规步骤。

1. 验证控制您的系统映像使用的许可证条款是否允许在虚拟化云环境中使用系统映像。
2. 在确认可在 Amazon EC2 中使用系统映像后，使用 VM Import/Export 导入该映像。有关如何导入系统映像的信息，请参阅 VM Import/Export 用户指南。
3. 在导入系统映像后，可以在您的账户中的活动专用主机上从该映像中启动实例。
4. 在运行这些实例时，您可能需要针对自己的 KMS 服务器。

> **Note**
>
> 要跟踪您的映像在 Amazon 中的使用方式，请在 Amazon Config 中启用主机记录。您可以使用 Amazon Config 来记录专用主机的配置更改并将输出用作许可证报告的数据源。有关更多信息，请参阅跟踪配置更改 (p. 532)。

专用主机实例容量

以下实例系列支持同一专属主机上的多个实例大小：A1、C5、M5、R5、C5n、M5n、R5n 和 T3。其他实例系列仅支持同一 专用主机 上的单个实例大小。

例如，当您分配 R5 专用主机 时，它有 2 个套接字和 48 个物理内核，您可以在其上运行不同的实例大小（例如 `r5.2xlarge` 和 `r5.4xlarge`），最多可运行与主机关联的内核容量。但是，对于每个实例系列，每个实例大小可以运行的实例数量都有限制。例如，R5 专用主机 支持最多 2 个 `r5.8xlarge` 实例，其中使用 32 个物理内核。然后，可以使用其他大小的另外 R5 个实例将主机填充到内核容量。

> **Note**
>
> 对于支持多种实例尺寸的专属主机，我们建议您首先启动较大的实例大小，然后根据需要用较小的实例大小填充剩余的实例容量。

下表显示了您可以在 专用主机 上运行的不同实例大小组合的示例。

实例系列	实例大小组合示例	
R5	• 示例 1：4 x r5.4xlarge + 4 x r5.2xlarge • 示例 2：1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large	
C5	• 示例 1：1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge • 示例 2：4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large	
M5	• 示例 1：4 x m5.4xlarge + 4 x m5.2xlarge • 示例 2：1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large	

专属主机上的可突发 T3 实例

专属主机支持突增性能 T3 实例。T3 实例提供了在专用硬件上使用符合条件的 BYOL 许可证软件的经济高效的方式。T3 实例较小的 vCPU 占用空间使您能够在更少的主机上整合工作负载，并最大限度地提高每核心许可利用率。

T3 专属主机最适合运行具有低到中等 CPU 利用率的 BYOL 软件。这包括符合条件的按插槽、按内核或按虚拟机授权的软件许可证，例如 Windows Server、Windows 桌面、SQL Server、SUSE Enterprise Linux Server、红帽 Enterprise Linux Linux 和 Oracle 数据库。适用 T3 专属主机的工作负载示例包括中小型数据库、虚拟桌面、开发和测试环境、代码存储库以及产品原型。不建议使用 T3 专属主机用于持续高 CPU 利用率的工作负载或同时出现相关 CPU 突发的工作负载。

专属主机上的 T3 实例使用与共享租赁硬件上的 T3 实例相同的信用模型。但是，它们支持 `standard` 信用模式；不支持 `unlimited` 积分模式。在 `standard` 模式下，专属主机上的 T3 实例赚取、消耗和累积配额，其方式与共享租赁硬件上的突增实例相同。突增实例具有在基准 CPU 性能，并能够在需要时提升到基准水平之上。为了突增到基准以上，实例会花费在其 CPU 积分余额中累积的积分。当累积积分耗尽时，CPU 利用率将降低到基准水平。有关 `standard` 模式的更多信息，请参阅 标准可突增性能实例的工作原理 (p. 289)。

T3 专属主机支持 Amazon EC2 专属主机提供的所有功能，包括单个主机上的多个实例大小、主机 Resource Groups 和 BYOL。

支持的 T3 实例大小和配置

T3 专属主机通过提供基准 CPU 性能和在需要时突发到更高级别的能力来运行通用的可爆发 T3 实例，这些实例共享主机的 CPU 资源。这使得拥有 48 个核心的 T3 专属主机能够支持每台主机最多 192 个实例。为了有效利用主机的资源并提供最佳实例性能，Amazon EC2 实例放置算法会自动计算支持的可在主机上启动的实例数和实例大小组合。

T3 专属主机支持同一主机上的多个实例类型。专属主机上不是支持所有 T3 实例。您可以运行不同的 T3 实例组合，直到主机的 CPU 限制为止。

下表列出了支持的实例类型，总结了每种实例类型的性能，并指出了每种大小可以启动的最大实例数。

实例类型	vCPU	内存（GiB）	每个 vCPU 的基准 CPU 利用率	网络突增带宽 (Gbps)	Amazon EBS 突增带宽 (Mbps)	每个专属主机的最大实例数
t3.nano	2	0.5	5%	5	最多 2,085	192

实例类型	vCPU	内存（GiB）	每个 vCPU 的基准 CPU 利用率	网络突增带宽 (Gbps)	Amazon EBS 突增带宽 (Mbps)	每个专属主机的最大实例数
t3.micro	2	1	10%	5	最多 2,085	192
t3.small	2	2	20%	5	最多 2,085	192
t3.medium	2	4	20%	5	最多 2,085	192
t3.large	2	8	30%	5	2,780	96
t3.xlarge	4	16	40%	5	2,780	48
t3.2xlarge	8	32	40%	5	2,780	24

监控 T3 专属主机的 CPU 利用率

您可以使用 `DedicatedHostCPUUtilization` Amazon CloudWatch 指标，用于监控专属主机的 vCPU 利用率。EC2 命名空间和 `Per-Host-Metrics` 维度中可用指标。有关更多信息，请参阅专属主机指标 (p. 1006)。

专用主机 限制

在分配专用主机之前，请注意以下限制：

- 要在专用主机上运行 RHEL、SUSE Linux 和 SQL Server，您必须自带 AMI。由Amazon提供或 Amazon Web Services Marketplace 上提供的 RHEL、SUSE Linux 和 SQL Server AMI 不可用于专用主机。有关如何创建自己的 AMI 的更多信息，请参阅自带许可 (p. 505)。

  此限制不适用于分配给高内存实例（`u-6tb1.metal`、`u-9tb1.metal`、`u-12tb1.metal`、`u-18tb1.metal` 和 `u-24tb1.metal`）的主机。由 Amazon 提供或在 Amazon Web Services Marketplace 上可用的 RHEL 和 SUSE Linux AMI 可以用于这些主机。
- 每个区域每个 Amazon 账户的每个实例系列运行的专属主机数量具有一定的限制。要查看账户限额或请求增加限额，请使用服务限额控制台。
- 在专用主机上运行的实例只能在 VPC 中启动。
- 在使用指定主机资源组的启动模板时，支持 Auto Scaling 组。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的为 Auto Scaling 组创建启动模板。
- 不支持 Amazon RDS 实例。
- Amazon免费使用套餐不适用于专用主机。
- 实例置放控制是指管理专用主机中的实例启动。您无法在置放群组中启动专用主机。
- 如果为虚拟化实例类型分配主机，在主机分配完成后，您无法将该实例类型修改为 `.metal` 实例类型。例如，如果您为 `m5.large` 实例类型分配主机，则无法将实例类型修改为 `m5.metal`。

  如果为 `.metal` 实例类型分配主机，在主机分配完成后，您无法将该实例类型修改为虚拟化实例类型。例如，如果您为 `m5.metal` 实例类型分配主机，则无法将实例类型修改为 `m5.large`。

定价和计费

专用主机的价格因付款选项而异。有关更多信息，请参阅 Amazon EC2 专用主机定价。

付款选项

- 按需专用主机 (p. 508)

- Dedicated Host Reservations (p. 508)

按需专用主机

按需计费在您将专用主机分配到您的账户时自动激活。

专用主机的按需价格因实例系列和区域而异。您需要为处于活动状态的专用主机按每秒支付费用（至少 60 秒），无论您选择在专用主机上启动的实例的数量或大小如何。

您可以随时释放按需专用主机以停止产生费用。有关释放专用主机的信息，请参阅版本 专用主机 (p. 520)。

Dedicated Host Reservations

与运行按需 专用主机 相比，专用主机预留 可提供账单折扣。预留提供三种付款选项：

- 无预付费用 — 无预付费用预留为某个期限内的专用主机使用提供折扣，并且不需要预付款。可以选择一年或三年期限。只有一些实例系列支持三年期无预付预留。
- 预付部分费用 — 必须支付一部分预留费用，期限内的剩余时间享受折扣。可以选择一年或三年期限。
- 预付全费 — 提供最低的有效价格。提供一年和三年期限，覆盖整个前期费用，无需额外将来付费。

账户中必须有活动的专用主机才能购买预留。每个预留可以涵盖在单个可用区中支持同一实例系列的一个或多个主机。预留应用于主机上的实例系列，而不是实例大小。如果有三个不同实例大小的专用主机（`m4.xlarge`、`m4.medium` 和 `m4.large`），则可以将一个 `m4` 预留与所有这些专用主机关联。预留的实例系列和可用区必须与您希望与之关联的专用主机的实例系列和可用区相匹配。

当预留与专用主机关联后，将无法释放专用主机，直到预留期限结束。

使用 专用主机

要使用专用主机，首先在您的账户中分配要使用的主机。然后通过为实例指定一个主机 租赁，在主机上启动实例。您必须选择在其中启动实例的特定主机，或者您可以允许实例在任何已启用自动置放且匹配其实例类型的主机上启动。当某个实例停止并重新启动时，主机关联 设置将确定该实例是在同一主机上还是在另一个主机上重新启动。

如果您不再需要某个按需主机，则可以停止在该主机上运行的实例，指示它们在另一个主机上启动，然后释放 该主机。

专用主机也与 Amazon License Manager 相集成。使用 License Manager，您可以创建主机资源组，该组是作为单个实体进行管理的专用主机的集合。创建主机资源组时，可以为专用主机指定主机管理首选项，如自动分配和自动释放。这允许您在专用主机上启动实例，而无需手动分配和管理这些主机。有关更多信息，请参阅 Amazon License Manager 用户指南中的主机 Resource Groups。

目录

- 分配 专用主机 (p. 509)
- 在 专用主机 上启动实例。 (p. 511)
- 在主机资源组中启动实例 (p. 512)
- 了解自动置放与关联 (p. 513)
- 修改 专用主机 自动放置 (p. 513)
- 修改支持实例类型 (p. 514)
- 修改实例租赁和关联 (p. 516)
- 视图 专用主机 (p. 517)
- 标记专用主机 (p. 518)

- 显示器 专用主机 (p. 519)
- 版本 专用主机 (p. 520)
- 购买 专用主机预留 (p. 521)
- 查看 专用主机 预留 (p. 523)
- 标签 专用主机预留 (p. 523)

分配 专用主机

要开始使用专用主机，您必须使用 Amazon EC2 控制台或命令行工具在您的账户中分配专用主机。在分配专用主机后，将在您的账户中立即提供专用主机容量，您可以开始在专用主机上启动实例。

以下实例系列支持同一专属主机上同一实例系列的多个实例大小：A1、C5、M5、R5、C5n、M5n、R5n 和 T3。其他实例系列在相同 专用主机 上仅支持一个实例大小。

由于 N 型 专用主机（如 C5n、M5n 和 R5n）的硬件限制，您不能将较小的实例大小（`large` `xlarge`、和 `2xlarge`）与较大的实例大小（`4xlarge`、`9xlarge` `18xlarge`、和 `.metal`）混合使用。如果您在 N 型主机上同时需要较小和较大的实例大小，则必须为较小和较大的实例大小分配单独的主机。

您可以使用以下方法分配专用主机。

New console

分配专用主机

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 专用主机，然后选择 Allocate 专用主机 (分配专用主机)。
3. 对于 Instance family (实例系列)，为专用主机选择实例系列。
4. 指定 专用主机 是支持选定实例系列中的多种实例大小，还是仅支持特定的实例类型。请执行以下任一操作。
   - 要将专用主机配置为支持选定实例系列中的多种实例类型，请为 Support multiple instance types (支持多种实例类型) 选择 Enable (启用)。通过启用该选项，您可以在 专用主机 上启动同一实例系列中的不同实例大小。例如，如果您选择 `m5` 实例系列并选择该选项，则可以在专用主机上启动 `m5.xlarge` 和 `m5.4xlarge` 实例。
   - 要将专用主机配置为支持选定实例系列中的单个实例类型，请清除 Support multiple instance types (支持多种实例类型)，然后为 Instance type (实例类型) 选择要支持的实例类型。这样，您就可以在专用主机上启动单个实例类型。例如，如果选择该选项并将 `m5.4xlarge` 指定为支持的实例类型，则只能在专用主机上启动 `m5.4xlarge` 实例。
5. 对于 Availability Zone (可用区)，选择要在其中分配专用主机的可用区。
6. 要允许专用主机接受与其实例类型匹配的非定向实例启动，请为实例自动置放选择启用。有关自动置放的更多信息，请参阅了解自动置放与关联 (p. 513)。
7. 要为专用主机启用主机恢复，请为 Host recovery (主机恢复) 选择 Enable (启用)。有关更多信息，请参阅主机恢复 (p. 524)。
8. 对于 Quantity (数量)，输入要分配的专用主机数量。
9. （可选）选择 Add new tag (添加新标签)，然后输入标签键和标签值。
10. 选择 Allocate。

Old console

分配专用主机

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机、分配 专用主机。

3. 对于 Instance family (实例系列)，为专用主机选择实例系列。
4. 指定 专用主机 是支持选定实例系列中的多种实例大小，还是仅支持特定的实例类型。请执行以下任一操作。

   - 要将专用主机配置为支持选定实例系列中的多种实例类型，请选择 Support multiple instance types (支持多种实例类型)。通过启用该选项，您可以在 专用主机 上启动同一实例系列中的不同实例大小。例如，如果您选择 m5 实例系列并选择该选项，则可以在专用主机上启动 m5.xlarge 和 m5.4xlarge 实例。实例系列必须由 Nitro 系统提供支持。
   - 要将专用主机配置为支持选定实例系列中的单个实例类型，请清除 Support multiple instance types (支持多种实例类型)，然后为 Instance type (实例类型) 选择要支持的实例类型。这样，您就可以在专用主机上启动单个实例类型。例如，如果选择该选项并将 m5.4xlarge 指定为支持的实例类型，则只能在专用主机上启动 m5.4xlarge 实例。
5. 对于 Availability Zone (可用区)，选择要在其中分配专用主机的可用区。
6. 要允许专用主机接受与其实例类型匹配的非定向实例启动，请为实例自动置放选择启用。有关自动置放的更多信息，请参阅了解自动置放与关联 (p. 513)。
7. 要为专用主机启用主机恢复，请为主机恢复选择启用。有关更多信息，请参阅主机恢复 (p. 524)。
8. 对于 Quantity (数量)，输入要分配的专用主机数量。
9. （可选）选择添加标签，然后输入标签键和标签值。
10. 选择 Allocate host。

Amazon CLI

分配专用主机

使用 allocate-hosts Amazon CLI 命令。以下命令分配一个专用主机，它在 m5 可用区中支持 us-east-1a 实例系列中的多种实例类型。该主机还启用了主机恢复，并禁用了自动置放。

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --auto-
placement "off" --host-recovery "on" --quantity 1
```

以下命令分配一个在 m4.large 可用区中支持非定向 eu-west-1a 实例启动的专用主机，启用主机恢复，并应用一个具有键 purpose 和值 production 的标签。

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

分配专用主机

使用 New-EC2Host Amazon Tools for Windows PowerShell 命令。以下命令分配一个专用主机，它在 m5 可用区中支持 us-east-1a 实例系列中的多种实例类型。该主机还启用了主机恢复，并禁用了自动置放。

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -AutoPlacement Off
 -HostRecovery On -Quantity 1
```

以下命令分配一个在 m4.large 可用区中支持非定向 eu-west-1a 实例启动的专用主机，启用主机恢复，并应用一个具有键 purpose 和值 production 的标签。

TagSpecification 参数用于在创建时标记专用主机，需要一个指定所标记资源类型、标签键和标签值的对象。以下命令创建所需对象。

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
```

```
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

以下命令分配专用主机并应用在 $tagspec 对象中指定的标签。

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

在 专用主机 上启动实例。

在分配一个专用主机后，您可以在其中启动实例。对于您启动的实例类型，如果没有具有足够可用容量的活动专用主机，则无法启动具有 host 租赁的实例。

Tip

对于支持多种实例尺寸的专属主机，我们建议您首先启动较大的实例大小，然后根据需要用较小的实例大小填充剩余的实例容量。

在启动实例之前，请注意限制。有关更多信息，请参阅专用主机 限制 (p. 507)。

您可以使用以下方法在专用主机上启动实例。

Console

从专用主机页面中在特定专用主机上启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 在 专用主机 页面上，选择一个主机，选择 Actions (操作)，然后选择 Launch Instance(s) onto Host (在主机上启动实例)。
4. 从列表中选择一个 AMI。SQL Server、SUSE 和 Amazon EC2 提供的 RHEL AMI 无法用于专用主机。
5. 在 Choose an Instance Type (选择实例类型) 页面上，选择要启动的实例类型，然后选择 Next: Configure Instance Details (下一步：配置实例详细信息)。

   如果专用主机仅支持一种实例类型，则默认选择支持的实例类型，而无法进行更改。

   如果专用主机支持多种实例类型，您必须根据专用主机的可用实例容量在支持的实例系列中选择一种实例类型。建议您首先启动较大的实例大小，然后根据需要用较小的实例大小填充剩余的实例容量。
6. 在配置实例详细信息页面上，配置实例设置以满足需求，然后为关联选择下列选项之一：

   - 关闭 — 实例在指定的主机上启动，但不保证停止后仍在同一专用主机上重新启动。
   - 主机 — 如果停止，实例将始终在此特定主机上重新启动。

   有关关联的更多信息，请参阅了解自动置放与关联 (p. 513)。

   租赁和主机选项是根据您选择的主机预配置的。
7. 选择 Review and Launch。
8. 在 Review Instance Launch 页面上，选择 Launch。
9. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

使用启动实例向导在专用主机上启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择实例、启动实例。
3. 从列表中选择一个 AMI。SQL Server、SUSE 和 Amazon EC2 提供的 RHEL AMI 无法用于专用主机。
4. 选择要启动的实例类型，然后选择下一步：配置实例详细信息。
5. 在 Configure Instance Details (配置实例详细信息) 页面上，配置所需的实例设置，然后配置以下专用主机特定的设置：

   - 租赁 — 选择专用主机 – 在专用主机上启动此实例。
   - 主机 — 选择使用自动置放可在任何已启用自动置放的专用主机或在列表中选择特定的专用主机上启动实例。该列表仅显示支持选定实例类型的专用主机。
   - 关联 — 请选择下列选项之一：
     - 关闭 — 实例在指定的主机上启动，但不保证停止后仍在其上重新启动。
     - 主机 — 如果停止，实例将始终在指定主机上重新启动。

   有关更多信息，请参阅了解自动置放与关联 (p. 513)。

   如果您无法看到这些设置，请检查是否在 Network 菜单中选择了一个 VPC。
6. 选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

Amazon CLI

在专用主机上启动实例

使用 run-instances Amazon CLI 命令并在 `Placement` 请求参数中指定实例关联、租赁和主机。

PowerShell

在专用主机上启动实例

使用 New-EC2Instance Amazon Tools for Windows PowerShell 命令并在 `Placement` 请求参数中指定实例关联、租赁和主机。

在主机资源组中启动实例

在包含具有可用实例容量的专用主机的主机资源组中启动实例时，Amazon EC2 将在该主机上启动实例。如果主机资源组没有包含具有可用实例容量的主机，Amazon EC2 将自动分配主机资源组中的新主机，然后在该主机上启动实例。有关更多信息，请参阅 Amazon License Manager 用户指南中的主机资源组。

要求和限制

- 您必须将基于核心或套接字的许可证配置与 AMI 关联。
- 您不能将 Amazon EC2 提供的 SQL Server、SUSE 或 RHEL AMI 用于专用主机。
- 您无法通过选择主机 ID 来定位特定主机，并且无法在主机资源组中启动实例时启用实例关联。

您可以使用以下方法在主机资源组中启动实例。

Console

在主机资源组中启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择实例、启动实例。
3. 选择 AMI。
4. 选择要启动的实例类型，然后选择下一步：配置实例详细信息。
5. 在配置实例详细信息页面上，配置实例设置以满足需求，然后执行以下操作：
   a. 对于租赁，选择专用主机。
   b. 对于 Host resource group (主机资源组)，选择 Launch instance into a host resource group (在主机资源组中启动实例)。
   c. 对于 Host resource group name (主机资源组名称)，选择要在其中启动实例的主机资源组。
6. 选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 在系统提示时，选择现有密钥对或创建新的密钥对，然后选择启动实例。

Amazon CLI

在主机资源组中启动实例

使用 run-instances Amazon CLI 命令，并在 `Placement` 请求参数中省略“Tenancy”（租赁）选项并指定主机资源组 ARN。

PowerShell

在主机资源组中启动实例

使用 New-EC2Instance Amazon Tools for Windows PowerShell 命令，并在 `Placement` 请求参数中省略“Tenancy”（租赁）选项并指定主机资源组 ARN。

了解自动置放与关联

专用主机的置放控制是在实例级别和主机级别进行的。

自动置放

自动置放是在主机级别配置的。通过使用该功能，您可以管理启动的实例是在特定主机上启动，还是在具有匹配配置的任何可用主机上启动。

如果专用主机的自动置放已禁用，则它将仅接受指定其唯一主机 ID 的主机租赁实例启动。这是新专用主机的默认设置。

如果专用主机的自动置放已启用，则它会接受任何与其实例类型配置相匹配的非定向实例启动。

在启动实例时，您需要配置其租赁。如果在专用主机上启动实例而不提供特定 `HostId`，则将允许实例在任何已启用自动置放且匹配其实例类型的专用主机上启动。

主机关联

在实例级别配置主机关联。它在实例和专用主机之间建立启动关系。

当关联设置为 `Host` 时，启动到特定主机的实例在停止时始终在同一主机上重新启动。这适用于定向启动和非定向启动。

如果关联设置为 `Off`，并且您停止并重新启动实例，则实例可在任何可用主机上重新启动。但是，它将尝试在上次运行它的专用主机上启动 (尽最大努力)。

修改 专用主机 自动放置

将专用主机分配到Amazon账户后，您可以使用以下方法之一修改其自动置放设置。

New console

修改专用主机的自动置放

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择一个主机，然后依次选择 Actions (操作)、Modify host (修改主机)。
4. 对于 Instance auto-placement (实例自动置放)，选择 Enable (启用) 来启用自动置放，或者取消选择 Enable (启用) 来禁用自动置放。有关更多信息，请参阅了解自动置放与关联 (p. 513)。
5. 选择保存。

Old console

修改专用主机的自动置放

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择一个主机，然后依次选择操作、修改自动置放。
4. 在“修改自动置放”窗口中，对于允许自动置放，选择是以启用自动置放，或选择否以禁用自动置放。有关更多信息，请参阅了解自动置放与关联 (p. 513)。
5. 选择保存。

Amazon CLI

修改专用主机的自动置放

使用 modify-hosts Amazon CLI 命令。以下示例为指定专用主机启用自动置放。

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

修改专用主机的自动置放

使用 Edit-EC2Host Amazon Tools for Windows PowerShell 命令。以下示例为指定专用主机启用自动置放。

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

修改支持实例类型

以下实例系列支持同一专属主机上的多个实例类型：C5、M5、R5、C5n、R5n、M5n 和 T3。其他实例系列仅支持同一专用主机上的单个实例类型。

您可以使用以下方法分配专用主机。

您可以修改专用主机以更改它支持的实例类型。如果它当前支持一种实例类型，您可以对其进行修改以支持该实例系列中的多种实例类型。类似地，如果它当前支持多种实例类型，您可以对其进行修改以仅支持特定的实例类型。

要修改专用主机以支持多种实例类型，您必须先停止主机上正在运行的所有实例。完成修改大约需要 10 分钟。在进行修改时，专用主机将转变为 pending 状态。在处于 pending 状态时，您无法在专用主机上启动停止的实例或启动新实例。

要将支持多种实例类型的专用主机修改为仅支持单个实例类型，主机不能具有运行中的实例，或者运行中的实例必须是您希望主机支持的实例类型。例如，要将支持 m5 实例系列中的多种实例类型的主机修改为仅支持 m5.large 实例，则专用主机不能具有正在运行的实例，或者只能在主机上运行 m5.large 实例。

如果为虚拟化实例类型分配主机，在主机分配完成后，您无法将该实例类型修改为 .metal 实例类型。例如，如果您为 m5.large 实例类型分配主机，则无法将实例类型修改为 m5.metal。如果为 .metal 实例类型分配主机，在主机分配完成后，您无法将该实例类型修改为虚拟化实例类型。例如，如果您为 m5.metal 实例类型分配主机，则无法将实例类型修改为 m5.large。

您可以使用以下方法之一修改支持的实例类型。

New console

修改专用主机的支持实例类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 专用主机。
3. 选择要修改的专用主机，然后依次选择 Actions (操作)、Modify host (修改主机)。
4. 根据专用主机的当前配置，执行以下某项操作：

   - 如果专用主机当前支持特定实例类型，则未启用 Support multiple instance types (支持多种实例类型)，并且 Instance type (实例类型) 会列出所支持的实例类型。要修改主机以支持当前实例系列中的多种类型，请为 Support multiple instance types (支持多种实例类型) 选择 Enable (启用)。

     您必须先停止主机上正在运行的所有实例，然后再修改主机以支持多种实例类型。
   - 如果专用主机当前支持实例系列中的多种实例类型，则为 Support multiple instance types (支持多种实例类型) 选择了 Enabled (已启用)。要修改主机以支持特定的实例类型，请为 Support multiple instance types (支持多种实例类型) 取消选择 Enable (启用)，然后为 Instance type (实例类型) 选择要支持的特定实例类型。

     您无法更改专用主机支持的实例系列。
5. 选择保存。

Old console

修改专用主机的支持实例类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 专用主机。
3. 选择要修改的专用主机，然后依次选择 Actions (操作) 和 Modify Supported Instance Types (修改支持的实例类型)。
4. 根据专用主机的当前配置，执行以下某项操作：

   - 如果专用主机当前支持特定的实例类型，则为 Support multiple instance types (支持多种实例类型) 选择 No (否)。要修改主机以支持当前实例系列中的多种类型，请为 Support multiple instance types (支持多种实例类型) 选择 Yes (是)。

     您必须先停止主机上正在运行的所有实例，然后再修改主机以支持多种实例类型。
   - 如果专用主机当前支持实例系列中的多种实例类型，则为 Support multiple instance types (支持多种实例类型) 选择 Yes (是)，Instance family (实例系列) 将显示支持的实例系列。要修改主机以支持特定的实例类型，请为 Support multiple instance types (支持多种实例类型) 选择 No (否)，然后为 Instance type (实例类型) 选择要支持的特定实例类型。

     您无法更改专用主机支持的实例系列。
5. 选择保存。

Amazon CLI

修改专用主机的支持实例类型

使用 modify-hosts Amazon CLI 命令。

以下命令修改专用主机以支持 m5 实例系列中的多种实例类型。

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

以下命令修改专用主机以仅支持 m5.xlarge 实例。

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

修改专用主机的支持实例类型

使用 Edit-EC2Host Amazon Tools for Windows PowerShell 命令。

以下命令修改专用主机以支持 m5 实例系列中的多种实例类型。

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

以下命令修改专用主机以仅支持 m5.xlarge 实例。

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

修改实例租赁和关联

启动实例后，可以更改其租赁属性。您也可以修改实例与主机之间的关联。要修改实例租赁或关联，实例必须处于 stopped 状态。

Note

对于 T3 实例，您不能将租期从 dedicated 改为 host，或从 host 改为 dedicated。尝试进行这些不受支持的租赁更改会导致 InvalidTenancy 错误代码。

您可以使用以下方法修改实例的租赁和关联。

Console

修改实例租赁或关联

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择实例并选择要修改的实例。
3. 依次选择实例状态、停止。
4. 打开实例的上下文 (右键单击) 菜单，选择 Instance Settings，然后选择 Modify Instance Placement。
5. 在修改实例置放页面上，配置以下项：
   - 租赁 — 选择下列项之一：
     - 运行专用硬件实例 — 将实例作为专用实例启动。有关更多信息，请参阅Dedicated Instances (p. 533)。
     - 在专用主机上启动实例 — 在具有可配置关联的专用主机上启动实例。

- 关联 — 选择下列项之一：
  - 此实例可以在任一主机上运行 — 实例在您的账户中支持该实例类型的任何可用专用主机上启动。
  - 此实例只能在选定的主机上运行 — 实例只能在为目标主机选择的专用主机上运行。
- 目标主机 — 选择实例必须在其中运行的专用主机。如果未列出目标主机，则账户中可能没有可用的兼容专用主机。

有关更多信息，请参阅了解自动置放与关联 (p. 513)。

6. 选择保存。

Amazon CLI

修改实例租赁或关联

使用 modify-instance-placement Amazon CLI 命令。以下示例将指定实例的关联从 `default` 更改为 `host`，并指定实例已关联到的专用主机。

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host --
host-id h-012a3456b7890cdef
```

PowerShell

修改实例租赁或关联

使用 Edit-EC2InstancePlacement Amazon Tools for Windows PowerShell 命令。以下示例将指定实例的关联从 `default` 更改为 `host`，并指定实例已关联到的专用主机。

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
HostId h-012a3456b7890cdef
```

视图 专用主机

您可以使用以下方法查看专用主机以及其上的各个实例的详细信息。

New console

查看专用主机的详细信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 在 专用主机 页面上，选择一个主机。
4. 要查看主机的信息，请选择 Details (详细信息)。

   Available vCPUs (可用的 vCPU) 指示专用主机上可用于启动新实例的 vCPU。例如，如果专用主机支持 c5 实例系列中的多种实例类型，并且没有在上面运行实例，则它具有 72 个可用的 vCPU。这意味着，您可以在专用主机上启动不同的实例类型组合，以使用 72 个可用的 vCPU。

   要查看主机上运行的实例的信息，请选择 Running instances (运行实例)。

Old console

查看专用主机的详细信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择专用主机。
3. 在 专用主机 页面上，选择一个主机。
4. 有关主机的信息，请选择描述。Available vCPUs (可用的 vCPU) 指示专用主机上可用于启动新实例的 vCPU。例如，如果专用主机支持 c5 实例系列中的多种实例类型，并且没有在上面运行实例，则它具有 72 个可用的 vCPU。这意味着，您可以在专用主机上启动不同的实例类型组合，以使用 72 个可用的 vCPU。

   有关主机上运行的实例的信息，请选择实例。

Amazon CLI

查看专用主机的容量

使用 describe-hosts Amazon CLI 命令。

以下示例使用 describe-hosts (Amazon CLI) 命令查看支持 c5 实例系列中的多种实例类型的专用主机的可用实例容量。已在专用主机上运行两个 c5.4xlarge 实例和 4 个 c5.2xlarge 实例。

```
$  aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [
    { "AvailableCapacity": 2,
      "InstanceType": "c5.xlarge",
      "TotalCapacity": 18 },
    { "AvailableCapacity": 4,
      "InstanceType": "c5.large",
      "TotalCapacity": 36 }
  ],
"AvailableVCpus": 8
```

PowerShell

查看专用主机的实例容量

使用 Get-EC2Host Amazon Tools for Windows PowerShell 命令。

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

标记专用主机

您可以为现有专用主机分配自定义标签，以不同的方式对它们分类，例如按用途、所有者或环境。这有助于您根据所分配的自定义标签快速查找特定专用主机。专用主机标签也可用于成本分配跟踪。

您还可以在创建时向专用主机应用标签。有关更多信息，请参阅分配 专用主机 (p. 509)。

您可以使用以下方法为专用主机添加标签。

New console

为专用主机添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择要添加标签的专用主机，然后依次选择 Actions (操作)、Manage tags (管理标签)。
4. 在 Manage tags (管理标签) 界面中，选择 Add tag (添加标签)，然后指定标签的键和值。

5. （可选）选择 Add tag (添加标签)，为专用主机添加其他标签。
6. 选择保存更改。

Old console

为专用主机添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择要标记的专用主机，然后选择标签。
4. 选择 Add/Edit Tags。
5. 在添加/编辑标签对话框中，选择创建标签，然后指定该标签的键和值。
6. （可选）选择创建标签以将其他标签添加到专用主机。
7. 选择保存。

Amazon CLI

为专用主机添加标签

使用 create-tags Amazon CLI 命令。

以下命令将使用 Owner=TeamA 标记指定 专用主机。

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

为专用主机添加标签

使用 New-EC2Tag Amazon Tools for Windows PowerShell 命令。

New-EC2Tag 命令需要 Tag 对象，此对象指定要用于专用主机标签的键值对。以下命令使用 Tag 和 $tag 键值对创建一个名为 Owner 的 TeamA 对象。

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

以下命令使用 $tag 对象标记指定的专用主机。

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

显示器 专用主机

Amazon EC2 持续监控专用主机的状态。将在 Amazon EC2 控制台上显示更新的状态。您可以使用以下方法查看有关专用主机的信息。

Console

查看专用主机的状态

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。

3. 在列表中找到专用主机，并查看状态列中的值。

Amazon CLI

查看专用主机的状态

使用 describe-hosts Amazon CLI 命令，然后查看 `state` 响应元素中的 `hostSet` 属性。

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

查看专用主机的状态

使用 Get-EC2Host Amazon Tools for Windows PowerShell 命令，然后查看 `state` 响应元素中的 `hostSet` 属性。

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

下表说明了可能的专用主机状态。

状态	描述
`available`	Amazon未检测到专用主机的问题。不会安排维护或修复。实例可在此专用主机上启动。
`released`	已释放专用主机。主机 ID 不再使用。无法重新使用已释放的主机。
`under-assessment`	Amazon正在寻找专用主机可能存在的问题。如果必须采取措施，系统将通过 Amazon Web Services Management Console或电子邮件通知您。无法在处于该状态的专用主机上启动实例。
`pending`	无法使用专用主机启动新的实例。正在对其进行修改以支持多种实例类型 (p. 514)，或者正在进行主机恢复 (p. 524)。
`permanent-failure`	检测到了一个不可恢复的故障。您将通过您的实例和通过电子邮件接收到一个移出通知。实例可能会继续运行。如果在处于此状态的专用主机上停止或终止所有实例，Amazon将停用该主机。Amazon不会在此状态下重新启动实例。无法在处于该状态的专用主机上启动实例。
`released-permanent-failure`	Amazon永久释放已发生故障的专用主机，不再在这些主机上运行实例。专用主机 ID 不再可供使用。

版本 专用主机

必须先停止专用主机上运行的所有实例，然后才能释放主机。这些实例可以迁移至您账户的其他专用主机，这样您就可以继续使用它们。这些步骤只适用于按需专用主机。

您可以使用以下方法释放专用主机。

New console

释放专用主机

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择要释放的专用主机。
4. 依次选择 Actions (操作)、Release host (释放主机)。
5. 选择 Release (释放) 确认。

Old console

释放专用主机

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择要释放的专用主机。
4. 选择 Actions、Release Hosts。
5. 选择释放以确认。

Amazon CLI

释放专用主机

使用 release-hosts Amazon CLI 命令。

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

释放专用主机

使用 Remove-EC2Hosts Amazon Tools for Windows PowerShell 命令。

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

在释放专用主机后，您无法再次重新使用同一主机或主机 ID，并将不再根据按需账单费率向您收费。专用主机的状态将变为 `released`，您将无法在该主机上启动任何实例。

Note

如果您是刚刚释放的专用主机，则系统可能需要过一些时间才会停止将其计入限制。如果您在这段时间内尝试分配新的专用主机，可能会遇到 `LimitExceeded` 错误。如果出现这种情况，请在几分钟后再次尝试分配新的主机。

已停止的实例仍可以使用和列在 Instances 页面上。这些实例将保留其 `host` 租赁设置。

购买 专用主机预留

您可以使用以下方法购买预留：

Console

购买预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 专用主机、专用主机预留 和 Purchase 专用主机预留 (购买专用主机预留)。

3. 在 Purchase 专用主机预留 (购买专用主机预留) 屏幕上，您可以使用默认设置搜索可用的服务产品，也可以为以下内容指定自定义值：
   - 主机实例系列 — 列出的选项对应于您的账户中尚未分配给预留的专用主机。
   - 可用区 — 您的账户中尚未分配给预留的专用主机的可用区。
   - 付款选项 — 产品的付款选项。
   - 期限 — 预留期限，可以是一年或三年。
4. 选择查找产品，并选择符合您要求的产品。
5. 选择要与预留关联的专用主机，然后选择审核。
6. 审核您的订单，然后选择 Order (订单)。

Amazon CLI

购买预留

1. 使用 describe-host-reservation-offerings Amazon CLI 命令列出符合您需求的可用服务产品。以下示例列出了支持 m4 实例系列中的实例并具有一年期限的服务产品。

   Note

   期限以秒为单位指定。一年期限包括 31536000 秒，三年期限包括 94608000 秒。

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4
 --max-duration 31536000
```

   这条命令会返回符合您条件的服务产品的列表。记下要购买的产品的 offeringId。
2. 使用 purchase-host-reservation Amazon CLI 命令购买服务产品并提供上一步中提到的 offeringId。以下示例购买指定的预留，并将其与Amazon账户中已分配的特定专用主机关联，同时还应用具有键 purpose 和值 production 的标签。

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --
host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

购买预留

1. 使用 Get-EC2HostReservationOffering Amazon Tools for Windows PowerShell 命令列出符合您需求的可用服务产品。以下示例列出了支持 m4 实例系列中的实例并具有一年期限的产品。

   Note

   期限以秒为单位指定。一年期限包括 31536000 秒，三年期限包括 94608000 秒。

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

   这条命令会返回符合您条件的服务产品的列表。记下要购买的产品的 offeringId。
2. 使用 New-EC2HostReservation Amazon Tools for Windows PowerShell 命令购买服务产品并提供上一步中提到的 offeringId。以下示例购买指定的预留，并将其与Amazon账户中已分配的特定专用主机关联。

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
HostIdSet h-013abcd2a00cbd123
```

查看 专用主机 预留

您可以查看与预留关联的专用主机的信息，包括：

- 预留期限
- 付款选项
- 开始和结束日期

您可以使用以下方法查看专用主机预留的详细信息。

Console

查看专用主机预留的详细信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 在专用主机页面上，选择专用主机预留，然后从提供的列表中选择预留。
4. 有关预留的信息，请选择 Details。
5. 如需与预留关联的专用主机的信息，请选择主机。

Amazon CLI

查看专用主机预留的详细信息

使用 describe-host-reservations Amazon CLI 命令。

```
aws ec2 describe-host-reservations
```

PowerShell

查看专用主机预留的详细信息

使用 Get-EC2HostReservation Amazon Tools for Windows PowerShell 命令。

```
PS C:\> Get-EC2HostReservation
```

标签 专用主机预留

可以为您的 专用主机预留 分配自定义标签以便按不同的方式将它们分类，例如按用途、拥有者或环境分类。这有助于您根据所分配的自定义标签快速查找特定专用主机预留。

您只能使用命令行工具为专用主机预留添加标签。

Amazon CLI

为专用主机预留添加标签

使用 create-tags Amazon CLI 命令。

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

为专用主机预留添加标签

使用 New-EC2Tag Amazon Tools for Windows PowerShell 命令。

New-EC2Tag 命令需要 Tag 参数来指定要用于 专用主机预留 标签的键值对。以下命令创建 Tag 参数。

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

主机恢复

如果在专属主机上检测到具有特定问题的条件，专属主机恢复自动在新的替换主机上重新启动实例。主机恢复减少了人工干预的需求，并降低了发生关于系统电源或网络连接的意外专属主机故障时的运营负担。其它专属主机问题需要进行手动干预才能从中恢复。

目录

- 主机恢复基础知识 (p. 524)
- 支持的实例类型 (p. 525)
- 配置主机恢复 (p. 526)
- 主机恢复状态 (p. 527)
- 手动恢复不支持的实例 (p. 527)
- 相关服务 (p. 528)
- 定价 (p. 528)

主机恢复基础知识

专属主机和主机资源组恢复程序使用主机级运行状况检查以评估专用主机可用性，以及检测基本系统故障。专属主机故障的类型决定了专属主机能否自动恢复。可能导致主机级运行状况检查失败的问题示例包括：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的硬件或软件问题

> **Important**
>
> 主机计划停用后，专属主机将无法自动恢复。

专属主机自动恢复

在专属主机上检测到系统电源或网络连接故障时，将启动专属主机自动恢复，并且 Amazon EC2 自动分配替换专用主机。替换专用主机收到新的主机 ID，但保留与原始专用主机相同的属性，包括：

- 可用区

- 实例类型
- 标签
- 自动置放设置
- 预留

在分配替换专属主机时，实例将恢复到替换专属主机上。恢复的实例保留与原始实例相同的属性，包括：

- 实例 ID
- 私有 IP 地址
- 弹性 IP 地址
- EBS 卷附加
- 所有实例元数据

此外，与 Amazon License Manager 的内置集成自动跟踪和管理您的许可证。

> **Note**
>
> 仅在提供了 Amazon License Manager 的区域中支持 Amazon License Manager 集成。

如果实例与受损专用主机之间具有主机关联关系，恢复的实例将与替换专用主机建立主机关联。

在所有实例已恢复到替换专用主机时，将释放受损专用主机并且替换专用主机变为可用。

在启动了主机恢复时，将通过电子邮件和 Amazon 事件通知 Amazon Health Dashboard 账户所有者。在成功完成主机恢复后，将发送第二个通知。

如果使用 Amazon License Manager 跟踪您的许可证，Amazon License Manager 根据许可证配置限制为替换专用主机分配新的许可证。如果由于主机恢复而违反许可证配置的硬限制，则不允许执行恢复过程，并通过 Amazon SNS 通知向您通知主机恢复失败（如果已经为 Amazon License Manager 配置了通知设置）。如果由于主机恢复而违反许可证配置的软限制，则允许继续执行恢复，并通过 Amazon SNS 通知向您通知违反了限制。有关更多信息，请参阅 Amazon License Manager 用户指南中的使用许可证配置和 License Manager 中的设置。

专属主机无法自动恢复的场景

主机计划停用后，专属主机将无法自动恢复。您将在 Amazon Health Dashboard 中收到停用通知、Amazon CloudWatch 活动以及 Amazon 账户所有者的电子邮件地址会收到有关专属主机故障的消息。在指定的时间段内，按照停用通知中所述的纠正步骤手动恢复停用主机上的实例。

停止的实例不会恢复到替换专用主机上。如果您尝试启动将受损专用主机作为目标的停止实例，实例启动将失败。我们建议您修改停止的实例以将不同的专用主机作为目标，或者在任何可用的专用主机上启动并启用匹配的配置和自动置放。

具有实例存储的实例不会恢复到替换专用主机上。作为一项纠正措施，将受损专用主机标记为停用，并且您在主机恢复完成后收到停用通知。在指定的时间段内，按照停用通知中所述的纠正步骤手动恢复受损专用主机上的其余实例。

支持的实例类型

以下实例系列支持主机恢复：
A1、C3、C4、C5、C5n、C6a、C6g、C6i、Inf1、G2、G3、G5g、M3、M4、M5、M5n、M5zn、M6a、M6g、M6i、P2 和 u-24tb1。

要恢复不支持的实例，请参阅手动恢复不支持的实例 (p. 527)。

Note

与非裸机实例类型相比，受支持的裸机实例类型的专属主机的自动恢复将需要更长时间来进行检测和恢复。

配置主机恢复

您可以在分配专用主机时配置主机恢复，也可以在分配后使用 Amazon EC2 控制台或 Amazon Command Line Interface (CLI) 配置主机恢复。

目录

- 启用主机恢复 (p. 526)
- 禁用主机恢复 (p. 526)
- 查看主机恢复配置 (p. 527)

启用主机恢复

您可以在分配专用主机时或分配后启用主机恢复。

有关在分配专用主机时启用主机恢复的更多信息，请参阅分配 专用主机 (p. 509)。

使用控制台在分配后启用主机恢复

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择要启用主机恢复的专用主机，选择操作，然后选择修改主机恢复。
4. 对于主机恢复，请选择启用，然后选择保存。

使用 Amazon CLI 在分配后启用主机恢复

可以使用 modify-hosts 命令并指定 `host-recovery` 参数。

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

禁用主机恢复

您可以在分配专用主机后随时禁用主机恢复。

使用控制台在分配后禁用主机恢复

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择要禁用主机恢复的专用主机，选择操作，然后选择修改主机恢复。
4. 对于主机恢复，请选择禁用，然后选择保存。

使用 Amazon CLI 在分配后禁用主机恢复

可以使用 modify-hosts 命令并指定 `host-recovery` 参数。

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

查看主机恢复配置

您可以随时查看专用主机的主机恢复配置。

使用控制台查看专用主机的主机恢复配置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择专用主机，然后在描述选项卡中查看主机恢复字段。

使用 Amazon CLI 查看专用主机的主机恢复配置

可以使用 describe-hosts 命令。

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

HostRecovery 响应元素指示是启用还是禁用主机恢复。

主机恢复状态

当检测到专用主机故障时，受损专用主机将进入 under-assessment 状态，并且所有实例会进入 impaired 状态。在处于 under-assessment 状态时，您无法在受损的专用主机上启动实例。

在分配替换专用主机后，它进入 pending 状态。它保持该状态，直到主机恢复过程完成。在处于 pending 状态时，您无法在替换专用主机上启动实例。在恢复过程中，在替换专用主机上恢复的实例保持 impaired 状态。

在主机恢复完成后，替换专用主机进入 available 状态，并且恢复的实例恢复为 running 状态。在进入 available 状态后，您可以在替换专用主机上启动实例。将永久释放原始受损专用主机，并且它进入 released-permanent-failure 状态。

如果受损专用主机具有不支持主机恢复的实例（例如，具有实例存储支持的卷的实例），则不会释放专用主机。相反，它标记为停用并进入 permanent-failure 状态。

手动恢复不支持的实例

主机恢复不支持恢复使用实例存储卷的实例。请按照以下说明手动恢复无法自动恢复的任何实例。

> **Warning**
>
> 在您停止、休眠或终止实例后，实例存储卷上的数据将会丢失。这包括附加到使用 EBS 卷作为根设备的实例的实例存储卷。要保护实例存储卷中的数据，请在停止或终止实例之前将其备份到持久性存储中。

手动恢复 EBS 支持的实例

对于无法自动恢复的 EBS 支持的实例，我们建议您手动停止并启动实例以将其恢复到新的专用主机上。有关停止实例以及在停止实例后对实例配置进行的更改的更多信息，请参阅停止和启动您的实例 (p. 610)。

手动恢复实例存储支持的实例

有关无法自动恢复的实例存储支持的实例，我们建议您执行以下操作：

1. 在新的专用主机上从最新的 AMI 中启动替换实例。
2. 将所需的所有数据迁移到替换实例中。

3. 终止受损专用主机上的原始实例。

相关服务

专用主机 与以下服务集成在一起：

- Amazon License Manager – 在 Amazon EC2 专用主机之间跟踪许可证（仅在提供了 Amazon License Manager 的区域中支持）。有关更多信息，请参阅 Amazon License Manager 用户指南。

定价

使用主机恢复不会收取额外的费用，但会收取正常的专用主机费用。有关更多信息，请参阅 Amazon EC2 专用主机定价。

一旦启动了主机恢复，将不再对受损专用主机计费。仅在进入 `available` 状态后，才会开始对替换专用主机计费。

如果使用按需费率对受损专用主机进行计费，还会使用按需费率对替换专用主机进行计费。如果受损专用主机具有有效专用主机预留，则会将其转移到替换专用主机。

主机维护

启用主机维护后，降级专属主机上的 Amazon EC2 实例会在计划维护事件期间，在新分配的专属主机上自动重启。这有助于减少应用程序停机时间，并将千篇一律的繁重维护工作分载到 Amazon。此外，还会针对计划内和例行的 Amazon EC2 维护，执行主机维护。

所有通过 Amazon EC2 控制台新分配的专属主机均支持主机维护。对于 Amazon Web Services 账户 中的任何专属主机或通过 AllocateHosts API 分配的任何新专属主机，您可以为受支持的专属主机配置主机维护。有关更多信息，请参阅the section called “配置主机维护” (p. 530)。

目录

- 主机维护基础知识 (p. 528)
- 主机维护与主机恢复 (p. 529)
- 支持的实例类型 (p. 529)
- 专属主机上的实例 (p. 529)
- 配置主机维护 (p. 530)
- 维护事件 (p. 531)
- 主机维护状态 (p. 531)
- 相关服务 (p. 532)
- 定价 (p. 532)

主机维护基础知识

当在专属主机上检测到降级时，会分配新的专属主机。基础硬件降级或检测到具有特定问题的条件可能会导致降级。将会计划降级专属主机上的实例在新分配的专属主机上自动重启。

替换专属主机将接收新的主机 ID，但会保留与原始专属主机相同的属性。属性包括以下内容。

- 自动置放设置
- 可用区：
- 预留

- 主机关联
- 主机维护设置
- 主机恢复设置
- 实例类型
- 标签

对于所有受支持的专属主机，可以在所有 Amazon Web Services 区域 中进行主机维护。有关不支持主机维护的专属主机的更多信息，请参阅 the section called “限制” (p. 529)。

所有实例重启到新专属主机或停止后，会释放降级专属主机。您可以在计划维护事件之前访问降级专属主机上的实例，但不支持在降级专属主机上启动实例。

在计划维护事件之前，您可以使用新分配的专属主机，在主机上启动新实例。新主机上保留了一些容量，用于从降级主机重启实例。有关更多信息，请参阅the section called “专属主机上的实例” (p. 529)。

限制

- Amazon Outposts、Amazon Local Zone 和 Amazon Wavelength Zone 不支持主机维护。
- 无法为主机资源组中已有的主机开启或关闭主机维护。添加到主机资源组的主机保留其主机维护设置。有关更多信息，请参阅主机资源组。
- 仅特定实例类型支持主机维护。有关更多信息，请参阅the section called “支持的实例类型” (p. 529)。

主机维护与主机恢复

下表显示了主机恢复与主机维护之间的主要区别。

	主机恢复	主机维护
可访问性	无法访问	可以访问
状态	`under-assessment`	`permanent-failure`
操作	恢复将立即进行	维护将按计划进行
计划灵活性	无法重新计划	可以重新计划
主机资源组	支持	不支持

有关主机恢复的更多信息，请参阅主机恢复。

支持的实例类型

以下实例系列支持主机维护：`A1`、`C4`、`C5`、`C5n`、`C6a`、`C6g`、`C6iInf1`、`G3`、`G5g`、`M4`、`M5`、`M5n`、`M5zn`、`M6a`、`M6g`、`M6i`、`P2`、`P3`、`R4`、`R` 和 `X2iezn`。

专属主机上的实例

计划维护事件期间，降级主机上的实例会在新分配的专属主机上重启。实例会保留与降级主机上的实例相同的属性，包括以下内容。

- Amazon EBS 卷附加
- 弹性 IP 地址

- 实例 ID
- 实例元数据
- 私有 IP 地址

计划维护事件启动之前，您可以随时停止和启动降级主机上的实例。这将在另一台主机上重启实例，并且不会定期维护实例。您必须将实例的主机关联更新到要重启实例的新主机。有关更多信息，请参阅停止和启动实例。

Note

停止和启动实例后，不会保留任何本地存储卷上的数据。

以实例存储卷作为根设备的实例会在指定终止日期后终止。实例终止后，实例存储卷上的所有数据均会删除。已终止实例将永久删除，无法再次启动。对于以实例存储卷作为根设备的实例，建议使用最新的 Amazon Machine Image 在不同的专属主机上启动替换实例，并在指定终止日期之前将所有可用数据迁移到替换实例。有关更多信息，请参阅实例停用。

无法自动重启的实例将在指定日期后停止。您可以在其他主机上将其再次启动。以 Amazon EBS 卷作为根设备的实例在新主机上启动后，将继续使用相同的 Amazon EBS 卷。

您可以通过在 https://console.aws.amazon.com/ec2/ 中重新计划实例重启的开始时间，来设置实例重启顺序。

配置主机维护

您可以通过 Amazon Web Services Management Console 或 Amazon CLI 为所有支持的专属主机配置主机维护。有关更多信息，请参阅下表。

Amazon Web Services Management Console

使用 Amazon Web Services Management Console 为专属主机启用主机维护。

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 依次选择专属主机 > 操作 > 修改主机。
4. 在主机维护字段中选择启用。

使用 Amazon Web Services Management Console 为专属主机禁用主机维护。

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 依次选择专属主机 > 操作 > 修改主机。
4. 在主机维护字段中选择关闭。

使用 Amazon Web Services Management Console 查看专属主机的主机恢复配置。

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择专用主机。
3. 选择专属主机，然后在描述选项卡中查看主机维护字段。

Amazon CLI

在分配期间使用 Amazon CLI 为新专属主机启用或禁用主机维护。

使用 allocate-hosts 命令。

启用

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

禁用

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

使用 Amazon CLI 为现有专属主机启用或禁用主机维护。

使用 modify-hosts 命令。

启用

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

禁用

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

使用 Amazon CLI 查看专属主机的主机恢复配置。

可以使用 describe-hosts 命令。

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

Note

如果禁用主机维护，您会收到一封电子邮件通知，要求在 28 天内驱逐降级主机并将实例手动迁移到另一台主机。如果您有专属主机预留，则会分配替换主机。28 天后，降级主机上运行的实例将终止，主机会自动释放。

维护事件

检测到降级后，将在 14 天后安排维护事件，以在新专属主机上重启实例。您将收到一封电子邮件通知，其中包含有关降级主机、计划维护事件和维护时段的详细信息。有关更多信息，请参阅查看计划事件。

您可以将维护事件重新计划到计划日期后一周内的任何一天。有关重新计划的更多信息，请参阅重新计划计划事件。

维护事件通常需要几分钟才能完成。在极少数失败的情况下，您会收到一封电子邮件通知，要求在指定时间范围内驱逐降级主机上的实例。

主机维护状态

检测到降级后，专属主机将设置为 `permanent-failure` 状态。专属主机处于 `permanent-failure` 状态时，无法启动实例。维护事件完成后，降级主机将释放并置于 `released, permanent-failure` 状态。

在检测到专属主机降级之后，计划维护事件之前，主机维护会自动在账户中分配新专属主机。计划维护事件之前，新分配的替换主机将处于 pending 状态。计划维护事件之后，新专属主机将转换为 available 状态。您可以随时在此主机上启动新实例，甚至可以在维护事件之前启动。

Note

为在维护事件期间实现平稳过渡，将现有实例从降级主机迁移到新主机所需的容量将不可用。

相关服务

专属主机与Amazon License Manager 集成 – 跨 Amazon EC2 专属主机跟踪许可证（仅在提供 Amazon License Manager 的区域支持跟踪）。有关更多信息，请参阅 Amazon License Manager 用户指南。

Amazon Web Services 账户 必须具备足够许可证才能使用新专属主机。计划维护事件完成后会释放主机，此时将发放与降级主机关联的许可证。

定价

使用主机维护不会产生额外费用，但会收取正常的专属主机费用。有关更多信息，请参阅 Amazon EC2 专用主机定价。

启动主机维护后，不再对降级专属主机计费。仅在进入 available 状态后，才会开始对新分配的专属主机计费。

如果使用按需费率对降级专属主机进行计费，也会使用按需费率对新分配的专属主机进行计费。如果降级专属主机具有有效专属主机预留，则会将其转移到新专属主机。

跟踪配置更改

您可以使用 Amazon Config 记录专用主机的配置更改，以及记录在主机上启动、停止或终止的实例的配置更改。然后，您可以将由 Amazon Config 捕获的信息用作许可证报告的数据源。

Amazon Config 分别记录专用主机和实例的配置信息，并通过关系将这些信息配对。具有三种报告条件：

- Amazon Config 记录状态 – 当其状态为开启时，Amazon Config 将记录一个或多个 Amazon 资源类型，其中可包含专用主机和专用实例。要捕获许可证报告所需的信息，请使用以下字段验证是否记录了主机和实例。
- 主机记录状态 — 当其状态为启用时，将记录专用主机的配置信息。
- 实例记录状态 — 当其状态为启用时，将记录专用实例的配置信息。

如果禁用了这三个条件中的任一个，则 Edit Config Recording 按钮中的图标为红色。要发挥此工具的所有优点，请确保这三种记录方法都已启用。当这三种方法全部启用时，图标为绿色。要编辑设置，请选择 Edit Config Recording。您将被定向到 Amazon Config 控制台中的 Set up Amazon Config 页面，在该页面中，您可以设置 Amazon Config 并启动对您的主机、实例和其他支持的资源类型的记录。有关更多信息，请参阅 Amazon Config 开发人员指南 中的使用控制台设置 Amazon Config。

Note

Amazon Config 将在发现您的资源后记录它们，此过程可能需要几分钟。

在 Amazon Config 开始记录对您的主机和实例的配置更改后，您可以获取已分配或已释放的任何主机以及已启动、已停止或已终止的任何实例的配置历史记录。例如，在专用主机的配置历史记录中的任何时间点上，您均可以查看在该主机上启动的实例的数量以及该主机上的套接字和内核的数量。对于其中的任何实例，您还可以查找其 Amazon Machine Image (AMI) 的 ID。您可以使用此信息来报告您拥有的服务器端绑定软件 (按插槽或按内核授予许可) 的许可。

您可以使用以下任一方式查看配置历史记录：

- 通过使用 Amazon Config 控制台。对于每个已记录的资源，您可以查看一个时间线页面，该页面提供了配置详细信息的历史记录。要查看此页面，请选择专用主机页面的配置时间线列中的灰色图标。有关更多信息，请参阅 Amazon Config 开发人员指南 中的在 Amazon Config 控制台中查看配置详细信息。
- 通过运行 Amazon CLI 命令。首先，您可以使用 list-discovered-resources 命令获取一个包含所有主机和实例的列表。然后，您可以使用 get-resource-config-history 命令获取特定时间间隔内某个主机或实例的配置详细信息。有关更多信息，请参阅 Amazon Config 开发人员指南 中的使用 CLI 查看配置详细信息。
- 通过在您的应用程序中使用 Amazon Config API。首先，您可以使用 ListDiscoveredResources 操作获取一个包含所有主机和实例的列表。然后，您可以使用 GetResourceConfigHistory 操作获取特定时间间隔内某个主机或实例的配置详细信息。

例如，要从 Amazon Config 中获取所有专用主机的列表，请运行 CLI 命令，如下所示。

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

要从 Amazon Config 中获取专用主机的配置历史记录，请运行 CLI 命令，如下所示。

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

使用控制台管理 Amazon Config 设置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在专用主机页面上，选择编辑配置记录。
3. 在 Amazon Config 控制台中，按照提供的步骤来启用记录。有关更多信息，请参阅使用控制台设置 Amazon Config。

有关更多信息，请参阅在 Amazon Config 控制台中查看配置详细信息。

使用命令行或 API 激活 Amazon Config

- Amazon CLI：Amazon CLI 开发人员指南 中的查看配置详细信息 (Amazon Config)。
- Amazon EC2 API：GetResourceConfigHistory.

Dedicated Instances

专用实例是在单一客户专用硬件上的 Virtual Private Cloud (VPC) 中运行的 Amazon EC2 实例。属于不同的 Amazon账户的专用实例在硬件层面上物理隔离，即使这些账户关联到单个付款人账户。不过，专用实例可能与来自同一 Amazon 账户但非专用实例的其他实例共享硬件。

> **Note**
>
> 专用主机也是一种专供您使用的物理服务器。使用 专用主机，您可以查看和控制在服务器上放置实例的方式。有关更多信息，请参阅Dedicated Hosts (p. 504)。

主题

- 专用实例 基础知识 (p. 534)
- 支持的功能 (p. 534)
- 专用实例与专属主机的区别 (p. 535)
- 专用实例 限制 (p. 535)
- 专用实例定价 (p. 536)
- 使用 专用实例 (p. 536)

专用实例 基础知识

专用实例只能在 Amazon VPC 中启动。

当您启动实例时，该实例的租赁属性决定了该实例在其上运行的硬件。要启动专用实例，您必须指定 `dedicated` 的实例租赁。

> **Note**
>
> `default` 租赁值的实例在共享租赁硬件上运行。`host` 租赁值的实例在专属主机上运行。有关使用专属主机的更多信息，请参阅 Dedicated Hosts (p. 504)。

您在其中启动实例的 VPC 的租赁也可以决定实例的租赁。VPC 的租赁可以为 `default` 或 `dedicated`。如果您将实例启动到具有 `default` 租赁的 VPC，预设情况下，该实例将在共享租赁硬件上运行，除非您为该实例指定了不同的租赁。如果您将实例启动到具有 `dedicated` 租赁的 VPC，预设情况下，该实例作为专用实例运行，除非您为该实例指定了不同的租赁。

要启动专用实例，可以执行以下操作：

- 创建具有 `dedicated` 租赁的 VPC，并在预设情况下将所有实例作为专用实例启动。有关更多信息，请参阅创建有专用实例租赁的 VPC (p. 536)。
- 创建具有 `default` 租赁的 VPC，并为您要作为专用实例运行的实例手动指定 `dedicated` 租赁。有关更多信息，请参阅在 VPC 中启动 专用实例： (p. 536)。

支持的功能

专用实例支持以下功能和 Amazon 服务集成：

主题

- 预留实例 (p. 534)
- 自动扩展 (p. 534)
- 自动恢复 (p. 534)
- 专用竞价型实例 (p. 535)
- 具爆发能力的实例 (p. 535)

预留实例

若要确保足够的容量来启动专用实例，可以购买专用预留实例或容量预留。有关更多信息，请参阅 Reserved Instances (p. 408) 和 On-Demand Capacity Reservations (p. 538)：

如果购买专用Reserved Instance，可以按相当优惠的使用价同时购买到在 VPC 中启动专用实例的容量；而这种优惠的使用价只有在您启动专用租赁实例时才适用。当您购买具有原定设置租赁的预留实例时，它仅适用于具有 `default` 租赁的运行实例；它不适用于具有 `dedicated` 租赁的运行实例。

您在购买Reserved Instance之后将无法使用修改过程来更改其租赁。但是，您可以将可转换预留实例换成具有不同租赁的新可转换预留实例。

自动扩展

您可以使用 Amazon EC2 Auto Scaling 启动专用实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的在 VPC 中启动 Auto Scaling 实例。

自动恢复

如果专用实例因需要 Amazon 参与才能修复的基础硬件故障或问题而受损，您可以为它配置自动恢复。有关更多信息，请参阅恢复实例 (p. 640)。

专用竞价型实例

创建 Spot 实例请求时，您可以通过指定租赁 `dedicated` 来运行专用 Spot 实例。有关更多信息，请参阅指定竞价型实例的租期 (p. 458)。

具爆发能力的实例

您可以通过the section called “可突增性能实例” (p. 274)，利用在专用租赁硬件上运行的优势。默认情况下，T3 专用实例以无限模式启动，提供了基准水平的 CPU 性能，并且在工作负载需要时能够突增到更高的 CPU 性能水平。T3 基准性能和突增能力由 CPU 积分控制。由于 T3 实例类型的可突增性质，我们建议您监控 T3 实例如何使用专用硬件的 CPU 资源，以获得最佳性能。T3 专用实例面向具有多种工作负载的客户，这些工作负载表现出随机 CPU 行为，但理想情况下，平均 CPU 使用率等于或低于基准使用率。有关更多信息，请参阅the section called “重要概念” (p. 276)。

Amazon EC2 具有识别和纠正性能可变性的系统。但是，如果您启动多个具有关联 CPU 使用模式的 T3 专用实例，仍可能遇到短暂的变化。对于这些要求更高或关联的工作负载，我们建议使用 M5 或 M5a 专用实例，而不是 T3 专用实例。

专用实例与专属主机的区别

专用实例和专用主机均可用于在专供您使用的物理服务器上启动 Amazon EC2 实例。

专用实例与专属主机上的实例在性能、安全性或物理特性方面没有区别。但是，这两者之间也存在一些差异。下表重点介绍专用实例和专用主机之间的一些重要区别：

	Dedicated Host	Dedicated Instance
计费	按主机计费	按实例计费
套接字、内核和主机 ID 的可见性	提供主机上套接字数和物理内核数的可见性	无可见性
主机和实例关联	允许您在一段时间内将您的实例一致地部署到同一主机	不支持
定向实例置放	控制在主机上放置实例的方式	不支持
自动实例恢复	支持	支持
自带许可 (BYOL)	支持	部分支持*

* 通过软件保障计划提供许可证移动性的 Microsoft SQL Server 和 Windows 虚拟桌面访问 (VDA) 许可证可用于专用实例。

有关专属主机的更多信息，请参阅 Dedicated Hosts (p. 504)。

专用实例 限制

使用专用实例时请记住以下事项：

- 某些 Amazon 服务或其功能不受实例租期设置为 `dedicated` 的 VPC 支持。请参阅各自的服务文档以确认是否存在任何限制。
- 某些实例类型无法启动至实例租期设置为 `dedicated` 的 VPC 中。有关支持的实例类型的更多信息，请参阅 Amazon EC2 专用实例。

- 当启动 Amazon EBS 支持的专用实例时，EBS 卷不会在单一租户硬件上运行。

专用实例定价

专用实例的定价不同于按需实例的定价。有关更多信息，请参阅 Amazon EC2 专用实例产品页面。

使用 专用实例

您可以创建一个实例租期设置为 `dedicated` 的 VPC，以确保在该 VPC 内启动的所有实例都是专用实例。或者，您可以在启动时指定实例的租期。

主题

- 创建有专用实例租赁的 VPC (p. 536)
- 在 VPC 中启动 专用实例： (p. 536)
- 显示租期信息 (p. 537)
- 更改实例的租期 (p. 538)
- 更改 VPC 的租期 (p. 538)

创建有专用实例租赁的 VPC

当您创建 VPC 时，您可以选择指定它的实例租期。如果在实例租赁已设置为 `dedicated` 的 VPC 中启动实例，则无论实例的租赁如何，实例都将自动为专用实例。

有关创建 VPC 和选择租赁选项的更多信息，请参阅《Amazon VPC 用户指南》中的创建 VPC。

在 VPC 中启动 专用实例：

可以使用 Amazon EC2 启动实例向导来启动专用实例。

Console

使用控制台在默认租赁 VPC 中启动专用实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页上，选择某个 AMI，然后选择 Select。
4. 在 Choose an Instance Type 页面上，选择实例类型并选择 Next: Configure Instance Details。

   Note

   确保选择作为专用实例受支持的实例类型。有关更多信息，请参阅 Amazon EC2 专用实例。
5. 在配置实例详细信息页上，选择 VPC 和子网。对于 Tenancy (租期)，选择 Dedicated - Run a dedicated instance (专用 - 运行专用实例)，然后选择 Next: Add Storage (下一步：添加存储)。
6. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动以选择一个密钥对并启动专用实例。

Command line

使用命令行在启动过程中设置实例的租赁选项

- run-instances (Amazon CLI)

- New-EC2Instance（Amazon Tools for Windows PowerShell）

有关启动租期为 host 的实例的更多信息，请参阅在 专用主机 上启动实例。 (p. 511)。

显示租期信息

Console

使用控制台显示您的 VPC 的租赁信息

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs。
3. 在 Tenancy (租区) 一栏中查看您的 VPC 实例的租区。
4. 如果未显示 Tenancy（租赁）列，请选择右上角的设置图标 ()，切换选择 Tenancy（租赁），然后选择 Confirm.（确认）。

使用控制台显示您的实例的租赁信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 在 Tenancy (租期) 一栏中查看您的实例的租期。
4. 如果未显示 Tenancy (租期) 栏，您可以执行以下操作：
   - 选择右上角的设置图标 ()，切换选择 Tenancy（租赁），然后选择 Confirm.（确认）。
   - 选择实例。在页面底部附近的 Details (详细信息) 选项卡上的 Host and placement group (主机和置放群组) 下，检查 Tenancy (租期) 的值。

Command line

使用命令行描述您的 VPC 的租赁

- describe-vpcs (Amazon CLI)
- Get-EC2Vpc (Amazon Tools for Windows PowerShell)

使用命令行描述您的实例的租赁

- describe-instances (Amazon CLI)
- Get-EC2InstanceAmazon Tools for Windows PowerShell

使用命令行描述Reserved Instance的租赁值

- describe-reserved-instances (Amazon CLI)
- Get-EC2ReservedInstance (Amazon Tools for Windows PowerShell)

使用命令行描述Reserved Instance产品的租赁值

- describe-reserved-instances-offerings (Amazon CLI)
- Get-EC2ReservedInstancesOffering (Amazon Tools for Windows PowerShell)

更改实例的租期

启动实例后，可以更改已停止实例的租赁属性。您所做的更改将在下次实例开启时生效。

Note

对于 T3 实例，您不能将租期从 dedicated 改为 host，或从 host 改为 dedicated。尝试进行这些不受支持的租赁更改会导致InvalidTenancy错误代码。

Console

使用控制台更改实例的租赁

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 依次选择 Instance state (实例状态)、Stop instance (停止实例)、Stop (停止)。
4. 依次选择操作、实例设置、修改实例放置。
5. 在 Tenancy (租期) 列表中，选择是在专用硬件上还是在 专用主机 上运行您的实例。选择保存。

Command line

使用命令行修改实例的租赁值

- modify-instance-placement (Amazon CLI)
- Edit-EC2InstancePlacement (Amazon Tools for Windows PowerShell)

更改 VPC 的租期

在创建 VPC 之后，可以将其租赁属性从 dedicated 改为 default。修改 VPC 的实例租赁不会影响 VPC 中任何现有实例的租赁。下次在 VPC 中启动一个实例时，该实例将具有 default 租赁，除非您在启动过程中另有指定。

Note

在创建 VPC 之后，您无法将其实例租期从 default 更改为 dedicated。

可以使用 Amazon CLI、Amazon SDK 或仅使用 Amazon EC2 API 修改 VPC 的实例租赁属性。

Command line

使用 Amazon CLI 修改 VPC 的实例租赁属性

使用 modify-vpc-tenancy 命令并指定 VPC 的 ID 和实例租赁值。default 是唯一受支持的值。

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

On-Demand Capacity Reservations

通过使用按需容量预留，您可以在特定可用区中为Amazon EC2实例预留计算容量达任意持续时间。容量预留可降低在存在容量限制的情况下无法获得按需容量的风险。如果您有严格的容量要求，并且正在运行需要一定级别的长期或短期容量保证的业务关键型工作负载，我们建议您创建容量预留，以确保在需要时始终可以获得所需时长的 Amazon EC2 容量。

以下是容量预留的一些常见用例：

- 灾难恢复 – 您可以在不同的可用区或区域预留容量，以确保在失效转移事件期间所需的容量可用。
- 监管要求 – 您可以使用容量预留来满足针对高可用性的监管要求。容量预留可确保容量准备妥当以满足这些需求，即使未使用这些资源也是如此。
- 事件 – 您可以在业务关键型事件之前创建容量预留，以确保在需要时进行扩容。

您随时可以创建容量预留，而无需作出一年或三年期限承诺。在您的账户中预置容量预留后，容量即可用且账单开始。当您不再需要容量保证时，请取消容量预留以释放容量并停止产生费用。您还可以使用 区域性预留实例提供的账单折扣来减少容量预留的成本。

在创建容量预留时，您将指定：

- 在其中预留容量的可用区
- 为其预留容量的实例的数量
- 实例属性，包括实例类型、租期和平台/操作系统

容量预留只能由匹配其属性的实例使用。默认情况下，这些容量由与属性匹配的运行中实例使用。如果您没有任何正在运行的实例与容量预留的容量匹配，则这些容量将保持未使用的状态，直至启动具有匹配属性的实例。

目录

- 支持的平台 (p. 539)
- 配额 (p. 540)
- 限制 (p. 540)
- 容量预留定价和计费 (p. 540)
- 使用 容量预留 (p. 541)
- 使用 容量预留 组 (p. 547)
- 集群置放群组中的容量预留 (p. 550)
- Local Zones 中的容量预留 (p. 553)
- Wavelength 区中的 容量预留 (p. 554)
- 使用共享 容量预留 (p. 554)
- 容量预留机群 (p. 558)
- 按需容量预留的 CloudWatch 指标 (p. 569)

支持的平台

您必须使用正确的平台创建容量预留，以确保它与您的实例正确匹配。容量预留支持以下平台：

- Linux/UNIX
- 含有 SQL Server Standard 的 Linux
- 含有 SQL Server Web 的 Linux
- 含有 SQL Server Enterprise 的 Linux
- SUSE Linux
- Red Hat Enterprise Linux
- 含有 SQL Server Standard 的 RHEL
- 含有 SQL Server Enterprise 的 RHEL
- 含有 SQL Server Web 的 RHEL
- 含有 HA 的 RHEL

- 含有 HA 和 SQL Server Standard 的 RHEL
- 含有 HA 和 SQL Server Enterprise 的 RHEL

您购买 容量预留 时，必须指定代表适用于您实例的操作系统的平台。

- 对于 SUSE Linux 和 RHEL 发行版（不包括 BYOL），您必须选择特定的平台。例如，SUSE Linux 或 Red Hat Enterprise Linux 平台。
- 对于所有其他 Linux 发行版（包括 Ubuntu），选择 Linux/UNIX 平台。
- 如果您携带现有的 RHEL 订阅 (BYOL)，则必须选择 Linux/UNIX 平台。

有关受支持的 Windows 平台的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的支持的平台。

配额

允许您预留容量的实例数基于您账户的个按需型实例配额。您可以在配额允许的数量减去已经运行的实例数量范围内，为任意数量的实例预留容量。

限制

在创建容量预留之前，请注意以下限制。

- 活动和未使用的容量预留会计入您的个按需型实例限制中。
- 容量预留无法从一个Amazon账户转移到另一个账户。但是，您可以与其他Amazon账户共享容量预留。有关更多信息，请参阅 使用共享 容量预留 (p. 554)。
- 区域Reserved Instance账单折扣不适用于容量预留。
- 您可以在集群置放群组中创建容量预留。不支持分布和分区置放群组。
- 容量预留不能与专用主机一起使用。容量预留可以与专用实例一起使用。
- 容量预留不能确保休眠的实例在尝试启动后可以恢复。

容量预留定价和计费

主题

- 定价 (p. 540)
- 计费 (p. 541)
- 账单折扣 (p. 541)
- 查看您的账单 (p. 541)

定价

无论您是否在预留容量中运行实例，都按等同的按需费率为您计算容量预留费用。如果您没有使用预留，这将在您的 Amazon EC2 账单中显示为未使用的预留。如果您运行的实例属性与预留匹配，则您只需要为该实例付费，不需要为预留付费。没有任何预付费用或额外收费。

例如，如果您为 20 个 `m4.large` Linux 实例创建容量预留并在同一个可用区中运行 15 个 `m4.large` Linux 实例，则会向您收取 15 个活动的实例和预留中 5 个未使用的实例的费用。

区域预留实例的账单折扣适用于容量预留。有关更多信息，请参阅账单折扣 (p. 541)。

有关更多信息，请参阅 Amazon EC2 定价。

计费

计费在您的账户中预置容量预留后立即开始，并在容量预留保持在账户中预置状态期间继续计费。

容量预留以秒为单位计费。这意味着会向您收取不足一小时的费用。例如，如果容量预留在您的账户中保持预置状态 24 小时 15 分钟，则会向您收取 24.25 个预留小时的费用。

下面的示例说明如何对容量预留计费。为一个 m4.large Linux 实例创建了容量预留，其按需费率为每使用一小时 0.10 美元。在此示例中，账户内的容量预留预置了五个小时。第一个小时未使用容量预留，因此按照 m4.large 实例类型的标准按需费率计入一小时未使用费用。从第二个小时到第五个小时，m4.large 实例占用了容量预留。在这段时间内，容量预留不会产生任何费用，改为向账户收取占用这部分容量的 m4.large 实例的费用。在第六个小时取消了容量预留，并在预留容量之外正常运行 m4.large 实例。对于这一个小时，将以 m4.large 实例类型的按需费率进行收费。

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

账单折扣

区域预留实例的账单折扣适用于容量预留。Amazon 自动将这些折扣应用于具有匹配属性的容量预留。当容量预留由某个实例使用时，折扣将适用于该实例。折扣将优先适用于已产生的实例使用量，然后再用于未使用的容量预留。

区域预留实例的账单折扣不适用于容量预留。

有关更多信息，请参阅下列内容：

- Reserved Instances (p. 408)

查看您的账单

您可以在 Amazon Billing and Cost Management 控制台上查看您账户的费用情况。

- 控制面板显示了您的账户的花费汇总。
- 在 Bills (账单) 页面上的 Details (详细信息) 下，展开 Elastic Compute Cloud 部分及区域，以获取有关您的容量预留的账单信息。

您可以在线查看费用，也可以下载 CSV 文件。有关更多信息，请参阅 Amazon Billing and Cost Management 用户指南中的容量预留行项目。

使用 容量预留

要开始使用容量预留，您可以在所需的可用区中创建容量预留。然后，您可以在预留容量中启动实例，实时查看其容量使用情况，以及根据需要增加或减少其容量。

默认情况下，容量预留自动将新实例与具有匹配属性（实例类型、平台和可用区）的运行中实例进行匹配。这意味着，任何具有匹配属性的实例都将自动在容量预留中运行。不过，您还可以将容量预留定位到特定工作负载。这使您可以明确控制允许哪些实例在预留容量中运行。

您可以指定预留如何结束。您可以选择取消 容量预留 或者在指定时间自动结束它。如果您指定结束时间，则容量预留在指定时间的一小时之内取消。例如，如果您指定“5/31/2019, 13:30:55”，则容量预留可确保在 2019 年 5 月 31 日的 13:30:55 到 14:30:55 之间结束。预留结束后，您无法再将实例定位到容量预留中。在预留容量中运行的实例继续运行，不会中断。如果定位到容量预留中的实例停止，在您删除其容量预留定位首选项或者将其配置为定位到其他容量预留之前，无法重新启动这些实例。

目录

- 创建 容量预留 (p. 542)
- 在现有 容量预留 中启动实例 (p. 543)
- 修改 容量预留 (p. 544)
- 修改实例的 容量预留 设置 (p. 544)
- 查看 容量预留 (p. 545)
- 取消 容量预留 (p. 546)

创建 容量预留

创建容量预留之后，容量立即可用。只要容量预留活动，该容量就为您预留，您可以随时在其中启动实例。如果容量预留处于开放状态，具有匹配属性的新实例和现有实例将会自动在容量预留的容量中运行。如果容量预留处于 `targeted` 状态，只有专门定位到其中的实例才能在预留容量中运行。

如果出现以下情况之一，创建容量预留的请求会失败：

- Amazon EC2没有足够的容量来满足请求。请稍后重试、尝试不同的可用区或者尝试较小的容量。如果您的应用程序灵活地跨实例类型和大小，请尝试不同的实例属性。
- 请求的数量超过选定实例系列的个按需型实例限制。增加该实例系列的个按需型实例限制，然后重试。有关更多信息，请参阅个按需型实例限制 (p. 406)。

使用控制台创建容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 容量预留 (容量预留)，然后选择 Create 容量预留 (创建容量预留)。
3. 在“Create a 容量预留 (创建容量预留)”页面上的实例详细信息部分中，配置以下设置。您启动的实例的实例类型、平台和可用区必须与您在此处指定的实例类型、平台和可用区匹配，否则将不会应用容量预留。例如，如果开放的容量预留不匹配，则明确针对此容量预留的实例启动将失败。

   a. 实例类型 — 在预留容量中启动的实例类型。
   b. 启动 EBS 优化的实例 — 指定是否为 EBS 优化的实例预留容量。一些实例类型默认情况下会选中此选项。有关 EBS 优化实例的更多信息，请参阅 Amazon Elastic Block Store (p. 1323)。
   c. 平台 — 实例的操作系统。有关更多信息，请参阅支持的平台 (p. 539)。有关受支持的 Windows 平台的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的支持的平台。
   d. 可用区 — 在其中预留容量的可用区。
   e. 租赁 — 指定要在共享硬件（默认）还是专用实例上运行。
   f. (可选）置放群组 ARN — 要在其中创建容量预留的集群置放群组的 ARN。有关更多信息，请参阅集群置放群组中的容量预留 (p. 550)。
   g. Quantity (数量) – 为其预留容量的实例的数量。如果指定的数量超过了选定实例类型的剩余个按需型实例限制，将拒绝该请求。
4. 在预留详细信息部分中配置以下设置：

   a. 预留结束 — 选择以下选项之一：

      - 手动 — 容量将预留，直至您明确取消。
      - Specific time (特定时间) – 在指定的日期和时间自动取消容量预留。

   b. 实例资格 — 选择以下选项之一：

      - 开放 —（默认值）容量预留匹配任意具有匹配属性（实例类型、平台和可用区）的实例。如果您启动具有匹配属性的实例，则会自动将其放置到预留容量中。
      - targeted (定位) – 容量预留仅接受具有匹配属性（实例类型、平台和可用区）并明确针对预留的实例。

5. 选择请求预留。

使用 Amazon CLI 创建容量预留

使用 create-capacity-reservation 命令。有关更多信息，请参阅支持的平台 (p. 539)。有关受支持的 Windows 平台的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的支持的平台。

例如，以下命令会创建一个容量预留，它将为 3 个在 m5.2xlarge 可用区中运行 Red Hat Enterprise Linux AMI 的 us-east-1a 实例保留容量。

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red Hat
 Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

在现有 容量预留 中启动实例

启动实例时，可以指定在任意 open 容量预留中、特定容量预留中还是容量预留组中启动实例。您仅可在具有匹配属性（实例类型、平台和可用区）和充足容量的容量预留中启动实例。或者，您也可以将实例配置为避免在容量预留中运行，即使您拥有具有匹配属性和可用容量的 open 容量预留也是如此。

在容量预留中启动实例会将其可用容量减去所启动实例的数量。例如，如果您启动 3 个实例，容量预留的可用容量将减去 3。

使用控制台在现有容量预留中启动实例

1. 通过从控制面板或实例选择启动实例来打开启动实例向导。
2. 选择 Amazon Machine Image (AMI) 和实例类型。
3. 完成配置实例详细信息页面。对于容量预留，请选择下列选项之一：
   - 无 — 阻止实例在容量预留中启动。实例使用按需容量运行。
   - 开放 — 在具有匹配属性以及对于所选实例数具有足够容量的任意容量预留中启动实例。如果没有匹配的容量预留具有足够容量，实例使用按需容量。
   - 按 ID 定位 — 在选定的容量预留中启动实例。如果选定的容量预留没有足够的容量来运行所选数量的实例，实例启动将失败。
   - 按组定位 — 在所选容量预留组中任何具有匹配属性和可用容量的容量预留中启动实例。如果所选组中没有具有匹配属性和可用容量的容量预留，将会在按需容量中启动实例。
4. 完成剩余步骤以启动实例。

使用 Amazon CLI 在现有容量预留中启动实例

使用 run-instances 命令并指定 --capacity-reservation-specification 参数。

以下示例在任意具有匹配属性和可用容量的开放容量预留中启动 t2.micro 实例。

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-
name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationPreference=open
```

以下示例在 t2.micro 容量预留中启动 targeted 实例：

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-
name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

以下示例在容量预留组中启动 t2.micro 实例：

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-
name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:us-
west-1:123456789012:group/my-cr-group}
```

修改 容量预留

创建活动容量预留后，您可以更改它的属性。在某个容量预留过期后，或者您明确取消后，您无法对其进行修改。

修改容量预留时，您只能增加或减少数量以及更改释放容量的方式。您无法更改容量预留的实例类型、EBS 优化、平台、可用区或实例资格。如果您需要修改任意这些属性，我们建议您取消预留，然后使用所需属性创建新的预留。

如果指定的新数量超过了选定实例类型的剩余个按需型实例限制，更新将失败。

使用控制台修改容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择容量预留，选择要修改的容量预留，然后选择编辑。
3. 根据需要修改数量或预留结束选项，然后选择保存更改。

使用 Amazon CLI 修改容量预留

使用 modify-capacity-reservations 命令：

例如，以下命令将修改容量预留，使其为 8 个实例预留容量。

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --
instance-count 8
```

修改实例的 容量预留 设置

您随时可以为已停止实例修改以下容量预留设置：

- 在具有匹配属性（实例类型、平台和可用区）以及可用容量的任意 容量预留 上启动。
- 在特定容量预留中启动实例。
- 在容量预留组中任何具有匹配属性和可用容量的容量预留中启动
- 阻止实例在容量预留中启动。

使用控制台修改实例的容量预留设置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择实例并选择要修改的实例。停止实例（如果尚未停止）。
3. 依次选择操作和修改容量预留设置。
4. 对于容量预留，请选择下列选项之一：
   - 开放 — 在具有匹配属性以及对于所选实例数具有足够容量的任意容量预留中启动实例。如果没有匹配的容量预留具有足够容量，实例使用按需容量。
   - 无 — 阻止实例在容量预留中启动。实例使用按需容量运行。
   - 指定容量预留 — 在选定的容量预留中启动实例。如果选定的容量预留没有足够的容量来运行所选数量的实例，实例启动将失败。

- 指定容量预留 — 在所选容量预留组中任何具有匹配属性和可用容量的容量预留中启动实例。如果所选组中没有具有匹配属性和可用容量的容量预留，将会在按需容量中启动实例。

使用 Amazon CLI 修改实例的容量预留设置

使用 modify-instance-capacity-reservation-attributes 命令。

例如，以下命令会将实例的容量预留设置更改为 open 或 none。

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id i-1234567890abcdef0
 --capacity-reservation-specification CapacityReservationPreference=none|open
```

例如，以下命令会将实例修改为定位到特定容量预留。

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

例如，以下命令会将实例修改为定位到特定容量预留组。

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:us-
west-1:123456789012:group/my-cr-group}
```

查看 容量预留

容量预留可能具有以下几种状态：

- active — 容量可供使用。
- expired — 容量预留已在您预留请求中指定的日期和时间自动失效。预留容量不再可供您使用。
- cancelled—容量预留 已取消。预留容量不再可供您使用。
- pending — 容量预留请求已成功，但容量预配置仍待处理。
- failed — 容量预留请求失败。请求可能由于无效的请求参数、容量限制或实例限制等约束条件失败。您可以查看 60 分钟内的失败请求。

> **Note**
>
> 由于 Amazon EC2 API 遵循的最终一致性模型，创建容量预留后，控制台和 describe-capacity-reservations 响应最高会花费 5 分钟来表明容量预留处于 active 状态。在此期间，控制台和 describe-capacity-reservations 响应可能会表明容量预留位于 pending 状态。但是，容量预留可能已经可供使用，您可以尝试在其中启动实例。

使用控制台查看容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择容量预留并选择要查看的容量预留。
3. 选择查看此预留已启动的实例。

使用 Amazon CLI 查看容量预留

使用 describe-capacity-reservations 命令：

例如，以下命令会描述所有容量预留。

```
aws ec2 describe-capacity-reservations
```

输出示例。

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
}
```

取消 容量预留

如果不在需要预留容量，您可以随时取消容量预留。取消容量预留之后，该容量将立即释放，不再保留供您使用。

您可以取消空容量预留以及具有正在运行的实例的容量预留。如果您取消具有正在运行的实例的容量预留，这些实例将继续在容量预留之外正常运行并应用标准按需型实例费率；或者，如果您有匹配的 区域预留实例，则应用折扣费率。

取消容量预留之后，定位到其中的实例无法再启动。修改这些实例，使其定位到不同容量预留、启动到任意处于“开放”状态且具有匹配属性和充足容量的容量预留，或者避免将其启动到容量预留中。有关更多信息，请参阅修改实例的 容量预留 设置 (p. 544)。

使用控制台取消容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择容量预留，然后选择要取消的容量预留。

3. 依次选择取消预留、取消预留。

使用 Amazon CLI 取消容量预留

使用 cancel-capacity-reservation 命令：

例如，以下命令会取消 ID 为 cr-1234567890abcdef0 的容量预留。

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

使用 容量预留 组

您可以使用 Amazon Resource Groups 创建称为 Resource Groups 的容量预留逻辑集合。资源组是全部位于同一 Amazon 区域的 Amazon 资源的逻辑分组。有关 Resource Groups 的更多信息，请参阅 Amazon Resource Groups 用户指南中的什么是 Resource Groups？

您可以在单个资源组中包含具有不同属性（实例类型、平台和可用区）的多个容量预留。

为容量预留创建 Resource Groups 时，可以将实例定位到一组容量预留，而不是单个容量预留。定位到一组容量预留的实例与该组中具有匹配属性（实例类型、平台和可用区）和可用容量的任何容量预留匹配。如果该组中没有具有匹配属性和可用容量的容量预留，相关实例将会使用按需容量运行。如果稍后将匹配的容量预留添加到目标组中，则实例将自动与其预留容量匹配并移动到该容量中。

为防止意外使用组中的容量预留，请将组中的容量预留配置为仅接受明确定位到该容量预留的实例。为此，在使用 Amazon EC2 控制台创建容量预留时，请将实例资格设置为目标（旧控制台）或仅指定此预留的实例（新控制台）。如果使用 Amazon CLI，请在创建容量预留时指定 `--instance-match-criteria targeted`。这样做可确保只有明确定位到该组或该组中的某个容量预留的实例才能在该组中运行。

如果组中的容量预留在其中的实例正在运行时被取消或过期，则这些实例会自动移动到该组中具有匹配属性和可用容量的另一个容量预留中。如果该组中没有其他具有匹配属性和可用容量的容量预留，则实例将使用按需容量运行。如果稍后将匹配的容量预留添加到目标组中，则实例将自动移动到其预留容量中。

为容量预留创建组

使用 create-group Amazon CLI 命令。对于 `name`，请为组提供一个描述性名称，对于 `configuration`，请指定 2 个 `Type` 请求参数：

- `AWS::EC2::CapacityReservationPool`，可确保资源组可以作为实例启动的目标
- `AWS::ResourceGroups::Generic`，并将 `allowed-resource-types` 设置为 `AWS::EC2::CapacityReservation`，可确保资源组仅接受容量预留

例如，以下命令将创建一个名为 `MyCRGroup` 的组。

```
$ aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}' '{"Type":"AWS::ResourceGroups::Generic",
 "Parameters": [{"Name": "allowed-resource-types", "Values":
 ["AWS::EC2::CapacityReservation"]}]}'
```

下面显示了示例输出。

```
{
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
```

```
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

向组中添加容量预留

使用 group-resources Amazon CLI 命令。对于 `group`，请指定要添加容量预留的组的名称，对于 `resources`，请指定要添加的容量预留的 ARN。若要添加多个容量预留，请用空格分隔 ARN。要获取要添加的容量预留的 ARN，请使用 describe-capacity-reservations Amazon CLI 命令并指定容量预留的 ID。

例如，以下命令会将 2 个容量预留添加到名为 `MyCRGroup` 的组中。

```
$ aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

下面显示了示例输出。

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

查看特定组中的容量预留

使用 list-group-resources Amazon CLI 命令。对于 `group`，请指定组的名称。

例如，以下命令会列出名为 `MyCRGroup` 的组中的容量预留。

```
$ aws resource-groups list-group-resources --group MyCRGroup
```

下面显示了示例输出。

```
{
    "QueryErrors": [],
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
```

```
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

查看添加了特定容量预留的组 (Amazon CLI)

使用 get-groups-for-capacity-reservation Amazon CLI 命令。

例如，以下命令会列出添加了容量预留 cr-1234567890abcdef1 的组。

```
$ aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

下面显示了示例输出。

```
{
    "CapacityReservationGroups": [
        {
            "OwnerId": "123456789012",
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup"
        }
    ]
}
```

查看添加了特定容量预留的组（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择容量预留，再选择要查看的容量预留，然后选择查看。

   组选项卡中会列出添加了容量预留的组。

从组中删除容量预留

使用 ungroup-resources Amazon CLI 命令。对于 group，请指定要从中删除容量预留的组的 ARN，对于 resources，请指定要删除的容量预留的 ARN。若要添加多个容量预留，请用空格分隔 ARN。

以下示例会从名为 MyCRGroup 的组中删除 2 个容量预留。

```
$ aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-
east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-
east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

下面显示了示例输出。

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

删除组

使用 delete-group Amazon CLI 命令。对于 group，提供要删除的组的名称。

例如，以下命令会删除名为 MyCRGroup 的组。

```
$ aws resource-groups delete-group --group MyCRGroup
```

下面显示了示例输出。

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

集群置放群组中的容量预留

您可以在集群置放群组中创建容量预留，以便为您的工作负载预留 Amazon EC2 计算容量。集群置放群组具有低网络延迟和高网络吞吐量的好处。

在集群置放群组中创建容量预留可以确保您在需要时访问集群置放群组中的计算容量。这非常适合为需要计算扩缩的高性能 (HPC) 工作负载预留容量。它允许您向下扩展群集，同时确保容量仍可供您使用，以便在需要时可以扩展备份。

主题

- 限制 (p. 550)
- 使用集群置放群组中的容量预留 (p. 550)

限制

在集群置放群组中创建容量预留时，请牢记以下几点：

- 您无法修改不在置放群组中的现有容量预留以在置放群组中预留容量。要在置放群组中预留容量，您必须在置放群组中创建容量预留。
- 在置放群组中创建容量预留后，您无法对其进行修改以在置放群组之外预留容量。
- 您可以通过修改置放群组中的现有容量预留或在置放群组中创建其他容量预留来增加置放群组中的预留容量。但是，您增加了出现容量不足错误的机会。
- 您无法共享在集群置放群组中创建的容量预留。
- 您无法删除具有 active 容量预留的集群置放群组。删除前，您必须先取消集群置放群组中的所有容量预留。

使用集群置放群组中的容量预留

要开始对集群置放群组使用容量预留，请执行以下步骤。

> **Note**
>
> 如果要在现有集群置放群组中创建容量预留，请跳过步骤 1。然后，对于步骤 2 和 3，请指定现有集群置放群组的 ARN。有关如何查找现有集群置放群组的 ARN 的更多信息，请参阅 describe-placement-groups。

主题

- 步骤 1：（条件）创建用于容量预留的集群置放群组 (p. 551)
- 步骤 2：在集群置放群组中创建容量预留 (p. 551)

- 步骤 3：在集群置放群组中启动实例 (p. 552)

步骤 1：（条件）创建用于容量预留的集群置放群组

仅在需要创建新的集群置放群组时，执行此步骤。要使用现有的集群置放群组，请跳过此步骤，然后对于步骤 2 和 3，使用该集群置放群组的 ARN。有关如何查找现有集群置放群组的 ARN 的更多信息，请参阅 describe-placement-groups。

您可以使用以下一种方法创建集群置放群组。

Console

使用控制台创建集群置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Placement Groups（置放群组），然后选择 Create placement group（创建置放群组）。
3. 对于 Name（名称），为置放群组指定一个描述性名称。
4. 对于 Placement strategy（置放策略），选择 Cluster（集群）。
5. 选择创建组。
6. 找到您创建的集群置放群组的 ARN。

```
$ aws ec2 describe-placement-groups --group-names placement_group_name
```

请记下命令输出中返回的置放群组 ARN，因为下一个步骤需要用到。

Amazon CLI

使用 Amazon CLI 创建集群置放群组

使用 create-placement-group 命令。对于 `--group-name`，为置放群组指定一个描述性名称，对于 `--strategy`，请指定 `cluster`。

以下示例创建一个名为 `MyPG` 的使用 `cluster` 置放策略的置放群组。

```
$ aws ec2 create-placement-group \
--group-name MyPG \
--strategy cluster
```

请记下命令输出中返回的置放群组 ARN，因为下一个步骤需要用到。

步骤 2：在集群置放群组中创建容量预留

在集群置放群组中创建容量预留的方式与创建任何容量预留的方式相同。但是，您还必须指定要在其中创建容量预留的集群置放群组的 ARN。有关更多信息，请参阅创建 容量预留 (p. 542)。

注意事项

- 指定的集群置放群组必须处于 `available` 状态。如果集群置放群组处于 `pending`、`deleting` 或 `deleted` 状态，则请求将失败。
- 容量预留和集群置放群组必须位于同一可用区。如果创建容量预留的请求指定的可用区与集群置放群组的可用区不同，则请求将失败。
- 您只能为集群置放群组支持的实例类型创建容量预留。如果您指定了不受支持的实例类型，则请求将失败。有关更多信息，请参阅集群置放群组规则和限制 (p. 1179)。

- 如果您在集群置放群组中创建 open 容量预留，并且现有正在运行的实例具有匹配属性（置放群组 ARN、实例类型、可用区、平台和租期），这些实例将在容量预留中自动运行。
- 如果出现以下情况之一，创建容量预留的请求会失败：
  - Amazon EC2没有足够的容量来满足请求。请稍后重试、尝试不同的可用区或者尝试较小的容量。如果您的工作负载灵活地跨实例类型和大小，请尝试不同的实例属性。
  - 请求的数量超过选定实例系列的个按需型实例限制。增加该实例系列的个按需型实例限制，然后重试。有关更多信息，请参阅个按需型实例限制 (p. 406)。

您可以使用以下一种方法在集群置放群组中创建容量预留。

Console

使用控制台创建容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 容量预留 (容量预留)，然后选择 Create 容量预留 (创建容量预留)。
3. 在 Create a Capacity Reservation（创建容量预留）页面上，根据需要配置实例类型、平台、可用区、租赁、数量和结束日期。
4. 对于 Placement group ARN（置放群组 ARN），请指定要在其中创建容量预留的集群置放群组的 ARN。
5. 选择 Create（创建）。

有关更多信息，请参阅创建 容量预留 (p. 542)。

Amazon CLI

使用 Amazon CLI 创建容量预留

使用 create-capacity-reservation 命令。对于 `--placement-group-arn`，请指定要在其中创建容量预留的集群置放群组的 ARN。

```
$ aws ec2 create-capacity-reservation \
--instance-type instance_type \
--instance-platform platform \
--availability-zone az \
--instance-count quantity \
--placement-group-arn placement_group_ARN
```

有关更多信息，请参阅创建 容量预留 (p. 542)。

步骤 3：在集群置放群组中启动实例

您将实例启动到集群置放群组的容量预留中，与在任何容量预留中启动实例的方式相同。但是，您还必须指定要在其中启动实例的集群置放群组的 ARN。有关更多信息，请参阅创建 容量预留 (p. 543)。

注意事项

- 如果容量预留为 open，您无需在实例启动请求中指定容量预留。如果实例具有匹配指定置放群组中的容量预留的属性（置放群组 ARN、实例类型、可用区、平台和租期），这些实例将在容量预留中自动运行。
- 如果容量预留仅接受目标实例启动，则除了请求中的集群置放群组之外，还必须指定目标容量预留。
- 如果容量预留在容量预留组中，则除了请求中的集群置放群组之外，还必须指定目标容量预留组。有关更多信息，请参阅使用 容量预留 组 (p. 547)。

您可以使用以下一种方法将实例启动到集群置放群组中的容量预留。

Console

使用控制台在现有容量预留中启动实例

1. 通过从控制面板或 Instances（实例）屏幕选择 Launch Instances（启动实例）来打开启动实例向导。
2. 选择 Amazon Machine Image (AMI) 和实例类型。
3. 完成 Configure Instance Details（配置实例详细信息）页面：
   a. 对于 Placement group（置放群组），选择 Add instance to placement group（将实例添加到置放群组），选择 Add to existing placement group（添加到现有置放群组），然后选择要在其中启动实例的集群置放群组。
   b. 对于 Capacity Reservation（容量预留），请选择以下选项之一，具体取决于容量预留的配置：
      - Open（打开）— 将实例启动到集群置放群组中任何具有匹配属性和足够容量的 open 容量预留。
      - Target by ID（按 ID 定位）— 将实例启动到只接受目标实例启动的容量预留中。
      - Target by group（按组定位）— 在所选容量预留组中任何具有匹配属性和可用容量的容量预留中启动实例。
4. 完成剩余步骤以启动实例。

有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。

Amazon CLI

使用 Amazon CLI 在现有容量预留中启动实例

可以使用 run-instances 命令。如果您需要定位特定容量预留或容量预留组，请指定 `--capacity-reservation-specification` 参数。对于 `--placement`，请指定 `GroupName` 参数，然后指定您在上述步骤中创建的置放群组的名称。

以下命令将实例启动到集群置放群组中的 `targeted` 容量预留。

```
$ aws ec2 run-instances \
--image-id ami_id \
--count quantity \
--instance-type instance_type \
--key-name key_pair_name \
--subnet-id subnetid \
--capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
--placement "GroupName=cluster_placement_group_name"
```

有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。

Local Zones 中的容量预留

本地区域是在地理位置上靠近用户的Amazon区域的扩展。在本地区域中创建的资源可以通过非常低延迟的通信为本地用户提供服务。有关更多信息，请参阅 Amazon Local Zones。

您可以通过在本地区域中创建新的子网，将 VPC 从其父Amazon区域扩展到该本地区域。当您在本地扩展区中创建子网时，VPC 也会扩展到该本地扩展区。本地区域中的子网与 VPC 中其他子网的运行相同。

通过使用 Local Zones，您可以将容量预留放在更靠近用户的多个位置。您可以按照在常规可用区中创建和使用容量预留的方法，在 Local Zones 中创建和使用容量预留。相同的功能和实例匹配行为适用。有关在 Local Zones 中支持的定价模式的更多信息，请参阅 Amazon Local Zones 常见问题解答。

注意事项

您不能在本地区域中使用容量预留组。

在本地区域中使用容量预留

1. 启用本地区域以在您的Amazon账户中使用。有关更多信息，请参阅选择加入 Local Zones (p. 1049)。
2. 在本地区域中创建容量预留。对于 Availability Zone (可用区)，选择本地区域。本地区域由Amazon区域代码后跟一个指示位置的标识符表示，例如 `us-west-2-lax-1a`。有关更多信息，请参阅创建 容量预留 (p. 542)。
3. 在本地扩展区中创建子网。对于 Availability Zone (可用区)，选择本地区域。有关更多信息，请参阅 Amazon VPC 用户指南 中的在 VPC 中创建子网。
4. 启动一个实例。对于 Subnet (子网)，在本地区域（例如 `subnet-123abc | us-west-2-lax-1a`）中选择子网，对于 Capacity Reservation (容量预留)，选择您在本地区域中创建的容量预留所需的规格（可以为 `open` 或按 ID 定位）。有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。

Wavelength 区中的 容量预留

利用 Amazon Wavelength，开发人员可以为移动设备和最终用户打造具有超低延迟的应用程序。Wavelength 可以将标准 Amazon 计算和存储服务部署到电信运营商的 5G 网络边缘。您可以将 Amazon Virtual Private Cloud (VPC) 扩展到一个或多个 Wavelength 区域。然后，您可以使用 Amazon EC2 实例之类的Amazon资源来运行需要超低延迟和连接到该区域中的Amazon服务的应用程序。有关更多信息，请参阅 Amazon Wavelength 域。

创建按需 容量预留 时，您可以选择 Wavelength 区域，然后通过指定与 Wavelength 区域关联的子网，将实例启动到 Wavelength 区域内的 容量预留 中。Wavelength 区域由Amazon区域代码后跟一个指示位置的标识符表示，例如 `us-east-1-wl1-bos-wlz-1`。

Wavelength 区域并非在每个区域中都可用。有关支持 Wavelength 区域的区域的信息，请参阅 Amazon Wavelength 开发人员指南中的可用 Wavelength 区域。

注意事项

您不能在 Wavelength 区中使用 容量预留 组。

在 Wavelength 区中使用 容量预留

1. 启用 Wavelength 区域以在您的Amazon账户中使用。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的启用 Wavelength 区。
2. 在 Wavelength 区中创建 容量预留。对于可用区，选择 Wavelength。Wavelength 由Amazon区域代码后跟一个指示位置的标识符表示，例如 `us-east-1-wl1-bos-wlz-1`。有关更多信息，请参阅创建 容量预留 (p. 542)。
3. 在 Wavelength 区中创建子网。对于可用区，选择 Wavelength 区。有关更多信息，请参阅 Amazon VPC 用户指南 中的在 VPC 中创建子网。
4. 启动一个实例。对于子网，在 Wavelength 区（例如 `subnet-123abc | us-east-1-wl1-bos-wlz-1`）中选择子网，对于容量预留，选择您在 Wavelength 中创建的 容量预留 所需的规格（可以为 `open` 或按 ID 定位）。有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。

使用共享 容量预留

容量预留共享使容量预留拥有者能够与其他Amazon账户或在Amazon组织内共享其预留容量。这使您能够集中创建和管理容量预留，并跨多个Amazon账户或在Amazon组织内共享预留容量。

在此模型中，拥有容量预留的Amazon账户（拥有者）将与其他Amazon账户（使用者）共享它。使用者可以在与其共享的容量预留中启动实例，所用方式与他们在自己的账户中拥有的容量预留中启动实例的方式相

同。容量预留拥有者负责管理容量预留以及它们启动到其中的实例。拥有者无法修改使用者启动到已共享的容量预留中的实例。使用者负责管理启动到与其共享的容量预留中的实例。使用者无法查看或修改由其他使用者或容量预留拥有者拥有的实例。

容量预留拥有者可与以下对象共享容量预留：

- 其 Amazon 组织内部或外部的特定 Amazon 账户
- 其 Amazon 组织内的组织部门
- 其整个 Amazon 组织

目录

- 共享容量预留的先决条件 (p. 555)
- 相关服务 (p. 555)
- 跨可用区共享 (p. 555)
- 共享 容量预留 (p. 556)
- 停止共享容量预留 (p. 556)
- 标识和查看共享的容量预留 (p. 557)
- 查看共享 容量预留 使用情况 (p. 557)
- 共享的容量预留权限 (p. 558)
- 计费和计量 (p. 558)
- 实例限制 (p. 558)

共享容量预留的先决条件

- 要共享容量预留，您必须在您的Amazon账户拥有它。无法共享已与您共享的容量预留。
- 您只能为共享租赁实例共享 容量预留。您无法为专用租赁实例共享 容量预留。
- 容量预留共享不适用于新的Amazon账户或具有有限账单历史记录的Amazon账户。
- 要与您的Amazon组织或Amazon组织内的组织部门共享容量预留，您必须允许与 Amazon Organizations 共享。有关更多信息，请参阅 Amazon RAM 用户指南中的允许与 Amazon Organizations 共享。

相关服务

容量预留共享与 Amazon Resource Access Manager (Amazon RAM) 集成。Amazon RAM 是一项服务，允许您与任何Amazon账户或通过 Amazon Organizations 共享Amazon资源。利用 Amazon RAM，您可通过创建资源共享来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用者可以是单个 Amazon 账户或 Amazon Organizations 中的组织部门或整个组织。

Amazon RAM有关 的更多信息，请参阅 Amazon RAM 用户指南。

跨可用区共享

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的名称。这可能会导致账户之间的可用区命名差异。例如，您的 `us-east-1a` 账户的可用区 Amazon 可能与另一 `us-east-1a` 账户的 Amazon 不在同一位置。

要确定容量预留相对于账户的位置，您必须使用可用区 ID (AZ ID)。AZ ID 是跨所有 Amazon 账户的可用区的唯一且一致的标识符。例如，`use1-az1` 是 `us-east-1` 区域的 AZ ID，它在每个 Amazon 账户中的位置均相同。

查看账户中的可用区的 AZ ID

1. 通过以下网址打开 Amazon RAM 控制台：https://console.aws.amazon.com/ram。

2. 当前区域的 AZ ID 显示在屏幕右侧的 Your AZ ID (您的 AZ ID) 面板中。

共享 容量预留

在与其他Amazon账户共享您拥有的容量预留时，您必须启用它们以便将实例启动到预留容量中。如果您共享开放容量预留，请记住以下内容，因为它可能导致意外的容量预留使用：

- 如果使用者拥有与容量预留的属性匹配的运行中实例、已将 `CapacityReservationPreference` 参数设置为 `open` 且尚未在预留容量中运行，他们将自动使用共享容量预留。
- 如果使用者启动具有匹配属性（实例类型、平台和可用区）的实例，并且已将 `CapacityReservationPreference` 参数设置为 `open`，它们将自动启动到共享容量预留中。

要共享容量预留，您必须将它添加到资源共享。资源共享是一项 Amazon RAM 资源，可让您跨 Amazon 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。在使用 Amazon EC2 控制台共享容量预留时，必须将它添加到现有资源共享。要将容量预留添加到新的资源共享，您必须使用 Amazon RAM 控制台创建资源共享。

如果您属于 Amazon Organizations 中的某个企业并且已在您的组织中启用共享，当达到共享的先决条件 (p. 555)时，组织中的使用者将自动获得对所共享容量预留的访问权限。如果与外部账户共享了容量预留，他们会收到加入资源共享的邀请，并在接受邀请后获得对所共享容量预留的访问权限。

> **Important**
>
> 在与您共享的容量预留中启动实例之前，请通过以下任一方式验证您是否拥有访问共享的容量预留的权限：在控制台中进行查看，或使用 describe-capacity-reservations Amazon CLI 命令对其进行描述。如果您可以在控制台中查看共享的容量预留或者使用 Amazon CLI 描述它，即表示您可以使用它，并且可以在其中启动实例。如果您尝试在容量预留中启动实例，但由于共享失败而无法访问容量预留，则实例将在按需型容量中启动。

您可以使用 Amazon EC2 控制台、Amazon RAM 控制台或 Amazon CLI 共享您拥有的容量预留。

使用 Amazon EC2 控制台共享您拥有的容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择容量预留。
3. 选择要共享的容量预留，然后选择操作、共享预留。
4. 选择要将容量预留添加到的资源共享，然后选择共享容量预留。

   使用者可能需要几分钟的时间才能访问共享容量预留。

使用 Amazon RAM 控制台共享您拥有的容量预留

请参阅 Amazon RAM 用户指南中的创建资源共享。

使用 Amazon CLI 控制台共享您拥有的容量预留

使用 create-resource-share 命令。

停止共享容量预留

容量预留拥有者可以随时停止共享容量预留。以下规则适用：

- 在停止共享时在共享容量中运行的使用者所拥有的实例继续在预留容量之外正常运行，并且根据 Amazon EC2 容量可用性将容量还原到容量预留。
- 与之共享容量预留的使用者不再能够在预留容量中启动新实例。

要停止共享您拥有的共享容量预留，必须从资源共享中将其删除。您可以使用 Amazon EC2 控制台、Amazon RAM 控制台或 Amazon CLI 完成此操作。

使用 Amazon EC2 控制台停止共享您拥有的容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择容量预留。
3. 选择容量预留并选择共享选项卡。
4. 共享选项卡列出了已将容量预留添加到的资源共享。选择要从中删除容量预留的资源共享，然后选择从资源共享中删除。

使用 Amazon RAM 控制台停止共享您拥有的容量预留

请参阅 Amazon RAM 用户指南中的更新资源共享。

使用 Amazon CLI 控制台停止共享您拥有的容量预留

使用 disassociate-resource-share 命令。

标识和查看共享的容量预留

Important

在与您共享的容量预留中启动实例之前，请通过以下任一方式验证您是否拥有访问共享的容量预留的权限：在控制台中进行查看，或使用 Amazon CLI 对其进行描述。如果您可以在控制台中查看共享的容量预留或者使用 Amazon CLI 描述它，即表示您可以使用它，并且可以在其中启动实例。如果您尝试在容量预留中启动实例，但由于共享失败而无法访问容量预留，则实例将在按需型容量中启动。

拥有者和使用者可以使用 Amazon EC2 控制台及 Amazon CLI 标识和查看共享的容量预留。

使用 Amazon EC2 控制台标识共享的容量预留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择容量预留。屏幕列出了您拥有的容量预留以及与您共享的容量预留。Owner (拥有者) 列显示了容量预留拥有者的Amazon账户 ID。Amazon账户 ID 旁边的（me）指示您是拥有者。

使用 Amazon CLI 标识共享的容量预留

使用 describe-capacity-reservations 命令。此命令返回您拥有的容量预留以及与您共享的容量预留。`OwnerId` 显示容量预留拥有者的Amazon账户 ID。

查看共享 容量预留 使用情况

共享的容量预留的拥有者可随时使用 Amazon EC2 控制台和 Amazon CLI 查看其使用情况。

使用 Amazon EC2 控制台查看容量预留的使用情况

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择容量预留。
3. 选择要查看其使用情况的容量预留，然后选择使用情况选项卡。

   Amazon account ID (亚马逊云科技账户 ID) 列显示了当前使用容量预留的使用者的账户 ID。启动的实例列显示了每个使用者当前在预留容量中运行的实例数。

使用 Amazon CLI 查看容量预留的使用情况

使用 get-capacity-reservation-usage 命令。`AccountId` 显示使用容量预留的账户的 ID。`UsedInstanceCount` 显示使用者当前在预留容量中运行的实例数。

共享的容量预留权限

拥有者的权限

拥有者负责管理和取消其共享的容量预留。拥有者无法修改由其他账户拥有的共享容量预留中运行的实例。拥有者仍然负责管理其启动到共享的容量预留中的实例。

使用者的权限

使用者负责管理其正在运行共享的容量预留的实例。使用者不能以任何方式修改共享的容量预留，也不能查看或修改由其他使用者或容量预留拥有者拥有的实例。

计费和计量

共享容量预留不会产生额外的费用。

容量预留拥有者需要为他们在容量预留内部运行的实例以及未使用的预留容量付费。使用者需要为他们在共享的容量预留中运行的实例付费。

如果容量预留所有者属于不同的付款人账户，并且容量预留由区域预留实例或 Savings Plan 承保，则容量预留所有者将继续为区域预留实例或 Savings Plan 付费。在这些情况下，容量预留所有者将为区域预留实例或 Savings Plan 付费，使用者需要为在共享容量预留中运行的实例付费。

实例限制

所有容量预留使用量都计入容量预留拥有者的个按需型实例限制。这包括：

- 未使用的预留容量
- 容量预留拥有者拥有的实例的使用情况
- 使用者拥有的实例的使用情况

使用者在共享容量中启动的实例将计入容量预留拥有者的个按需型实例限制。使用者的实例限制是他们自己的个按需型实例限制和他们可以访问的共享容量预留中的可用容量的总和。

容量预留机群

按需容量预留机群是一组容量预留。

容量预留机群请求包含启动容量预留机群所需的所有配置信息。使用单个请求，您可以跨多个实例类型为您的工作负载预留大量 Amazon EC2 容量，最多可达到您指定的目标容量。

创建容量预留机群后，您可以通过修改或取消容量预留机群来集体管理机群中的容量预留。

主题

- 容量预留机群的工作原理 (p. 179)
- 注意事项 (p. 399)
- 定价 (p. 559)
- 容量预留机群概念 (p. 559)
- 使用容量预留机群 (p. 560)
- 容量预留机群配置示例 (p. 566)
- 将服务相关角色用于容量预留实例集 (p. 567)

容量预留机群的工作原理

创建容量预留机群时，机群会尝试创建单个容量预留以满足您在机群请求中指定的总目标容量。

实例集为其预留容量的实例数取决于您指定的总目标容量 (p. 559)和实例类型权重 (p. 560)。实例集为其预留容量的实例类型取决于您使用的分配策略 (p. 560)和实例类型优先级 (p. 560)。

如果机群创建时容量不足，且无法立即满足其总目标容量，则机群会异步尝试创建容量预留，直到其预留了请求的容量为止。

当机群达到其总目标容量时，它会尝试维持该容量。如果机群中的容量预留被取消，机群将根据您的机群配置自动创建一个或多个容量预留，以替换丢失的容量并维持其总目标容量。

机群中的容量预留无法单独管理。它们必须通过修改机群进行集体管理。修改机群时，机群中的容量预留将自动更新以反映更改。

目前，容量预留机群支持 open 实例匹配条件，且机群启动的所有容量预留都会自动使用此实例匹配条件。在此条件下，具有匹配属性（实例类型、平台和可用区）的新实例和现有实例在机群创建的容量预留中自动运行。容量预留机群不支持 `target` 实例匹配条件。

注意事项

使用容量预留机群时，请记住以下事项：

- 容量预留机群可以使用 Amazon CLI 和 Amazon API 创建、修改、查看和取消。
- 机群中的容量预留无法单独管理。它们必须通过修改或取消机群进行集体管理。
- 容量预留机群不能跨区域。
- 容量预留机群不能跨可用区。
- 容量预留机群创建的容量预留会自动使用 Amazon 生成的以下标签进行标记：
  - 密钥 — `aws:ec2-capacity-reservation-fleet`
  - 值 — *`fleet_id`*

  您可以使用此标签来标识容量预留机群创建的容量预留。

定价

使用容量预留机群不会产生额外的费用。您需要为容量预留机群创建的单个容量预留付费。有关预留容量计费方式的更多信息，请参阅 容量预留定价和计费 (p. 540)。

容量预留机群概念

本主题介绍容量预留机群的一些概念。

主题

- 总目标容量 (p. 559)
- 分配策略 (p. 560)
- 实例类型权重 (p. 560)
- 实例类型优先级 (p. 560)

总目标容量

总目标容量定义容量预留机群预留的总计算容量。在创建容量预留机群时，您需要指定总目标容量。机群创建后，Amazon EC2 会自动创建容量预留，以预留最高可达到总目标容量的容量。

容量预留机群为其预留容量的实例的数量取决于总目标容量和您在容量预留机群中为每个实例类型指定的实例类型权重 (`total target capacity/instance type weight=number of instances`)。

您可以根据对您的工作负载有意义的单位分配总目标容量。例如，如果您的工作负载需要一定数量的 vCPU，则可以根据所需的 vCPU 数量分配总目标容量。如果您的工作负载需要 2048 个 vCPU，则指定总目标容量 2048，然后根据机群中的实例类型提供的 vCPU 数量分配实例类型权重。有关示例，请参阅 实例类型权重 (p. 560)。

分配策略

容量预留机群的分配策略决定了如何根据容量预留机群配置中的实例类型规范来满足针对预留容量的请求。

目前，仅支持 `prioritized` 分配策略。通过此策略，容量预留机群使用您在容量预留机群配置中为每个实例类型规范分配的优先级来创建容量预留。优先级值越低表示使用优先级越高。例如，假设您创建了使用以下实例类型和优先级的容量预留机群：

- `m4.16xlarge` — 优先级 = 1
- `m5.16xlarge` — 优先级 = 3
- `m5.24xlarge` — 优先级 = 2

机群首先尝试为 `m4.16xlarge` 创建容量预留。如果 Amazon EC2 的 `m4.16xlarge` 容量不足，机群将尝试为 `m5.24xlarge` 创建容量预留。如果 Amazon EC2 的 `m5.24xlarge` 容量不足，机群将为 `m5.16xlarge` 创建容量预留。

实例类型权重

实例类型权重是您分配给容量预留机群中每种实例类型的权重。权重决定了该指定实例类型的每个实例计入机群的总目标容量的容量单位数。

您可以根据对您的工作负载有意义的单位分配权重。例如，如果您的工作负载需要一定数量的 vCPU，则可以根据容量预留机群中每种实例类型提供的 vCPU 数量来分配权重。在这种情况下，如果您使用 `m4.16xlarge` 和 `m5.24xlarge` 实例创建容量预留机群，您将为每个实例分配与 vCPU 数量对应的权重，如下所示：

- `m4.16xlarge` — 64 个 vCPU，权重 = 64 个单位
- `m5.24xlarge` — 96 个 vCPU，权重 = 96 个单位

实例类型权重决定了容量预留机群为其预留容量的实例的数量。例如，如果总目标容量为 384 个单位的容量预留机群使用前面示例中的实例类型和权重，机群可以为 6 个 `m4.16xlarge` 实例（384 总目标容量/64 实例类型权重=6 个实例）或 4 个 `m5.24xlarge` 实例 (384 / 96 = 4) 预留容量。

如果您没有分配实例类型权重，或者您将实例类型权重分配为 1，则总目标容量完全基于实例数量。例如，如果总目标容量为 384 个单位的容量预留机群使用前面示例中的实例类型，但忽略权重或为这两种实例类型都指定了 1 的权重，则机群都可以为 384 个 `m4.16xlarge` 实例或 384 个 `m5.24xlarge` 实例预留容量。

实例类型优先级

实例类型优先级是您分配给机群中的实例类型的值。优先级用于确定为机群指定的哪些实例类型应优先使用。

优先级值越低表示使用的优先级越高。

使用容量预留机群

主题

- 开始前的准备工作 (p. 561)
- 容量预留机群状态 (p. 561)
- 创建容量预留机群 (p. 561)

- 查看容量预留机群 (p. 563)
- 修改容量预留机群 (p. 564)
- 取消容量预留机群 (p. 565)

开始前的准备工作

在创建容量预留机群之前：

1. 确定您的工作负载所需的计算容量。
2. 决定要使用的实例类型和可用区。
3. 根据您的需求和首选项为每种实例类型分配优先级。有关更多信息，请参阅实例类型优先级 (p. 560)。
4. 创建对您的工作负载有意义的容量加权系统。为每种实例类型分配权重并确定您的总目标容量。有关更多信息，请参阅 实例类型权重 (p. 560) 和 总目标容量 (p. 559)。
5. 确定您是无限期需要容量预留还是仅在指定时间段内需要容量预留。

容量预留机群状态

容量预留机群可以处于以下某种状态：

- `submitted` — 容量预留机群请求已提交，且 Amazon EC2 正在准备创建容量预留。
- `modifying` — 容量预留机群正在修改中。在修改完成之前，机群将保持这一状态。
- `active` — 容量预留机群已实现其总目标容量，并正在尝试维持此容量。机群会保持这一状态，直到其被修改或删除。
- `partially_fulfilled` — 容量预留机群已部分实现其总目标容量。Amazon EC2 容量不足，无法实现总目标容量。机群正在尝试异步实现其总目标容量。
- `expiring` — 容量预留机群已到达结束日期，目前正在到期的过程中。其中一个或多个容量预留可能仍处于活动状态。
- `expired` — 容量预留机群已到达结束日期。机群及其容量预留已过期。机群无法创建新的容量预留。
- `cancelling` — 容量预留机群正在取消过程中。其中一个或多个容量预留可能仍处于活动状态。
- `cancelled` — 容量预留机群已手动取消。机群及其容量预留已被取消，而且机群无法创建新的容量预留。
- `failed` — 容量预留机群未能为指定的实例类型预留容量。

创建容量预留机群

当您创建容量预留机群时，它会自动为机群请求中指定的实例类型创建容量预留，最多可达到指定的总目标容量。容量预留机群为其预留容量的实例数取决于总目标容量和您在请求中指定的实例类型权重。有关更多信息，请参阅 实例类型权重 (p. 560) 和 总目标容量 (p. 559)。

创建机群时，您必须指定要使用的实例类型以及每种实例类型的优先级。有关更多信息，请参阅 分配策略 (p. 560) 和 实例类型优先级 (p. 560)。

> **Note**
>
> Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 服务相关角色在您首次创建容量预留机群时将在您的账户中自动创建。有关更多信息，请参阅将服务相关角色用于容量预留实例集 (p. 567)。

目前，容量预留机群仅支持 open 实例匹配条件。

您只能使用命令行创建容量预留机群。

要创建容量预留机群

使用 create-capacity-reservation-fleet Amazon CLI 命令。

```
$ aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

下面是 instanceTypeSpecification.json 的内容。

```
{
    "InstanceType": "instance_type",
    "InstancePlatform":"platform",
    "Weight": instance_type_weight
    "AvailabilityZone":"availability_zone",
    "AvailabilityZoneId" : "az_id",
    "EbsOptimized": true|false,
    "Priority" : instance_type_priority
}
```

预期输出。

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
}
```

示例

```
$ aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

instanceTypeSpecification.json

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

输出示例。

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
```

```
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

查看容量预留机群

您可以随时查看容量预留机群的配置和容量信息。查看机群还提供了有关机群内部各个容量预留的详细信息。

您只能使用命令行查看容量预留机群。

要查看容量预留机群

使用 describe-capacity-reservation-fleets Amazon CLI 命令。

```
$ aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

预期输出

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

示例

```
$ aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

输出示例

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

修改容量预留机群

您可以随时修改容量预留机群的总目标容量和日期。当您修改容量预留机群的总目标容量时，机群会自动创建新的容量预留，或者修改或取消机群中的现有容量预留以满足新的总目标容量。当您修改机群的结束日期时，所有单个容量预留的结束日期都会相应更新。

修改机群后，其状态将转换为 `modifying`。当机群处于 `modifying` 状态时，您无法尝试对其进行其他修改。

您无法修改容量预留机群使用的租赁、可用区、实例类型、实例平台、优先级或权重。如果您需要更改这些参数中的任何一个，您可能需要取消现有机群并创建具有所需参数的新机群。

您只能使用命令行修改容量预留机群。

要修改容量预留机群

使用 modify-capacity-reservation-fleet Amazon CLI 命令。

> **Note**
>
> 您不能在同一个命令中指定 `--end-date` 和 `--remove-end-date`。

```
$ aws ec2 modify-capacity-reservation-fleet \
```

```
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

预期输出

```
{
    "Return": true
}
```

示例：修改总目标容量

```
$ aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

示例：修改结束日期

```
$ aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

示例：删除结束日期

```
$ aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

输出示例

```
{
    "Return": true
}
```

取消容量预留机群

当您不再需要容量预留机群及其预留的容量时，可以取消它。当您取消机群时，机群状态将更改为 `cancelled`，且其不能再创建新的容量预留。此外，机群中的所有单个容量预留都将被取消，之前在预留容量中运行的实例将继续以共享容量正常运行。

您只能使用命令行取消容量预留机群。

要取消容量预留机群

使用 cancel-capacity-reservation-fleet Amazon CLI 命令。

```
$ aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

预期输出

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
```

```
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
              "Code": "code",
                    "Message": "message"
          }
         ]
     }
    ]
}
```

示例：成功取消

```
$ aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

输出示例

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

容量预留机群配置示例

主题

- 示例 1：基于 vCPU 数量预留容量 (p. 566)

示例 1：基于 vCPU 数量预留容量

以下示例创建了使用两种实例类型的容量预留机群：m5.4xlarge 和 m5.12xlarge。

它基于指定实例类型提供的 vCPU 数量使用权重系统。总目标容量是 480 个 vCPU。m5.4xlarge 提供 16 个 vCPU 并获取 16 的权重，m5.12xlarge 提供 48 个 vCPU 并获取 48 的权重。此权重系统对容量预留机群进行了配置，为 30 个 m5.4xlarge 实例 (480/16=30) 或 10 个 m5.12xlarge 实例 (480/48=10) 预留容量。

机群被配置为确定 m5.12xlarge 容量的优先级并获得优先级 1，而 m5.4xlarge 则会获得较低的优先级 2。这意味着机群首先将尝试预留 m5.12xlarge 容量，并在 Amazon EC2 的 m5.12xlarge 容量不足时仅尝试预留 m5.4xlarge 容量。

机群为 Windows 实例预留容量，且预留在 October 31, 2021 的 23:59:59 UTC 时会自动过期。

```
$ aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 48 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

下面是 instanceTypeSpecification.json 的内容。

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1",
        "EbsOptimized": true,
        "Priority" : 2
 },
 {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

将服务相关角色用于容量预留实例集

按需容量预留机群将使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与容量预留机群直接相关。服务相关角色由容量预留机群预定义，并包含该服务代表您调用其它 Amazon 服务所需的一切权限。

服务相关角色可让您更轻松地设置容量预留机群，因为您不必手动添加必要的权限。容量预留机群定义其服务相关角色的权限，除非另外定义，否则只有容量预留机群可以代入其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其它 IAM 实体的权限策略。

只有在首先删除相关资源后，才能删除服务相关角色。这将保护您的容量预留机群资源，因为您不会无意中删除对资源的访问权限。

容量预留实例集的服务相关角色权限

容量预留机群使用名为 Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 的服务相关角色创建、描述、修改和取消以前由容量预留机群代表您创建的容量预留。

Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 服务相关角色信任以下实体来代入角色：capacity-reservation-fleet.amazonaws.com。

该角色使用 AWSEC2CapacityReservationFleetRolePolicy 策略，其中包含以下权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-reservation-
fleet/crf-*"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

创建容量预留实例集的服务相关角色

无需手动创建服务相关角色。使用 `create-capacity-reservation-fleet` Amazon CLI 命令或 `CreateCapacityReservationFleet` API 创建容量预留机群时，系统将自动为您创建服务相关角色。

如果删除此服务相关角色，然后需要再次创建，可以使用相同流程在账户中重新创建此角色。创建容量预留机群时，容量预留机群会再次为您创建服务相关角色。

编辑容量预留实例集的服务相关角色

容量预留机群不允许您编辑 Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见 IAM 用户指南中的编辑服务相关角色。

删除容量预留实例集的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先删除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时容量预留机群服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除 Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 服务相关角色

1. 使用 `delete-capacity-reservation-fleet` Amazon CLI 命令或 `DeleteCapacityReservationFleet` API 删除您的账户中的容量预留机群。
2. 使用 IAM 控制台、Amazon CLI 或 Amazon API 删除 Amazon Web Services ServiceRoleForEC2CapacityReservationFleet 服务相关角色。有关更多信息，请参见 IAM 用户指南中的删除服务相关角色。

容量预留实例集服务相关角色支持的区域

容量预留机群支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Amazon 区域和终端节点。

按需容量预留的 CloudWatch 指标

使用 CloudWatch 指标，您可以通过设置 CloudWatch 警报以在达到使用情况阈值时通知您，高效地监控您的容量预留并识别未使用的容量。这可以帮助您保持恒定的容量预留卷并实现更高级别的利用率。

按需容量预留每五分钟向 CloudWatch 发送一次指标数据。对于处于活动状态少于五分钟的容量预留，不支持指标。

有关在 CloudWatch 控制台中查看指标的更多信息，请参阅使用 Amazon CloudWatch 指标。有关创建警报的更多信息，请参阅创建 Amazon CloudWatch 警报。

目录

- 容量预留使用情况指标 (p. 569)
- 容量预留指标维度 (p. 569)
- 查看用于 容量预留 的 CloudWatch 指标 (p. 570)

容量预留使用情况指标

`AWS/EC2CapacityReservations` 命名空间包括以下使用情况指标，可用于监控和维护在为预留指定的阈值内的按需容量。

指标	描述
`UsedInstanceCount`	当前正在使用的实例数。 单位：计数
`AvailableInstanceCount`	可用实例的数量。 单位：计数
`TotalInstanceCount`	您预留的实例总数。 单位：计数
`InstanceUtilization`	当前正在使用的预留容量实例的百分比。 单位：百分比

容量预留指标维度

您可以使用以下维度来优化上表中列出的指标。

维度	描述
CapacityReservationId	此全局唯一的维度仅筛选您为已识别的容量预留请求的数据。

查看用于 容量预留 的 CloudWatch 指标

指标首先按服务命名空间进行分组，然后按支持的维度进行分组。您可以按照以下过程查看容量预留的各项指标。

使用 CloudWatch 控制台查看容量预留指标

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 如果需要，可以更改区域。从导航栏中，选择您的容量预留所在的区域。有关更多信息，请参阅 Regions and Endpoints。
3. 在导航窗格中，选择指标。
4. 对于所有指标，选择 EC2 容量预留。
5. 选择按容量预留指标维度。指标将按 CapacityReservationId 分组。
6. 要对指标进行排序，请使用列标题。要为指标绘制图表，请选中该指标旁的复选框。

查看容量预留指标 (Amazon CLI)

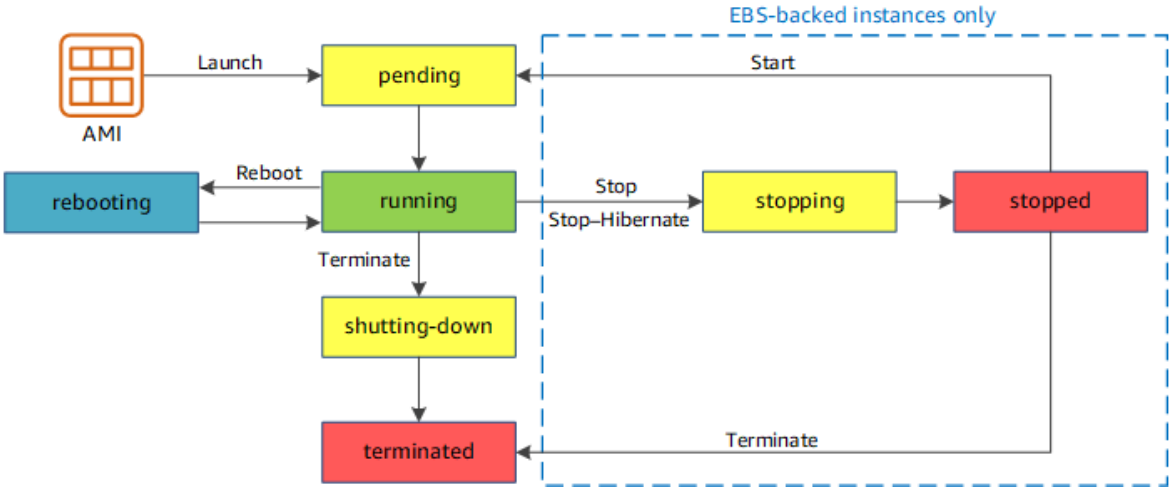
使用以下 list-metrics 命令：

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

实例生命周期

一个 Amazon EC2 实例从启动一直到其终止，将经过不同的状态转换。

下图显示实例状态之间的转换。请注意，您无法停止和启动实例存储支持的实例。有关实例存储支持实例的更多信息，请参阅根设备存储 (p. 103)。



下表提供了每个实例状态的简短说明，并指示它是否已计费。

Note

该表仅指示用于实例使用率的计费。一些Amazon资源（如 Amazon EBS 卷和弹性 IP 地址）无论实例的状态如何，都将产生费用。有关更多信息，请参阅 Amazon Billing 用户指南中的避免意外费用。

实例状态	描述	实例使用率计费
pending	实例正准备进入 running 状态。实例在首次启动时进入 pending 状态，或者在处于 stopped 状态后启动。	不计费
running	实例正在运行，并且做好了使用准备。	已计费
stopping	实例正准备处于停止状态或休眠停止状态。	如果准备停止，则不计费 如果准备休眠，则计费
stopped	实例已关闭，不能使用。可随时启动实例。	不计费
shutting-down	实例正准备终止。	不计费
terminated	实例已永久删除，无法启动。	不计费 Note 应用于已终止实例的预留实例将按照其付款选项进行计费，直到其期限结束。有关更多信息，请参阅 Reserved Instances (p. 408)

Note

重新启动实例不会启动新的实例计费周期，因为实例停留在 running 状态。

实例启动

当您启动实例时，实例进入 pending 状态。启动时指定的实例类型将决定您的实例的主机硬件。我们使用您在启动时指定的 Amazon Machine Image (AMI) 来启动实例。当实例准备就绪后，其进入 running 状态。您可以连接到正在运行的实例，然后像使用您面前的计算机一样来使用它。

只要您的实例转换为 running 状态，您就需要为实例运行的每一秒，至少一分钟付费，即使实例处于闲置状态并且您并未连接到实例也是如此。

有关更多信息，请参阅启动实例 (p. 574)和连接到您的 Linux 实例 (p. 644)。

实例停止和启动（仅限 Amazon EBS 支持的实例）

如果您的实例无法通过状态检查或未按预期运行应用程序，并且实例的根卷为 Amazon EBS 卷，则您可以先停止该实例再启动，以尝试解决该问题。

当您停止实例时，它会进入 stopping 状态，然后进入 stopped 状态。我们不对已停止的实例收取使用费或数据传输费，但会对所有 Amazon EBS 卷的存储收费。当实例处于 stopped 状态时，您可以修改实例的某些属性，包括实例类型。

当您启动实例时，它会进入 pending 状态，然后我们会将其移动到新的主机上（尽管在某些情况下，它仍将保留在当前主机上）。如果您停止并启动实例，将丢失先前主机的实例存储卷上的所有数据。

您的实例会保留其私有 IPv4 地址，这意味着与该私有 IPv4 地址或网络接口关联的弹性 IP 地址仍然与您的实例关联。如果您的实例具有 IPv6 地址，则它将保留其 IPv6 地址。

您每次将实例从stopped状态转换到running状态时，我们都按实例运行的每秒收费，您每次启动实例时至少一分钟。

有关更多信息，请参阅停止和启动您的实例 (p. 610)。

实例休眠（仅限 Amazon EBS 支持的实例）

当您使实例休眠时，我们向操作系统发出信号来执行休眠 (suspend-to-disk)，这会将实例内存 (RAM) 中的内容保存到您的 Amazon EBS 根卷。我们保留实例的 Amazon EBS 根卷以及任何附加的 Amazon EBS 数据卷。当您启动实例时，Amazon EBS 根卷将还原到其之前的状态，并且 RAM 内容将重新加载。之前附加的数据卷会重新附加，实例也会保留其实例 ID。

当您将实例休眠时，它会进入 stopping 状态，然后进入 stopped 状态。当已休眠的实例处于 stopped 状态时，我们不会对其收取使用费，但是这些实例处于 stopping 状态时，这与您停止实例 (p. 571)而未将其休眠时不同，我们会对其进行收费。我们不收取数据传输费，但我们会对所有 Amazon EBS 卷的存储（包括 RAM 数据的存储）收费。

当您启动休眠实例时，它会进入 pending 状态，然后我们会将其移动到新的主机上（尽管在某些情况下，它仍将保留在当前主机上）。

您的实例会保留其私有 IPv4 地址，这意味着与该私有 IPv4 地址或网络接口关联的弹性 IP 地址仍然与您的实例关联。如果您的实例具有 IPv6 地址，则它将保留其 IPv6 地址。

有关更多信息，请参阅休眠 Linux 按需型实例 (p. 616)。

实例重启

您可以使用 Amazon EC2 控制台、命令行工具和 Amazon EC2 API 来重启实例。我们建议您使用 Amazon EC2 来重启实例，而非在实例中运行操作系统重启命令。

重启实例相当于重启操作系统。实例位于同一主机上并保留其公有 DNS 名称、私有 IP 地址以及其实例存储卷上的所有数据。完成重启通常需要花费几分钟的时间，该时间具体取决于实例配置。

重启实例不会启动新的实例计费周期；将继续按秒计费，不再收取最低一分钟的费用。

有关更多信息，请参阅重启实例 (p. 631)。

实例指令引退

实例计划在 Amazon 检测到托管实例的基础硬件发生无法弥补的故障时停用。等到实例的计划停用日期，便会停止或终止实例Amazon 如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

有关更多信息，请参阅实例指令引退 (p. 632)。

实例终止

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 shutting-down 或 terminated，就不再产生与该实例相关的费用。

如果您启用终止保护，则无法使用控制台、CLI 或 API 终止实例。

在您终止实例之后，短时间内仍可在控制台中看见该实例，然后该条目将自动被删除。您还可以使用 CLI 和 API 来描述已终止的实例。资源 (例如标签) 会逐步与终止的实例取消关联，因此过一小段时间后，它们可能在终止的实例上不再可见。您无法连接到或恢复已终止的实例。

Amazon EBS 支持的每个实例都支持 `InstanceInitiatedShutdownBehavior` 属性，该属性决定当从实例内部启动关闭命令时（例如，在 Linux 上使用 shutdown 命令），实例是停止还是终止。默认行为是停止实例。您可以在实例运行或停止时修改此属性的设置。

每个 Amazon EBS 卷都支持 `DeleteOnTermination` 属性，该属性控制当您终止卷所连接的实例时是删除还是保留该卷。默认为删除根设备卷并保留所有其他 EBS 卷。

有关更多信息，请参阅终止实例 (p. 634)。

重启、停止、休眠和终止之间的区别

下表总结了重启、停止、休眠与终止实例之间的主要区别。

特征	重启	停止/启动 (仅限 Amazon EBS 支持的实例)	休眠（仅限 Amazon EBS 支持的实例）	终止
主机	实例保持在同一主机上运行	我们会将实例移动到新的主机上（尽管在某些情况下，它仍将保留在当前主机上）。	我们会将实例移动到新的主机上（尽管在某些情况下，它仍将保留在当前主机上）。	无
私有和公有 IPv4 地址	这些地址保持不变	实例保留其私有 IPv4 地址。实例将获取新的公有 IPv4 地址，除非它具有弹性 IP 地址 (该地址在停止/启动过程中不更改)。	实例保留其私有 IPv4 地址。实例将获取新的公有 IPv4 地址，除非它具有弹性 IP 地址 (该地址在停止/启动过程中不更改)。	无
弹性 IP 地址 (IPv4)	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址仍旧与实例相关联	弹性 IP 地址不再与实例相关联
IPv6 地址	地址保持不变	实例保留其 IPv6 地址	实例保留其 IPv6 地址	无
实例存储卷	数据保留	数据将擦除	数据将擦除	数据将擦除
根设备卷	卷将保留	卷将保留	卷将保留	默认情况下将删除卷
RAM（内存中的内容）	RAM 将擦除	RAM 将擦除	RAM 将保存到根卷上的某一文件	RAM 将擦除
计费	实例计费小时不更改。	实例的状态一旦变为 `stopping`，就不再产生与该实例相关的费用。实例每次从`stopped`转换为`running`时，我们都会启动新的实例计费周期，您每次启动实例时，最低收取一分钟费用。	当实例处于 `stopping` 状态时，将会产生费用；但实例处于 `stopped` 状态时，将会停止产生费用。实例每次从`stopped`转换为`running`时，我们都会启动新的实例计费周期，您每次启动实例时，最低收取一分钟费用。	实例的状态一旦变为 `shutting-down`，就不再产生与该实例相关的费用。

操作系统的关闭命令始终会终止实例存储支持的实例。您可以控制操作系统关闭命令是停止还是终止 Amazon EBS 支持的实例。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。

启动实例

实例是 Amazon 云中的虚拟服务器。您可以从 Amazon Machine Image (AMI) 中启动实例。AMI 为实例提供操作系统、应用程序服务器和应用程序。

注册 Amazon 后，您可以通过AmazonFree Tier（免费套餐）开始免费使用 Amazon EC2。您可以使用免费套餐在 12 个月内免费启动和使用 `t2.micro` 实例（在 `t2.micro` 不可用的区域，您可以使用免费套餐下的 `t3.micro` 实例）。如果您启动不在免费套餐范围内的实例，则需要为该实例支付标准 Amazon EC2 使用费。有关更多信息，请参阅Amazon EC2定价。

您可以使用以下方法启动实例。

方法	文档
[Amazon EC2 控制台] 使用启动实例向导指定启动参数。	使用旧的启动实例向导启动实例 (p. 583)
[Amazon EC2控制台] 创建启动模板并通过启动模板启动实例。	通过启动模板启动实例 (p. 588)
[Amazon EC2 控制台] 将现有实例作为基础。	使用来自现有实例的参数启动实例 (p. 607)
[Amazon EC2 控制台] 使用从 Amazon Web Services Marketplace 购买的 AMI。	启动 Amazon Web Services Marketplace 实例 (p. 608)
[Amazon CLI] 使用所选 AMI。	通过 Amazon CLI 使用 Amazon EC2
[Amazon Tools for Windows PowerShell] 使用所选 AMI。	Amazon EC2 来自Amazon Tools for Windows PowerShell
[Amazon CLI] Amazon EC2 使用 EC2 实例集跨不同的 EC2 实例类型和可用区以及跨按需型实例、预留实例和竞价型实例购买模式预置容量。	EC2 Fleet (p. 814)
[Amazon CloudFormation] 使用 Amazon CloudFormation 模板指定实例。	Amazon CloudFormation 用户指南中的 AWS::EC2::Instance
[Amazon 开发工具包] 使用特定于语言的 Amazon 开发工具包启动实例。	Amazon SDK for .NET 适用于 C++ 的 Amazon SDK 适用于 Go 的 Amazon SDK 适用于 Java 的Amazon开发工具包 适用于 JavaScript 的 Amazon SDK 适用于 PHP V3 的 Amazon SDK 适用于 Python 的 Amazon SDK 适用于 Ruby V3 的 Amazon SDK

Note

要在仅 IPv6 的子网中启动 EC2 实例，您必须使用 基于 Nitro 系统构建的实例 (p. 246)。

Note

启动仅 IPv6 实例时，DHCPv6 可能不会立即为该实例提供 IPv6 DNS 名称服务器。在此初始延迟期间，实例可能无法解析公有域。
对于在 Amazon Linux 2 上运行的实例，如果您希望立即使用 IPv6 DNS 名称服务器更新 /etc/resolv.conf 文件，请在启动时运行以下 cloud-init 指令：

```
#cloud-config
bootcmd:
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver fd00:ec2::253,' /
etc/resolv.conf
```

另一种选择是更改配置文件并重新映像 AMI，以便该文件在启动时立即具有 IPv6 DNS 名称服务器地址。

当您启动实例时，可以在与以下一项资源关联的子网中启动实例：

- 可用区 - 此选项为默认选项。
- 本地扩展区 - 要在本地扩展区中启动实例，您必须选择加入本地扩展区，然后在该区域中创建子网。有关更多信息，请参阅本地扩展区。
- Wavelength 区域 - 要在 Wavelength 区域中启动实例，您必须选择加入 Wavelength 区域，然后在区域中创建子网。有关如何在 Wavelength 区域中启动实例的信息，请参阅 Amazon Wavelength 开发人员指南中的 Amazon Wavelength 入门。
- Outpost - 要在 Outpost 中启动实例，您必须创建 Outpost。有关如何创建 Outpost 的信息，请参阅 Amazon Outposts 用户指南中的 Amazon Outposts 入门。

启动实例之后，您可以连接并使用该实例。开始时，实例的状态为 `pending`。当实例状态为 `running` 时，实例已经开始启动。可能要过一小段时间才能连接到实例。请注意，裸机实例类型可能需要更长时间才能启动。有关裸机实例的更多信息，请参阅基于 Nitro 系统构建的实例 (p. 246)。

实例将获得一个公有 DNS 名称，您可使用此名称通过 Internet 与实例通信。实例还会获得一个私有 DNS 名称，相同 VPC 网络内的其他实例可以用其与该实例通信。有关连接到实例的更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

当您完成实例时，请确保终止该实例。有关更多信息，请参阅终止实例 (p. 634)。

使用新启动实例向导启动实例

您可以使用新的启动实例向导启动一个实例。启动实例向导指定启动实例所需的启动参数。在启动实例向导提供默认值的情况下，您可以接受默认值或指定自己的值。如果您接受默认值，则可以通过仅选择密钥对来启动实例。

在启动实例之前，请确保您已进行了相应设置。有关更多信息，请参阅设置以使用 Amazon EC2 (p. 5)。

Important

当您启动不在 Amazon 免费套餐 范围内的实例时，即使该实例处于闲置状态，您也需为该实例运行的时间付费。

主题

- 关于新启动实例向导 (p. 576)
- 快速启动实例 (p. 576)
- 使用定义的参数启动实例 (p. 577)
- 使用旧的启动实例向导启动实例 (p. 583)

关于新启动实例向导

欢迎使用全新改进后的启动体验，这是一种更快、更简单的实例启动方法。

我们正在推出新的启动实例向导。如果在当前选定的区域中不可用，则可以选择其他区域来检查该区域是否可用。

最新改进

- 单页布局具有摘要侧面板

  使用新的单页设计实现快速启动和运行。在同一位置查看所有设置。无需在步骤之间反复导航以确保配置正确。使用 Summary（摘要）面板获得概览并轻松导航至页面。
- 改进的 AMI 选择器

  新用户 – 使用 Quick Start Amazon Machine Image（AMI）选择器来选择操作系统，以快速启动实例。

  有经验的用户 – AMI 选择器显示您最近使用的 AMI 和您拥有的 AMI，以使您更轻松地选择您关心的 AMI。您仍然可以浏览完整目录以查找新的 AMI。

持续改善

我们不断努力，持续改善体验。以下是我们目前正在研究的内容：

- 默认值和依赖项协助
  - 默认值将运用于所有字段。
  - 其它逻辑的添加将帮助您正确设置实例配置（例如，我们将禁用当前设置中的不可用参数）。
- 更加简洁的设计
  - 简洁的视图与摘要和响应速度更快的设计将使一页式体验更具可扩展性。
  - 便捷联网功能将帮助您快速轻松地配置防火墙规则（例如，选择通用的预设规则）。

在接下来的几个月里，我们将针对启动体验完成更多改善。

期待您的反馈

非常感谢您对新启动实例向导的反馈。在接下来的几个月里，我们将根据您的反馈继续改善体验。您可以通过 EC2 控制台向我们直接发送反馈，也可以使用此页面底部的提供反馈链接进行反馈。

快速启动实例

如需快速设置实例以进行测试，请按照以下步骤。您需要选择操作系统和密钥对，然后接受默认值。有关启动实例向导中所有参数的信息，请参阅 使用定义的参数启动实例 (p. 577)。

快速启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，会显示当前 Amazon 区域 [例如，美国东部（俄亥俄）]。选择要在其中启动实例的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅资源位置 (p. 1656)。
3. 从 Amazon EC2 控制台控制面板中，选择启动实例。
4. （可选）在 Name and tags（名称与标签）下，为 Name（名称）输入实例的描述性名称。
5. 在 Application and OS Images（Amazon Machine Image）（应用程序和操作系统镜像（Amazon Machine Image））下，选择 Quick Start（快速启动），然后为您的实例选择操作系统（OS）。
6. （可选）在 Key pair (login)（密钥对（登录））下，为 Key pair name（密钥对名称）选择一个现有密钥对或新建一个密钥对。

7. 在 Summary（摘要）面板中，选择 Launch instance（启动实例）。

使用定义的参数启动实例

除了密钥对外，启动实例向导还会为所有参数提供默认值。您可以接受任何或全部默认值，也可以通过为每个参数指定自己的值来配置实例。启动实例向导中这些参数进行了分组。以下说明将引导您完成每个参数组。

实例配置的参数

- 发起实例启动 (p. 577)
- 名称和标签 (p. 577)
- 应用程序和操作系统镜像 (Amazon Machine Image) (p. 577)
- 实例类型 (p. 578)
- 密钥对（登录） (p. 579)
- Network settings (网络设置) (p. 579)
- 配置存储 (p. 580)
- 高级详细信息 (p. 581)
- 摘要 (p. 582)

发起实例启动

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，会显示当前 Amazon 区域 [例如，美国东部（俄亥俄）]。选择要在其中启动实例的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅资源位置 (p. 1656)。
3. 从 Amazon EC2 控制台控制面板中，选择启动实例。

名称和标签

实例名称是一个标签，其中密钥为 Name（名称），而值为您指定的名称。您可以标记实例、卷、弹性图形和网络接口。对于竞价型实例，您只能标记竞价型实例请求。有关标签的信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

指定实例名称和其它标签为可选项。

- 对于 Name（名称），为实例输入一个描述性名称。如果您没有指定名称，则可以通过其 ID 标识实例，该 ID 将在您启动实例时自动生成。
- 要添加其它标签，请选择 Add additional tags（添加其它标签）。选择 Add tag（添加标签），然后输入密钥和值，然后选择要标记的资源类型。为每个要添加的其它标签选择 Add tag（添加标签）。

应用程序和操作系统镜像 (Amazon Machine Image)

Amazon Machine Image (AMI) 中包含了创建实例所需的信息。例如，AMI 可能包含充当 Web 服务器所需的软件，例如 Linux、Apache 和您的网站。

您可以找到适合的 AMI，如下所示。通过查找 AMI 的每个选项，您可以选择右上角的 Cancel（取消）以返回启动实例向导，而不选择 AMI。

搜索栏

要搜索所有可用的 AMI，请在 AMI 搜索栏中输入关键字，然后按 Enter 键。要选择 AMI，请选择 Select（选择）。

最近使用的项目

您最近使用的 AMI。

选择 Recently launched（最近启动）或 Currently in use（当前使用），然后在 Amazon Machine Image (AMI) 中，选择一个 AMI。

我的 AMI

您拥有的私有 AMI，或与您共享的私有 AMI。

选择 Owned by me（我拥有的）或 Shared with me（与我共享），然后在 Amazon Machine Image (AMI) 中选择一个 AMI。

Quick Start（快速入门）

AMI 按操作系统 (OS) 分组以助您快速入门。

首先选择所需的操作系统，然后从 Amazon Machine Image (AMI) 中选择一个 AMI。要选择符合免费套餐条件的 AMI，请确保该 AMI 已标记 Free tier eligible（符合免费套餐条件）。

浏览更多 AMI

选择 Browse more AMIs（浏览更多 AMI）以浏览完整的 AMI 目录。

- 要搜索所有可用的 AMI，请在搜索栏中输入关键字，然后按 Enter 键。
- 要使用 Systems Manager 参数查找 AMI，请选择搜索栏右侧的箭头按钮，然后选择 Search by Systems Manager parameter（按 Systems Manager 参数搜索）。有关更多信息，请参阅使用 Systems Manager 参数查找 AMI (p. 119)。
- 要按类别搜索，请依次选择 Quickstart AMI、My AMIs（我的 AMI）、Amazon Web Services Marketplace AMI 或者 Community AMIs（社区 AMI）。

  Amazon Web Services Marketplace 是一个在线商店，您可以从中购买在 Amazon 上运行的软件（包括 AMI）。有关从 Amazon Web Services Marketplace 启动实例的更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。在 Community AMIs（社区 AMI）中，您可以找到 Amazon 社区成员提供给其它人使用的 AMI。将来自 Amazon 或经过验证的合作伙伴的 AMI 标记为经过验证的提供商。
- 要筛选 AMI 列表，请在屏幕左侧的 Refine results（优化结果）下方选中一个或多个复选框。筛选条件选项会因所选搜索类别而有所不同。
- 检查对每个 AMI 列出的 Root device type (根设备类型)。请注意哪些 AMI 是您需要的类型：即 ebs（由 Amazon EBS 支持）或 instance-store（由实例存储支持）。有关更多信息，请参阅根设备存储 (p. 103)。
- 检查对每个 AMI 列出的 Virtualization type (虚拟化类型)。注意哪些 AMI 类型是您需要的类型：即 hvm（全虚拟化）或 paravirtual（半虚拟化）。例如，一些实例类型需要 HVM。有关更多信息，请参阅 Linux AMI 虚拟化类型 (p. 106)。
- 检查对每个 AMI 列出的启动模式。请注意哪些 AMI 使用您需要的启动模式：legacy-bios、uefi 或 uefi-preferred。有关更多信息，请参阅启动模式 (p. 107)。
- 选择满足您的需求的 AMI，然后选择 Select。

更改 AMI 时发出警告

如果您修改了与所选 AMI 关联的任何卷或安全组的配置，然后选择了其他 AMI，则会打开一个窗口，警告您当前的某些设置将被更改或删除。您可以查看对安全组和卷的更改。此外，您可以查看将添加和删除哪些卷，也可以仅查看要添加的卷。

实例类型

实例类型定义了实例的硬件配置和大小。更大的实例类型拥有更多的 CPU 和内存。有关更多信息，请参阅实例类型。

- 对于 Instance type（实例类型），请为实例选择实例类型。

  Free tier（免费套餐）– 如果您的 Amazon 账户的使用时间未满 12 个月，您可以通过选择 t2.micro 实例类型（或在 t2.micro 不可用时选择“Regions”（区域）中的 t3.micro 实例类型）来使用免费套餐下的 Amazon EC2。如果实例类型符合 Free Tier（免费套餐）条件，则会标记为 Free tier eligible（符合免费套餐条件）。有关 t2.micro 和 t3.micro 的更多信息，请参阅 可突增性能实例 (p. 274)。

密钥对（登录）

为 Key pair name（密钥对名称）选择一个现有密钥对，或选择 Create new key pair（创建新密钥对）来新建一个密钥对。有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

> **Important**
>
> 如果您选择 Proceed without key pair (Not recommended)（在没有密钥对的情况下继续（不推荐））选项，则将无法连接到此实例，除非您选择配置为允许用户以其它方式登录的 AMI。

Network settings (网络设置)

根据需要配置网络设置。

- VPC：为您的实例选择现有 VPC。您可以选择默认 VPC 或您创建的 VPC。有关更多信息，请参阅the section called “Virtual Private Cloud” (p. 1194)。
- 子网：您可以在与可用区、本地扩展区、Wavelength 区域或 Outpost 关联的子网中启动实例。

  要在可用区中启动实例，请选择要在其中启动实例的子网。要创建新子网，请选择 Create new subnet 转到 Amazon VPC 控制台。完成此操作后，返回到启动实例向导并选择“Refresh”（刷新）图标，以便将您的子网加载到列表中。

  要在本地区域中启动实例，请选择您在本地区域中创建的子网。

  要在 Outpost 中启动实例，请在 VPC 中选择与 Outpost 关联的子网。
- 自动分配公有 IP：指定您的实例是否会收到公有 IPv4 地址。默认情况下，默认子网中的实例会收到公有 IPv4 地址，而非默认子网中的实例不会收到。可以选择 Enable (启用) 或 Disable (禁用) 以覆盖子网的默认设置。有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。
- Firewall (security groups)（防火墙（安全组））：使用安全组为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。所有其他的流量将被忽略。有关安全组的更多信息，请参阅 适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

  添加网络接口时，您必须在网络接口中指定相同安全组。

  按如下所示进行选择或创建安全组：
  - 若要为您的 VPC 选择现有安全组，请选择 Select existing security group（选择现有安全组），然后从 Common security groups（通用安全组）中选择您的安全组。
  - 若要为您的 VPC 创建新安全组，请选择 Create security group（创建安全组）。启动实例向导会自动定义 launch-wizard-x 安全组并提供以下复选框以快速添加安全组规则：

    Allow SSH traffic from（允许入站 SSH 流量）- 创建入站规则以允许您通过 SSH（端口 22）连接至您的实例。指定流量是来自 Anywhere（任何地方）、Custom（自定义）还是 My IP（我的 IP）。

    Allow HTTPs traffic from the internet（允许来自 Internet 的 HTTPs 流量）- 创建一个打开端口 443（HTTPS）的入站规则，以允许来自任何地方的互联网流量。如果您的实例将是 Web 服务器，则需要此规则。

    Allow HTTP traffic from the internet（允许来自 Internet 的 HTTP 流量）- 创建一个打开端口 80（HTTP）的入站规则，以允许来自任何地方的互联网流量。如果您的实例将是 Web 服务器，则需要此规则。

您可以根据需要编辑规则并添加规则以适应您的需要。

要编辑或添加规则，请选择位于右上角的 Edit（编辑）。要添加规则，请选择 Add security group rule（添加安全组规则）。对于 Type（类型），请选择网络流量类型。将使用为网络流量打开的协议自动填充 Protocol（协议）字段。对于 Source type（源类型），请选择一种源类型。若要让启动实例向导添加您电脑的公有 IP 地址，请选择 My IP（我的 IP）。但是，如果您在没有静态 IP 地址的情况下通过 ISP 或从防火墙后面进行连接，则您需要了解客户端电脑使用的 IP 地址范围。

Warning

如果您要短时启动测试实例并将很快停止或终止，那么允许所有 IP 地址 (`0.0.0.0/0`) 通过 SSH 或 RDP 访问您的实例的规则是可以接受的，但此规则对生产环境来说是不安全的。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

- Advanced network configuration（高级网络配置）– 仅在选择子网时可用。

  网络接口

  - Device index（设备索引）：网卡的索引。必须将主网络接口分配给网卡索引 0。有些实例类型支持多个网卡。
  - Network interface（网络接口）：选择 New interface（新接口）即可让 Amazon EC2 创建新的接口，或选择现有且可用的网络接口。
  - Description (描述)：（可选）新网络接口的描述。
  - Subnet（子网）：要在其中创建新网络接口的子网。对于主网络接口 (`eth0`)，这是在其中启动实例的子网。如果为 `eth0` 输入了现有的网络接口，将在该网络接口所在的子网中启动实例。
  - 安全组：VPC 中要与网络接口关联的一个或多个安全组。
  - Primary IP (主要 IP)：您的子网范围内的一个私有 IPv4 地址。保留空白会让 Amazon EC2 为您选择一个私有 IPv4 地址。
  - Secondary IP（辅助 IP）：您的子网范围内的一个或多个其它私有 IPv4 地址。选择 Manually assign（手动分配）然后输入 IP 地址。选择 Add IP（添加 IP）以添加另一个 IP 地址。或者，选择 Automatically assign（自动分配）以使 Amazon EC2 来为您选择，然后输入一个值来指明要添加的 IP 地址的数量。
  - (仅限 IPv6) IPv6 IP：子网范围内的一个 IPv6 地址。选择 Manually assign（手动分配）然后输入 IP 地址。选择 Add IP（添加 IP）以添加另一个 IP 地址。或者，选择 Automatically assign（自动分配）以使 Amazon EC2 来为您选择，然后输入一个值来指明要添加的 IP 地址的数量。
  - IPv4 前缀：网络接口的 IPv4 前缀。
  - IPv6 前缀：网络接口的 IPv6 前缀。
  - Delete on termination (终止时删除)：选择在删除实例时是否删除网络接口。
  - Elastic Fabric Adapter：指示网络接口是否为 Elastic Fabric Adapter。有关更多信息，请参阅 Elastic Fabric Adapter。

  选择 Add network interface（添加网络接口）以添加辅助网络接口。辅助网络接口可以与 VPC 位于不同的子网中，但必须位于您的实例所在的可用区内。

  有关更多信息，请参阅弹性网络接口 (p. 1104)。如果指定多个网络接口，则您的实例无法收到公有 IPv4 地址。此外，如果您为 eth0 指定某个现有网络接口，则无法使用 Auto-assign Public IP 覆盖子网的公有 IPv4 设置。有关更多信息，请参阅在实例启动期间分配公有 IPv4 地址 (p. 1057)。

配置存储

您选择的 AMI 包含一个或多个存储卷，包括根卷。您可以指定要附加到实例的其它卷。

您可以使用 Simple（简单）或 Advanced（高级）视图。借助 Simple（简单）视图，您可以指定卷的大小和类型。若要指定所有卷参数，请选择位于卡片的右上角的 Advanced（高级）视图。

在 Advanced（高级）视图中，您可以按如下方式配置每个卷：

- Storage type（存储类型）：选择要与实例关联的 Amazon EBS 或实例存储卷。列表中可用的卷类型取决于您选择的实例类型。有关更多信息，请参阅 Amazon EC2 实例存储 (p. 1579) 和 Amazon EBS 卷 (p. 1324)。
- Device name（设备名称）：从卷的可用设备名称列表中进行选择。
- Snapshot（快照）：选择要从其中还原卷的快照。您可以通过在 Snapshot（快照）字段中输入文本来搜索可用的共享快照和公有快照。
- Size (GiB)（大小 (GiB)）：对于 EBS 卷，您可以指定存储大小。如果您选择了有资格享用免费套餐的 AMI 和实例，请记住，若要享用免费套餐，您必须将总存储大小保持为 30GiB 以下。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
- 卷类型：对于 EBS 卷，请选择卷类型。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。
- IOPS：如果选择了Provisioned IOPS SSD 卷类型，则可以输入卷支持的每秒 I/O 操作数 (IOPS)。
- Delete on termination（终止时删除）：对于 Amazon EBS 卷，选择 Yes（是）以在终止实例时删除此卷或选择 No（否）以保留此卷。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。
- Encrypted（加密）：如果实例类型支持 EBS 加密，则可以选择 Yes（是）以为此卷启用加密。如果默认情况下在此区域中启用了加密，则会为您启用加密。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。
- KMS key（KMS 密钥）：如果您将 Encrypted（加密）选择为 Yes（是），则您必须选择一个客户托管式密钥来加密卷。如果默认情况下在此区域中启用了加密，则将为您选择默认的客户托管密钥。您可以选择不同的密钥或指定由您创建的任何客户托管密钥的 ARN。
- File systems（文件系统）：将 Amazon EFS 或 Amazon FSx 文件系统挂载到实例。有关挂载 Amazon EFS 文件系统的更多信息，请参阅 将 Amazon EFS 与 Amazon EC2 结合使用 (p. 1602)。有关挂载 Amazon FSx 文件系统的更多信息，请参阅 将 Amazon FSx 与 Amazon EC2 结合使用 (p. 1603)

高级详细信息

对于Advanced details (高级详细信息)，请展开该部分以查看字段并为实例指定任何其他参数。

- Purchasing option（购买选项）：选择 Request Spot Instances（请求竞价型实例）即可按照 Spot 价格请求竞价型实例，以按需价格为上限，而选择 Customize（自定义）即可更改默认的竞价型实例设置。您可以设置最高价（不建议），并更改请求类型、请求时长和中断行为。如果您未请求竞价型实例，则默认情况下 Amazon EC2 会启动按需型实例。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。
- 域加入目录：选择您的 Linux 实例在启动后加入到的 Amazon Directory Service 目录（域）。如果选择一个域，则必须选择一个具有所需权限的 IAM 角色。有关更多信息，请参阅将 Linux EC2 实例无缝加入到您的 Amazon 托管的 Microsoft AD 目录中。
- IAM instance profile（IAM 实例配置文件）：选择 Amazon Identity and Access Management (IAM) 实例配置文件以与实例关联。有关更多信息，请参阅适用于 Amazon EC2 的 IAM 角色 (p. 1277)。
- Hostname type（主机名类型）：选择实例的来宾操作系统主机名将包括资源名称还是 IP 名称。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- DNS Hostname（DNS 主机名）：确定对资源名称或 IP 名称的 DNS 查询（根据您对 Hostname type（主机名类型）的选择）是否将以 IPv4 地址（A 记录）、IPv6 地址（AAAA 记录）响应，还是同时以两者响应。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- Shutdown behavior (关闭行为)：选择关闭时实例应该停止还是终止。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。
- Stop - Hibernate behavior（停止 – 休眠行为）：要启用休眠，请选择 Enable（启用）。只有当实例满足休眠先决条件时，此字段才可用。有关更多信息，请参阅休眠 Linux 按需型实例 (p. 616)。
- Termination protection（终止保护）：要防止意外终止，请选择 Enable（启用）。有关更多信息，请参阅启用终止保护 (p. 637)。
- Stop protection（停止保护）：为防止意外停止，请选择 Enable（启用）。有关更多信息，请参阅启用停止保护 (p. 613)。
- Detailed CloudWatch monitoring（详细的 CloudWatch 监控）：选择 Enable（启用）将使用 Amazon CloudWatch 开启对您的实例的详细监控。将收取额外费用。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。

- Elastic inference (弹性推理)：要连接到 EC2 CPU 实例的弹性推理加速器。有关更多信息，请参阅 Amazon Elastic Inference 开发人员指南 中的使用 Amazon Elastic Inference。

  Note

  自 2023 年 4 月 15 日起，Amazon 不再允许新客户加入 Amazon Elastic Inference（EI），并将帮助现有客户将其工作负载迁移到价格更低廉且性能更出色的选项。2023 年 4 月 15 日之后，新客户将无法在 Amazon SageMaker、Amazon ECS 或Amazon EC2 中使用 Amazon EI 加速器启动实例。但是，在过去 30 天内至少使用过一次 Amazon EI 的客户将视为当前客户，可继续使用该服务。

- Credit specification（积分规范）：选择 Unlimited（无限）以允许应用程序只要有需要即突增到基准以上。此字段仅适用于 T 实例。可能收取额外费用。有关更多信息，请参阅可突增性能实例 (p. 274)。
- Placement group name (置放群组名称)：指定要在其中启动实例的置放群组。您可以选择现有置放群组或创建新组。并非所有实例类型都支持在放置群组中启动实例。有关更多信息，请参阅置放群组 (p. 1177)。
- EBS-optimized instance（EBS 优化的实例）：Amazon EBS 优化的实例使用优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。如果实例类型支持此功能，请选择 Enable（启用）来启用该功能。将收取额外费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。
- Capacity Reservation（容量预留）：指定是在任何开放容量预留 [Open（开放）]、特定容量预留 [Target by ID（按 ID 定位）]，还是容量预留组 [Target by group（按组定位）] 中启动实例。要指定不使用容量预留，请选择 None（无）。有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。
- Tenancy (租期)：选择是在共享硬件（Shared (共享)）、隔离的专用硬件（Dedicated (专用)），还是在专用主机（Dedicated host (专用主机)）上运行您的实例。如果您选择在专用主机上启动实例，则可以指定是否在主机资源组中启动实例，也可以定位特定专用主机。可能收取额外费用。有关更多信息，请参阅 Dedicated Instances (p. 533) 和 Dedicated Hosts (p. 504)。
- RAM disk ID（RAM 磁盘 ID）：[仅对半虚拟 (PV) AMI 有效] 为实例选择一个 RAM 磁盘。如果您选择了一个内核，则您可能需要选择带有可支持该内核的驱动程序的某个特定 RAM 磁盘。
- Kernel ID（内核 ID）：[仅对半虚拟 (PV) AMI 有效] 为实例选择一个内核。
- Nitro Enclave：允许您从 Amazon EC2 实例创建隔离的执行环境，称为 Enclave。选择 Enable（启用）以启用 Amazon Nitro Enclaves 的实例。有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？
- 许可证配置：您可以根据指定的许可证配置启动实例，以跟踪您的许可证使用情况。有关更多信息，请参阅《Amazon License Manager 用户指南》中的创建许可证配置。
- Metadata accessible (元数据可访问)：您可以启用或禁用对实例元数据的访问。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- Metadata transport（传输元数据）：使实例能够访问本地 IMDSv2 IPv6 地址链接（`fd00:ec2::254`）来检索实例元数据。此选项仅在您将 基于 Nitro 系统构建的实例 (p. 246) 启动到仅限 IPv6 的子网中时可用。有关检索实例元数据的更多信息，请参阅 检索实例元数据 (p. 766)。
- Metadata version (元数据版本)：如果您启用对实例元数据的访问，您可以选择在请求实例元数据时要求使用 实例元数据服务版本 2。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- 元数据响应跳数限制：如果启用实例元数据，则可以为元数据标记设置允许的网络跃点数。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- Allow tags in metadata（允许元数据中的标签）：如果选择Enable（启用），该实例将允许从其元数据访问其所有标签。如果未指定值，则默认情况下，将不允许对实例元数据中的标签的访问。有关更多信息，请参阅允许访问实例元数据中的标签 (p. 1676)。
- User data：您可以指定用户数据在启动时配置实例或运行配置脚本。有关更多信息，请参阅启动时在 Linux 实例上运行命令 (p. 748)。

摘要

使用 Summary（摘要）面板来指定要启动的实例数、查看实例配置和启动实例。

- Number of instances (实例的数量)：输入要启动的实例的数量。所有实例都将以相同的配置启动。

Tip

为确保更快地启动实例，请将大量请求分成较小的批次。例如，创建五个独立的请求批次，每个批次包含 100 个实例启动请求，而不要创建一个包含 500 个实例的启动请求。

- （可选）如果您指定的实例不止一个，为了帮助确保保持正确数量的实例来处理应用程序的需求，您可以选择 consider EC2 Auto Scaling（考虑 EC2 Auto Scaling）以创建启动模板和 Auto Scaling 组。Auto Scaling 将根据您的规格来扩展组中的实例数。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。

  Note

  如果 Amazon EC2 Auto Scaling 将某个 Auto Scaling 组中的实例标记为运行状况不佳，则会自动安排该实例进行替换，此时将终止此实例而启动另一个实例，并且您将丢失原始实例上的数据。如果您停止或重新引导实例，或者其他事件将实例标记为运行状况不佳，则此实例将被标记为运行状况不佳。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 Auto Scaling 实例的运行状况检查。
- 查看实例的详细信息并进行必要的更改。您可以在 Summary（摘要）面板选择某部分的链接以直接导航到该部分。
- 当您准备好启动您的实例时，请选择 Launch instance（启动实例）。

  如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

  （可选）您可以为实例创建账单提醒。在确认屏幕上的 Next Steps（下一步）下选择 Create billing alerts（创建账单提醒）并按照指示操作。还可以在启动实例后创建账单提醒。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的创建账单告警以监控预估 Amazon 费用。

使用旧的启动实例向导启动实例

Important

您不能在支持新启动实例向导的 Amazon Web Services 区域 中使用旧启动实例向导。每个区域要么支持新启动体验，要么支持旧启动体验，但不能同时支持两者。

仅当您所在的区域支持旧启动体验时，您才能使用旧启动实例向导来启动实例。启动实例向导指定启动实例所需的所有启动参数。在启动实例向导提供默认值的情况下，您可以接受默认值或指定自己的值。您必须指定 AMI 和密钥对才能启动实例。

有关使用新启动实例向导的说明，请参阅 使用新启动实例向导启动实例 (p. 575)。

在启动实例之前，请确保您已进行了相应设置。有关更多信息，请参阅设置以使用 Amazon EC2 (p. 5)。

Important

当您启动不在 Amazon 免费套餐 范围内的实例时，即使该实例处于闲置状态，您也需为该实例运行的时间付费。

启动实例的步骤：

- 发起实例启动 (p. 584)
- 步骤 1：选择 Amazon Machine Image (AMI) (p. 584)
- 步骤 2：选择实例类型 (p. 585)
- 步骤 3：配置实例详细信息 (p. 585)
- 步骤 4：添加存储 (p. 587)
- 步骤 5：添加标签 (p. 587)
- 步骤 6：配置安全组 (p. 588)

- 步骤 7：查看实例启动并选择密钥对 (p. 588)

发起实例启动

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在屏幕顶部的导航栏中，会显示当前区域（例如，US East (Ohio)）。为实例选择一个满足您需求的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。有关更多信息，请参阅资源位置 (p. 1656)。
3. 从 Amazon EC2 控制台控制面板中，选择启动实例。

步骤 1：选择 Amazon Machine Image (AMI)

启动实例时，您必须选择配置 (称为 Amazon Machine Image (AMI))。AMI 包含创建新实例所需的信息。例如，AMI 可能包含充当 Web 服务器所需的软件，例如 Linux、Apache 和您的网站。

启动实例时，您可以从列表中选择 AMI，也可以选择指向 AMI ID 的 Systems Manager 参数。有关更多信息，请参阅使用 Systems Manager 参数查找 AMI。

在选择一个 Amazon Machine Image (AMI) 页面上，使用两个选项之一选择 AMI。搜索 AMI 列表 (p. 584)，或者按 Systems Manager 参数搜索 (p. 584)。

通过搜索 AMI 列表

1. 在左侧窗格中选择要使用的 AMI 类型：

   Quick Start（快速入门）

   一组精选的常用 AMI 可帮助您快速开始。要选择符合免费套餐条件的 AMI，请在左侧窗格中选择 Free Tier Only（仅免费套餐）。这些 AMI 标记为 Free tier eligible (符合条件的免费套餐)。

   我的 AMI

   您拥有的私有 AMI，或与您共享的私有 AMI。要查看已与您共享的 AMI，请在左侧窗格中选择与我共享。

   Amazon Web Services Marketplace

   一个在线商店，您可以从中购买在 Amazon 上运行的软件 (包括 AMI)。有关从 Amazon Web Services Marketplace 启动实例的更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。

   社区 AMI

   Amazon 社区成员提供给其他人使用的 AMI。要按操作系统筛选 AMI 列表，请在 Operating system 下选中相应复选框。还可以按架构和根设备类型进行筛选。
2. 检查对每个 AMI 列出的 Root device type (根设备类型)。请注意哪些 AMI 是您需要的类型，即 `ebs`（由 Amazon EBS 支持）或 `instance-store`（由实例存储支持）。有关更多信息，请参阅根设备存储 (p. 103)。
3. 检查对每个 AMI 列出的 Virtualization type (虚拟化类型)。注意哪些 AMI 类型是您需要的类型，即 `hvm` 或 `paravirtual`。例如，一些实例类型需要 HVM。有关更多信息，请参阅 Linux AMI 虚拟化类型 (p. 106)。
4. 检查对每个 AMI 列出的启动模式。请注意哪些 AMI 使用您需要的启动模式，`legacy-bios` 或 `uefi`。有关更多信息，请参阅启动模式 (p. 107)。
5. 选择满足您的需求的 AMI，然后选择 Select。

按 Systems Manager 参数

1. 选择 Search by Systems Manager parameter (按 Systems Manager 参数搜索)（位于右上角）。

2. 对于 Systems Manager 参数 (Systems Manager 参数)，请选择一个参数。相应的 AMI ID 将显示在 Currently resolves to (当前解析为) 的旁边。
3. 选择搜索。与 AMI ID 匹配的 AMI 将显示在列表中。
4. 从列表中选择 AMI，然后选择选择。

步骤 2：选择实例类型

在 Choose an Instance Type (选择一个实例类型) 页面上，选择要启动的实例的硬件配置和大小。更大的实例类型拥有更多的 CPU 和内存。有关更多信息，请参阅实例类型 (p. 238)。

要保持免费套餐的资格，请选择 t2.micro 实例类型（在 t2.micro 不可用的区域，选择 t3.micro 实例类型）。如果实例类型符合免费套餐条件，则会标记为 Free tier eligible（符合免费套餐条件）。有关 t2.micro 和 t3.micro 的更多信息，请参阅 可突增性能实例 (p. 274)。

默认情况下，向导显示当前一代实例类型，并根据您选择的 AMI 选择第一可用实例类型。要查看上一代实例类型，请从筛选列表中选择 All generations。

> **Note**
>
> 要快速设置实例以便进行测试，请选择 Review and Launch 以接受默认配置设置，然后启动您的实例。否则，若要进一步配置实例，请选择 Next: Configure Instance Details。

步骤 3：配置实例详细信息

在 Configure Instance Details 页面上，根据需要更改以下设置（展开 Advanced Details 查看所有设置），然后选择 Next: Add Storage：

- Number of instances (实例的数量)：输入要启动的实例的数量。

  > **Tip**
  >
  > 为确保更快地启动实例，请将大量请求分成较小的批次。例如，创建五个独立的请求批次，每个批次包含 100 个实例启动请求，而不要创建一个包含 500 个实例的启动请求。

- （可选）为帮助确保保持正确数量的实例来处理应用程序，您可选择 Launch into Auto Scaling Group (启动至 Auto Scaling 组) 以创建启动配置和 Auto Scaling 组。Auto Scaling 将根据您的规格来扩展组中的实例数。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南。

  > **Note**
  >
  > 如果 Amazon EC2 Auto Scaling 将某个 Auto Scaling 组中的实例标记为运行状况不佳，则会自动安排该实例进行替换，此时将终止此实例而启动另一个实例，并且您将丢失原始实例上的数据。如果您停止或重新引导实例，或者其他事件将实例标记为运行状况不佳，则此实例将被标记为运行状况不佳。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 Auto Scaling 实例的运行状况检查。

- Purchasing option (购买选项)：选择 Request Spot instances (请求竞价型实例) 以启动竞价型实例。这将在此页面中添加和删除选项。您可以选择设置最高价（不建议），还可以选择更改请求类型、中断行为和请求效力。有关更多信息，请参阅创建竞价型实例请求 (p. 460)。
- Network（网络）：选择 VPC，或者如果要创建新 VPC，请选择 Create new VPC（创建新 VPC）以转到 Amazon VPC 控制台。完成后，返回到启动实例向导并选择 Refresh（刷新），以便将您的 VPC 加载到列表中。
- 子网：您可以在与可用区、本地扩展区、Wavelength 区域或 Outpost 关联的子网中启动实例。

  要在可用区中启动实例，请选择要在其中启动实例的子网。您可以选择 No preference，让 Amazon 在任何可用区中选择默认子网。要创建新子网，请选择 Create new subnet 转到 Amazon VPC 控制台。完成此操作后，返回到向导并选择 Refresh 按钮，以便将您的子网加载到列表中。

  要在本地区域中启动实例，请选择您在本地区域中创建的子网。

要在 Outpost 中启动实例，请在 VPC 中选择与 Outpost 关联的子网。

- 自动分配公有 IP：指定您的实例是否会收到公有 IPv4 地址。默认情况下，默认子网中的实例会收到公有 IPv4 地址，而非默认子网中的实例不会收到。可以选择 Enable (启用) 或 Disable (禁用) 以覆盖子网的默认设置。有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。
- 自动分配 IPv6 IP：指定您的实例是否会收到处于子网范围内的 IPv6 地址。选择启用或禁用可以覆盖子网的默认设置。该选项仅在您已将 IPv6 CIDR 块与您的 VPC 和子网关联的情况下可用。有关更多信息，请参阅《Amazon VPC 用户指南》中的将 IPv6 CIDR 块与您的 VPC 关联。
- Hostname type（主机名类型）：选择实例的来宾操作系统主机名将包括资源名称还是 IP 名称。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- DNS Hostname（DNS 主机名）：确定对资源名称或 IP 名称的 DNS 查询（根据您对 Hostname type（主机名类型）的选择）是否将以 IPv4 地址（A 记录）、IPv6 地址（AAAA 记录）响应，还是同时以两者响应。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- 域加入目录：选择您的 Linux 实例在启动后加入到的 Amazon Directory Service 目录（域）。如果选择一个域，则必须选择一个具有所需权限的 IAM 角色。有关更多信息，请参阅将 Linux EC2 实例无缝加入到您的 Amazon 托管的 Microsoft AD 目录中。
- 置放组：置放组确定您的实例的置放策略。选择现有置放群组或创建新组。仅当您选择了支持置放群组的实例类型时，此选项才可用。有关更多信息，请参阅置放群组 (p. 1177)。
- 容量预留：指定是在共享容量中、任何 open 容量预留中、特定容量预留中还是现有容量预留组中启动实例。有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。
- IAM role (IAM 角色)：选择要与实例关联的 Amazon Identity and Access Management (IAM) 角色。有关更多信息，请参阅适用于 Amazon EC2 的 IAM 角色 (p. 1277)。
- CPU options (CPU 选项)：选择 Specify CPU options (指定 CPU 选项) 可在实例启动期间指定自定义 vCPU 数。设置 CPU 内核数和每内核线程数。有关更多信息，请参阅优化 CPU 选项 (p. 721)。
- Shutdown behavior (关闭行为)：选择关闭时实例应该停止还是终止。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。
- Stop - Hibernate behavior (停止 - 休眠行为)：要启用休眠，请选中该复选框。只有当实例满足休眠先决条件时，此选项才可用。有关更多信息，请参阅休眠 Linux 按需型实例 (p. 616)。
- Enable termination protection (启用终止保护)：要防止意外终止，请选中该复选框。有关更多信息，请参阅启用终止保护 (p. 637)。
- Enable stop protection（启用停止保护）：为防止意外停止，请选中该复选框。有关更多信息，请参阅启用停止保护 (p. 613)。
- Monitoring（监控）：选中此复选框将使用 Amazon CloudWatch 开启对您的实例的详细监控。将收取额外费用。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。
- EBS-optimized instance (EBS 优化的实例)：Amazon EBS 优化的实例使用优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。如果实例类型支持此功能，请选中此复选框来启动该功能。将收取额外费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。
- Tenancy：如果您要在 VPC 内启动实例，可选择在独立的专用硬件 (Dedicated) 或专用主机 (Dedicated host) 上运行实例。可能收取额外费用。有关更多信息，请参阅Dedicated Instances (p. 533) 和 Dedicated Hosts (p. 504)。
- T2/T3 Unlimited (T2/T3 无限)：选中此复选框可允许应用程序突增到基准以上所需的时间。可能收取额外费用。有关更多信息，请参阅可突增性能实例 (p. 274)。
- Network interfaces：如果您选择了特定的子网，则可为实例指定最多两个网络接口：
  - 对于 Network Interface，选择 New network interface 可让 Amazon 创建新的实例，或选择现有且可用的网络接口。
  - 对于 Primary IP，请输入一个您的子网范围内的私有 IPv4 地址，或保留 Auto-assign，让 Amazon 为您选择一个私有 IPv4 地址。
  - 对于 Secondary IP addresses，请选择 Add IP 以将多个私有 IPv4 地址分配给所选网络接口。
  - （仅限 IPv6）对于 IPv6 IP，请选择 Add IP（添加 IP），然后输入子网范围内的 IPv6 地址；或保留 Auto-assign（自动分配），以让 Amazon 为您选择一个地址。
  - 网卡索引：网卡的索引。必须将主网络接口分配给网卡索引 0。有些实例类型支持多个网卡。

  - 选择 Add Device 可添加辅助网络接口。辅助网络接口可以与 VPC 位于不同的子网中，但必须位于您的实例所在的可用区内。

  有关更多信息，请参阅弹性网络接口 (p. 1104)。如果指定多个网络接口，则您的实例无法收到公有 IPv4 地址。此外，如果您为 eth0 指定某个现有网络接口，则无法使用 Auto-assign Public IP 覆盖子网的公有 IPv4 设置。有关更多信息，请参阅在实例启动期间分配公有 IPv4 地址 (p. 1057)。
- Kernel ID (内核 ID)：（仅对半虚拟化 (PV) AMIs 有效）除非您想使用某个特定内核，否则选择 Use default (使用默认值)。
- RAM disk ID (RAM 磁盘 ID)：（仅对半虚拟化 (PV) AMIs 有效）除非您想使用某个特定 RAM 磁盘，否则选择 Use default (使用默认值)。如果您选择了一个内核，则您可能需要选择带有可支持该内核的驱动程序的某个特定 RAM 磁盘。
- Enclave：选择 Enable (启用) 启用 Amazon Nitro Enclaves 的实例。有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？
- 可访问的元数据：您可以启用或禁用对实例元数据服务（IMDS）的访问权限。有关更多信息，请参阅使用 IMDSv2 (p. 755)。
- Metadata transport（传输元数据）：使实例能够访问本地 IMDSv2 IPv6 地址链接（`fd00:ec2::254`）来检索实例元数据。此选项仅在您将 基于 Nitro 系统构建的实例 (p. 246) 启动到仅限 IPv6 的子网中时可用。有关检索实例元数据的更多信息，请参阅 检索实例元数据 (p. 766)。
- 元数据版本：如果您启用对 IMDS 的访问权限，可以选择在请求实例元数据时要求使用实例元数据服务版本 2。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- 元数据标记响应跃点限制：如果您启用 IMDS，可以为元数据标记设置允许的网络跃点数。有关更多信息，请参阅使用 IMDSv2 (p. 755)。
- User data：您可以指定用户数据在启动时配置实例或运行配置脚本。要附加文件，请选择 As file (以文件形式) 选项并浏览到要附加的文件。

步骤 4：添加存储

您选择的 AMI 包含一个或多个存储卷，包括根设备卷。在添加存储页面上，您可以选择添加新卷来指定要附加到实例的其他卷。如下所示配置每个卷，然后选择 Next: Add Tags (下一步：添加标记)。

- Type (类型)：选择实例存储或 Amazon EBS 卷以便与实例关联。列表中可用的卷类型取决于您选择的实例类型。有关更多信息，请参阅Amazon EC2 实例存储 (p. 1579) 和 Amazon EBS 卷 (p. 1324)。
- Device (设备)：从卷的可用设备名称列表中进行选择。
- Snapshot (快照)：输入要从其中还原卷的快照的名称或 ID。您还可以通过在 Snapshot (快照) 字段中键入文本来搜索可用的共享快照和公有快照。快照描述区分大小写。
- Size (大小)：对于 EBS 卷，您可以指定存储大小。即使您选择了有资格享用免费套餐的 AMI 和实例，若要享用免费套餐，您必须将总存储大小保持为 30 GiB 以下。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
- 卷类型：对于 EBS 卷，请选择卷类型。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。
- IOPS：如果选择了Provisioned IOPS SSD 卷类型，则可以输入卷支持的每秒 I/O 操作数 (IOPS)。
- Delete on Termination (终止时删除)：对于 Amazon EBS 卷，请选中此复选框以在实例终止时删除卷。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。
- 加密：如果实例类型支持 EBS 加密，则可以指定卷的加密状态。如果默认情况下在此区域中启用了加密，则将为您选择默认的客户托管密钥。您可以选择其他密钥或禁用加密。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

步骤 5：添加标签

在 Add Tags 页面上，通过提供键和值组合来指定标签 (p. 1664)。您可以标记实例、卷或两者。对于竞价型实例，您只能标记竞价型实例请求。选择 Add another tag 向您的资源添加多个标签。完成时选择 Next: Configure Security Group。

步骤 6：配置安全组

在 Configure Security Group (配置安全组) 页面上，使用安全组为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。所有其他的流量将被忽略。(有关安全组的更多信息，请参阅 适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。) 按如下所示选择或创建安全组，然后选择 Review and Launch。

- 要选择现有安全组，请选择 Select an existing security group (选择现有安全组)，然后选择您的安全组。您无法编辑现有安全组的规则，但是可以通过选择 Copy to new (复制到新项目) 将它们复制到新组。随后您可以按下一步所述添加规则。
- 要创建新安全组，请选择 Create a new security group (创建新安全组)。向导会自动定义 launch-wizard-x 安全组并创建入站规则，以允许您通过 SSH（端口 22）连接到实例。
- 您可以根据需要添加规则。例如，如果您的实例是 Web 服务器，请打开端口 80 (HTTP) 和 443 (HTTPS) 以允许 Internet 流量。

  要添加规则，请选择 Add Rule，选择用于打开网络流量的协议，然后指定源。从 Source 列表中选择 My IP 可让向导添加您计算机的公有 IP 地址。但是，如果您在没有静态 IP 地址的情况下通过 ISP 或从防火墙后面进行连接，则您需要了解客户端计算机使用的 IP 地址范围。

  > Warning
  >
  > 在本次简短练习中，可以接受启用所有 IP 地址 (`0.0.0.0/0`) 以通过 SSH 或 RDP 访问您实例的规则，但这种规则在生产环境中不安全。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

步骤 7：查看实例启动并选择密钥对

在 Review Instance Launch 页面上，检查您的实例的详细信息，然后选择相应的 Edit 链接进行任何必要更改。

如果准备就绪，请选择 Launch。

在 Select an existing key pair or create a new key pair (选择现有密钥对或创建新密钥对) 对话框中，您可以选择现有密钥对，也可以创建新的密钥对。例如，选择 Choose an existing key pair，然后选择您在进行设置时创建的密钥对。有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

> Important
>
> 如果您选择 Proceed without key pair 选项，则将无法连接到此实例，除非您选择配置为允许用户以其他方式登录的 AMI。

要启动您的实例，请选中确认复选框，然后选择 Launch Instances。

(可选) 您可以为实例创建一个状态检查警报 (可能需要额外付费)。在确认屏幕上，选择 Create status check alarms 并按照指示操作。还可以在您启动实例后创建状态检查告警。有关更多信息，请参阅创建和编辑状态检查警报 (p. 978)。

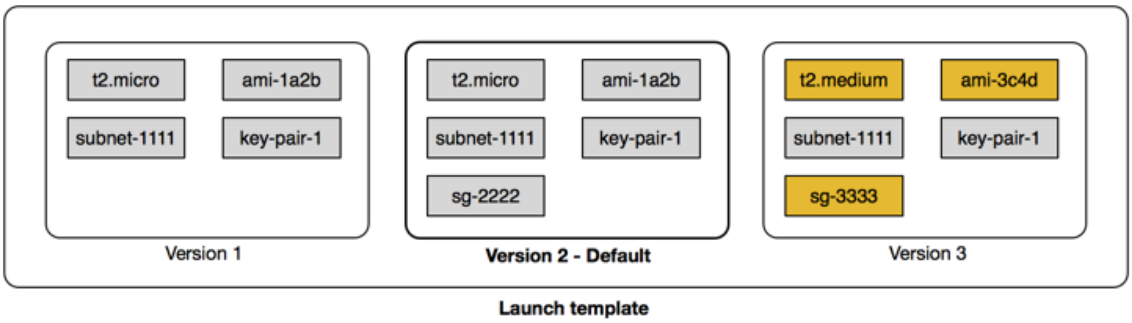
如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

通过启动模板启动实例

您可以创建一个启动模板，其中包含用于启动实例的配置信息。您可以使用启动模板来存储启动参数，而无需在每次启动实例时都指定这些参数。例如，启动模板可能包含您通常用于启动实例的 AMI ID、实例类型和网络设置。在使用 Amazon EC2 控制台、Amazon开发工具包或命令行工具启动实例时，您可以指定要使用的启动模板。

对于每个启动模板，您可以创建一个或多个编号的启动模板版本。每个版本可能具有不同的启动参数。在通过启动模板启动实例时，您可以使用任何版本的启动模板。如果未指定版本，则使用默认版本。您可以将任何启动模板版本设置为默认版本 — 默认情况下，这是启动模板的第一个版本。

下图显示了具有三个版本的启动模板。第一个版本指定用于启动实例的实例类型、AMI ID、子网和密钥对。第二个版本基于第一个版本，并且还为实例指定了一个安全组。第三个版本在某些参数中使用不同的值。版本 2 设置为默认版本。如果通过该启动模板启动实例，并且未指定任何其他版本，则使用版本 2 中的启动参数。



目录

- 启动模板限制 (p. 589)
- 使用启动模板控制启动实例 (p. 589)
- 创建启动模板 (p. 590)
- 修改启动模板（管理启动模板版本） (p. 602)
- 删除启动模板 (p. 604)
- 从启动模板启动实例 (p. 605)

启动模板限制

以下规则适用于启动模板和启动模板版本：

- 限额 – 每个区域最多可以创建 5,000 个启动模板，每个启动模板最多可以有 10,000 个版本。
- 参数可选 – 启动模板参数是可选的。不过，您必须确保启动实例的请求包含所需的所有参数。例如，如果启动模板不包含 AMI ID，您必须在启动实例时指定启动模板和 AMI ID。
- 参数未验证 – 创建启动模板时，不会完全验证启动模板参数。如果您为参数指定了错误的值，或者如果您未使用受支持的参数组合，则任何实例都无法通过此启动模板启动。确保您为参数指定正确的值，并使用支持的参数组合。例如，要在置放群组中启动实例，您必须指定一种支持的实例类型。
- 标签 – 您可以标记启动模板，但无法标记启动模板版本。
- 不可变 – 启动模板不可变。要修改启动模板，必须创建新版本启动模板。
- 版本号 – 启动模板版本按创建顺序编号。在创建启动模板版本时，您无法自行指定版本号。

使用启动模板控制启动实例

您可以指定用户仅在使用启动模板时才能启动实例，且只能使用特定的启动模板。您还可以控制哪些用户能创建、修改、描述和删除启动模板和启动模板版本。

使用启动模板控制启动参数

启动模板可以包含用于启动实例的全部或部分参数。在使用启动模板启动实例时，您可以覆盖启动模板中指定的参数。或者，也可以指定在启动模板中不包含的额外参数。

> **Note**
>
> 您无法在启动期间删除启动模板参数 (例如，无法为参数指定空值)。要删除某个参数，请创建不包含该参数的新启动模板版本，并使用该版本启动实例。

要启动实例，用户必须有权使用 ec2:RunInstances 操作。用户还必须有权创建或使用已创建或与该实例关联的资源。您可以使用 ec2:RunInstances 操作的资源级权限控制用户可以指定的启动参数。或者，您可以为用户授予使用启动模板启动实例的权限。这样，您就可以在启动模板中管理启动参数，而不是在 IAM policy 中管理，并将启动模板作为授权方法以启动实例。例如，您可以指定用户只能使用启动模板启动实例，并且他们只能使用特定的启动模板。您还可以控制用户可以在启动模板中覆盖的启动参数。有关示例策略，请参阅 启动模板 (p. 1254)。

控制启动模板的使用

默认情况下，用户无权使用启动模板。您可以创建一个策略，以便为用户授予创建、修改、描述和删除启动模板和启动模板版本的权限。您还可以将资源级权限应用于某些启动模板操作，以控制用户能否在这些操作中使用特定的资源。有关更多信息，请参阅以下示例策略：示例：使用启动模板 (p. 1265)。

在为用户授予使用 ec2:CreateLaunchTemplate 和 ec2:CreateLaunchTemplateVersion 操作的权限时，应格外小心。您不能使用资源级权限来控制用户可以在启动模板中指定的资源。要限制用于启动实例的资源，请确保仅为相应的管理员授予创建启动模板和启动模板版本的权限。

创建启动模板

使用定义的参数创建新的启动模板，或者将现有的启动模板或实例作为基础以创建新的启动模板。

任务

- 使用您定义的参数创建新启动模板 (p. 590)
- 从现有启动模板创建启动模板 (p. 598)
- 从实例创建启动模板 (p. 598)
- 使用 Systems Manager 参数而非 AMI ID (p. 599)

使用您定义的参数创建新启动模板

您可以使用控制台或 Amazon CLI 创建启动模板：

- 控制台 (p. 590)
- Amazon CLI (p. 596)

控制台

要创建启动模板，您必须指定启动模板名称和至少一个实例配置参数。

启动模板参数在启动模板中进行分组。以下说明将引导您完成每个参数组。

启动模板配置的参数

- 开始创建启动模板 (p. 591)
- 启动模板名称、描述和标签 (p. 591)
- 应用程序和操作系统镜像 (Amazon Machine Image) (p. 591)
- 实例类型 (p. 592)
- 密钥对（登录） (p. 592)
- Network settings (网络设置) (p. 593)
- 配置存储 (p. 594)
- 资源标签 (p. 595)
- 高级详细信息 (p. 595)
- 摘要 (p. 596)

开始创建启动模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择启动模板，然后选择创建启动模板。

启动模板名称、描述和标签

1. 对于设备模板名称，请为您的启动模板输入描述性名称。
2. 对于模板版本说明，提供此版本的启动模板的简短说明。
3. 要在创建时标记 (p. 1664)启动模板，请展开 Template tags（模板标签），选择 Add tag（添加标签），然后输入标签键值对。为每个要添加的其它标签选择 Add tag（添加标签）。

   Note

   要标记启动实例时创建的资源，必须在 Resource tags（资源标签）下面指定标签。有关更多信息，请参阅资源标签 (p. 595)。

应用程序和操作系统镜像 (Amazon Machine Image)

Amazon Machine Image (AMI) 中包含了创建实例所需的信息。例如，AMI 可能包含充当 Web 服务器所需的软件，例如 Linux、Apache 和您的网站。

您可以找到适合的 AMI，如下所示。通过查找 AMI 的每个选项，您可以选择右上角的 Cancel（取消）以返回启动模板，而不选择 AMI。

搜索栏

要搜索所有可用的 AMI，请在 AMI 搜索栏中输入关键字，然后按 Enter 键。要选择 AMI，请选择 Select（选择）。

最近使用的项目

您最近使用的 AMI。

选择 Recently launched（最近启动）或 Currently in use（当前使用），然后在 Amazon Machine Image (AMI) 中，选择一个 AMI。

我的 AMI

您拥有的私有 AMI，或与您共享的私有 AMI。

选择 Owned by me（我拥有的）或 Shared with me（与我共享），然后在 Amazon Machine Image (AMI) 中选择一个 AMI。

Quick Start（快速入门）

AMI 按操作系统 (OS) 分组以助您快速入门。

首先选择所需的操作系统，然后从 Amazon Machine Image (AMI) 中选择一个 AMI。要选择符合免费套餐条件的 AMI，请确保该 AMI 已标记 Free tier eligible（符合免费套餐条件）。

浏览更多 AMI

选择 Browse more AMIs（浏览更多 AMI）以浏览完整的 AMI 目录。

- 要搜索所有可用的 AMI，请在搜索栏中输入关键字，然后按 Enter 键。
- 要使用 Systems Manager 参数查找 AMI，请选择搜索栏右侧的箭头按钮，然后选择 Search by Systems Manager parameter（按 Systems Manager 参数搜索）。有关更多信息，请参阅使用 Systems Manager 参数查找 AMI (p. 119)。
- 要指定在从启动模板启动实例时解析为 AMI 的 Systems Manager 参数，请选择搜索栏右侧的箭头按钮，然后选择指定自定义值/Systems Manager 参数。有关更多信息，请参阅使用 Systems Manager 参数而非 AMI ID (p. 599)。

- 要按类别搜索，请依次选择 Quickstart AMI、My AMIs（我的 AMI）、Amazon Web Services Marketplace AMI 或者 Community AMIs（社区 AMI）。

  Amazon Web Services Marketplace 是一个在线商店，您可以从中购买在 Amazon 上运行的软件（包括 AMI）。有关从 Amazon Web Services Marketplace 启动实例的更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。在 Community AMIs（社区 AMI）中，您可以找到 Amazon 社区成员提供给其它人使用的 AMI。将来自 Amazon 或经过验证的合作伙伴的 AMI 标记为经过验证的提供商。
- 要筛选 AMI 列表，请在屏幕左侧的 Refine results（优化结果）下方选中一个或多个复选框。筛选条件选项会因所选搜索类别而有所不同。
- 检查对每个 AMI 列出的 Root device type (根设备类型)。请注意哪些 AMI 是您需要的类型：即 ebs（由 Amazon EBS 支持）或 instance-store（由实例存储支持）。有关更多信息，请参阅根设备存储 (p. 103)。
- 检查对每个 AMI 列出的 Virtualization type (虚拟化类型)。注意哪些 AMI 类型是您需要的类型：即 hvm（全虚拟化）或 paravirtual（半虚拟化）。例如，一些实例类型需要 HVM。有关更多信息，请参阅 Linux AMI 虚拟化类型 (p. 106)。
- 检查对每个 AMI 列出的启动模式。请注意哪些 AMI 使用您需要的启动模式：legacy-bios、uefi 或 uefi-preferred。有关更多信息，请参阅启动模式 (p. 107)。
- 选择满足您的需求的 AMI，然后选择 Select。

实例类型

实例类型定义了实例的硬件配置和大小。更大的实例类型拥有更多的 CPU 和内存。有关更多信息，请参阅实例类型。

对于 Instance type（实例类型），可以选择一个实例类型或指定实例属性并让 Amazon EC2 使用这些属性识别实例类型。

> **Note**
>
> 仅当使用 Auto Scaling 组、EC2 机群和竞价型实例集来启动实例时，才支持指定实例属性。有关更多信息，请参阅使用基于属性的实例类型选择创建 Auto Scaling 组、EC2 机群的基于属性的实例类型选择 (p. 836) 和 竞价型实例集的基于属性的实例类型选择 (p. 874)。
> 如果您计划使用启动实例向导 (p. 575)中的启动模板，或搭配使用 RunInstances API，则必须选择实例类型。

- Instance type (实例类型)：确保实例类型与指定的 AMI 兼容。有关更多信息，请参阅实例类型 (p. 238)。
- Advanced（高级）：若要指定实例属性并让 Amazon EC2 使用这些属性识别实例类型，请选择 Advanced（高级），然后选择 Specify instance type attributes（指定实例类型属性）。
  - Number of vCPUs（vCPU 量）：输入您的计算要求的最小 vCPU 数和最大 vCPU 数。若要表示为无限制，请输入最小值为 **0**，然后将最大值留空。
  - Amount of memory (MiB) (内存量 (MiB))：输入您的计算要求的最小内存量和最大内存量（以 MiB 为单位）。若要表示为无限制，请输入最小值为 **0**，然后将最大值留空。
  - 展开 Optional instance type attributes（可选的实例类型属性），然后选择 Add attribute（添加属性）以更详细地表达您的计算需求。有关每个属性的信息，请参阅 Amazon EC2 API 参考中的 InstanceRequirementsRequest。
  - Resulting instance types（生成的实例类型）：您可以预览与指定属性匹配的实例类型。若要排除实例类型，请选择 Add attribute（添加属性），并从 Attribute（属性）列表中选择 Excluded instance types（排除的实例类型）。从 Attribute value（属性值）列表中，选择要排除的实例类型。

密钥对（登录）

实例的密钥对。

为 Key pair name（密钥对名称）选择一个现有密钥对，或选择 Create new key pair（创建新密钥对）来新建一个密钥对。有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

Network settings (网络设置)

根据需要配置网络设置。

- 子网：您可以在与可用区、本地扩展区、Wavelength 区域或 Outpost 关联的子网中启动实例。

  要在可用区中启动实例，请选择要在其中启动实例的子网。要创建新子网，请选择 Create new subnet 转到 Amazon VPC 控制台。完成此操作后，返回到向导并选择 Refresh（刷新）图标，以便将您的子网加载到列表中。

  要在本地区域中启动实例，请选择您在本地区域中创建的子网。

  要在 Outpost 中启动实例，请在 VPC 中选择与 Outpost 关联的子网。

- Firewall (security groups)[防火墙（安全组）]：使用一个或多个安全组为实例定义防火墙规则。这些规则指定哪些传入的网络流量可传输到您的实例。所有其他的流量将被忽略。有关安全组的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

  添加网络接口时，您必须在网络接口中指定相同安全组。

  按如下所示进行选择或创建安全组：

  - 要选择现有安全组，请选择 Select an existing security group（选择现有安全组），然后从 Common security groups（通用安全组）中选择您的安全组。
  - 要创建新安全组，请选择 Create security group（创建安全组）。

    您可以根据需要添加规则。例如，如果您的实例是 Web 服务器，请打开端口 80 (HTTP) 和 443 (HTTPS) 以允许 Internet 流量。

    要添加规则，请选择 Add security group rule（添加安全组规则）。对于 Type（类型），请选择网络流量类型。将使用为网络流量打开的协议自动填充 Protocol（协议）字段。对于 Source type（源类型），请选择一种源类型。如需让启动模板添加您计算机的公有 IP 地址，请选择 My IP（我的 IP）。但是，如果您在没有静态 IP 地址的情况下通过 ISP 或从防火墙后面进行连接，则您需要了解客户端电脑使用的 IP 地址范围。

    > Warning
    >
    > 如果您要短时启动测试实例并将很快停止或终止，那么允许所有 IP 地址 (`0.0.0.0/0`) 通过 SSH 或 RDP 访问您的实例的规则是可以接受的，但此规则对生产环境来说是不安全的。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

- Advanced network configuration（高级网络配置）

  网络接口

  - Device index (设备索引)：网络接口的设备号；例如，`eth0` 表示主网络接口。如果将该字段保留空白，Amazon 将创建主网络接口。
  - Network interface（网络接口）：选择 New interface（新接口）即可让 Amazon EC2 创建新的接口，或选择现有且可用的网络接口。
  - Description (描述)：（可选）新网络接口的描述。
  - Subnet（子网）：要在其中创建新网络接口的子网。对于主网络接口 (`eth0`)，这是在其中启动实例的子网。如果为 `eth0` 输入了现有的网络接口，将在该网络接口所在的子网中启动实例。
  - 安全组：VPC 中要与网络接口关联的一个或多个安全组。
  - Auto-assign public IP（自动分配公有 IP）：指定您的实例是否会收到公有 IPv4 地址。默认情况下，默认子网中的实例会收到公有 IPv4 地址，而非默认子网中的实例不会收到。可以选择 Enable (启用) 或 Disable (禁用) 以覆盖子网的默认设置。有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。
  - Primary IP (主要 IP)：您的子网范围内的一个私有 IPv4 地址。保留空白会让 Amazon EC2 为您选择一个私有 IPv4 地址。
  - Secondary IP（辅助 IP）：您的子网范围内的一个或多个其它私有 IPv4 地址。选择 Manually assign（手动分配）然后输入 IP 地址。选择 Add IP（添加 IP）以添加另一个 IP 地址。或者，选择

Automatically assign（自动分配）以使 Amazon EC2 来为您选择，然后输入一个值来指明要添加的 IP 地址的数量。

- (仅限 IPv6) IPv6 IP：子网范围内的一个 IPv6 地址。选择 Manually assign（手动分配）然后输入 IP 地址。选择 Add IP（添加 IP）以添加另一个 IP 地址。或者，选择 Automatically assign（自动分配）以使 Amazon EC2 来为您选择，然后输入一个值来指明要添加的 IP 地址的数量。
- IPv4 前缀：网络接口的 IPv4 前缀。
- IPv6 前缀：网络接口的 IPv6 前缀。
- Delete on termination (终止时删除)：选择在删除实例时是否删除网络接口。
- Elastic Fabric Adapter：指示网络接口是否为 Elastic Fabric Adapter。有关更多信息，请参阅 Elastic Fabric Adapter。
- 网卡索引 ：网卡的索引。必须将主网络接口分配给网卡索引 0。有些实例类型支持多个网卡。

选择 Add network interface（添加网络接口）以添加更多网络接口。您可以添加的网络接口数量取决于选定实例类型支持的数量。辅助网络接口可以与 VPC 位于不同的子网中，但必须位于您的实例所在的可用区内。

有关更多信息，请参阅弹性网络接口 (p. 1104)。如果指定多个网络接口，则您的实例无法收到公有 IPv4 地址。此外，如果您为 eth0 指定某个现有网络接口，则无法使用 Auto-assign Public IP 覆盖子网的公有 IPv4 设置。有关更多信息，请参阅在实例启动期间分配公有 IPv4 地址 (p. 1057)。

配置存储

如果您为启动模板指定了 AMI，则 AMI 会包含一个或多个存储卷，包括根卷 Volume 1 (AMI Root) [卷 1（AMI 根目录）]。您可以指定要附加到实例的其它卷。

您可以使用 Simple（简单）或 Advanced（高级）视图。在 Simple（简单）视图中，您可以指定卷的大小和类型。若要指定所有卷参数，请选择位于卡片的右上角的 Advanced（高级）视图。

要添加新卷，请选择 Add new volume（添加新卷）。

在 Advanced（高级）视图中，您可以按如下方式配置每个卷：

- Storage type（存储类型）：要与实例关联的卷类型（EBS 或临时卷）。仅当您选择支持实例存储（临时）卷类型的实例类型时，该卷类型才可用。有关更多信息，请参阅 Amazon EC2 实例存储 (p. 1579) 和 Amazon EBS 卷 (p. 1324)：
- Device name（设备名称）：从卷的可用设备名称列表中进行选择。
- Snapshot（快照）：选择要从其中创建卷的快照。您可以通过在 Snapshot（快照）字段中输入文本来搜索可用的共享快照和公有快照。
- Size (GiB)（大小 (GiB)）：对于 EBS 卷，您可以指定存储大小。如果您选择了有资格享用免费套餐的 AMI 和实例，请记住，若要享用免费套餐，您必须将总存储大小保持为 30GiB 以下。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
- 卷类型：对于 EBS 卷，请选择卷类型。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。
- IOPS：如果您已选择预置 IOPS SSD（`io1` 和 `io2`）以及通用型 SSD（`gp3`）卷类型，则您可以输入卷可支持的每秒输入/输出操作数（IOPS）。这对于 io1、io2 和 gp3 卷是必需的。gp2、st1、sc1 或标准卷不支持。如果您省略了启动模板中的此参数，必须在从启动模板启动实例时指定其值。
- Delete on termination（终止时删除）：对于 Amazon EBS 卷，选择 Yes（是）以在终止实例时删除此卷或选择 No（否）以保留此卷。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。
- Encrypted（加密）：如果实例类型支持 EBS 加密，则可以选择 Yes（是）以为此卷启用加密。如果默认情况下在此区域中启用了加密，则会为您启用加密。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。
- KMS key（KMS 密钥）：如果您将 Encrypted（加密）选择为 Yes（是），则您必须选择一个客户托管式密钥来加密卷。如果默认情况下在此区域中启用了加密，则将为您选择默认的客户托管密钥。您可以选择不同的密钥或指定由您创建的任何客户托管密钥的 ARN。

资源标签

要标记 (p. 1664)启动实例时创建的资源，在 Resource tags（资源标签）下，选择 Add tag（添加标签），然后输入标签键值对。对于 Resource types（资源类型），指定创建时要标记的资源。您可以为所有资源指定相同的标签，也可以为不同的资源指定不同的标签。为每个要添加的其它标签选择 Add tag（添加标签）。

您可以为使用启动模板时创建的以下资源指定标签：

- 实例
- 卷
- Elastic Graphics
- 竞价型实例请求
- 网络接口

> **Note**
>
> 要为启动模板本身添加标签，您必须在 Template tags（模板标签）下指定标签。有关更多信息，请参阅启动模板名称、描述和标签 (p. 591)。

高级详细信息

对于Advanced details (高级详细信息)，请展开该部分以查看字段并为实例指定任何其他参数。

- Purchasing option（购买选项）：选择 Request Spot Instances（请求竞价型实例）即可按照 Spot 价格请求竞价型实例，以按需价格为上限，而选择 Customize（自定义）即可更改默认的竞价型实例设置。您可以设置最高价（不建议），并更改请求类型、请求时长和中断行为。如果您未请求竞价型实例，则预设情况下 EC2 会启动按需型实例。有关更多信息，请参阅Spot Instances (p. 448)。
- IAM instance profile（IAM 实例配置文件）：选择 Amazon Identity and Access Management (IAM) 实例配置文件以与实例关联。有关更多信息，请参阅适用于 Amazon EC2 的 IAM 角色 (p. 1277)。
- Hostname type（主机名类型）：选择实例的来宾操作系统主机名将包括资源名称还是 IP 名称。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- DNS Hostname（DNS 主机名）：确定对资源名称或 IP 名称的 DNS 查询（根据您对 Hostname type（主机名类型）的选择）是否将以 IPv4 地址（A 记录）、IPv6 地址（AAAA 记录）响应，还是同时以两者响应。有关更多信息，请参阅Amazon EC2 实例主机名类型 (p. 1067)。
- Shutdown behavior (关闭行为)：选择关闭时实例应该停止还是终止。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。
- Stop - Hibernate behavior（停止 – 休眠行为）：要启用休眠，请选择 Enable（启用）。此字段仅适用于满足休眠先决条件的实例。有关更多信息，请参阅休眠 Linux 按需型实例 (p. 616)。
- Termination protection（终止保护）：要防止意外终止，请选择 Enable（启用）。有关更多信息，请参阅启用终止保护 (p. 637)。
- Stop protection（停止保护）：为防止意外停止，请选择 Enable（启用）。有关更多信息，请参阅启用停止保护 (p. 613)。
- Detailed CloudWatch monitoring（详细的 CloudWatch 监控）：选择 Enable（启用）以使用 Amazon CloudWatch 启用实例的详细监控。将收取额外费用。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。
- Elastic inference (弹性推理)：要连接到 EC2 CPU 实例的弹性推理加速器。有关更多信息，请参阅 Amazon Elastic Inference 开发人员指南 中的使用 Amazon Elastic Inference。

> **Note**
>
> 自 2023 年 4 月 15 日起，Amazon 不再允许新客户加入 Amazon Elastic Inference（EI），并将帮助现有客户将其工作负载迁移到价格更低廉且性能更出色的选项。2023 年 4 月 15 日之后，新客户将无法在 Amazon SageMaker、Amazon ECS 或Amazon EC2 中使用 Amazon EI 加速器启

动实例。但是，在过去 30 天内至少使用过一次 Amazon EI 的客户将视为当前客户，可继续使用该服务。

- Credit specification（积分规范）：选择 Unlimited（无限）以允许应用程序只要有需要即突增到基准以上。此字段仅适用于 T 实例。可能收取额外费用。有关更多信息，请参阅可突增性能实例 (p. 274)。
- Placement group name (置放群组名称)：指定要在其中启动实例的置放群组。您可以选择现有置放群组或创建新组。并非可以在置放群组中启动所有实例类型。有关更多信息，请参阅置放群组 (p. 1177)。
- EBS-optimized instance（EBS 优化的实例）：选择 Enable（启用）为 Amazon EBS 输入/输出提供额外的专用容量。并非所有实例类型都支持此功能。将收取额外费用。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。
- Capacity Reservation（容量预留）：指定是在任何开放容量预留 [Open（开放）]、特定容量预留 [Target by ID（按 ID 定位）]，还是容量预留组 [Target by group（按组定位）] 中启动实例。要指定不使用容量预留，请选择 None（无）。有关更多信息，请参阅在现有 容量预留 中启动实例 (p. 543)。
- Tenancy (租期)：选择是在共享硬件（Shared (共享)）、隔离的专用硬件（Dedicated (专用)），还是在专用主机（Dedicated host (专用主机)）上运行您的实例。如果您选择在专用主机上启动实例，则可以指定是否在主机资源组中启动实例，也可以定位特定专用主机。可能收取额外费用。有关更多信息，请参阅 Dedicated Instances (p. 533) 和 Dedicated Hosts (p. 504)。
- RAM disk ID（RAM 磁盘 ID）：[仅对半虚拟 (PV) AMI 有效] 为实例选择一个 RAM 磁盘。如果您选择了一个内核，则您可能需要选择带有可支持该内核的驱动程序的某个特定 RAM 磁盘。
- Kernel ID（内核 ID）：[仅对半虚拟 (PV) AMI 有效] 为实例选择一个内核。
- Nitro Enclave：允许您从 Amazon EC2 实例创建隔离的执行环境，称为 Enclave。选择 Enable（启用）以启用 Amazon Nitro Enclaves 的实例。有关更多信息，请参阅 Amazon Nitro Enclaves 用户指南中的什么是 Amazon Nitro Enclaves？
- 许可证配置：您可以根据指定的许可证配置启动实例，以跟踪您的许可证使用情况。有关更多信息，请参阅《Amazon License Manager 用户指南》中的创建许可证配置。
- Specify CPU options（指定 CPU 选项）：选择 Specify CPU options（指定 CPU 选项）可在启动期间指定自定义 vCPU 数。设置 CPU 内核数和每内核线程数。有关更多信息，请参阅优化 CPU 选项 (p. 721)。
- 元数据传输：您可以根据实例的 IP 地址类型（IPv4、IPv6 或 IPv4 和 IPv6）启用或禁用对该 EC2 实例可用的实例元数据服务（IMDS）的访问方法。有关更多信息，请参阅检索实例元数据 (p. 766)。
- 可访问的元数据：您可以启用或禁用对 IMDS 的访问权限。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- 元数据版本：如果您启用对 IMDS 的访问权限，可以选择在请求实例元数据时要求使用实例元数据服务版本 2。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- 元数据响应跃点限制：如果您启用 IMDS，可以为元数据标记设置允许的网络跃点数。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。
- Allow tags in metadata（允许元数据中的标签）：如果选择 Enable（启用），该实例将允许从其元数据访问其所有标签。如果不在模板中包含此设置，则默认情况下，将不允许对实例元数据中的标签的访问。有关更多信息，请参阅允许访问实例元数据中的标签 (p. 1676)。
- User data：您可以指定用户数据在启动时配置实例或运行配置脚本。有关更多信息，请参阅启动时在 Linux 实例上运行命令 (p. 748)。

摘要

使用 Summary（摘要）面板来查看启动模板配置并创建启动模板。

- 查看启动模板的详细信息并进行任何必要的更改。您可以在 Summary（摘要）面板选择某部分的链接以直接导航到该部分。
- 当您准备好创建启动模板时，请选择 Create launch template（创建启动模板）。

Amazon CLI

要创建启动模板，您必须指定启动模板名称和至少一个实例配置参数。

使用 Amazon CLI 创建启动模板

- 使用 create-launch-template 命令。下面的示例创建一个指定以下内容的启动模板：
  - 启动模板的名称（*TemplateForWebServer*）
  - 启动模板的描述（*WebVersion1*）
  - 启动模板的标签 (*purpose*=*production*)
  - 在 JSON 文件中指定的实例配置数据：
    - 要启动的实例类型 (*r4.4xlarge*) 和 AMI (*ami-8c1be5f6*)
    - 总共 8 个 vCPU 的内核数 (*4*) 和每内核线程数 (*2*)（4 个内核 x 2 个线程）
    - 要在其中启动实例的子网 (*subnet-7b16de0c*)
    - 要分配给实例的公有 IP 地址和 IPv6 地址
    - 实例的标签（*Name*=*webserver*）

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

以下是一个示例 JSON 文件，其中包含实例配置的启动模板数据。

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

下面是示例输出。

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

从现有启动模板创建启动模板

您可以克隆现有的启动模板，然后调整参数以创建新的启动模板。但是，您只能在使用 Amazon EC2 控制台时执行此操作；Amazon CLI 不支持克隆模板。

Console

从现有启动模板创建启动模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择启动模板，然后选择创建启动模板。
3. 对于设备模板名称，请为您的启动模板输入描述性名称。
4. 对于模板版本说明，提供此版本的启动模板的简短说明。
5. 要在创建时标记启动模板，请展开 Template tags (模板标签)，选择 Add tag (添加标签)，然后输入标签键值对。
6. 展开源模板，对于启动模板名称，选择要作为新启动模板基础的启动模板。
7. 对于源模板版本，请选择新启动模板版本所基于的启动模板版本。
8. 根据需要，调整任何启动参数，然后选择Create launch template (创建启动模板)。

从实例创建启动模板

Console

从实例创建启动模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择操作、从实例创建模板。
4. 提供名称、描述和标签，然后根据需要调整启动参数。

   Note

   通过实例创建启动模板时，该实例的网络接口 ID 和 IP 地址将不包含在模板中。
5. 选择创建启动模板。

Amazon CLI

您可以使用 Amazon CLI 从现有实例创建启动模板，方法是先从实例获取启动模板数据，然后使用启动模板数据创建启动模板。

从实例获取启动模板数据

- 使用 get-launch-template-data 命令，并指定实例 ID。您可以将输出作为基础以创建新的启动模板或启动模板版本。默认情况下，输出包含一个顶级 `LaunchTemplateData` 对象，无法在启动模板数据中指定该对象。请使用 `--query` 选项排除该对象。

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

下面是示例输出。

```
    {
```

```
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
                    {
                        "Ipv6Address": "2001:db8:1234:1a00::123"
                    }
                ],
                "PrivateIpAddress": "10.0.0.72"
            }
        ]
    }
```


您可以将输出直接写入到一个文件中，例如：

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

使用启动模板数据创建启动模板

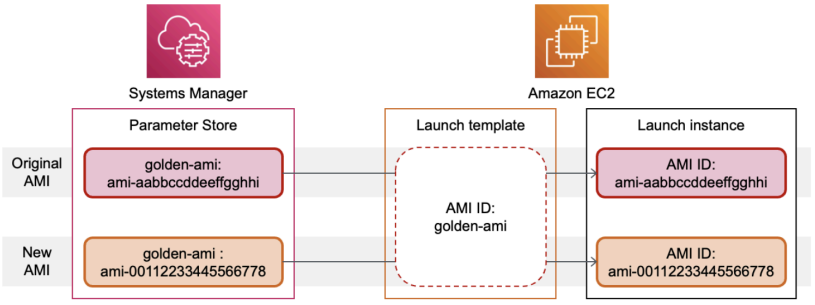
- 使用 create-launch-template 命令可以使用上一步骤的输出创建启动模板。有关使用 Amazon CLI 创建启动模板的更多信息，请参阅使用您定义的参数创建新启动模板 (p. 590)。

使用 Systems Manager 参数而非 AMI ID

您可以指定 Amazon Systems Manager 参数，而不是在启动模板中指定 AMI ID。如果 AMI ID 发生变更，您可以通过更新 Systems Manager Parameter Store 中的 Systems Manager 参数在一个位置更新 AMI ID。使用 Systems Manager 参数，只需一次操作即可更新所有启动模板。

Systems Manager 参数是用户定义的键值对，您可以在 Systems Manager Parameter Store 中创建该键值对。Parameter Store 提供了一个集中位置来存储应用程序配置值。有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的 Amazon Systems Manager Parameter Store。

在下图中，golden-ami 参数首先映射到 Parameter Store 中的原始 AMI ami-aabbccddeeffgghhi。在启动模板中，AMI ID 的值为 golden-ami。使用此启动模板启动实例时，AMI ID 解析为 ami-aabbccddeeffgghhi。之后，AMI 会更新，从而生成新的 AMI ID。在 Parameter Store 中，golden-ami 参数将映射到新的 ami-00112233445566778。启动模板保持不变。使用此启动模板启动实例时，AMI ID 解析为新的 ami-00112233445566778。



AMI ID 的 Systems Manager 参数格式

根据启动模板要求，用户定义的 Systems Manager 参数在替换 AMI ID 时应遵循以下格式：

- 参数类型：String
- 参数数据类型：aws:ec2:image – 确保 Parameter Store 验证您输入的值是否采用 AMI ID 的正确格式。

有关为 AMI ID 创建有效参数的更多信息，请参阅《Amazon Systems Manager 用户指南》中的创建 Systems Manager 参数。

启动模板中的 Systems Manager 参数格式

要在启动模板中使用 Systems Manager 参数替换 AMI ID，必须在启动模板中指定参数时采用以下格式之一：

- resolve:ssm:*parameter-name*
- resolve:ssm:*parameter-name*:*version-number* – 版本号本身是默认标签
- resolve:ssm:*parameter-name*:*label*

参数版本

Systems Manager 参数是版本控制资源。更新参数时，会创建该参数的连续新版本。Systems Manager 支持参数标签，您可以将其映射到参数的特定版本。

例如，golden-ami 参数可能有三个版本：1、2 和 3。您可以创建映射到版本 2 的参数标签 beta，以及映射到版本 3 的参数标签 prod。

在启动模板中，您可以使用以下任一格式指定 golden-ami 参数的版本 3：

- resolve:ssm:golden-ami:3
- resolve:ssm:golden-ami:prod

指定版本或标签是可选的。如果未指定版本或标签，将使用参数的最新版本。

在启动模板中指定 Systems Manager 参数

创建启动模板或其新版本时，可以在启动模板中指定 Systems Manager 参数，而不是 AMI ID。

Console

在启动模板中指定 Systems Manager 参数

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择启动模板，然后选择创建启动模板。
3. 对于设备模板名称，请为您的启动模板输入描述性名称。
4. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统镜像（Amazon 机器映像）] 下，选择 Browse more AMIs（浏览其他 AMI）。
5. 选择搜索栏右侧的箭头按钮，然后选择指定自定义值/Systems Manager 参数。
6. 在指定自定义值或 Systems Manager 参数对话框中，执行以下操作：
   a. 对于 AMI ID 或 Systems Manager 参数字符串，使用以下格式之一输入 Systems Manager 参数名称：
      - resolve:ssm:***parameter-name***
      - resolve:ssm:***parameter-name***:***version-number***
      - resolve:ssm:***parameter-name***:***label***
   b. 选择 Save（保存）。
7. 根据需要指定任何其他启动模板参数，然后选择创建启动模板。

有关更多信息，请参阅使用您定义的参数创建新启动模板 (p. 590)。

Amazon CLI

在启动模板中指定 Systems Manager 参数

- 使用 create-launch-template 命令创建启动模板。要指定要使用的 AMI，请使用以下格式之一输入 Systems Manager 参数名称：
  - `resolve:ssm:`*`parameter-name`*
  - `resolve:ssm:`*`parameter-name`*`:`*`version-number`*
  - `resolve:ssm:`*`parameter-name`*`:`*`label`*

  下面的示例创建一个指定以下内容的启动模板：
  - 启动模板的名称（*TemplateForWebServer*）
  - 启动模板的标签 (*purpose*=*production*)
  - 在 JSON 文件中指定的实例配置数据：
    - 要使用的 AMI (`resolve:ssm:`*`golden-ami`*)
    - 要启动的实例类型 (*m5.4xlarge*)
    - 实例的标签（*Name*=*webserver*）

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

以下是一个示例 JSON 文件，其中包含实例配置的启动模板数据。`ImageId` 的值是以所需格式 `resolve:ssm:`*`golden-ami`* 输入的 Systems Manager 参数名称。

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

有关在自动扩缩组中使用启动模板的更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的在启动模板中使用 Amazon Systems Manager 参数而非 AMI ID。

修改启动模板（管理启动模板版本）

启动模板是不可变的；在创建启动模板之后，您无法修改它。相反，您可以创建包含所需更改的新版本启动模板。

您可以创建不同版本的启动模板，设置默认版本，描述启动模板版本以及删除不再需要的版本。

任务

- 创建启动模板版本 (p. 602)
- 设置默认启动模板版本 (p. 603)
- 描述启动模板版本 (p. 603)
- 删除启动模板版本 (p. 604)

创建启动模板版本

在创建启动模板版本时，您可以指定新的启动参数，或者将现有版本作为基础以创建新的版本。有关启动参数的更多信息，请参阅创建启动模板 (p. 590)。

Console

创建启动模板版本

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Launch Templates。
3. 选择启动模板，然后依次选择 Actions 操作、Modify template (Create new version) (修改模板(创建新版本))。
4. 对于 Template version description（模板版本说明），输入此版本启动模板的说明。
5. （可选）展开 Source template (源模板)，然后选择要用作新启动模板版本基础的启动模板版本。新启动模板版本从此启动模板版本继承启动参数。
6. 根据需要修改启动参数，然后选择创建启动模板。

Amazon CLI

创建启动模板版本

- 使用 create-launch-template-version 命令。您可以指定新版本所基于的源版本。新版本从此版本继承启动参数，您可以使用 `--launch-template-data` 覆盖参数。以下示例根据启动模板的版本 1 创建新的版本并指定不同的 AMI ID。

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

设置默认启动模板版本

您可以设置启动模板的默认版本。如果通过启动模板启动实例并且未指定版本，将使用默认版本的参数启动实例。

Console

设置默认启动模板版本

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Launch Templates。
3. 选择启动模板，然后依次选择操作和设置默认版本。
4. 对于 Template version (模板版本)，选择要设置为默认版本的版本号，然后选择 Set as default version (设置为默认版本)。

Amazon CLI

设置默认启动模板版本

- 使用 modify-launch-template 命令，并指定要设置为默认版本的版本。

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

描述启动模板版本

使用控制台，您可以查看所选启动模板的所有版本，或获取其最新版本或默认版本与特定版本号匹配的启动模板列表。使用 Amazon CLI，您可以描述指定启动模板的所有版本、单个版本或一系列版本。您还可以描述账户中所有启动模板的所有最新版本或所有默认版本。

Console

描述启动模板版本

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Launch Templates。
3. 您可以查看特定启动模板的某个版本，或获取其最新版本或默认版本与特定版本号匹配的启动模板列表。
   - 要查看启动模板的版本，请执行以下操作：选择该启动模板。在版本选项卡上，从版本中选择一个版本以查看其详细信息。
   - 要获取最新版本与特定版本号匹配的所有启动模板的列表，请执行以下操作：从搜索栏中选择最新版本，然后选择版本号。
   - 要获取其默认版本与特定版本号匹配的所有启动模板的列表，请执行以下操作：从搜索栏中选择默认版本，然后选择版本号。

Amazon CLI

描述启动模板版本

- 使用 describe-launch-template-versions 命令，并指定版本号。在以下示例中，指定了版本 *1* 和 *3*。

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

描述您账户中的所有最新的和默认的启动模板版本

- 使用 describe-launch-template-versions 命令并指定 `$Latest` 和/或 `$Default`。您必须在调用中省略启动模板 ID 和名称。您不能指定版本号。

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

删除启动模板版本

如果不再需要某个启动模板版本，您可以将其删除。在删除该版本后，无法替换版本号。您无法删除启动模板的默认版本；您必须先分配一个不同的版本以作为默认版本。要在单个操作中删除所有启动模板版本，请参阅 删除启动模板 (p. 604)。

Console

删除启动模板版本

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Launch Templates。
3. 选择启动模板，然后依次选择操作、删除模板版本。
4. 选择要删除的版本，然后选择 Delete (删除)。

Amazon CLI

删除启动模板版本

- 使用 delete-launch-template-versions 命令，并指定要删除的版本号。

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

删除启动模板

如果不再需要某个启动模板，您可以将其删除。如果删除启动模板，则会删除该模板的所有版本。要删除启动模板的特定版本，请参阅 删除启动模板版本 (p. 604)。

Console

删除启动模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Launch Templates。
3. 选择启动模板，然后依次选择操作、删除模板。
4. 输入 **Delete** 以确认删除，然后选择删除。

Amazon CLI

删除启动模板

- 使用 delete-launch-template (Amazon CLI) 命令，并指定启动模板。

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

从启动模板启动实例

多项实例启动服务均支持启动模板。本主题介绍如何在使用 EC2 启动实例向导、Amazon EC2 Auto Scaling、EC2 实例集和竞价型实例集启动实例时，使用启动模板。

主题

- 通过启动模板启动实例 (p. 605)
- 将启动模板与 Amazon EC2 Auto Scaling 结合使用 (p. 606)
- 将启动模板与 EC2 队列 结合使用 (p. 607)
- 将启动模板与 Spot 实例集结合使用 (p. 607)

通过启动模板启动实例

您可以使用启动模板中包含的参数启动实例。在启动实例之前，您可以选择覆盖或添加启动参数。

将自动为使用启动模板启动的实例分配两个具有 `aws:ec2launchtemplate:id` 和 `aws:ec2launchtemplate:version` 键的标签。您无法删除或编辑这些标签。

Console

使用控制台通过启动模板启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Launch Templates。
3. 选择启动模板，然后依次选择操作、从模板启动实例。
4. 对于 Source template version (源模板版本)，选择要使用的启动模板版本。
5. 对于 Number of instances (实例数)，请指定要启动的实例数。
6. (可选) 您可以在实例详细信息部分中更改和添加参数以覆盖或添加启动模板参数。
7. 选择通过模板启动实例。

Amazon CLI

使用 Amazon CLI 通过启动模板启动实例

- 使用 run-instances 命令并指定 `--launch-template` 参数。可以选择指定要使用的启动模板版本。如果未指定版本，则使用默认版本。

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- 要覆盖启动模板参数，请在 run-instances 命令中指定该参数。以下示例覆盖在启动模板 (如果有) 中指定的实例类型。

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- 如果指定复杂结构包含的嵌套参数，则使用启动模板中指定的复杂结构以及您指定的任何其他嵌套参数启动实例。

  在以下示例中，将使用标签 *Owner*=*TeamA* 以及在启动模板中指定的任何其他标签启动实例。如果启动模板包含具有 *Owner* 键的现有标签，该值将替换为 *TeamA*。

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  在以下示例中，将使用具有设备名称 */dev/xvdb* 的卷以及在启动模板中指定的任何其他块储存设备映射启动实例。如果启动模板为 */dev/xvdb* 定义了一个现有的卷，它的值将替换为指定的值。

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

将启动模板与 Amazon EC2 Auto Scaling 结合使用

您可以创建一个 Auto Scaling 组，并指定一个用于该组的启动模板。在 Amazon EC2 Auto Scaling 启动 Auto Scaling 组中的实例时，它使用关联的启动模板中定义的启动参数。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的使用启动模板创建 Auto Scaling 组 。

在可以使用启动模板创建 Auto Scaling 组之前，您必须创建启动模板，其中包括启动 Auto Scaling 组中的实例所需的参数，例如 AMI 的 ID。控制台提供指导，以帮助您创建可与 Auto Scaling 结合使用的模板。

使用控制台创建要与 Auto Scaling 结合使用的启动模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择启动模板，然后选择创建启动模板。
3. 对于设备模板名称，请为您的启动模板输入描述性名称。
4. 对于模板版本说明，提供此版本的启动模板的简短说明。
5. 在 Auto Scaling guidance（Auto Scaling 指导）下，选中复选框让 Amazon EC2 提供指导，以帮助创建要与 Auto Scaling 结合使用的模板。
6. 根据需要修改启动参数。由于您选择了 Auto Scaling 指导，因此某些字段是必填字段，某些字段不可用。有关创建启动模板时要记住的注意事项以及有关如何为 Auto Scaling 配置启动参数的信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的为 Auto Scaling 组创建启动模板。
7. 选择创建启动模板。
8. （可选）要使用此启动模板创建自动扩缩组，请在 Next steps（后续步骤）页面中选择 Create Auto Scaling group（创建自动扩缩组）。

使用 Amazon CLI 通过启动模板创建或更新 Amazon EC2 Auto Scaling 组

- 使用 create-auto-scaling-group 或 update-auto-scaling-group 命令，并指定 `--launch-template` 参数。

将启动模板与 EC2 队列 结合使用

您可以创建一个 EC2 队列请求，并在实例配置中指定一个启动模板。在 Amazon EC2 完成 EC2 队列 请求时，它使用关联的启动模板中定义的启动参数。您可以覆盖启动模板中指定的某些参数。

有关更多信息，请参阅创建 EC2 队列 (p. 860)。

使用 Amazon CLI 通过启动模板创建 EC2 实例集

- 使用 create-fleet 命令。请使用 `--launch-template-configs` 参数指定启动模板，并为启动模板指定任何覆盖值。

将启动模板与 Spot 实例集结合使用

您可以创建一个 Spot 实例集请求，并在实例配置中指定一个启动模板。在 Amazon EC2 完成 Spot 实例集请求时，它使用关联的启动模板中定义的启动参数。您可以覆盖启动模板中指定的某些参数。

有关更多信息，请参阅创建 Spot 队列请求 (p. 900)。

使用控制台通过启动模板创建竞价型实例集请求

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 在导航窗格中，选择 Spot Requests（竞价型请求），然后选择 Request Spot Instances（请求竞价型实例）。
3. 在 Launch parameters（启动参数）下，选择 Use a launch template（使用启动模板）。
4. 对于 Launch template（启动模板），选择一个启动模板，然后从右侧字段中选择启动模板版本。
5. 在此屏幕上选择不同的选项来配置竞价型实例集。有关选项的更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台） (p. 901)。
6. 准备好创建竞价型实例集后，请选择 Launch（启动）。

使用 Amazon CLI 通过启动模板创建 Spot 实例集请求

- 使用 request-spot-fleet 命令。请使用 `LaunchTemplateConfigs` 参数指定启动模板，并为启动模板指定任何覆盖值。

使用来自现有实例的参数启动实例

Amazon EC2 控制台提供了 Launch more like this（启动更多类似实例）选项，允许将当前实例作为基础来启动其他实例。该选项自动使用所选实例中的特定配置详细信息来填充 Amazon EC2 启动实例向导。

> **Note**
>
> Launch more like this（启动更多类似实例）选项不会克隆所选实例，而只会复制某些配置详细信息。要创建实例的副本，请先从它创建 AMI，然后从 AMI 启动更多实例。
> 或者，创建一个启动模板 (p. 588)以存储您的实例的启动参数。

以下配置详细信息会从所选实例复制到启动实例向导中：

- AMI ID

- 实例类型
- 可用区，或所选实例所在的 VPC 和子网
- 公有 IPv4 地址。如果所选实例当前具有公有 IPv4 地址，则无论所选实例的默认公有 IPv4 地址设置如何，新实例都会收到公有 IPv4 地址。有关公有 IPv4 地址的更多信息，请参阅公有 IPv4 地址 (p. 1054)。
- 置放群组，如果适用
- 与实例关联的 IAM 角色 (如果适用)
- 关闭操作设置 (停止或中止)
- 终止保护设置 (true 或 false)
- CloudWatch 监控 (启用或禁用)
- Amazon EBS 优化的设置 (true 或 false)
- 租期设置 (如果在 VPC (共享或专用) 中启动)
- 内核 ID 和 RAM 磁盘 ID (如果适用)
- 用户数据，如果指定
- 与实例关联的标签 (如果适用)
- 与实例关联的安全组

向导不会从所选实例中复制以下配置详细信息，而会应用其默认设置或行为：

- 网络接口数量：默认为一个网络接口，即主网络接口 (eth0)。
- Storage (存储)：默认存储配置由 AMI 和实例类型确定。

将当前实例用作模板

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择要使用的实例，然后依次选择操作、映像和模板、启动更多类似实例。
4. 此时会打开启动实例向导。通过在此屏幕上选择不同的选项，您可以对实例配置进行必要的更改。

   当您准备好启动实例时，请选择 Launch instance（启动实例）。
5. 如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

启动 Amazon Web Services Marketplace 实例

您可以订阅 Amazon Web Services Marketplace 产品，可以使用 Amazon EC2 启动向导从产品的 AMI 启动实例。有关付费 AMI 的更多信息，请参阅付费 AMI (p. 133)。要在启动之后取消订阅，必须先停止从订阅运行的所有实例。有关更多信息，请参阅管理您的 Amazon Web Services Marketplace 订阅 (p. 136)。

New console

使用启动向导从 Amazon Web Services Marketplace 启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从 Amazon EC2 控制台控制面板中，选择启动实例。
3. （可选）在 Name and tags（名称与标签）下，为 Name（名称）输入实例的描述性名称。
4. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统映像（Amazon 机器映像）] 下，选择 Browse more AMIs（浏览更多 AMI），然后选择 Amazon Web Services Marketplace AMI 选项。通过浏览类别或使用搜索功能找到合适的 AMI。选择 Select（选择）以选择产品。

5. 系统将打开对话框，其中会显示所选产品的概览。您可以查看定价信息，以及供应商提供的任何其他信息。准备就绪后，选择 Continue。

   Note

   在使用 AMI 启动实例之前，您无需为使用产品付费。选择实例类型时，记下每种受支持实例类型的定价。还可能对产品征收其他税款。

6. 对于 Instance type（实例类型），请为您的实例选择实例类型。实例类型定义了要启动的实例的硬件配置和大小。
7. （可选）在 Key pair (login)（密钥对（登录））下，为 Key pair name（密钥对名称）选择一个现有密钥对或新建一个密钥对。
8. 在 Network settings（网络设置）、Firewall (security groups) [防火墙（安全组）] 下，记下按照产品供应商规格创建的新安全组。安全组中的规则可能允许通过 Linux 上的 SSH（端口 22）或 Windows 上的 RDP（端口 3389）进行所有 IPv4 地址 (`0.0.0.0/0`) 访问。我们建议您调整这些规则，以仅允许特定地址或地址范围通过这些端口访问您的实例。
9. 您可以使用屏幕上的其他字段来配置实例、添加存储以及添加标签。有关可以配置的不同选项的信息，请参阅 使用定义的参数启动实例 (p. 577)。
10. 在 Summary（摘要）面板的 Software Image (AMI) [软件映像（AMI）] 下，检查要从中启动实例的 AMI 的详细信息。此外，还要检查您指定的其他配置的详细信息。当您准备好启动您的实例时，请选择 Launch instance（启动实例）。
11. 根据订阅的产品，实例可能需要几分钟或更多时间来启动。您需要先订阅产品，然后才可启动实例。如果存在与信用卡详细信息有关的任何问题，会提示您更新账户详细信息。启动确认页面显示时，选择 View all instances（查看所有实例）以转到 Instances（实例）页面。

    Note

    只要实例处于 `running` 状态（即使处于空闲状态），就会收取订阅费用。如果实例停止，仍可能会收取存储费。

12. 当实例处于 `running` 状态时，可以连接到实例。为此，请在列表中选择实例，然后选择 Connect（连接）并选择一个连接选项。有关连接到实例的更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

    Important

    仔细查看供应商的使用说明，因为您可能需要使用特定用户名称来连接实例。有关访问订阅详细信息的信息，请参阅 管理您的 Amazon Web Services Marketplace 订阅 (p. 136)。

13. 如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

Old console

使用启动向导从 Amazon Web Services Marketplace 启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 Amazon EC2 控制面板中，选择 Launch Instance (启动实例)。
3. 在 Choose an Amazon Machine Image (AMI) (选择一个 Amazon Machine Image (AMI)) 页面上，选择左侧的 Amazon Web Services Marketplace 类别。通过浏览类别或使用搜索功能查找合适的 AMI。选择 Select 以选择产品。
4. 对话框中会显示所选产品的概览。您可以查看定价信息，以及供应商提供的任何其他信息。准备就绪后，选择 Continue。

   Note

   在使用 AMI 启动实例之前，您无需为使用产品付费。记下每种支持的实例类型的定价，向导的下一页会提示您选择实例类型。还可能对产品征收其他税款。

5. 在 Choose an Instance Type (选择一个实例类型) 页面上，选择要启动的实例的硬件配置和大小。完成后，选择 Next: Configure Instance Details。
6. 在向导的后续页面上，可以配置实例、添加存储和添加标签。有关可以配置的不同选项的更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。选择 Next，直至到达 Configure Security Group 页面。

   向导会根据产品的供应商规格来创建新的安全组。安全组中的规则可能允许通过 Linux 上的 SSH (端口 22) 或 Windows 上的 RDP (端口 3389) 进行所有 IPv4 地址 (`0.0.0.0/0`) 访问。我们建议您调整这些规则，以仅允许特定地址或地址范围通过这些端口访问您的实例。

   准备就绪后，选择 Review and Launch。
7. 在 Review Instance Launch (查看实例启动) 页面上，检查要通过其启动实例的 AMI 的详细信息，以及向导中设置的其他配置详细信息。准备就绪后，选择 Launch 以选择或创建密钥对，然后启动实例。
8. 根据订阅的产品，实例可能需要几分钟或更多时间来启动。您需要先订阅产品，然后才可启动实例。如果存在与信用卡详细信息有关的任何问题，会提示您更新账户详细信息。启动确认页面显示时，选择 View Instances 转到“Instances”页面。

   Note

   只要实例在运行 (即使处于空闲状态)，就会收取订阅费用。如果实例停止，仍会收取存储费。
9. 当实例处于 `running` 状态时，可以连接到实例。为此，请在列表中选择实例并选择 Connect。按照对话框中的说明执行。有关连接到实例的更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

   Important

   仔细查看供应商的使用说明，因为您可能需要使用特定用户名称登录实例。有关访问订阅详细信息的更多信息，请参阅管理您的 Amazon Web Services Marketplace 订阅 (p. 136)。
10. 如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

使用 API 和 CLI 启动 Amazon Web Services Marketplace AMI 实例

要使用 API 或命令行工具从 Amazon Web Services Marketplace 产品启动实例，请首先确保订阅了产品。然后您可使用以下方法通过该产品的 AMI ID 启动一个实例：

方法	文档
Amazon CLI	使用 run-instances 命令或参阅以下主题以了解更多信息：启动实例。
Amazon Tools for Windows PowerShell	使用 New-EC2Instance 命令，或参阅以下主题了解更多信息：使用 Windows PowerShell 启动 Amazon EC2 实例
查询 API	使用 RunInstances 请求。

停止和启动您的实例

您可以停止和启动将 Amazon EBS 卷作为其根设备的实例。该实例将保留其实例 ID，但是可以按照概览 (p. 611)部分中所述进行更改。

当您终止一个实例时，我们会将其关闭。我们不会对已停止的实例收费，也不会收取数据传输费，但我们会对所有 Amazon EBS 卷的存储收费。每次您启动已停用的实例时，我们便会收取最低一分钟的使用费用。一

分钟之后，我们仅按您使用实例的秒数收费。例如，如果您运行一个实例 20 秒后停止实例，我们将按一整分钟收取费用。如果您运行一个实例 3 分 40 秒，我们将收取 3 分 40 秒的使用费用。

当实例停止时，您可以像对待所有其他卷一样修改根卷 (例如，修复文件系统问题或更新软件)。您只需从停止的实例分离卷，将其附加到运行中的实例并进行修改，然后将其分离，再次附加到该已停止实例即可。请确保您已使用设备名称被指定为实例块储存设备映射中的根设备对其进行了重新附加。

当您决定不再需要实例时，可以终止该实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，我们就会停止收取与该实例相关的费用。有关更多信息，请参阅终止实例 (p. 634)。如果您愿意休眠实例，请参阅休眠 Linux 按需型实例 (p. 616)。有关更多信息，请参阅重启、停止、休眠和终止之间的区别 (p. 573)。

目录

- 概览 (p. 611)
- 在停止实例时发生的情况 (p. 611)
- 在启动实例时发生的情况 (p. 612)
- 停止和启动您的实例 (p. 612)
- 按计划停止和开启您的实例 (p. 613)
- 启用停止保护 (p. 613)
- 修改已停止的实例 (p. 615)
- 查找所有正在运行和已停止的实例 (p. 616)
- 排查实例的停止问题 (p. 616)

概览

您只能停止由 Amazon EBS 支持的实例。要验证您的实例的根设备类型，请描述实例并检查其根卷的设备类型是 `ebs`（由 Amazon EBS 支持的实例）还是 `instance store`（由实例存储支持的实例）。有关更多信息，请参阅确定 AMI 的根设备类型 (p. 104)。

只有在实例停止时，您才能修改以下实例属性：

- 实例类型
- 用户数据
- 内核
- RAM 磁盘

如果您在实例运行时尝试修改这些属性，Amazon EC2 会返回 `IncorrectInstanceState` 错误。

在停止实例时发生的情况

当您使用 StopInstances API 停止 EC2 实例时（例如，通过选择 Amazon EC2 控制台中的 Instance state（实例状态）、Stop instance（停止实例），或使用 stop-instances Amazon CLI 命令），则在操作系统级别注册以下内容：

- API 请求会向访客发送按钮按下事件。
- 该按钮按下事件致使各种系统服务停止。来自管理程序的 ACPI 关闭按钮按下事件触发正常关闭。
- 启动 ACPI 关闭。
- 当正常关闭进程退出时，实例即会关闭。没有可配置的操作系统关闭时间。
- 如果实例操作系统未在几分钟内完全关闭，则会执行硬关闭。
- 实例将停止运行。

- 实例的状态将先更改为 `stopping`，然后更改为 `stopped`。
- （Auto Scaling 组）如果您的实例处于 Auto Scaling 组中，则 Amazon EC2 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的 Auto Scaling 实例的运行状况检查。
- （Windows）当您停止和启动 Windows 实例时，EC2Config 服务将对该实例执行任务，例如更改所有附加的 Amazon EBS 卷的驱动器号。有关这些默认值以及如何更改它们的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的使用 EC2Config 服务配置 Windows 实例。
- （ClassicLink）当您停止 ClassicLink 实例时，它会从链接的 VPC 取消链接。您必须在开启之后将实例再次链接到 VPC。有关 ClassicLink 的更多信息，请参阅 ClassicLink (p. 1201)。

默认情况下，当您从 Amazon EBS 支持的实例启动关闭（例如，使用 shutdown 或 poweroff 命令）时，该实例会停止。您可以更改此行为，以便使其终止。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。

从实例中使用 halt 命令不会启动关闭。如果使用，实例并不会终止，而是将 CPU 置于 HLT 状态，实例将保持运行。

当您停止实例时，以下内容丢失：

- 存储在 RAM 中的数据。
- 实例存储卷中存储的数据。
- Amazon EC2 在启动或开始时自动分配给实例的公有 IPv4 地址。（要保留永不更改的公有 IPv4 地址，您可以将弹性 IP 地址 (p. 1094)与您的实例关联。）
- （EC2-Classic）使用 EC2-Classic 时，弹性 IP 地址会与实例分离。有关更多信息，请参阅EC2-Classic (p. 1196)。

当您停止实例时，以下内容持续存在：

- 存储在 Amazon EBS 卷中的数据。EBS 卷保持与实例的连接。
- 私有 IPv4 地址。
- IPv6 地址。
- 与实例关联的弹性 IP 地址。请注意，当实例停止时，我们开始向您收取相关弹性 IP 地址的费用 (p. 1094)。

有关更多信息，请参阅重启、停止、休眠和终止之间的区别 (p. 573)。

在启动实例时发生的情况

当您使用 StartInstances API 启动 EC2 实例时（例如，通过选择 Amazon EC2 控制台中的 Instance state（实例状态）、Start instance（启动实例），或使用 start-instances Amazon CLI 命令），将发生以下情况：

- 大多数情况下，实例会迁移到新的底层主机（尽管在某些情况下，它仍会保留在当前主机上）。
- 如果将实例配置为接收公有 IPv4 地址，Amazon EC2 会为实例分配一个新的公有 IPv4 地址。（要保留永不更改的公有 IPv4 地址，您可以将弹性 IP 地址 (p. 1094)与您的实例关联。）

有关更多信息，请参阅重启、停止、休眠和终止之间的区别 (p. 573)。

停止和启动您的实例

您可以使用控制台或命令行停止和启动由 Amazon EBS 支持的实例。

Console

停止和启动由 Amazon EBS 支持的实例

1. 当您停止某个实例时，任何实例存储卷上的数据都将被擦除。在停止实例之前，请确认您是否已将所需数据从实例存储卷复制到持久性存储，例如 Amazon EBS 或 Amazon S3。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择实例状态、停止实例。如果此选项处于禁用状态，则表示实例已停止，或者其根设备是实例存储卷。
4. 当系统提示您确认时，选择 Stop。停止实例可能需要几分钟时间。
5. （可选）当实例已停止时，您可以修改特定的实例属性。有关更多信息，请参阅 modify-stopped-instance。
6. 要启动已停止的实例，请选择该实例，然后依次选择实例状态、启动实例。
7. 实例进入 `running` 状态可能需要几分钟时间。

Command line

停止和启动由 Amazon EBS 支持的实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- stop-instances 和 start-instances (Amazon CLI)
- Stop-EC2Instance 和 Start-EC2Instance (Amazon Tools for Windows PowerShell)

运行受控的故障注入实验

您可以使用 Amazon Fault Injection Simulator 测试您的实例停止和启动时您的应用程序是如何响应的。有关更多信息，请参阅 Amazon Fault Injection Simulator 用户指南。

按计划停止和开启您的实例

您可以制定停止和开启 EC2 实例的计划。以下是配置此过程的两个选项。

在 Amazon 上使用实例调度器

您可以在 Amazon 上使用实例调度器以自动开启和停止 EC2 实例。有关更多信息，请参阅如何将实例调度器与 CloudFormation 一起使用来制定 EC2 实例的计划？ 请注意，需要支付额外费用。

使用 Amazon Lambda 和 Amazon EventBridge 规则

您可以使用 Lambda 和 EventBridge 规则按计划停止和开启您的实例。有关更多信息，请参阅如何使用 Lambda 定期停止和开启 Amazon EC2 实例？

启用停止保护

默认情况下，您可以使用 Amazon EC2 控制台、命令行界面或 API 停止您的实例。要防止实例意外停止，可以为实例启用停止保护。停止保护还可以保护您的实例免遭意外终止。

`DisableApiStop` 属性可控制是否可以使用 Amazon EC2 控制台、Amazon CLI 或 API 停止实例。您可以在实例启动、运行或已停止时设置该属性值。

`DisableApiStop` 属性不会阻止您通过从实例启动关闭来停止实例（使用操作系统的系统关闭命令）。

注意事项

- 启用停止保护不会阻止 Amazon 在实例具有停止实例的计划事件 (p. 981)时停止实例。

- 停止保护不仅可防止实例意外停止，还可以防止使用控制台、Amazon CLI 或 API 时意外终止实例。但是，它不会自动更改 `DisableApiTermination` 属性。请注意，当 `DisableApiStop` 属性设置为 False，`DisableApiTermination` 属性用于确定是否可以使用控制台、Amazon CLI 或 API 终止实例。
- 启用停止保护不会阻止 Amazon EC2 Auto Scaling 在实例运行状况不佳或在横向缩减事件期间终止实例。
- 无法针对由实例存储提供支持的实例启用停止保护。
- 无法针对竞价型实例启用停止保护。
- 启用或禁用停止保护时，Amazon EC2 API 遵循最终一致性模型。有关更多信息，请参阅《Amazon EC2 API 参考》中的最终一致性。

在实例启动时启用停止保护

您可以使用以下方法之一在启动实例时为实例启用停止保护。

Console

在实例启动时为实例启用停止保护

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制面板上，选择启动实例。
3. 在新启动实例向导 (p. 575)中配置您的实例。

   要启用停止保护，在 Advanced details（高级详细信息）下，针对 Stop protection（停止保护），选择 Enable（启用）。

Amazon CLI

在实例启动时启用停止保护

使用 run-instances Amazon CLI 命令启动实例，并指定 `disable-api-stop` 参数。

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

为正在运行或已停止的实例启用停止保护

您可以使用以下方法之一在实例正在运行或已停止时启用停止保护。

Console

为正在运行或已停止的实例启用停止保护

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances（实例）。
3. 选择实例，然后依次选择 Actions（操作）、Instance Settings（实例设置）、Change Stop Protection（更改停止保护）。
4. 选择 Enable（启用）复选框，然后选择 Save（保存）。

Amazon CLI

为正在运行或已停止的实例启用停止保护

使用 modify-instance-attribute Amazon CLI 命令并指定 `disable-api-stop` 参数。

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

为正在运行或已停止的实例禁用停止保护

您可以使用以下方法之一为正在运行或已停止的实例禁用停止保护。

Console

为正在运行或已停止的实例禁用停止保护

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances（实例）。
3. 选择实例，然后依次选择 Actions（操作）、Instance Settings（实例设置）、Change Stop Protection（更改停止保护）。
4. 取消选中 Enable（启用）复选框，然后选择 Save（保存）。

Amazon CLI

为正在运行或已停止的实例禁用停止保护

使用 modify-instance-attribute Amazon CLI 命令并指定 `no-disable-api-stop` 参数。

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --no-disable-api-stop
```

修改已停止的实例

您可以使用 Amazon Web Services Management Console或命令行界面来更改已停止实例的实例类型、用户数据或 EBS 优化属性。您无法使用 Amazon Web Services Management Console修改 `DeleteOnTermination`、内核或 RAM 磁盘属性。

修改实例属性

- 要更改实例类型，请参阅更改实例类型 (p. 399)。
- 要更改您的实例的用户数据，请参阅处理实例用户数据 (p. 774)。
- 要为您的实例启用或禁用 EBS 优化，请参阅修改 EBS 优化 (p. 1549)。
- 要更改您的实例的根卷的 `DeleteOnTermination` 属性，请参阅更新正在运行的实例的块储存设备映射 (p. 1621)。您无需停止实例即可更改此属性。

使用命令行修改实例属性

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- modify-instance-attribute (Amazon CLI)
- Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

查找所有正在运行和已停止的实例

您可以在 Amazon EC2 全局视图中的单个页面上找到所有 Amazon Web Services 区域 中正在运行和已停止的实例。这对于清点资源和查找忘记的实例特别有用。有关如何使用全局视图的信息，请参阅 使用 Amazon EC2 全局视图列出和筛选跨区域的资源 (p. 1663)。

排查实例的停止问题

如果您停止了由 Amazon EBS 支持的实例，而该实例“卡在”了 stopping 状态，则可以强制停止它。有关更多信息，请参阅排查实例的停止问题 (p. 1700)。

休眠 Linux 按需型实例

当您使实例休眠时，Amazon EC2 会向操作系统发出信号来执行休眠 (suspend-to-disk)。休眠会将实例内存 (RAM) 中的内容保存到您的 Amazon Elastic Block Store (Amazon EBS) 根卷。Amazon EC2 保存实例的 EBS 根卷以及任何附加的 EBS 数据卷。在启动实例时：

- EBS 根卷会恢复为之前的状态
- 会重新加载 RAM 内容
- 并恢复实例上之前运行的进程
- 之前附加的数据卷会重新附加，实例也会保留其实例 ID

只有当实例已启用休眠 (p. 625)并且满足休眠先决条件 (p. 617)，您才可以使该实例休眠。

如果实例或应用程序在引导和进行内存占用以开始发挥全部生产功能时所需的时间较长，您可以使用休眠来预热实例。要预热实例，您需要执行以下操作：

1. 启动实例时启用休眠。
2. 将其设置为所需的状态。
3. 使实例休眠，并在需要时随时恢复到所需状态。

在休眠实例处于 stopped 状态时，您不需要为其实例使用付费。但是，当实例处于 stopping 状态时，此时 RAM 的内容会转移到 EBS 根卷，会向您收取实例使用费用。（这不同于您停止一个实例 (p. 610)而不使其休眠。）您不需要支付数据传输费用。但会向您收取任何 EBS 卷的存储费用，包括存储 RAM 内容的费用。

如果您不再需要某个实例，可以随时终止它，包括当实例处于 stopped（已休眠）状态时。有关更多信息，请参阅终止实例 (p. 634)。

> **Note**
>
> 有关在 Windows 实例上使用休眠的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的使 Windows 实例休眠。
> 本主题介绍如何休眠按需型实例（包括预留实例或容量预留可能涵盖的实例）。有关将 Spot 实例休眠的信息，请参阅 休眠中断的竞价型实例 (p. 486)。

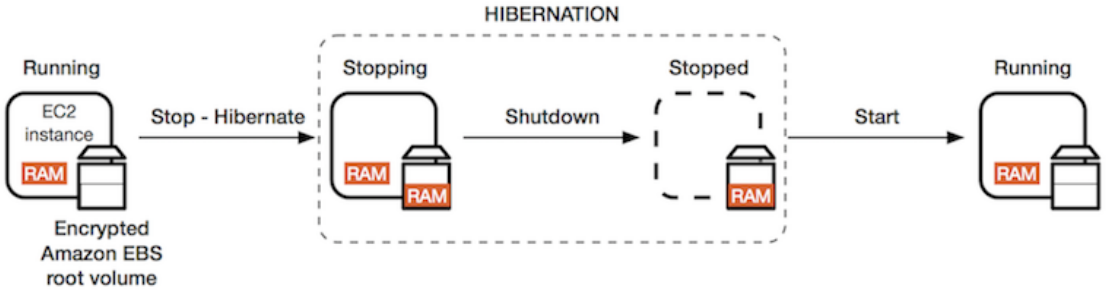
目录

- 休眠概述 (p. 617)
- 休眠先决条件 (p. 617)
- 限制 (p. 620)
- 配置现有 AMI 以支持休眠 (p. 620)
- 为实例启用休眠 (p. 625)
- 在实例上禁用 KASLR（仅限 Ubuntu） (p. 628)
- 休眠实例 (p. 628)

- 启动已休眠的实例 (p. 630)
- 休眠故障排除 (p. 630)

休眠概述

下图显示了休眠过程的基本概述。



当您使正在运行的实例休眠时，将出现以下情况：

- 启动休眠时，实例将进入 `stopping` 状态。Amazon EC2 会向操作系统发出信号来执行休眠 (suspend-to-disk)。休眠会冻结所有进程、将 RAM 中的内容保存到 EBS 根卷，然后执行常规关闭。
- 关闭完成后，实例将进入 `stopped` 状态。
- 所有 EBS 卷保持附加到实例，而且其数据将保留下来，包括已保存的 RAM 内容。
- 所有 Amazon EC2 实例存储卷都会继续保持连接到实例，但实例存储卷上的数据将会丢失。
- 大多数情况下，实例会在启动时迁移到新的底层主机。当您停止并启动实例时，也会发生此类情况。
- 当您启动实例时，实例将启动，操作系统从 EBS 根卷读取 RAM 内容，然后再对进程解除冻结以恢复其状态。
- 实例会保留其私有 IPv4 地址和任何 IPv6 地址。启动实例时，实例将继续保留其私有 IPv4 地址和任何 IPv6 地址。
- Amazon EC2 释放公有 IPv4 地址。启动实例时，Amazon EC2 会为实例分配一个新的公有 IPv4 地址。
- 实例会保留其关联的弹性 IP 地址。您需要为与已休眠实例关联的所有弹性 IP 地址付费。借助 EC2-Classic，弹性 IP 地址会在您将实例休眠时取消与它的关联。有关更多信息，请参阅EC2-Classic (p. 1196)。
- 当您使 ClassicLink 实例休眠时，它会与所链接的 VPC 取消链接。您必须在启动之后将实例再次链接到 VPC。有关更多信息，请参阅ClassicLink (p. 1201)。

有关休眠与重启、停止和终止之间的区别，请参阅重启、停止、休眠和终止之间的区别 (p. 573)。

休眠先决条件

若要休眠按需型实例，必须满足以下先决条件：

- 支持的 Linux AMI (p. 618)
- 支持的实例系列 (p. 618)
- 实例大小 (p. 619)
- 实例 RAM 大小 (p. 619)
- 根卷类型 (p. 619)
- EBS 根卷大小 (p. 619)
- 支持的 EBS 卷类型 (p. 619)
- EBS 根卷加密 (p. 619)

- 在启动时启用休眠 (p. 620)
- 购买选项 (p. 620)

支持的 Linux AMI

必须是支持休眠的 HVM AMI：

AMI	Xen - supported instance families only	Nitro - supported instance families only
Amazon Linux 2 AMI 发布了 2019.08.29 版或更高版本。	支持	支持
Amazon Linux AMI 2018.03 发布了 2018.11.16 版或更高版本。	支持	支持
CentOS 版本 8 AMI [1]（需要使用额外的配置 (p. 622)）	不支持	支持
Fedora 版本 34 或更高版本 AMI [1]（需要使用额外的配置 (p. 622)）	不支持	支持
Red Hat Enterprise Linux (RHEL) 8 AMI [1]（需要使用额外的配置 (p. 623)）	不支持	支持
Ubuntu 20.04 LTS - Focal AMI 发布了序列号 20210820 或更高版本 [2]	支持	支持
Ubuntu 18.04 LTS - Bionic AMI 发布了序列号 20190722.1 或更高版本 [2]	支持	支持
Ubuntu 16.04 LTS-Xenial AMI [2] [3]（需要使用额外的配置 (p. 624)）	支持	支持

[1] 对于 CentOS、Fedora 和 Red Hat Enterprise Linux，仅在基于 Nitro 的实例上支持休眠。

[2] 我们建议在采用 Ubuntu 20.04 LTS – Focal、Ubuntu 18.04 LTS - Bionic 和 Ubuntu 16.04 LTS - Xenial 的实例上禁用 KASLR。有关更多信息，请参阅在实例上禁用 KASLR（仅限 Ubuntu） (p. 628)。

[3] 对于 Ubuntu 16.04 LTS - Xenial AMI，在 `t3.nano` 实例类型上不支持休眠。补丁将不可用，因为 Ubuntu Xenial 于 2021 年 4 月终止了支持。如果想使用 `t3.nano` 实例类型，我们建议您升级到 Ubuntu 20.04 LTS - Focal AMI 或 Ubuntu 18.04 LTS - Bionic AMI。

要配置您自己的 AMI 以支持休眠，请参阅 配置现有 AMI 以支持休眠 (p. 620)。

即将支持 Ubuntu 的其他版本和其他操作系统。

有关支持的 Windows AMI 的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中支持的 Windows AMI。

支持的实例系列

- 通用型：M3、M4、M5、M5a、M5ad、M5d、M6i、M6id、T2、T3 和 T3a

- 计算优化型：C3、C4、C5、C5d、C6i 和 C6id
- 内存优化型：R3、R4、R5、R5a、R5ad 和 R5d
- 存储优化型：I3 和 I3en

查看特定区域中支持休眠的可用实例类型

可用的实例类型因区域而异。要查看某个区域中支持休眠的可用实例类型，请使用带 `--region` 参数的 describe-instance-types 命令。包括 `--filters` 参数以将结果范围限定为支持休眠的实例类型，并包括 `--query` 参数以将输出范围限定为 `InstanceType` 的值。

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --query
 "InstanceTypes[*].[InstanceType]" --output text | sort
```

输出示例

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
c4.8xlarge
...
```

实例大小

不支持裸机实例。

实例 RAM 大小

必须小于 150 GB。

根卷类型

必须是 EBS 卷，而不是实例存储卷。

EBS 根卷大小

必须足够大，以存储 RAM 内容并满足您的预期使用量，例如，操作系统或应用程序。如果您启用休眠，则启动时在根卷上分配空间以存储 RAM。

支持的 EBS 卷类型

- 通用型 SSD（`gp2` 和 `gp3`）
- 预置 IOPS SSD（`io1` 和 `io2`）

如果选择预置 IOPS SSD 卷类型，您必须为 EBS 卷预置合适的 IOPS，以实现休眠状态的最佳性能。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。

EBS 根卷加密

要使用休眠，必须加密根卷以确保在休眠时保护内存中的敏感内容。将 RAM 数据移动到 EBS 根卷时，它始终加密。根卷的加密在实例启动时实施。

可以使用以下三个选项之一，以确保根卷是加密的 EBS 卷：

- EBS encryption by default（EBS 原定设置加密）- 您可以启用 EBS 原定设置加密，以确保对在您的 Amazon 账户中创建的所有新 EBS 卷进行加密。这样，您就可以为实例启用休眠，而无需在实例启动时指定加密意图。有关更多信息，请参阅默认加密 (p. 1507)。
- EBS "single-step" encryption（EBS“单步”加密）- 您可以从未加密的 AMI 中启动 EBS 支持的加密 EC2 实例，并且还可以同时启用休眠。有关更多信息，请参阅将加密与 EBS 支持的 AMI 结合使用 (p. 196)。
- Encrypted AMI（加密的 AMI）- 您可以使用加密的 AMI 启动实例以启用 EBS 加密。如果 AMI 没有加密的根快照，则可以将其复制到新的 AMI 并请求加密。有关更多信息，请参阅 在复制过程中将未加密映像加密 (p. 200) 和 复制 AMI (p. 174)。

在启动时启用休眠

您不能在现有实例（正在运行或已停止）上启用休眠。有关更多信息，请参阅为实例启用休眠 (p. 625)。

购买选项

此功能仅适用于按需型实例，包括那些应用了预留实例计费折扣的实例。它不适用于竞价型实例。有关将 Spot 实例休眠的信息，请参阅 休眠中断的竞价型实例 (p. 486)。

限制

- 当您休眠某个实例时，任何实例存储卷上的数据都会丢失。
- 您不能将具有超过 150 GB 的 RAM 的实例休眠。
- 如果您从已休眠或已启用休眠的实例创建快照或 AMI，则可能无法连接到从该 AMI 启动的新实例，或者通过从快照创建的 AMI 启动的新实例。
- 您不能更改已启用休眠时的实例的实例类型或大小。
- 您不能使位于 Auto Scaling 组中或者由 Amazon ECS 使用的实例休眠。如果实例位于 Auto Scaling 组中并且您尝试使该实例休眠，则 Amazon EC2 Auto Scaling 服务会将已停止的实例标记为运行状况不佳，可能会终止它并启动替换实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的 Auto Scaling 实例的运行状况检查。
- 您不能使配置为在 UEFI 模式下启动的实例休眠。
- 如果您休眠启动到 容量预留 的实例，容量预留 不能确保休眠的实例在尝试启动后可以恢复。
- 如已启用美国联邦信息处理标准（FIPS）模式，则无法将内核低于 5.10 的实例休眠。
- 我们支持的实例持续休眠时间不超过 60 天。要保留实例超过 60 天，您必须启动已休眠的实例，停止该实例，然后启动它。
- 我们不断通过升级和安全补丁更新平台，这可能会与现有已休眠的实例冲突。我们会通知您有关需要启动已休眠实例的关键更新，这样我们才会执行关闭或重启操作以应用必需的升级和安全补丁。

配置现有 AMI 以支持休眠

以下 AMI 支持休眠，但要使通过其中一个 AMI 启动的实例休眠，您需要使用额外的配置，然后才能使实例休眠。

需要使用额外的配置：

- Amazon Linux 2 最小 AMI 发布了 2019.08.29 版或更高版本 (p. 621)
- 在 2019.08.29 前发布的 Amazon Linux 2 (p. 621)
- 在 2018.11.16 前发布的 Amazon Linux (p. 621)
- CentOS 版本 8 或更高版本 (p. 622)
- Fedora 34 版或更高版本 (p. 622)
- Red Hat Enterprise Linux 版本 8 或更高版本 (p. 623)

- Ubuntu 20.04 LTS - Focal 在序列号 20210820 前发布 (p. 623)
- Ubuntu 18.04 - Bionic 在序列号 20190722.1 前发布 (p. 624)
- Ubuntu 16.04 - Xenial (p. 624)

有关更多信息，请参阅更新 Amazon Linux 实例上的实例软件 (p. 700)。

以下 AMI 无需使用额外的配置，因为它们已配置为支持休眠：

- Amazon Linux 2 完整 AMI 发布了 2019.08.29 版或更高版本
- Amazon Linux AMI 2018.03 发布了 2018.11.16 版或更高版本。
- UUbuntu 20.04 LTS - Focal AMI 发布了序列号 20210820 或更高版本
- Ubuntu 18.04 LTS - Bionic AMI 发布了序列号 20190722.1 或更高版本。

Amazon Linux 2 最小 AMI 发布了 2019.08.29 版或更高版本

配置 2019.08.29 版或更高版本的 Amazon Linux 2 最小 AMI 以支持休眠

1. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. 重新启动 服务。

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

在 2019.08.29 前发布的 Amazon Linux 2

配置在 2019.08.29 前发布的 Amazon Linux 2 AMI 以支持休眠

1. 将内核更新为 4.14.138-114.102 或更高版本。

```
[ec2-user ~]$ sudo yum update kernel
```

2. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

4. 确认内核版本已更新为 4.14.138-114.102 或更高版本。

```
[ec2-user ~]$ uname -a
```

5. 停止实例并创建 AMI。有关更多信息，请参阅从实例创建 Linux AMI (p. 139)。

在 2018.11.16 前发布的 Amazon Linux

配置在 2018.11.16 前发布的 Amazon Linux AMI 以支持休眠

1. 将内核更新为 4.14.77-70.59 或更高版本。

```
[ec2-user ~]$ sudo yum update kernel
```

2. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

4. 确认内核版本已更新为 4.14.77-70.59 或更高版本。

```
[ec2-user ~]$ uname -a
```

5. 停止实例并创建 AMI。有关更多信息，请参阅从实例创建 Linux AMI (p. 139)。

CentOS 版本 8 或更高版本

配置 CentOS 版本 8 或更高版本 AMI 以支持休眠

1. 将内核更新为 4.18.0-305.7.1.el8_4.x86_64 或更高版本。

```
[ec2-user ~]$ sudo yum update kernel
```

2. 安装 Extra Packages for Enterprise Linux (EPEL) 存储库。

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-8.noarch.rpm
```

3. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. 启用休眠代理以在引导时开启。

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

6. 确认内核版本已更新为 4.18.0-305.7.1.el8_4.x86_64 或更高版本。

```
[ec2-user ~]$ uname -a
```

Fedora 34 版或更高版本

配置 Fedora 版本 34 或更高版本 AMI 以支持休眠

1. 将内核更新为 5.12.10-300.fc34.x86_64 或更高版本。

```
[ec2-user ~]$ sudo yum update kernel
```

2. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. 启用休眠代理以在引导时开启。

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

5. 确认内核版本已更新为 `5.12.10-300.fc34.x86_64` 或更高版本。

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux 版本 8 或更高版本

配置 Red Hat Enterprise Linux 版本 8 AMI 以支持休眠

1. 将内核更新为 `4.18.0-305.7.1.el8_4.x86_64` 或更高版本。

```
[ec2-user ~]$ sudo yum update kernel
```

2. 安装 Extra Packages for Enterprise Linux (EPEL) 存储库。

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. 从存储库安装 `ec2-hibinit-agent` 程序包。

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. 启用休眠代理以在引导时开启。

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

6. 确认内核版本已更新为 `4.18.0-305.7.1.el8_4.x86_64` 或更高版本。

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 LTS - Focal 在序列号 20210820 前发布

配置在序列号 20210820 前发布的 Ubuntu 20.04 LTS - Focal AMI 以支持休眠

1. 将 linux-aws-kernel 更新为 `5.8.0-1038.40` 或更高版本，并将 grub2 更新为 `2.04-1ubuntu26.13` 或更高版本。

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

3. 确认内核版本已更新为 5.8.0-1038.40 或更高版本。

```
[ec2-user ~]$ uname -a
```

4. 确认 grub2 版本已更新为 2.04-1ubuntu26.13 或更高版本。

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 - Bionic 在序列号 20190722.1 前发布

配置在序列号 20190722.1 前发布的 Ubuntu 18.04 LTS AMI 以支持休眠

1. 将内核更新为 4.15.0-1044 或更高版本。

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

4. 确认内核版本已更新为 4.15.0-1044 或更高版本。

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 - Xenial

要将 Ubuntu 16.04 LTS 配置为支持休眠，您需要安装 Linux-aws-hwe 内核软件包版本 4.15.0-1058-aws 或更高版本以及 ec2-hibinit-agent。

> **Important**
>
> linux-aws-hwe 内核程序包受规范支持。对 Ubuntu 16.04 LTS 的标准支持于 2021 年 4 月结束，该软件包不再定期更新。但是，它将接收其他安全更新，直到扩展安全性维护支持在 2024 年结束。有关更多信息，请参阅规范 Ubuntu 博客上现已提供的适用于 Ubuntu 16.04 LTS 的 Amazon EC2 休眠。
> 我们建议您升级到 Ubuntu 20.04 LTS - Focal AMI 或 Ubuntu 18.04 LTS - Bionic AMI。

配置 Ubuntu 16.04 LTS AMI 以支持休眠

1. 将内核更新为 4.15.0-1058-aws 或更高版本。

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. 从存储库安装 ec2-hibinit-agent 程序包。

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

4. 确认内核版本已更新为 4.15.0-1058-aws 或更高版本。

```
[ec2-user ~]$ uname -a
```

为实例启用休眠

要使实例休眠，您必须在启动实例时先为其启用休眠。

> **Important**
>
> 启动实例后，无法为实例启用或禁用休眠。

New console

使用控制台启用休眠

1. 按照步骤启动实例 (p. 576)，但请在完成以下步骤以启用休眠之后再启动实例。
2. 若要启用休眠，请在启动实例向导中配置以下字段：
   a. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统映像（Amazon 机器映像）] 下，选择支持休眠的 AMI。有关更多信息，请参阅支持的 Linux AMI (p. 618)。
   b. 在 Instance type（实例类型）下，选择一个受支持的实例类型。有关更多信息，请参阅支持的实例系列 (p. 618)。
   c. 在 Configure storage（配置存储）下，选择右侧的 Advanced（高级），并为根卷指定以下信息：
      - 在大小 (GiB) 中，输入 EBS 根卷大小。卷必须足够大，以存储 RAM 内容并满足您的预期使用量。
      - 对于 Volume Type（卷类型），选择支持的 EBS 卷类型：通用型 SSD（gp2 和 gp3）或预调配 IOPS SSD（io1 和 io2）。
      - 对于 Encrypted（已加密），选择 Yes（是）。如果您在此 Amazon 区域中启用了默认加密，则系统会选择 Yes（是）。
      - 对于 KMS key（KMS 密钥），请选择卷的加密密钥。如果您在此 Amazon 区域中启用了默认加密，则会选择默认加密密钥。

      有关根卷先决条件的更多信息，请参阅休眠先决条件 (p. 617)。
   d. 展开 Advanced details（高级详细信息），找到 Stop - Hibernate behavior（停止 – 休眠行为），然后选择 Enable（启用）。
3. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

Old console

使用控制台启用休眠

1. 按照使用旧的启动实例向导启动实例 (p. 583)过程操作。

2. 在选择一个 Amazon Machine Image (AMI) 页面上，选择一个支持休眠的 AMI。有关支持的 AMI 的更多信息，请参阅休眠先决条件 (p. 617)。
3. 在选择一个实例类型页面上，选择一种支持的实例类型，然后选择下一步：配置实例详细信息。有关支持的实例类型的信息，请参阅休眠先决条件 (p. 617)。
4. 在配置实例详细信息页面上，对于 Stop - Hibernate Behavior (停止 - 休眠操作)，选中 Enable hibernation as an additional stop behavior (启用休眠作为额外的停止操作) 复选框。
5. 在添加存储页面上，为根卷指定以下信息：

   - 在大小 (GiB) 中，输入 EBS 根卷大小。卷必须足够大，以存储 RAM 内容并满足您的预期使用量。
   - 对于 Volume Type (卷类型)，选择支持的 EBS 卷类型、通用型 SSD（gp2 和 gp3）或预置 IOPS SSD（io1 和 io2）。
   - 对于加密，请选择卷的加密密钥。如果您在此 Amazon 区域中启用了默认加密，则会选择默认加密密钥。

   有关根卷先决条件的更多信息，请参阅休眠先决条件 (p. 617)。
6. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。

Amazon CLI

使用 Amazon CLI 启用休眠

使用 run-instances 命令启动实例。使用 `--block-device-mappings file://mapping.json` 参数指定 EBS 根卷参数，并使用 `--hibernation-options Configured=true` 参数启用休眠。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

在 `mapping.json` 中指定以下内容。

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

Note

`DeviceName` 的值必须匹配与 AMI 关联的根设备名称。要查找根设备名称，请使用 describe-images 命令。

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

如果您在此 Amazon 区域中启用了默认加密，则可以省略 `"Encrypted": true`。

PowerShell

使用 Amazon Tools for Windows PowerShell 启用休眠

使用 New-EC2Instance 命令启动实例。通过首先定义块储存设备映射，然后使用 -BlockDeviceMappings 参数将其添加到命令来指定 EBS 根卷。使用 -HibernationOptions_Configured $true 参数启用休眠。

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
             -ImageId ami-0abcdef1234567890 `
             -InstanceType m5.large `
             -BlockDeviceMappings $ebs_encrypt `
             -HibernationOptions_Configured $true `
             -MinCount 1 `
             -MaxCount 1 `
             -KeyName MyKeyPair
```

Note

DeviceName 的值必须匹配与 AMI 关联的根设备名称。要查找根设备名称，请使用 Get-EC2Image 命令。

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

如果您在此 Amazon 区域中启用了默认加密，则可以在块储存设备映射中省略 Encrypted = $true。

Console

查看实例是否启用休眠

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后在详细信息选项卡上的实例详细信息部分中检查停止 – 休眠操作。已启用 表明已为实例启用休眠。

Amazon CLI

查看实例是否启用休眠

使用 describe-instances 命令并指定 --filters "Name=hibernation-options.configured,Values=true" 参数以筛选启用了休眠的实例。

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

输出中的以下字段指示实例已启用了休眠。

```
"HibernationOptions": {
```

```
    "Configured": true
}
```

PowerShell

查看是否已使用 Amazon Tools for Windows PowerShell 为实例启用休眠

使用 Get-EC2Instance 命令并指定 `-Filter @{ Name="hibernation-options.configured"; Value="true"}` 参数以筛选启用了休眠的实例。

```
Get-EC2Instance `
    -Filter @{ Name="hibernation-options.configured"; Value="true"}
```

输出会列出已启用休眠的 EC2 实例。

在实例上禁用 KASLR（仅限 Ubuntu）

要使用 Ubuntu 16.04 LTS - Xenial、Ubuntu 18.04 LTS - Bionic（通过序列号 20190722.1 或更高版本发布）或者 Ubuntu 20.04 LTS - Focal（通过序列号 20210820 或更高版本发布）在新启动的实例上运行休眠，我们建议禁用 KASLR（内核地址空间布局随机化）。在 Ubuntu 16.04 LTS、Ubuntu 18.04 LTS 或 Ubuntu 20.04 LTS 上，默认启用 KASLR。

KASLR 是一项标准 Linux 内核安全功能，它通过随机化内核的基本地址值，来帮助减少尚未发现的内存访问漏洞的风险和后果。启用 KASLR 后，实例在休眠后可能无法恢复。

要详细了解 KASLR，请参阅 Ubuntu 功能。

在使用 Ubuntu 启动的实例上禁用 KASLR

1. 使用 SSH 连接到您的实例。有关更多信息，请参阅使用 SSH 连接到 Linux 实例 (p. 649)。
2. 在选定编辑器中打开 `/etc/default/grub.d/50-cloudimg-settings.cfg` 文件。编辑 `GRUB_CMDLINE_LINUX_DEFAULT` 行以将 `nokaslr` 选项追加到其末尾，如以下示例所示。

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0 nvme_core.io_timeout=4294967295
 nokaslr"
```

3. 保存文件并退出您的编辑器。
4. 运行以下命令来重新构建 grub 配置。

```
[ec2-user ~]$ sudo update-grub
```

5. 重启实例。

```
[ec2-user ~]$ sudo reboot
```

6. 运行以下命令确认 `nokaslr` 已添加。

```
[ec2-user ~]$ cat /proc/cmdline
```

命令的输出应包含 `nokaslr` 选项。

休眠实例

当实例已启用休眠 (p. 625)并且满足休眠先决条件 (p. 617)时，您才可以使该实例休眠。如果无法成功使实例休眠，则会进行正常关闭。

Console

将由 Amazon EBS 支持的实例休眠

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择实例状态、休眠实例。如果休眠实例处于已禁用状态，则表示实例已经休眠或停止，或者无法休眠。有关更多信息，请参阅休眠先决条件 (p. 617)。
4. 当系统提示进行确认时，选择休眠。使实例休眠可能需要几分钟时间。实例状态首先会更改为 Stopping（正在停止），然后如果实例已休眠，实例状态会更改为 Stopped（已停止）。

Amazon CLI

将由 Amazon EBS 支持的实例休眠

使用 stop-instances 命令并指定 `--hibernate` 参数。

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

使用 Amazon Tools for Windows PowerShell 使 Amazon EBS 支持的实例休眠

使用 Stop-EC2Instance 命令并指定 `-Hibernate $true` 参数。

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

查看是否已在实例上启动休眠

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后在详细信息选项卡上的实例详细信息部分中检查状态转换消息。消息 Client.UserInitiatedHibernate: User initiated hibernate (Client.UserInitiatedHibernate: 用户启动了休眠) 指明实例上启动了休眠。

Amazon CLI

查看是否已在实例上启动休眠

使用 describe-instances 命令并指定 `state-reason-code` 筛选条件以查看已启动了休眠的实例。

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

输出中的以下字段指明实例上启动了休眠。

```
"StateReason": {
```

```
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

查看是否已使用 Amazon Tools for Windows PowerShell 在实例上启动休眠

使用 Get-EC2Instance 命令并指定 `state-reason-code` 筛选条件以查看已启动休眠的实例。

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

输出会列出已启动休眠的 EC2 实例。

启动已休眠的实例

按照启动已停止实例的相同方式，启动已休眠的实例。

Console

启动已休眠实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择已休眠的实例，然后依次选择实例状态、启动实例。实例进入 `running` 状态可能需要几分钟时间。在此期间，实例状态检查 (p. 975)显示实例处于失败状态，直至实例已启动。

Amazon CLI

启动已休眠实例

使用 start-instances 命令。

```
aws ec2 start-instances \
    --instance-ids i-1234567890abcdef0
```

PowerShell

使用 Amazon Tools for Windows PowerShell 启动已休眠的实例

使用 Start-EC2Instance 命令。

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

休眠故障排除

使用此信息帮助您诊断和修复在使实例休眠时可能遇到的问题。

在启动后无法立即休眠

如果您在实例启动之后过快地尝试使实例休眠，则会收到错误。

在启动之后，您必须等待大约两分钟，然后才能休眠。

从 stopping 转变为 stopped 用时太长，内存状态在启动后无法恢复

如果正在进入休眠的实例从 stopping 状态转变为 stopped 状态用时过长，并且在启动之后内存状态未恢复，则这可能表明未正确配置休眠。

检查实例系统日志，查找与休眠相关的消息。要访问系统日志，请连接 (p. 644)到实例或者使用 get-console-output 命令。从 hibinit-agent 中查找日志行。如果日志行指示出现故障或者缺少日志行，则很有可能在启动时配置休眠失败。

例如，以下消息指明实例根卷不够大：`hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

如果 hibinit-agent 中的最后日志行是 `hibinit-agent: Running: swapoff /swap`，则已成功配置休眠。

如果您未看到来自这些进程的任何日志，您的 AMI 可能不支持休眠。有关支持的 AMI 的信息，请参阅休眠先决条件 (p. 617)。如果您使用自己的 AMI，请确保按照 配置现有 AMI 以支持休眠 (p. 620) 的说明操作。

实例“停滞在”停止状态

如果您已使实例休眠并且实例卡在 stopping 状态，则可以强制停止它。有关更多信息，请参阅排查实例的停止问题 (p. 1700)。

重启实例

实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。

重启实例后，将保留以下内容：

- 公有 DNS 名称（IPv4）
- 私有 IPv4 地址
- 公有 IPv4 地址
- IPv6 地址（如适用）
- 其实例存储卷上的所有数据

与停止和开启 (p. 610)您的实例不同，重新引导实例不会开启新的实例计费周期（最低收取一分钟的费用）。

为进行必要的维护 (例如，为了应用需要重启的升级)，我们可能会为您的实例预定一次重启。您无需进行任何操作；我们建议您在其预定重启窗口期间等待重启完成。有关更多信息，请参阅实例的计划事件 (p. 981)。

我们建议您使用 Amazon EC2 控制台、命令行工具或 Amazon EC2 API 来重启实例，而非在实例中运行操作系统重启命令。如果您使用 Amazon EC2 控制台、命令行工具或 Amazon EC2 API 重启实例，而实例在几分钟内未完全关闭，我们会执行硬重启。如果您使用 Amazon CloudTrail，则使用 Amazon EC2 重启实例还会创建一条关于实例重启时间的 API 记录。

Console

使用控制台重启实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择实例。
3. 选择实例，然后选择 Instance state（实例状态）、Reboot instance（重新引导实例）。

   或者，选择实例，然后选择 Actions（操作）、Manage instance state（管理实例状态）。在打开的屏幕中，选择 Reboot（重新引导）、然后选择 Change state（更改状态）。
4. 当系统提示您确认时，选择重启。

   实例仍处于 `running` 状态。

Command line

重启实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- reboot-instances (Amazon CLI)
- Restart-EC2Instance（Amazon Tools for Windows PowerShell）

运行受控的故障注入实验

您可以使用 Amazon Fault Injection Simulator 测试您的实例重新启动时您的应用程序如何响应。有关更多信息，请参阅 Amazon Fault Injection Simulator 用户指南。

实例指令引退

计划在 Amazon 检测到托管实例的基础硬件发生无法弥补的故障时停用实例。等到实例的计划停用日期，Amazon 便会停止或终止实例。

- 如果实例的根设备是 Amazon EBS 卷，将停止实例，您可随时重新启动它。启动停止的实例会将其迁移到新的硬件。
- 如果实例的根设备是实例存储卷，实例将终止，且无法再次使用。

有关实例事件类型的更多信息，请参阅实例的计划事件 (p. 981)。

目录

- 确定计划停用的实例 (p. 632)
- 可对计划停用的由 EBS 支持的实例执行的操作 (p. 633)
- 可对计划停用的由实例存储支持的实例执行的操作 (p. 634)

确定计划停用的实例

如果已计划停用实例，您将在事件发生之前收到包含实例 ID 和停用日期的电子邮件。您还可以使用 Amazon EC2 控制台或命令行检查是否有计划停用的实例。

Important

如果计划要停用某个实例，建议您尽快采取操作，因为该实例可能会变得无法访问。（您收到的电子邮件通知内容如下：“由于这种降级，您的实例可能已经无法访问。”）有关建议采取的操作的更多信息，请参阅Check if your instance is reachable。

确定计划停用的实例的方法

- 电子邮件通知。 (p. 633)

- 通过控制台确定 (p. 633)

电子邮件通知。

如果已计划停用实例，您将在事件发生之前收到包含实例 ID 和停用日期的电子邮件。

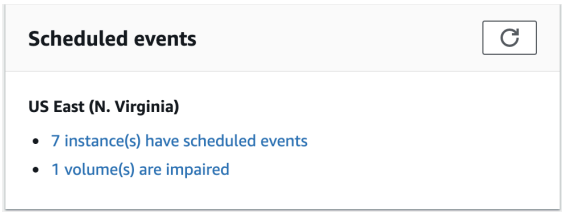
电子邮件将发送给主要账户持有人和运营联系人。有关更多信息，请参阅 Amazon Billing 用户指南中的添加、更改或删除备用联系人。

通过控制台确定

如果您不想定期检查电子邮件账户中是否收到了实例停用通知，也可以使用 Amazon EC2 控制台或命令行来确定是否有计划停用的实例。

使用控制台确定计划停用的实例

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 EC2 控制面板。在计划的事件下方，您可以看到与您的 Amazon EC2 实例和卷相关的事件，这些事件按区域列出。



3. 如果您的某个实例列有计划的事件，请选择区域名称下方的链接以转至 Events (事件) 页面。
4. 事件页面会列出与事件相关的所有资源。要查看计划停用的实例，请从第一个筛选列表中选择 Instance resources，然后从第二个筛选列表中选择 Instance stop or retirement。
5. 如果筛选结果显示有实例被计划停用，请选择该实例，并注意详细信息窗格中开始时间字段中的日期和时间。这就是您的实例停用的日期。

使用命令行确定计划停用的实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-instance-status (Amazon CLI)
- Get-EC2InstanceStatus (Amazon Tools for Windows PowerShell)

可对计划停用的由 EBS 支持的实例执行的操作

要保留即将停用的实例上的数据，您可以执行以下某项操作。请务必在实例停用日期之前执行该操作，以防止意外的停机和数据丢失。

如果您不确定您的实例是由 EBS 还是由实例存储支持，请参阅确定实例的根设备类型 (p. 1610)。

检查实例是否可访问

当您收到计划停用实例的通知时，建议您尽快采取以下操作：

- 通过连接 (p. 644)或 ping 实例来检查实例是否可以访问。
- 如果实例可以访问，则应计划在预定停用日期之前的某个适当的时间停止/启动实例，以影响最小为准。有关停止和启动实例以及在停止实例时可能发生的情况（例如，对与实例关联的公有、私有和弹性 IP 地址的

影响）的更多信息，请参阅停止和启动您的实例 (p. 610)。请注意，停止和启动实例后，实例存储卷上的数据将会丢失。
- 如果您的实例无法访问，您应立即采取操作，执行停止/启动 (p. 610)来恢复实例。
- 或者，如果您想终止 (p. 634)实例，请尽快计划终止，以便停止为实例产生费用。

创建实例备份

从实例创建由 EBS 支持的 AMI，以便您可以有一个备份。为确保数据的完整性，请在创建 AMI 之前停止实例。您可以等到计划的停用日期（实例停止的日期），或者在停用日期之前自行停止实例。您可随时重新启动实例。有关更多信息，请参阅 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。

启动替换实例

从实例创建 AMI 后，您可以使用 AMI 启动替换实例。在 Amazon EC2 控制台中，选择您的新 AMI，然后依次选择操作和启动。按照向导启动您的实例。有关向导中每个步骤的更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

可对计划停用的由实例存储支持的实例执行的操作

要保留即将停用的实例上的数据，您可以执行以下某项操作。请务必在实例停用日期之前执行该操作，以防止意外的停机和数据丢失。

> Warning
>
> 如果实例存储支持的实例超过了停用日期，则会终止该实例，并且无法恢复该实例或其中存储的任何数据。无论您的实例根设备是哪种类型，在停用实例后，存储在实例存储卷上的数据都会丢失，即使这些卷连接到由 EBS 提供支持的实例也不例外。

检查实例是否可访问

当您收到计划停用实例的通知时，建议您尽快采取以下操作：

- 通过连接 (p. 644)或 ping 实例来检查实例是否可以访问。
- 如果实例无法访问，则很可能无法恢复实例。有关更多信息，请参阅 排查无法访问的实例的问题 (p. 1723)。Amazon 将在计划的停用日期终止您的实例，因此，对于无法访问的实例，您可以立即自行将其终止 (p. 634)。

启动替换实例

使用 AMI 工具从实例创建由实例存储支持的 AMI，如创建由实例存储支持的 Linux AMI (p. 142)中所述。在 Amazon EC2 控制台中，选择您的新 AMI，然后依次选择操作和启动。按照向导启动您的实例。有关向导中每个步骤的更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

将实例转换为由 EBS 支持的实例

将数据传输到 EBS 卷，制作卷的快照，然后从快照创建 AMI。您可以从新 AMI 启动替换实例。有关更多信息，请参阅将实例存储支持的 AMI 转换为 Amazon EBS-backed AMI (p. 152)。

终止实例

当您不再需要实例时，可将其删除。这称为终止 实例。实例的状态一旦变为 `shutting-down` 或 `terminated`，就不再产生与该实例相关的费用。

在您终止之后，您将无法连接到或启动实例。但是您可以使用同一 AMI 启动其他实例。如果您愿意停止并启动您的实例，或者将其休眠，请参阅停止和启动您的实例 (p. 610) 或休眠 Linux 按需型实例 (p. 616)。有关更多信息，请参阅重启、停止、休眠和终止之间的区别 (p. 573)。

目录

- 实例终止 (p. 635)
- 通过跨可用区域终止保护来终止多个实例 (p. 635)
- 在终止实例时发生的情况 (p. 636)
- 终止实例 (p. 636)
- 启用终止保护 (p. 637)
- 更改实例启动的关闭操作 (p. 638)
- 在实例终止时保留 Amazon EBS 卷 (p. 638)
- 排查实例终止问题 (p. 640)

实例终止

在您终止实例之后，短时间内仍可在控制台中看见该实例，然后该条目将自动被删除。您无法自行删除已终止的实例条目。在实例终止后，标签和卷等资源会逐步与实例取消关联，因此过一小段时间后，它们可能在终止的实例上不再可见。

当实例终止时，与该实例关联的所有实例存储卷上的数据都会被删除。

默认情况下，当实例终止时，Amazon EBS 根设备卷将自动删除。但是，默认情况下，即使在实例终止后，您在启动时附加的所有额外 EBS 卷或您附加到现有实例的所有 EBS 卷也会保留。这一操作是由卷的 `DeleteOnTermination` 属性控制的，您可以对其进行修改。有关更多信息，请参阅在实例终止时保留 Amazon EBS 卷 (p. 638)。

您可以使用 Amazon Web Services Management Console、CLI 和 API 防止实例被别人意外终止。此功能对 Amazon EC2 实例存储支持的实例和 Amazon EBS 支持的实例都适用。每个实例的 `DisableApiTermination` 属性默认值均为 `false`（可以通过 Amazon EC2 终止实例）。您可以在实例运行或停止时修改此实例属性 (如果是由 Amazon EBS 支持的实例)。有关更多信息，请参阅启用终止保护 (p. 637)。

当使用操作系统中的系统关闭命令从实例启动关闭时，您可以控制是否应该关闭或终止实例。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。

如果您在实例终止时运行脚本，您的实例可能会异常终止，因为我们无法确保关闭脚本运行。Amazon EC2 尝试干净完全关闭实例并运行任何系统关闭脚本；但是，某些事件（例如硬件故障）可能会阻止这些系统关闭脚本运行。

通过跨可用区域终止保护来终止多个实例

如果您终止跨多个可用区域的多个实例，并且启用了一个或多个指定实例以进行终止保护，则请求失败，结果如下：

- 与受保护实例位于同一可用区中的指定实例不会终止。
- 位于不同可用区（其他指定实例不受保护）的指定实例将成功终止。

例如，假设您有以下实例：

实例	可用区	终止保护
实例 A	`us-east-1a`	`Disabled`
实例 B		`Disabled`

实例	可用区	终止保护
实例 C	us-east-1b	Enabled
实例 D		Disabled

如果您尝试终止同一请求中的所有这些实例，请求将报告失败，结果如下：

- 实例 A 和实例 B 已成功终止，因为 us-east-1a 中所有指定的实例都未启用终止保护。
- 实例 C 和实例 D 终止失败，因为 us-east-1b 中至少一个指定的实例（实例 C）已启用终止保护。

在终止实例时发生的情况

使用 terminate-instances 命令终止 EC2 实例后，将在操作系统级别注册以下内容：

- API 请求将向访客发送按钮按下事件。
- 由于此按钮按下事件，将停止各种系统服务。systemd 处理系统的正常关闭。来自管理程序的 ACPI 关闭按钮按下事件触发正常关闭。
- 启动 ACPI 关闭。
- 当正常关闭进程退出时，实例将关闭。没有可配置的操作系统关闭时间。

终止实例

您可以使用 Amazon Web Services Management Console或命令行终止实例。

默认情况下，当您从 Amazon EBS 支持的实例启动关闭（使用 shutdown 或 poweroff 命令）时，该实例会停止。halt 命令不会启动关闭。如果使用，实例并不会终止，而是将 CPU 置于 HLT 状态，实例将保持运行。

Console

终止实例

1. 在终止实例前，请确认您是否会丢失任何数据，方法是确认您的 Amazon EBS 卷是否会在终止时被删除，以及您是否已将所需数据从实例存储卷复制到持久性存储，例如 Amazon EBS 或 Amazon S3。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择实例。
4. 选择相应实例，然后依次选择 Instance state (实例状态)、Terminate instance (终止实例)。
5. 当系统提示您确认时，选择终止。

Command line

终止实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- terminate-instances (Amazon CLI)
- Remove-EC2Instance（Amazon Tools for Windows PowerShell)

运行受控的故障注入实验

您可以使用 Amazon Fault Injection Simulator 测试您的实例终止时您的应用程序如何响应。有关更多信息，请参阅 Amazon Fault Injection Simulator 用户指南。

启用终止保护

默认情况下，您可以使用 Amazon EC2 控制台、命令行界面或 API 终止您的实例。要使用 Amazon EC2 防止实例意外终止，可以为实例启用终止保护。`DisableApiTermination` 属性可控制是否可以使用控制台、CLI 或 API 终止实例。默认情况下，终止保护处于禁用状态。您可以在实例启动、运行或已停止时设置该属性值 (针对由 Amazon EBS 支持的实例)。

当设置 `DisableApiTermination` 属性时，`InstanceInitiatedShutdownBehavior` 属性不会阻止您通过从实例启动关闭来终止实例 (使用操作系统的系统关闭命令)。有关更多信息，请参阅更改实例启动的关闭操作 (p. 638)。

限制

您不能为竞价型实例启用终止保护，当 Spot 价格超过您愿意为竞价型实例支付的金额时，竞价型实例将终止。不过，您可以准备应用程序来处理竞价型实例中断。有关更多信息，请参阅竞价型实例中断 (p. 484)。

`DisableApiTermination` 属性不会阻止 Amazon EC2 Auto Scaling 终止实例。对于 Auto Scaling 组中的实例，请使用下列 Amazon EC2 Auto Scaling 功能而非 Amazon EC2 终止保护：

- 要阻止作为 Auto Scaling 组一部分的实例在缩小时终止，请使用实例缩小保护。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的使用实例横向缩减保护。
- 要阻止 Amazon EC2 Auto Scaling 终止运行状况不佳的实例，请暂停 `ReplaceUnhealthy` 流程。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的暂停和恢复扩展流程。
- 要指定 Amazon EC2 Auto Scaling 应先终止的实例，请选择终止策略。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的自定义终止策略。

要在实例启动时启用终止保护

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制面板中，选择 Launch Instance 并按照向导中的说明操作。
3. 在 Configure Instance Details (配置实例详细信息) 页面上，选中 Enable termination protection (启用终止保护) 复选框。

启用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions (操作)、Instance Settings (实例设置)、Change Termination Protection (更改终止保护)。
2. 选择 Yes, Enable (是，启用)。

禁用正在运行或已停止的实例的终止保护

1. 选择相应实例，然后依次选择 Actions (操作)、Instance Settings (实例设置)、Change Termination Protection (更改终止保护)。
2. 选择 Yes, Disable (是，禁用)。

使用命令行启用或禁用终止保护

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- modify-instance-attribute (Amazon CLI)
- Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

更改实例启动的关闭操作

默认情况下，从由 Amazon EBS 支持的实例启动关闭（使用 shutdown 或 poweroff 之类的命令），该实例将会停止。（请注意，halt 不会发出 poweroff 命令；如果使用 halt 命令，实例将不会终止；而是将 CPU 置于 HLT 状态，实例仍保持运行）。您可以使用实例的 `InstanceInitiatedShutdownBehavior` 属性更改此操作，以便终止实例。您可以在实例运行或停止时更新此属性。

您可以使用 Amazon EC2 控制台或命令行更新 `InstanceInitiatedShutdownBehavior` 属性。`InstanceInitiatedShutdownBehavior` 属性只在您从实例自身的操作系统执行关闭操作时适用；在您使用 `StopInstances` API 或 Amazon EC2 控制台停止实例时不适用。

Console

使用控制台更改实例的关闭行为

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 依次选择操作、实例设置、更改关闭操作。系统会选择当前操作。
5. 要更改操作，请从关闭操作中选择停止或终止，然后选择应用。

Command line

使用命令行更改实例的关闭行为

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- modify-instance-attribute (Amazon CLI)
- Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

在实例终止时保留 Amazon EBS 卷

当实例终止时，Amazon EC2 会使用每个挂载的 Amazon EBS 卷的 `DeleteOnTermination` 属性的值来确定是保留还是删除该卷。

根据卷是实例的根卷还是附加到实例的非根卷，`DeleteOnTermination` 属性的默认值会有所不同。

根卷

默认情况下，实例的根卷的 `DeleteOnTermination` 属性将设置为 `true`。因此，当某个实例终止时，默认为删除该实例的根卷。`DeleteOnTermination` 属性可由 AMI 的创建者以及实例的启动者设置。当 AMI 的创建者或实例的启动者更改属性时，新的设置将覆盖原始 AMI 默认设置。我们建议您在使用 AMI 启动实例后验证 `DeleteOnTermination` 属性的默认设置。

非根卷

默认情况下，当您将非根 EBS 卷附加到某个实例 (p. 1347)时，其 `DeleteOnTermination` 属性将设置为 `false`。因此，默认为保留这些卷。在该实例终止后，您可以为保留的卷拍摄快照，或将其附加到另一个实例。您必须删除卷以避免产生更多费用。有关更多信息，请参阅删除 Amazon EBS 卷 (p. 1366)。

要验证使用中的 EBS 卷的 `DeleteOnTermination` 属性的值，请查看该实例的块储存设备映射。有关更多信息，请参阅查看实例块储存设备映射中的 EBS 卷 (p. 1622)。

在启动该实例或在该实例正在运行时，您可以更改卷的 `DeleteOnTermination` 属性的值。

示例

- 使用控制台将根卷更改为在启动时持久保留 (p. 639)
- 使用命令行将根卷更改为在启动时持久保留 (p. 639)
- 使用命令行将运行的实例的根卷更改为持久保留 (p. 640)

使用控制台将根卷更改为在启动时持久保留

当您启动实例时，可以使用控制台更改 DeleteOnTermination 属性。要对正在运行的实例更改此属性，您必须使用命令行。

使用控制台在启动时更改实例要持久保留的根卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从控制台控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择一个 AMI，然后选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面上，取消选中根卷的 Delete On Termination (终止时删除) 复选框。
6. 完成其余向导页面上的操作，然后选择 Launch。

在新控制台中，您可以通过实例的详细信息窗格查看根设备卷的详细信息以验证设置。在存储库的存储选项卡，在块储存设备中，向右滚动以查看终止时删除设置。默认情况下，Delete on termination (终止时删除) 为 Yes。如果您更改默认行为，Delete on termination (终止时删除) 将为 No。

在旧控制台中，您可以通过实例的详细信息窗格查看根设备卷的详细信息以验证设置。在 Block devices (块储存设备) 旁，选择根设备卷的条目。默认情况下，Delete on termination (终止时删除) 为 True。如果您更改默认行为，Delete on termination (终止时删除) 将为 False。

使用命令行将根卷更改为在启动时持久保留

当您启动 EBS 支持的实例时，可以使用以下命令之一将根设备卷更改为持久保留。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- run-instances (Amazon CLI)
- New-EC2Instance (Amazon Tools for Windows PowerShell)

在要保留的卷的块设备映射中，纳入 --DeleteOnTermination，并指定 false。

例如，若要保留卷，需将以下选项添加到 run-instances 命令：

```
--block-device-mappings file://mapping.json
```

在 mapping.json 中，指定设备名称，例如 /dev/sda1 或 /dev/xvda，并为 --DeleteOnTermination 指定 false。

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
```

```
]
```

使用命令行将运行的实例的根卷更改为持久保留

您可以使用以下命令之一将正在运行的 EBS 支持实例的根设备卷更改为持久保留。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- modify-instance-attribute (Amazon CLI)
- Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

例如，使用以下命令：

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings
 file://mapping.json
```

在 mapping.json 中，指定设备名称，例如 /dev/sda1 或 /dev/xvda，并为 --DeleteOnTermination 指定 false。

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

排查实例终止问题

如果您终止您的实例而另一个实例启动，很可能您已通过 EC2 队列 或 Amazon EC2 Auto Scaling 等功能配置了自动扩展。

如果您的实例处于 shutting-down 状态的时间超出正常范围，Amazon EC2 服务中的自动进程应将对其进行清理（终止）。有关更多信息，请参阅延迟的实例终止 (p. 1703)。

恢复实例

要在系统状态检查失败时自动恢复实例，您可以使用实例的默认配置或创建 Amazon CloudWatch 告警。如果实例因需要 Amazon 参与才能修复的底层硬件故障或问题而无法访问，实例将自动恢复。

恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。如果受损实例具有公有 IPv4 地址，它会在恢复后保留公有 IPv4 地址。如果受损实例位于放置组中，则已恢复的实例将在放置组中运行。在实例恢复过程中，实例作为重启的一部分迁移，并且内存中的所有数据都将丢失。

需要实例恢复的问题示例：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上影响到网络连接状态的硬件问题

主题

- 基于实例配置的简化自动恢复 (p. 641)
- Amazon CloudWatch 基于操作的恢复 (p. 643)

- 实例恢复故障排除 (p. 644)

基于实例配置的简化自动恢复

支持简化自动恢复的实例将默认配置以恢复失败的实例。默认配置适用于您启动的新实例和之前启动的现有实例。针对系统状态检查故障启动了简化自动恢复。简化自动恢复不会在服务运行状况控制面板事件期间或影响底层硬件的任何其他事件期间进行。有关更多信息，请参阅the section called “实例恢复故障排除” (p. 644)。

当简化的自动恢复事件成功后，您将收到 Amazon Health 控制面板事件通知。当简化的自动恢复事件失败后，您将收到 Amazon Health 控制面板事件和电子邮件通知。您还可以使用 Amazon EventBridge 规则通过以下事件代码监控简化的自动恢复事件：

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS` — 成功的事件
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE` — 失败的事件

有关更多信息，请参阅 Amazon EventBridge 规则。

主题

- 要求 (p. 641)
- 限制 (p. 641)
- 验证恢复行为 (p. 641)
- 验证恢复行为 (p. 642)

要求

如果实例具有以下特性，则其支持简化自动恢复：

- 使用 `default` 或 `dedicated` 实例租赁。
- 不使用 Elastic Fabric Adapter。
- 使用以下其中一种实例类型：
  - 通用型：A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7g | T1 | T2 | T3 | T3a | T4g
  - 计算优化型：C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7g | Hpc6a
  - 内存优化型：R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7g | u-3tb1 | u-6tb1 | u-9tb1 | u-12tb1 | u-18tb1 | u-24tb1 | X1 | X1e | X2iezn
  - 加速计算型：G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
- 实例没有实例存储卷。

限制

- 简化自动恢复不支持具有实例存储卷和裸机实例类型的实例。
- 如果您的实例是启用了运行状况检查的 Auto Scaling 组的一部分，则在该实例损坏时替换该实例。对于 Auto Scaling 组中的实例，不会启动自动恢复。
- 简化的自动恢复仅适用于计划外事件。它不适用于已计划的事件。
- 无法恢复终止或停止的实例。

验证恢复行为

您可以使用 Amazon Web Services Management Console 或 Amazon CLI 查看支持简化自动恢复的实例类型。

Console

要查看支持简化自动恢复的实例类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instance Types（实例类型）。
3. 在筛选条件栏中，输入 Auto Recovery support: true（自动恢复支持：真）。或者，当您输入字符且过滤条件名称显示时，您可以选择它。

   Instance types（实例类型）表显示了支持简化自动恢复的所有实例类型。

Amazon CLI

要查看支持简化自动恢复的实例类型

请使用 describe-instance-types 命令。

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

验证恢复行为

启动实例期间或之后，您可以将自动恢复行为设置为 `disabled` 或 `default`。默认配置不能为不受支持的实例类型启用简化自动恢复。

Console

在实例启动时禁用简化自动恢复

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances（实例），然后选择 Launch instance（启动实例）。
3. 在 Advanced details（高级详细信息）部分，对于 Instance auto-recovery（实例自动恢复），请选择 Disabled（已禁用）。
4. 根据需要配置剩余的实例启动设置，然后启动实例。

禁用正在运行或已停止实例的简化自动恢复

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 请选择实例，然后依次选择 Actions（操作）、Instance settings（实例设置）、Change auto-recovery behavior（更改自动恢复行为）。
4. 选择 Off（关闭），然后选择 Save（保存）。

要将正在运行或已停止实例的自动恢复行为设置为 **`default`**

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 请选择实例，然后依次选择 Actions（操作）、Instance settings（实例设置）、Change auto-recovery behavior（更改自动恢复行为）。
4. 选择默认（开启），然后选择保存。

Amazon CLI

在启动时禁用简化自动恢复

可以使用 run-instances 命令。

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
  [...]
```

禁用正在运行或已停止实例的简化自动恢复

使用 modify-instance-maintenance-options 命令。

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

要将正在运行或已停止实例的自动恢复行为设置为 **default**

使用 modify-instance-maintenance-options 命令。

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery default
```

Amazon CloudWatch 基于操作的恢复

如果要自定义何时恢复实例，请使用 Amazon CloudWatch 基于操作的恢复。

当 StatusCheckFailed_System 告警触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。当恢复操作完成后，系统会向您为告警配置的 Amazon SNS 主题发布信息。任何订阅此 Amazon SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步指示。作为恢复操作的最后一个步骤，恢复的实例会重新启动。

CloudWatch 基于操作的恢复也支持所有简化自动恢复支持的 (p. 641)所有实例类型。此外，Amazon CloudWatch 基于操作的恢复还支持以下具有实例存储卷的实例类型。

- 通用型：M3
- 计算优化型：C3
- 内存优化型：R3 | X1 | X1e | X2idn | X2iedn

> **Important**
>
> 如果实例包含附加的实例存储卷，则数据将在恢复过程中丢失。

对于具有 Amazon EC2 专属主机租赁的实例和裸机实例，Amazon CloudWatch 基于操作的恢复不支持恢复。

即使没有禁用简化的自动恢复，也可以使用 Amazon CloudWatch 告警来恢复实例。有关创建用于恢复实例的 Amazon CloudWatch 警报的信息，请参阅 在 Amazon CloudWatch 警报中添加恢复操作 (p. 1024)。

实例恢复故障排除

以下问题可能会导致实例恢复失败：

- 服务运行状况控制面板事件或影响底层机架的事件。在此类事件中，简化自动恢复不能恢复实例。您将不会收到此类事件的恢复失败通知。任何持续的服务运行状况控制面板也可能阻止 Amazon CloudWatch 基于操作的恢复成功恢复实例。请参阅 http://status.aws.amazon.com/，了解最新服务可用性信息。
- 替换硬件的临时容量不足。
- 该实例有一个附加实例存储，而自动实例恢复不支持该配置。
- 该实例已达到每天最多三次的恢复尝试操作限制。

自动恢复过程将会尝试恢复您的实例 (每天最多针对三个不同的故障)。如果实例系统状态检查故障仍然存在，建议您手动停止并启动实例。有关更多信息，请参阅停止和启动您的实例 (p. 610)。

如果自动恢复失败，并且确定硬件性能下降是初始系统状态检查失败的根本原因，那么您的实例随后可能会被停用。

连接

《适用于 Linux 实例的 Amazon EC2 用户指南》的这一部分信息可帮助您在启动 Linux 实例后，连接到该实例。还可帮助您将 Linux 实例连接到其他 Amazon 资源。

主题

- 连接到您的 Linux 实例 (p. 644)
- 将 EC2 实例连接到 Amazon 资源 (p. 673)

连接到您的 Linux 实例

《Amazon EC2 用户指南》的这一部分信息涉及如何在启动 Linux 实例后连接到该实例，以及如何在本地计算机和实例之间传输文件。

有关如何连接到 Windows 实例的信息，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的连接到 Windows 实例。

要排查连接到实例的问题，请参阅 排查实例的连接问题。 (p. 1684)。

设置以连接到 Linux 实例

有关准备连接到 Linux 实例的一般步骤，请参阅 设置以连接到实例 (p. 645)。

连接选项

除了准备连接到实例的一般步骤外，本地计算机的操作系统还确定了从本地计算机连接到 Linux 实例的特定先决条件。

Linux 或 macOS X

如果您的本地计算机操作系统是 Linux 或 macOS X，请参阅以下选项的特定先决条件以连接到实例：

- SSH 客户端 (p. 649)
- EC2 Instance Connect (p. 652)
- Amazon Systems Manager 会话管理器

Windows

如果您的本地计算机操作系统是 Windows，请参阅以下选项的特定先决条件以连接到实例：

- OpenSSH (p. 661)
- PuTTY (p. 663)
- Amazon Systems Manager 会话管理器
- 适用于 Linux 的 Windows 子系统 (p. 669)

> **Note**
>
> 要排查基于 Amazon Nitro System 构建的实例的启动、网络配置和其他问题，您可以使用 适用于 Linux 实例的 EC2 Serial Console (p. 1736)。

设置以连接到实例

要设置以连接到 Windows 实例，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的先决条件。

执行本主题中的任务以进行设置，从而连接到 Amazon EC2 Linux 实例。有关特定于连接类型（例如 SSH、EC2 Instance Connect、OpenSSH、PuTTY）的先决条件，请参阅以下用于从 Linux、macOS X 或 Windows 进行连接的选项。

Linux 或 macOS X

如果您的本地计算机操作系统是 Linux 或 macOS X，则支持以下连接到实例的选项：

- SSH 客户端 (p. 649)
- EC2 Instance Connect (p. 652)
- Amazon Systems Manager 会话管理器

Windows

如果您的本地计算机操作系统是 Windows，则支持以下连接到实例的选项：

- OpenSSH (p. 661)
- PuTTY (p. 663)
- Amazon Systems Manager 会话管理器
- 适用于 Linux 的 Windows 子系统 (p. 669)

常规设置任务

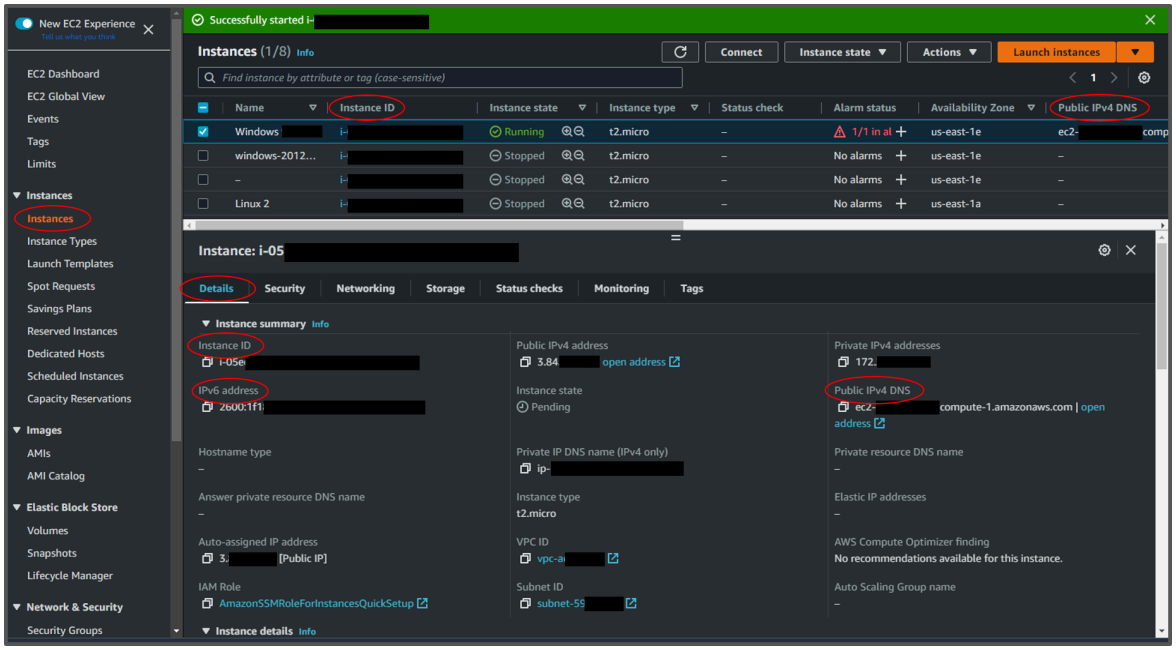
- 获取有关您的实例的信息 (p. 645)
- 查找私有密钥并设置权限 (p. 648)
- （可选）获取实例指纹 (p. 649)

排查实例的连接问题。

排查实例的连接问题。 (p. 1684)

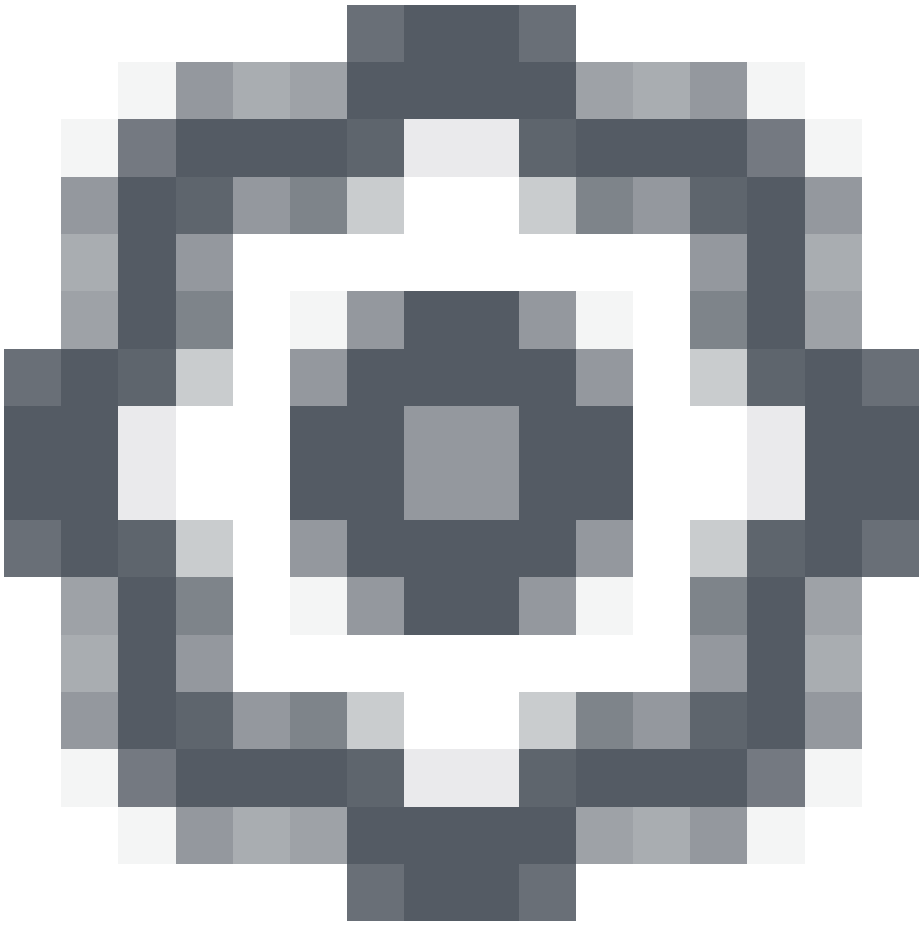
获取有关您的实例的信息

要准备连接到实例，请通过 Amazon EC2 控制台或使用 Amazon CLI 获取以下信息。



- 获取实例的公有 DNS 名称。

  您可以从 Amazon EC2 控制台获取实例的公有 DNS。查看实例窗格的公有 IPv4 DNS 列。如果此列已隐藏，请选择屏幕右上角的设置图标

（  ），然后选择公有 IPv4 DNS。您也可以在实例窗格的实例信息部分找到公有 DNS。在 Amazon EC2 控制台的实例窗格中选择实例时，有关该实例的信息将显示在页面的下半部分。在详细信息选项卡下，查找公有 IPv4 DNS。

如果您愿意，也可以使用 describe-instances（Amazon CLI）或 Get-EC2Instance（Amazon Tools for Windows PowerShell）命令。

如果未显示公有 IPv4 DNS，请验证实例状态是否正在运行，并确保您没有在私有子网中启动实例。如果您使用启动实例向导 (p. 575)来启动实例，则可能已编辑网络设置下的自动分配公有 IP 字段，并且已将值更改为禁用。如果您禁用自动分配公有 IP 选项，则启动实例后不会为其分配公有 IP 地址。

- （仅限 IPv6）获取实例的 IPv6 地址。

  如果您已为实例分配 IPv6 地址，则可以选择使用 IPv6 地址代替公有 IPv4 地址或公有 IPv4 DNS 主机名，以连接到实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。您可以从 Amazon EC2 控制台获取实例的 IPv6 地址。请查看实例窗格的 IPv6 IP 列。或者，您可以在实例信息部分找到 IPv6 地址。在 Amazon EC2 控制台的实例窗格中选择实例时，有关该实例的信息将显示在页面的下半部分。在详细信息选项卡下，查找 IPv6 地址。

  如果您愿意，也可以使用 describe-instances（Amazon CLI）或 Get-EC2Instance（Amazon Tools for Windows PowerShell）命令。有关 IPv6 的更多信息，请参阅 IPv6 地址 (p. 1055)。

- 获取实例的用户名。

  您可以使用用户账户的用户名或用于启动实例的 AMI 的默认用户名连接到实例。

  - 获取用户账户的用户名。

    有关如何创建用户账户的更多信息，请参阅管理 Linux 实例上的用户 (p. 705)。

- 获取用于启动实例的 AMI 的默认用户名：

用于启动实例的 AMI	默认用户名
Amazon Linux 2022 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` 或者 `ec2-user`
Debian	`admin`
Fedora	`fedora` 或者 `ec2-user`
RHEL	`ec2-user` 或者 `root`
SUSE	`ec2-user` 或者 `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
其他	检查 AMI 提供程序

查找私有密钥并设置权限

您必须知道私有密钥文件的位置，才能连接到实例。对于 SSH 连接，必须设置权限，以确保只有您可以读取文件。

有关使用 Amazon EC2 时密钥对工作原理的信息，请参阅 Amazon EC2 密钥对和 Linux 实例 (p. 1289)。

- 查找私有密钥

  获取适用于启用实例时所指定密钥对的 `.pem` 文件在电脑上的全限定路径。有关更多信息，请参阅确定启动时指定的公有密钥。如果找不到私有密钥文件，请参阅我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？

  如果您使用 Putty 连接到实例并且需要将 `.pem` 文件转换为 `.ppk`，请参阅本部分 使用 PuTTY 从 Windows 连接到 Linux 实例 (p. 663) 主题中的 使用 PuTTYgen 转换私有密钥 (p. 664)。
- 设置私有密钥文件的权限，以确保只有您可以读取该文件
  - 从 macOS 或 Linux 进行连接

    如果您计划在 macOS 或 Linux 计算机上使用 SSH 客户端连接到 Linux 实例，请使用以下命令设置私有密钥文件的权限，以确保只有您可以读取该文件。

    ```
    chmod 400 key-pair-name.pem
    ```

    如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅错误：未保护的私有密钥文件 (p. 1692)。
  - 从 Windows 进行连接

    打开“文件资源管理器”，然后右键单击 `.pem` 文件。依次选择属性 > 安全选项卡，然后选择高级。选择禁用继承。删除对所有用户（当前用户除外）的访问权限。

（可选）获取实例指纹

要防范中间人攻击，您可以在连接实例时验证实例指纹。如果您从第三方提供的公有 AMI 启动实例，验证指纹将很有用。

任务概述

首先，获取实例指纹。连接到实例后，系统会提示您验证指纹。将已获取的指纹与显示的指纹进行比较。如果指纹不匹配，则表示有人可能在试图实施中间人攻击。如果二者匹配，则您可以放心地连接到您的实例。

获取实例指纹的先决条件

- 要获取实例指纹，您必须使用 Amazon CLI。有关安装 Amazon CLI 的信息，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon Command Line Interface。
- 实例不能处于 pending 状态。只有在第一次引导实例完成后，才能使用指纹。

获取实例指纹

1. 在本地计算机上（而不是正在连接的实例上），按以下方式使用 get-console-output（Amazon CLI）命令以获取实例指纹。您必须为实例拥有者，才能获取控制台输出。如果输出过大，可将输出通过管道传输到文本文件，文本形式可能更易于阅读。请注意，使用 Amazon CLI 时，必须明确指定或通过设置默认区域来指定 Amazon Web Services 区域。有关如何设置或指定区域的信息，请参阅《Amazon Command Line Interface 用户指南》中的配置基础知识。

   ```
   aws ec2 get-console-output --instance-id instance_id --output text > temp.txt
   ```

2. 以下示例输出显示了运行 get-console-output 命令时应查找的内容。确切的输出可能因操作系统、AMI 版本以及是否是由 Amazon 创建密钥对而异。

   ```
   ec2: #############################################################
   ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
   ec2: 1024 SHA256:7HItIgTONZ/b0CH9c5Dq1ijgqQ6kFn86uQhQ5E/F9pU root@ip-10-0-2-182 (DSA)
   ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY root@ip-10-0-2-182 (ECDSA)
   ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
   ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc root@ip-10-0-2-182 (RSA)
   ec2: -----END SSH HOST KEY FINGERPRINTS-----
   ec2: #############################################################
   ```

使用 SSH 连接到 Linux 实例

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

以下说明介绍如何使用 SSH 客户端连接到您的实例。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。有关更多连接选项，请参阅连接到您的 Linux 实例 (p. 644)。

目录

- 先决条件 (p. 649)
- 使用 SSH 客户端连接到 Linux 实例 (p. 650)
- 使用 SCP 客户端将文件传输到 Linux 实例 (p. 651)
- 问题排查 (p. 652)

先决条件

在连接到 Linux 实例之前，请先完成以下先决条件：

检查实例状态

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查。您可以在实例页面的状态检查列中查看此信息。

获取公有 DNS 名称和用户名以连接到您的实例

要查找实例的公有 DNS 名称或 IP 地址以及用于连接到实例的用户名，请参阅 连接到实例的先决条件 (p. 645)。

查找私有密钥并设置权限

要查找连接到您的实例所需的私有密钥并设置密钥权限，请参阅 查找私有密钥并设置权限 (p. 648)。

根据需要在您的本地计算机上安装 SSH 客户端

您的本地计算机可能已默认安装了 SSH 客户端。您可以通过在命令行中键入 ssh 来验证这一点。如果您的计算机无法识别该命令，可安装 SSH 客户端。

- 最新版本的 Windows Server 2019 和 Windows 10 – OpenSSH 作为可安装组件包括在内。有关信息，请参阅 Windows 中的 OpenSSH。
- 较早版本的 Windows – 下载并安装 OpenSSH。有关更多信息，请参阅 Win32-OpenSSH。
- Linux 和 macOS X – 下载并安装 OpenSSH。有关更多信息，请参阅 https://www.openssh.com。

使用 SSH 客户端连接到 Linux 实例

通过以下过程使用 SSH 客户端连接到您的 Linux 实例。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 SSH 连接到您的实例

1. 在终端窗口中，使用 ssh 命令连接到该实例。您指定私有密钥的路径和文件名 (.pem)、实例的用户名以及实例的公有 DNS 名称或 IPv6 地址。有关如何查找私有密钥、实例的用户名以及实例的 DNS 名称或 IPv6 地址的更多信息，请参阅查找私有密钥并设置权限 (p. 648)和获取有关您的实例的信息 (p. 645)。要连接到实例，请使用以下命令之一。
   - （公有 DNS）要使用实例的公有 DNS 名称进行连接，请输入以下命令。

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```

   - (IPv6) 或者，如果您的实例具有 IPv6 地址，要使用实例的 IPv6 地址进行连接，请输入以下命令。

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
     ```

   您会看到如下响应：

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
    can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

2. (可选) 验证安全警报中的指纹是否与您之前在 （可选）获取实例指纹 (p. 649) 中获得的指纹相匹配。如果这些指纹不匹配，则表示有人可能在试图实施中间人攻击。如果匹配，请继续到下一步。
3. 输入 **yes**。

   您会看到如下响应：

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to the
    list of known hosts.
   ```

使用 SCP 客户端将文件传输到 Linux 实例

在您的本地计算机与 Linux 实例之间传输文件的一种方法是使用安全复制协议 (SCP)。本节介绍了如何使用 SCP 传输文件。该步骤与使用 SSH 连接到实例的步骤类似。

先决条件

- 验证有关将文件传输到您的实例的常规先决条件。

  将文件传输到实例的常规先决条件与连接到实例的常规先决条件相同。有关更多信息，请参阅设置以连接到实例 (p. 645)。
- 安装 SCP 客户端

  默认情况下，大多数 Linux、Unix 和 Apple 计算机都包含 SCP 客户端。如果您的计算机不含 SSH 客户端，OpenSSH 项目提供了整套 SSH 工具免费使用的功能，包括 SCP 客户端。有关更多信息，请参阅 https://www.openssh.com。

以下过程将指导您使用实例的公有 DNS 名称或 IPv6 地址（如果实例具有该地址），通过 SCP 传输文件。

使用 SCP 在您的计算机和实例之间传输文件

1. 确定源文件在计算机上的位置以及在实例上的目标路径。在以下示例中，私有密钥文件的名称是 `key-pair-name.pem`，要传输的文件是 `my-file.txt`，实例的用户名是 ec2-user，实例的公有 DNS 名称是 `instance-public-dns-name`，实例的 IPv6 地址是 `instance-IPv6-address`。
   - （公有 DNS）要将文件传输到实例上的目标位置，请在计算机中输入以下命令。

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```
   - (IPv6) 如果实例具有 IPv6 地址，要将文件传输到实例上的目标位置，请在计算机中输入以下命令。IPv6 地址必须用方括号 ([ ]) 括起来，并且必须对方括号进行转义 (\)。

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
     ```
2. 如果您尚未使用 SSH 连接到实例，则会看到如下响应：

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```

   （可选）您可以选择验证安全警报中的指纹是否与实例指纹匹配。有关更多信息，请参阅（可选）获取实例指纹 (p. 649)。

   输入 **yes**。
3. 如果传输成功，则响应的形式与下方类似：

   ```
   Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
   to the list of known hosts.
   my-file.txt                                   100%   480     24.4KB/s   00:00
   ```
4. 要在另一个方向上传输文件（从 Amazon EC2 实例中传输到计算机），请颠倒主机参数的顺序。例如，您可以将 `my-file.txt` 从 EC2 实例传输到本地计算机上的目标位置，保存为 `my-file2.txt`，如以下示例所示。
   - （公有 DNS）要将文件传输到计算机中的目标位置，请在计算机中输入以下命令。

```
scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-file.txt
 path/my-file2.txt
```

- (IPv6) 如果实例具有 IPv6 地址，要将文件传输到计算机中的目标位置，请在计算机中输入以下命令。IPv6 地址必须用方括号 ([ ]) 括起来，并且必须对方括号进行转义 (\)。

```
scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-file.txt
 path/my-file2.txt
```

问题排查

如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 EC2 Instance Connect 连接到 Linux 实例

Amazon EC2 Instance Connect 提供了一种简单且安全的方法以使用安全 Shell (SSH) 连接到 Linux 实例。借助 EC2 Instance Connect，您可以使用 Amazon Identity and Access Management (IAM) 策略和主体来控制对实例的 SSH 访问，无需共享和管理 SSH 密钥。使用 EC2 Instance Connect 的所有连接请求将记录到 Amazon CloudTrail 中，以便您可以审核连接请求 (p. 1038)。

您可以使用 EC2 Instance Connect 通过 Amazon EC2 控制台、EC2 Instance Connect CLI 或您选择的 SSH 客户端连接到 Linux 实例。

在使用 EC2 Instance Connect 连接到实例时，Instance Connect API 将一次性使用的 SSH 公有密钥推送到实例元数据 (p. 754)，将在其中保留 60 秒。附加到用户的 IAM policy 会授权用户将公有密钥推送到实例元数据。SSH 守护程序使用在安装 Instance Connect 时配置的 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser`，从实例元数据中查找公有密钥以进行身份验证，并将您连接到实例。

您可以使用 EC2 Instance Connect 连接到具有公有或私有 IP 地址的实例。有关更多信息，请参阅使用 EC2 Instance Connect 进行连接 (p. 658)。

目录

- 设置 EC2 Instance Connect (p. 652)
- 使用 EC2 Instance Connect 进行连接 (p. 658)
- 卸载 EC2 Instance Connect (p. 661)

提示

如果从运行 Windows 的本地计算机连接到 Linux 实例，请转而参阅以下文档：

- 使用 PuTTY 从 Windows 连接到 Linux 实例 (p. 663)
- 使用 SSH 连接到 Linux 实例 (p. 649)
- 使用 Windows Subsystem for Linux 从 Windows 连接到 Linux 实例 (p. 669)

设置 EC2 Instance Connect

要使用 EC2 Instance Connect 连接到实例，您需要配置支持使用 Instance Connect 连接的每个实例（对于每个实例而言这是一次性的要求），并且需要向将要使用 Instance Connect 的每个 IAM 主体授予权限。完成以下设置任务后，您可以使用 EC2 Instance Connect 连接到实例 (p. 658)。

用于设置 EC2 Instance Connect 的任务

- 任务 1：配置对实例的网络访问 (p. 653)
- 任务 2：（视情况而定）在实例上安装 EC2 Instance Connect (p. 654)

- 任务 3：（可选）在电脑上安装 EC2 Instance Connect CLI (p. 656)
- 任务 4：为 EC2 Instance Connect 配置 IAM 权限 (p. 656)

有关设置 EC2 Instance Connect 的更多信息，请参阅使用 Amazon EC2 实例连接保护堡垒主机。

限制

- 您可以在以下受支持的 Linux 分发上安装 EC2 Instance Connect：
  - Amazon Linux 2（任何版本）
  - Ubuntu 16.04 或更高版本
- 如果为 SSH 身份验证配置了 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser` 设置，则 EC2 Instance Connect 安装不会更新它们。因此，您无法使用 Instance Connect。

安装 EC2 Instance Connect 的先决条件

- 确认满足使用 SSH 连接到实例的一般先决条件。

  有关更多信息，请参阅设置以连接到实例 (p. 645)。
- 获取实例 ID。

  您可以使用 Amazon EC2 控制台获取实例 ID（从 Instance ID (实例 ID) 列）。如果您愿意，可以使用 describe-instances (Amazon CLI) 或 Get-EC2Instance (Amazon Tools for Windows PowerShell) 命令。
- 在您的本地计算机上安装 SSH 客户端。

  您的本地计算机很可能已默认安装 SSH 客户端。您可以通过在命令行键入 ssh 来检查 SSH 客户端。如果您的本地计算机无法识别该命令，您可安装 SSH 客户端。有关在 Linux 或 macOS X 上安装 SSH 客户端的信息，请参阅 http://www.openssh.com。有关在 Windows 10 上安装 SSH 客户端的信息，请参阅 Windows 中的 OpenSSH。
- 在本地计算机上安装 Amazon CLI。

  要配置 IAM 权限，您必须使用 Amazon CLI。有关安装 Amazon CLI 的信息，请参阅《Amazon Command Line Interface 用户指南》中的安装 Amazon CLI。
- [Ubuntu] 在实例上安装 Amazon CLI。

  要在 Ubuntu 实例上安装 EC2 Instance Connect，您必须在实例上使用 Amazon CLI。有关安装 Amazon CLI 的信息，请参阅《Amazon Command Line Interface 用户指南》中的安装 Amazon CLI。

任务 1：配置对实例的网络访问

您必须配置以下网络访问权限，以便用户可以使用 EC2 Instance Connect 连接到您的实例：

- 如果您的用户将通过 Internet 访问您的实例，则您的实例必须具有公有 IP 地址，并位于公有子网中。有关更多信息，请参阅 Amazon VPC 用户指南中的启用 Internet 访问。
- 如果您的用户要通过实例的私有 IP 地址访问您的实例，则必须建立与您的 VPC 的私有网络连接，例如使用 Amazon Direct Connect、Amazon Site-to-Site VPN 或 VPC 对等连接，以便用户能够访问实例的私有 IP 地址。
- 确保与您实例关联的安全组允许来自您 IP 地址端口 22 或您网络上的传入 SSH 流量 (p. 1288)。默认情况下，VPC 的默认安全组不允许传入 SSH 流量。默认情况下，由启动向导创建的安全组允许传入的 SSH 流量。有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
- （Amazon EC2 控制台）确保与您的实例关联的安全组允许来自此服务的 IP 地址范围的入站 SSH 流量。要识别地址范围，请下载由 Amazon 提供的 JSON 文件并筛选 EC2 Instance Connect 的子网，使用 `EC2_INSTANCE_CONNECT` 作为服务值。有关下载 JSON 文件和按服务进行筛选的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon IP 地址范围。

任务 2：（视情况而定）在实例上安装 EC2 Instance Connect

如果您使用以下 AMI 之一启动了您的实例，那么您可以跳过此任务，因为它们预安装了 EC2 Instance Connect：

- Amazon Linux 2 2.0.20190618 或更高版本
- Ubuntu 20.04 或更高版本

对于这些 AMI 的早期版本，您必须在每个支持使用 Instance Connect 进行连接的实例上安装 Instance Connect。

安装 Instance Connect 将在实例上配置 SSH 守护程序。对于使用 Amazon Linux 2 和 Ubuntu 启动的实例，安装 Instance Connect 的过程是不同的。

Amazon Linux 2

在使用 Amazon Linux 2 启动的实例上安装 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。

   可以使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名。对于 Amazon Linux 2，默认用户名是 `ec2-user`。

   例如，如果实例是使用 Amazon Linux 2 启动的，实例的公有 DNS 名称是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   有关连接到实例的更多信息，请参阅使用 SSH 连接到 Linux 实例 (p. 649)。
2. 在实例上安装 EC2 Instance Connect 程序包。

   对于 Amazon Linux 2，请使用 yum install 命令。

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   您将会在 `/opt/aws/bin/` 文件夹中看到三个新脚本：

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```
3. （可选）验证是否在实例上成功安装了 Instance Connect。

   可以使用 sudo less 命令检查是否正确更新了 `/etc/ssh/sshd_config` 文件，如下所示：

   ```
   [ec2-user ~]$ sudo less /etc/ssh/sshd_config
   ```

   如果 `AuthorizedKeysCommand` 文件中的 `AuthorizedKeysCommandUser` 和 `/etc/ssh/sshd_config` 行包含以下值，则成功安装了 Instance Connect：

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   AuthorizedKeysCommandUser ec2-instance-connect
   ```

- `AuthorizedKeysCommand` 设置 `eic_run_authorized_keys` 文件以从实例元数据中查找密钥
- `AuthorizedKeysCommandUser` 将系统用户设置为 `ec2-instance-connect`

Note

如果以前配置了 `AuthorizedKeysCommand` 和 `AuthorizedKeysCommandUser`，则 Instance Connect 安装不会更改这些值，并且您无法使用 Instance Connect。

Ubuntu

在使用 Ubuntu 16.04 或更高版本启动的实例上安装 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。

   可以使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名。对于 Ubuntu AMI，用户名称是 `ubuntu`。

   如果实例是使用 Ubuntu 启动的，实例的公有 DNS 名称是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
   ```

   有关连接到实例的更多信息，请参阅使用 SSH 连接到 Linux 实例 (p. 649)。
2. （可选）确保您的实例具有最新 Ubuntu AMI。

   对于 Ubuntu，请使用以下命令更新实例上的所有程序包。

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```
3. 在实例上安装 Instance Connect 程序包。

   对于 Ubuntu，使用 sudo apt-get 命令。

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   您将会在 `/usr/share/ec2-instance-connect/` 文件夹中看到三个新脚本：

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```
4. （可选）验证是否在实例上成功安装了 Instance Connect。

   可以使用 sudo less 命令检查是否正确更新了 `/lib/systemd/system/ssh.service.d/ec2-instance-connect.conf`，如下所示：

   ```
   ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
   ```

如果 AuthorizedKeysCommand 文件中的 AuthorizedKeysCommandUser 和 /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf 行包含以下值，则成功安装了 Instance Connect：

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- AuthorizedKeysCommand 设置 eic_run_authorized_keys 文件以从实例元数据中查找密钥
- AuthorizedKeysCommandUser 将系统用户设置为 ec2-instance-connect

> **Note**
>
> 如果以前配置了 AuthorizedKeysCommand 和 AuthorizedKeysCommandUser，则 Instance Connect 安装不会更改这些值，并且您无法使用 Instance Connect。

有关 EC2 Instance Connect 程序包的更多信息，请参阅 GitHub 网站上的 aws/aws-ec2-instance-connect-config。

任务 3：（可选）在电脑上安装 EC2 Instance Connect CLI

EC2 Instance ConnectCLI 提供了通过单个命令连接到 EC2 实例的简化体验 mssh *instance_id*。有关更多信息，请参阅使用 EC2 Instance Connect CLI 进行连接 (p. 659)。

> **Note**
>
> 如果用户仅使用 Amazon EC2 控制台或 SSH 客户端连接到实例，则无需安装 EC2 Instance Connect CLI。

安装 EC2 Instance Connect CLI 程序包

使用 pip 安装 ec2instanceconnectcli 程序包。有关更多信息，请参阅 GitHub 网站上的 aws/aws-ec2-instance-connect-cli，以及 Python Package Index (PyPI) 网站上的 https://pypi.org/project/ec2instanceconnectcli/。

```
$ pip install ec2instanceconnectcli
```

任务 4：为 EC2 Instance Connect 配置 IAM 权限

如果 IAM 委托人将使用 EC2 Instance Connect 连接到实例，您必须为其授予将公有密钥推送到实例的权限。您可以通过创建 IAM policy 并将策略附加到需要权限的 IAM 委托人来向用户授予权限。有关更多信息，请参阅 Amazon EC2 Instance Connect 的操作、资源和条件键。

以下说明介绍如何使用 Amazon CLI 创建策略并将其附加到用户。同样的策略可以应用于其他 IAM 委托人，例如 IAM 角色。有关如何使用 Amazon Web Services Management Console 的说明，请参阅 IAM 用户指南中的创建 IAM policy（控制台）、将策略直接附加到用户以添加权限和创建 IAM 角色。

为 EC2 Instance Connect (Amazon CLI) 授予 IAM 委托人权限

1. 创建一个 JSON 策略文档，其中包含以下内容：

   - ec2-instance-connect:SendSSHPublicKey 操作。此操作为 IAM 委托人授予将公有密钥推送到实例的权限。使用 ec2-instance-connect:SendSSHPublicKey，考虑限制对特定 EC2 实例的访问。否则，具有此权限的所有 IAM 用户都可以连接到所有 EC2 实例。您还可以通过指定资源 ARN 或使用资源标签作为 条件键来限制访问。

- `ec2:osuser` 条件。这指定可以将公有密钥推送到实例的操作系统用户的名称。使用用于启动实例的 AMI 的默认用户名称。对于 Amazon Linux 2，默认用户名称为 `ec2-user`，对于 Ubuntu，为 `ubuntu`。
- `ec2:DescribeInstances` 操作。使用 EC2 Instance Connect CLI 时此操作是必需的，因为包装程序会调用此操作。IAM 委托人可能已经拥有从另一个策略调用此操作的权限。

下面是示例策略文档。如果您的用户将仅使用 SSH 客户端连接到您的实例，则可以省略 `ec2:DescribeInstances` 操作的语句。您可以使用通配符 `Resource` 替换 `*` 中的指定实例，以授予用户使用 EC2 Instance Connect 访问所有 EC2 实例的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "ec2-instance-connect:SendSSHPublicKey",
        "Resource": [
            "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
            "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:osuser": "ami-username"
            }
        }
      },
      {
        "Effect": "Allow",
        "Action": "ec2:DescribeInstances",
        "Resource": "*"
      }
    ]
}
```

上述策略允许访问特定的实例（由其实例 ID 标识）。或者，您也可以使用资源标签控制对实例的访问。基于属性的访问控制是一种授权策略，它根据可附加到用户和 Amazon 资源的标签来定义权限。例如，只有在实例具有包含 `tag-key` 键和 `tag-value` 值的资源标签时，以下策略才允许用户访问该实例。有关使用标签控制对Amazon资源的访问的更多信息，请参阅 IAM 用户指南中的控制对Amazon资源的访问。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ec2-instance-connect:SendSSHPublicKey",
         "Resource": "arn:aws:ec2:region:account-id:instance/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/tag-key":"tag-value"
            }
         }
      },
      {
        "Effect": "Allow",
        "Action": "ec2:DescribeInstances",
        "Resource": "*"
      }
   ]
}
```

2. 使用 create-policy 命令创建新的托管式策略，并指定您创建的 JSON 文档以作为新策略的内容。

```
$ aws iam create-policy --policy-name my-policy --policy-document file://JSON-file-name
```

3. 使用 attach-user-policy 命令将托管式策略附加到指定用户。对于 `--user-name` 参数，请指定用户的友好名称（而不是 ARN）。

```
$ aws iam attach-user-policy --policy-arn arn:aws:iam::account-id:policy/my-policy --
user-name IAM-friendly-name
```

使用 EC2 Instance Connect 进行连接

以下说明介绍如何使用 EC2 Instance Connect 连接到 Linux 实例。

主题

- 限制 (p. 658)
- 先决条件 (p. 658)
- 使用 EC2 Instance Connect 进行连接 (p. 659)
- 问题排查 (p. 660)

限制

- 支持的 Linux 分配：
  - Amazon Linux 2（任何版本）
  - Ubuntu 16.04 或更高版本
- 所有 Amazon Web Services 区域均支持，但非洲（开普敦）、亚太地区（香港）、亚太地区（雅加达）、亚太地区（大阪）、中国（北京）、中国（宁夏）、欧洲地区（米兰）和中东（巴林）区域除外。
- 要使用 Amazon EC2 控制台进行连接，实例必须具有一个公有 IPv4 地址。
- 如果实例没有公有 IP 地址，则可以使用 SSH 客户端或 EC2 Instance Connect CLI，通过私有网络连接到实例。例如，您可以从同一 VPC 内，或通过 VPN 连接、Transit Gateway 或 Amazon Direct Connect 进行连接。
- EC2 Instance Connect 不支持使用 IPv6 地址进行连接。

先决条件

- 在实例上安装 EC2 Instance Connect。

  有关更多信息，请参阅设置 EC2 Instance Connect (p. 652)。
- （可选）在本地计算机上安装 SSH 客户端。

  如果用户仅使用 Amazon EC2 控制台或 EC2 Instance Connect CLI 连接到实例，则无需安装 SSH 客户端。您的本地计算机很可能已默认安装 SSH 客户端。您可以通过在命令行键入 ssh 来检查 SSH 客户端。如果您的本地计算机无法识别该命令，您可安装 SSH 客户端。有关在 Linux 或 macOS X 上安装 SSH 客户端的信息，请参阅 http://www.openssh.com。有关在 Windows 10 上安装 SSH 客户端的信息，请参阅 Windows 中的 OpenSSH。
- （可选）在本地计算机上安装 EC2 Instance Connect CLI。

  如果用户仅使用 Amazon EC2 控制台或 SSH 客户端连接到实例，则无需安装 EC2 Instance Connect CLI。有关更多信息，请参阅任务 3：（可选）在电脑上安装 EC2 Instance Connect CLI (p. 656)。此连接方法适用于具有公有 IP 地址的实例。

使用 EC2 Instance Connect 进行连接

选项

- 使用 Amazon EC2 控制台连接 (p. 659)
- 使用 EC2 Instance Connect CLI 进行连接 (p. 659)
- 使用您自己的密钥和 SSH 客户端进行连接 (p. 660)

使用 Amazon EC2 控制台连接

您可以在控制台中选择实例，然后选择使用 EC2 Instance Connect 进行连接，从而使用 Amazon EC2 控制台连接到实例。Instance Connect 处理权限并提供成功的连接。

从 Amazon EC2 控制台使用基于浏览器的客户端连接到您的实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例，然后选择连接。
4. 选择 EC2 Instance Connect。
5. 验证用户名并选择连接以打开终端窗口。

使用 EC2 Instance Connect CLI 进行连接

您可以使用 EC2 Instance Connect CLI 并仅提供实例 ID 以连接到实例，同时 Instance Connect CLI 在一次调用中执行以下三个操作：它生成一次性使用的 SSH 公有密钥，将密钥推送到实例以在其中保留 60 秒，并将用户连接到实例。您可以在 Instance Connect CLI 中使用基本 SSH/SFTP 命令。

此连接方法适用于具有公有和私有 IP 地址的实例。当连接到仅具有私有 IP 地址的实例时，启动会话的本地计算机必须连接到 EC2 Instance Connect 服务终端节点（将 SSH 公钥推送到实例）以及到实例的私有 IP 地址的网络连接。EC2 Instance Connect 服务终端节点可以通过互联网或 Amazon Direct Connect 公共虚拟接口访问。要连接到实例的私有 IP 地址，您可以利用 Amazon Direct Connect、Amazon Site-to-Site VPN 或 VPC 对等连接等服务。

> **Note**
>
> `-i`使用 时不支持 mssh。在使用 mssh 命令连接到实例时，无需指定任何类型的身份文件，因为 Instance Connect 会管理密钥对。

Amazon Linux 2

使用 EC2 Instance Connect CLI 连接到实例

将 mssh 命令与实例 ID 一起使用，如下所示。您无需指定 AMI 的用户名。

```
$ mssh i-001234a4bf70dec41EXAMPLE
```

Ubuntu

使用 EC2 Instance Connect CLI 连接到实例

将 mssh 命令与实例 ID 以及 Ubuntu AMI 的默认用户名一起使用，如下所示。您必须指定 AMI 的用户名，否则会出现以下错误：身份验证失败。

```
$ mssh ubuntu@i-001234a4bf70dec41EXAMPLE
```

使用您自己的密钥和 SSH 客户端进行连接

您可以使用自己的 SSH 密钥，并在使用 EC2 Instance Connect API 时从您选择的 SSH 客户端连接到您的实例。这使您能够从将公有密钥推送到实例的 Instance Connect 功能中受益。此连接方法适用于具有公有和私有 IP 地址的实例。

要求

- 密钥对的要求
  - 支持的类型：RSA（OpenSSH 和 SSH2）和 ED25519
  - 支持的长度：2048 和 4096
  - 有关更多信息，请参阅使用第三方工具创建密钥对，并将公有密钥导入 Amazon EC2 (p. 1293)。
- 当连接到仅具有私有 IP 地址的实例时，启动 SSH 会话的本地计算机必须连接到 EC2 Instance Connect 服务终端节点（将 SSH 公钥推送到实例）以及到实例的私有 IP 地址的网络连接，才能建立 SSH 会话。EC2 Instance Connect 服务终端节点可以通过互联网或 Amazon Direct Connect 公共虚拟接口访问。要连接到实例的私有 IP 地址，您可以利用 Amazon Direct Connect、Amazon Site-to-Site VPN 或 VPC 对等连接等服务。

使用您自己的密钥和任何 SSH 客户端连接到实例

1. （可选）生成新的 SSH 私有密钥和公有密钥

   您可以使用以下命令生成新的 SSH 私有密钥和公有密钥（`my_key` 和 `my_key.pub`）：

   ```
   $ ssh-keygen -t rsa -f my_key
   ```

2. 将 SSH 公有密钥推送到实例

   使用 send-ssh-public-key 命令可将 SSH 公有密钥推送到实例。如果使用 Amazon Linux 2 启动实例，则 AMI 的默认用户名是 `ec2-user`。如果使用 Ubuntu 启动实例，则 AMI 的默认用户名是 `ubuntu`。

   以下示例将公有密钥推送到指定的可用区中的指定实例，以对 `ec2-user` 进行身份验证。

   ```
   $ aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. 使用私有密钥连接到实例

   从实例元数据中删除公有密钥之前，可以使用 ssh 命令通过私有密钥连接到实例（在 60 秒后删除）。指定与公有密钥对应的私有密钥、用于启动实例的 AMI 的默认用户名以及实例的公有 DNS 名称（如果通过私有网络连接，请指定私有 DNS 名称或 IP 地址）。添加 `IdentitiesOnly=yes` 选项以确保仅使用 ssh config 中的文件和指定的密钥进行连接。

   ```
   $ ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

问题排查

如果您在尝试连接到实例时遇到错误，请参阅下文：

- 排查实例的连接问题。 (p. 1684)
- 如何排查使用 EC2 Instance Connect 连接 EC2 实例时遇到的问题？

卸载 EC2 Instance Connect

要禁用 EC2 Instance Connect，请连接到您的实例并卸载您在操作系统上安装的 ec2-instance-connect 程序包。如果 sshd 配置与您安装 EC2 Instance Connect 时设置的配置匹配，卸载 ec2-instance-connect 还会删除 sshd 配置。如果在安装 EC2 Instance Connect 后修改了 sshd 配置，您必须手动更新该配置。

Amazon Linux 2

您可以在 Amazon Linux 2 2.0.20190618 或更高版本上卸载 EC2 Instance Connect，其中预配置了 EC2 Instance Connect。

在使用 Amazon Linux 2 启动的实例上卸载 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。指定您在启动实例时用于实例的 SSH 密钥对以及 Amazon Linux 2 AMI 的默认用户名，即 ec2-user。

   例如，以下 ssh 命令使用密钥对 ec2-a-b-c-d.us-west-2.compute.amazonaws.com 连接到具有公有 DNS 名称 my_ec2_private_key.pem 的实例。

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

2. 使用 ec2-instance-connect 命令卸载 yum 软件包。

   ```
   [ec2-user ~]$ sudo yum remove ec2-instance-connect
   ```

Ubuntu

在使用 Ubuntu AMI 启动的实例上卸载 EC2 Instance Connect

1. 使用 SSH 连接到您的实例。指定您在启动实例时用于实例的 SSH 密钥对以及 Ubuntu AMI 的默认用户名，即 ubuntu。

   例如，以下 ssh 命令使用密钥对 ec2-a-b-c-d.us-west-2.compute.amazonaws.com 连接到具有公有 DNS 名称 my_ec2_private_key.pem 的实例。

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
   ```

2. 使用 ec2-instance-connect 命令卸载 apt-get 软件包。

   ```
   ubuntu:~$ sudo apt-get remove ec2-instance-connect
   ```

使用 OpenSSH 从 Windows 连接到 Linux 实例

以下步骤将说明如何使用 OpenSSH（一种使用 SSH 协议进行远程登录的开源连接工具）从 Windows 连接到 Linux 实例。Windows Server 2019 及更高版本操作系统支持 OpenSSH。

目录

- 先决条件 (p. 662)
- 使用 PowerShell 安装适用于 Windows 的 OpenSSH (p. 662)
- 使用 OpenSSH 从 Windows 连接到 Linux 实例 (p. 662)
- 使用 PowerShell 将 OpenSSH 从 Windows 卸载 (p. 663)

先决条件

使用 OpenSSH 从 Windows 连接到您的 Linux 实例之前，请先完成以下先决条件。

验证该实例是否就绪

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查。您可以在实例页面的状态检查列中查看此信息。

验证有关连接到您的实例的常规先决条件

要查找实例的公有 DNS 名称或 IP 地址以及您在连接到实例时应使用的用户名，请参阅设置以连接到实例 (p. 645)。

确定您的 Windows 版本

若要使用 OpenSSH 从 Windows 连接到您的 Linux 实例，Windows 版本必须为 Windows Server 2019 及更高版本。

确定 PowerShell 先决条件

若要在 Windows 操作系统上使用 PowerShell 安装 OpenSSH，您必须运行 PowerShell 版本 5.1 或更高版本，并且您的账户必须是内置管理员组的成员。在 PowerShell 中运行 `$PSVersionTable.PSVersion` 以查看 PowerShell 版本。

若要查看您是否是内置管理员组的成员，请运行以下 PowerShell 命令：

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).IsInRole(
```

如果您是内置管理员组的成员，则输出为 `True`。

使用 PowerShell 安装适用于 Windows 的 OpenSSH

若要使用 PowerShell 安装适用于 Windows 的 OpenSSH，请运行以下 PowerShell 命令：

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

预期输出：

```
Path          :
Online        : True
RestartNeeded : False
```

使用 OpenSSH 从 Windows 连接到 Linux 实例

安装 OpenSSH 后，按照以下步骤使用 OpenSSH 从 Windows 连接到您的 Linux 实例。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 OpenSSH 连接到您的实例

1. 在 PowerShell 或命令提示符中，使用 ssh 命令连接到实例。您指定私有密钥的路径和文件名 (`.pem`)、实例的用户名以及实例的公有 DNS 名称或 IPv6 地址。有关如何查找私有密钥、实例的用户名以及实例的 DNS 名称或 IPv6 地址的更多信息，请参阅查找私有密钥并设置权限 (p. 648)和获取有关您的实例的信息 (p. 645)。要连接到实例，请使用以下命令之一。
   - （公有 DNS）要使用实例的公有 DNS 名称进行连接，请输入以下命令。

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
     ```

- (IPv6) 或者，如果您的实例具有 IPv6 地址，要使用实例的 IPv6 地址进行连接，请输入以下命令。

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

您会看到如下响应：

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

2. (可选) 验证安全警报中的指纹是否与您之前在（可选）获取实例指纹 (p. 649) 中获得的指纹相匹配。如果这些指纹不匹配，则表示有人可能在试图实施中间人攻击。如果匹配，请继续到下一步。
3. 输入 **yes**。

您会看到如下响应：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to the
 list of known hosts.
```

使用 PowerShell 将 OpenSSH 从 Windows 卸载

若要使用 PowerShell 将 OpenSSH 从 Windows 卸载，请运行以下 PowerShell 命令：

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

预期输出：

```
Path          :
Online        : True
RestartNeeded : True
```

使用 PuTTY 从 Windows 连接到 Linux 实例

如果您运行的是 Windows Server 2019 或更高版本，我们建议使用 OpenSSH，这是一款使用 SSH 协议进行远程登录的开源连接工具。有关使用 OpenSSH 从 Windows 连接到 Linux 实例的步骤，请参阅 使用 OpenSSH 从 Windows 连接到 Linux 实例 (p. 661)。

以下说明介绍如何使用 PuTTY (适用于 Windows 的免费 SSH 客户端) 连接到您的实例。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

目录

- 先决条件 (p. 663)
  - 使用 PuTTYgen 转换私有密钥 (p. 664)
- 连接到您的 Linux 实例 (p. 664)
- 使用 PuTTY 安全复制客户端将文件传输到您的 Linux 实例 (p. 666)
- 使用 WinSCP 将文件传输到您的 Linux 实例 (p. 666)

先决条件

使用 PuTTY 连接到您的 Linux 实例之前，请先完成以下先决条件。

验证该实例是否就绪

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查。您可以在实例页面的状态检查列中查看此信息。

验证有关连接到您的实例的常规先决条件

要查找实例的公有 DNS 名称或 IP 地址以及您在连接到实例时应使用的用户名，请参阅设置以连接到实例 (p. 645)。

在本地计算机上安装 PuTTY

从 PuTTY 下载页面下载 PuTTY 并安装。如果您安装的是旧版本的 PuTTY，建议您下载最新版本。确保安装整个套件。

使用 PuTTYgen 将您的私有 .pem 密钥转换为 .ppk

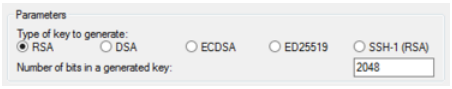
对于您在启动实例时指定的密钥对，如果您选择以 .pem 格式创建私有密钥，则您必须将其转换为 .ppk 文件，以便与 PuTTY 一起使用。找到私有 .pem 文件，然后按照下一节中的步骤操作。

使用 PuTTYgen 转换私有密钥

PuTTY 自身并不支持适用于 SSH 密钥的 PEM 格式。PuTTY 提供一种名为 PuTTYgen 的工具，该工具可以将 PEM 密钥转换为 PuTTY 所需的 PPK 格式。您必须如下所示将私有密钥（.pem 文件）转换为此格式（.ppk 文件），以便使用 PuTTY 连接到您的实例。

将您的私有 .pem 密钥转换为 .ppk

1. 从 Start (开始) 菜单中，依次选择 All Programs (所有程序)、PuTTY、PuTTYgen。
2. 在 Type of key to generate 下，选择 RSA。如果您的 PuTTYgen 版本不包含此选项，请选择 SSH-2 RSA。



3. 选择 Load。默认情况下，PuTTYgen 仅显示扩展名为 .ppk 的文件。要找到您的 .pem 文件，请选择显示所有类型的文件的选项。



4. 选择在启动实例时指定的密钥对的 .pem 文件，然后选择打开。PuTTYgen 显示一个通知，即 .pem 文件已导入成功。选择 OK (确定)。
5. 要以 PuTTY 可以使用的格式保存密钥，请选择 Save private key (保存私有密钥)。PuTTYgen 显示一条关于在没有密码的情况下保存密钥的警告。选择是。

   Note

   私有密钥上的密码提供额外一层保护。即使发现了您的私有密钥，也不能在没有密码的情况下使用该密钥。使用密码的缺点是自动化更难实现，因为需要人工干预以登录到实例或将文件复制到实例中。

6. 为密钥指定您用于密钥对的相同名称（例如 key-pair-name）并选择 Save (保存)。PuTTY 会自动添加 .ppk 文件扩展名。

您的私有密钥格式现在是正确的 PuTTY 使用格式了。您现在可以使用 PuTTY 的 SSH 客户端连接到实例。

连接到您的 Linux 实例

通过以下过程使用 PuTTY 连接到您的 Linux 实例。您需要使用为私有密钥创建的 .ppk 文件。有关更多信息，请参阅上一个部分中的使用 PuTTYgen 转换私有密钥 (p. 664)。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 PuTTY 连接到您的实例

1. 启动 PuTTY（在开始菜单中，选择所有程序 > PuTTY > PuTTY）。
2. 在 Category 窗格中，选择 Session 并填写以下字段：

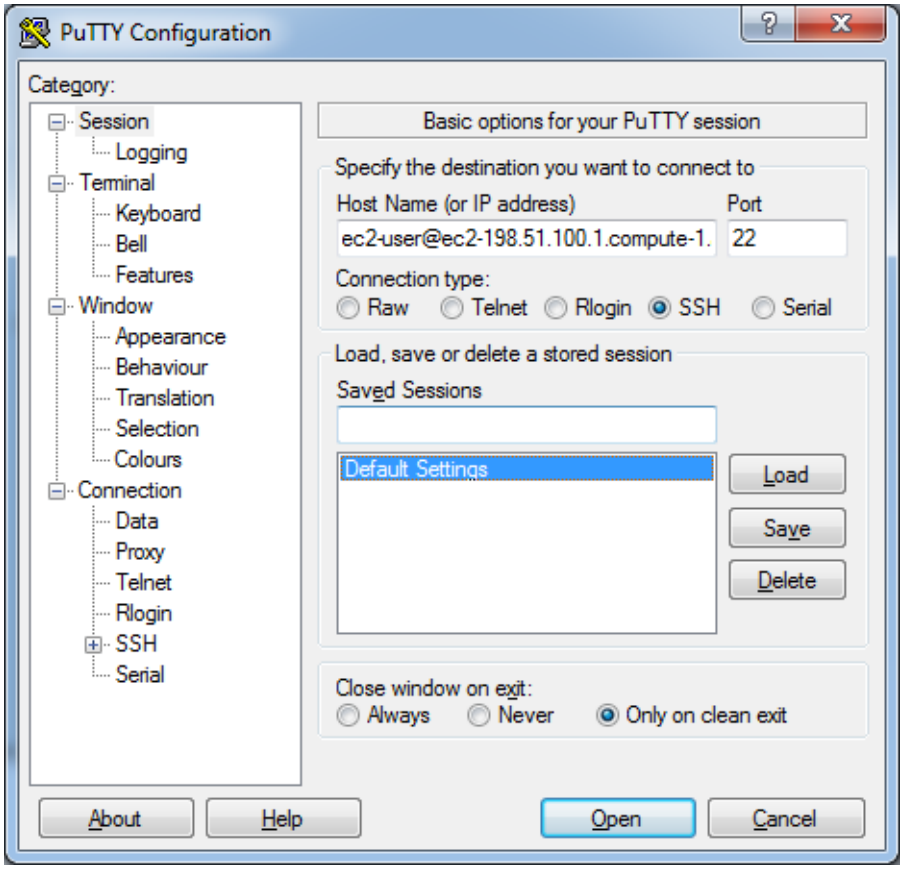
   a. 在主机名框中，执行以下操作之一：

   - （公有 DNS）要使用实例的公有 DNS 名称进行连接，请输入 *instance-user-name*@*instance-public-dns-name*。
   - （IPv6）或者，如果实例具有 IPv6 地址，要使用实例的 IPv6 地址进行连接，请输入 *instance-user-name*@*instance-IPv6-address*。

   有关如何获取实例的用户名以及实例的公有 DNS 名称或 IPv6 地址的信息，请参阅获取有关您的实例的信息 (p. 645)。

   b. 确保端口值为 22。

   c. 在连接类型下，选择 SSH。



3. (可选) 您可以配置 PuTTY 以定期自动发送“保持连接”数据以将会话保持活动状态。要避免由于会话处于不活动状态而与实例断开连接，这是非常有用的。在 Category 窗格中，选择 Connection，然后在 Seconds between keepalives 字段中输入所需的间隔。例如，如果您的会话在处于不活动状态 10 分钟后断开连接，请输入 180 以将 PuTTY 配置为每隔 3 分钟发送一次保持活动数据。
4. 在 Category 窗格中，展开 Connection，再展开 SSH，然后选择 Auth。完成以下操作：

   a. 选择 Browse。

   b. 选择为密钥对生成的 `.ppk` 文件，然后选择打开。

c. (可选) 如果打算稍后重新启动此会话，则可以保存此会话信息以便日后使用。在类别下面，选择会话，在保存的会话中输入会话的名称，然后选择保存。

d. 选择 Open。

5. 如果这是第一次连接到该实例，PuTTY 将显示安全警报对话框，以询问您是否信任要连接到的主机。

a. (可选) 验证安全警报对话框中的指纹是否与您之前在（可选）获取实例指纹 (p. 649) 中获得的指纹相匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。

b. 选择是。将打开一个窗口，并且您连接到实例。

Note

如果您在将私有密钥转换成 PuTTY 格式时指定了密语，当您登录到实例时，您必须提供该密语。

如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 PuTTY 安全复制客户端将文件传输到您的 Linux 实例

PuTTY 安全复制客户端 (PSCP) 是一个命令行工具，可用于在 Windows 计算机和 Linux 实例之间传输文件。如果您更喜欢图形用户界面 (GUI)，您可以使用一种叫作“WinSCP”的开源 GUI 工具。有关更多信息，请参阅使用 WinSCP 将文件传输到您的 Linux 实例 (p. 666)。

要使用 PSCP，您需要使用在使用 PuTTYgen 转换私有密钥 (p. 664)中生成的私有密钥。您还需要使用 Linux 实例的公有 DNS 名称或 IPv6 地址（如果实例具有该地址）。

以下示例将 `Sample_file.txt` 文件从 Windows 计算机上的 C:\ 驱动器传输到 Amazon Linux 实例上的 `instance-user-name` 主目录。要传输文件，请使用以下命令之一。

- （公有 DNS）要使用实例的公有 DNS 名称传输文件，请输入以下命令。

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) 或者，如果实例具有 IPv6 地址，要使用实例的 IPv6 地址传输文件，请输入以下命令。IPv6 地址必须用方括号 ([ ]) 括起来。

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

使用 WinSCP 将文件传输到您的 Linux 实例

WinSCP 是适用于 Windows 的基于 GUI 的文件管理器，您可以通过它来使用 SFTP、SCP、FTP 和 FTPS 协议将文件上传并传输到远程计算机。WinSCP 允许您将文件从 Windows 计算机拖放到 Linux 实例，或者在两个系统之间同步整个目录结构。

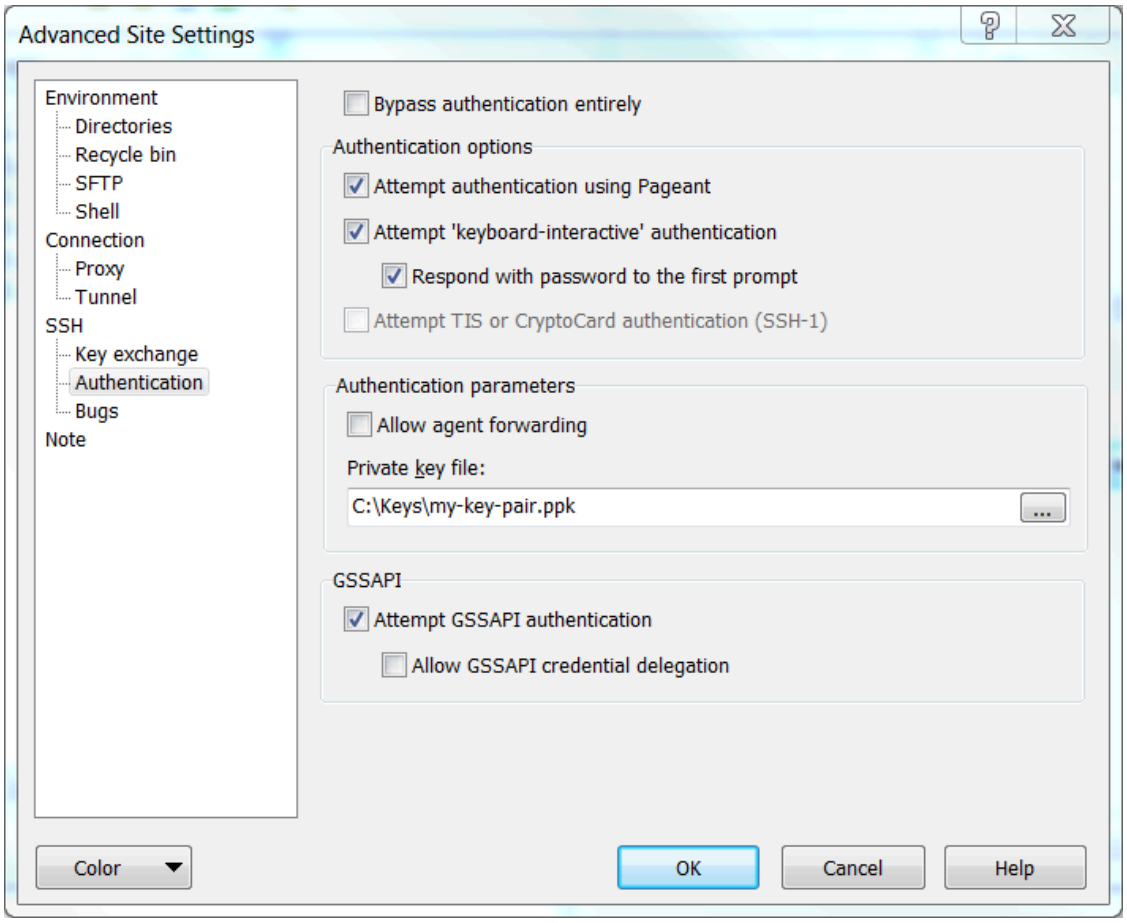
要求

- 您必须拥有在使用 PuTTYgen 转换私有密钥 (p. 664)中生成的私有密钥。
- 您必须拥有 Linux 实例的公有 DNS 名称。
- 您的 Linux 实例必须已安装 `scp`。对于某些操作系统，您需要安装 `openssh-clients` 软件包。对于其他操作系统（例如经 Amazon ECS 优化的 AMI），您需要安装 `scp` 软件包。请参阅您的 Linux 发行版的文档。

使用 WinSCP 连接到您的实例

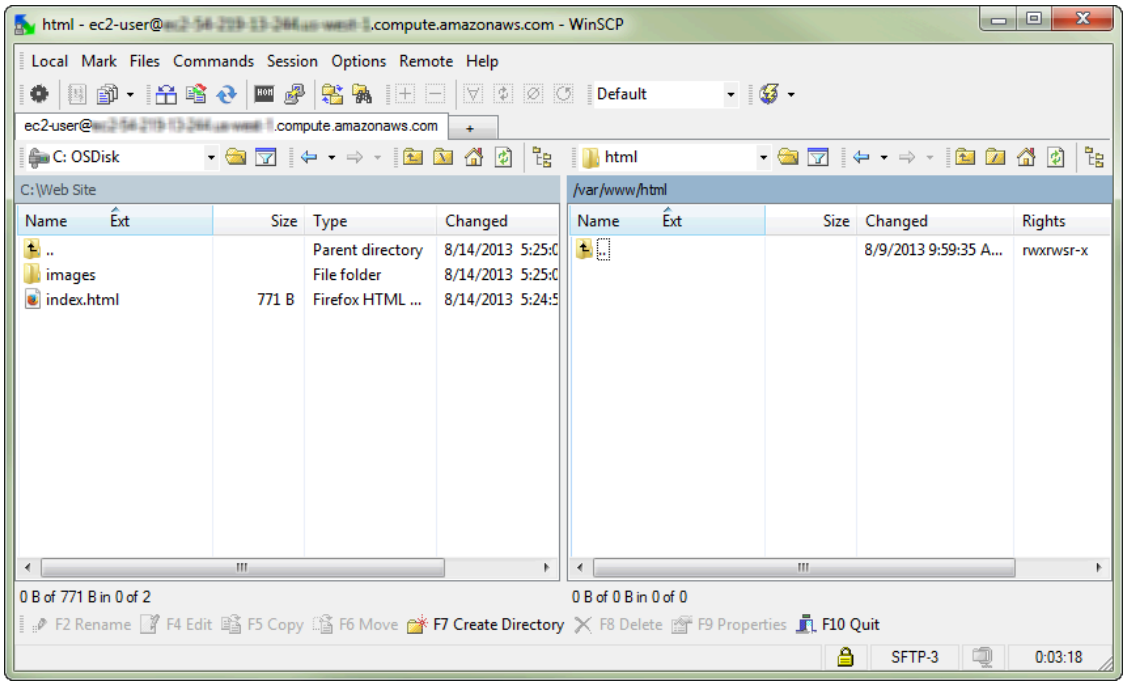
1. 从 http://winscp.net/eng/download.php 上下载并安装 WinSCP。对于大多数用户而言，采用默认安装选项就可以了。
2. 启动 WinSCP。
3. 在 WinSCP login (WinSCP 登录) 屏幕上，为 Host name (主机名) 输入以下内容之一：
   - （公有 DNS 或 IPv4 地址）要使用实例的公有 DNS 名称或公有 IPv4 地址登录，请输入实例的公有 DNS 名称或公有 IPv4 地址。
   - (IPv6) 或者，如果实例具有 IPv6 地址，要使用实例的 IPv6 地址登录，请输入实例的 IPv6 地址。
4. 对于用户名，请输入默认的 AMI 用户名。
   - 对于 Amazon Linux 2022、Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。
   - 对于 CentOS AMI，用户名是 `centos` 或 `ec2-user`。
   - 对于 Debian AMI，用户名称是 `admin`。
   - 对于 Fedora AMI，用户名是 `fedora` 或 `ec2-user`。
   - 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
   - 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
   - 对于 Ubuntu AMI，用户名称是 `ubuntu`。
   - 对于 Oracle AMI，用户名是 `ec2-user`。
   - 对于 Bitnami AMI，用户名称是 `bitnami`。
   - 否则，检查 AMI 提供程序。
5. 为您的实例指定私有密钥。对于私有密钥，请输入私有密钥的路径，或选择 ... 按钮以浏览文件。要打开高级站点设置，对于较高版本的 WinSCP，请选择高级。要查找私有密钥文件设置，请在 SSH 下面选择身份验证。

   以下是 WinSCP 版本 5.9.4 中的屏幕截图：



WinSCP 需要 PuTTY 私有密钥文件 (.ppk)。您可以使用 PuTTYgen 将 .pem 安全密钥文件转换成 .ppk 格式。有关更多信息，请参阅使用 PuTTYgen 转换私有密钥 (p. 664)。

6. （可选）在左侧面板中，选择目录。对于远程目录，请输入要将文件添加到的目录的路径。要打开高级站点设置，对于较高版本的 WinSCP，请选择高级。要查找远程目录设置，请在环境下面选择目录。
7. 选择登录。要将主机指纹添加到主机缓存中，请选择是。



8. 建立连接后，在连接窗口中，您的 Linux 实例显示在右侧，本地计算机显示在左侧。您可以在远程文件系统和本地计算机之间拖放文件。有关 WinSCP 的更多信息，请参阅 http://winscp.net/eng/docs/start 中的项目文档。

   如果您收到无法运行 SCP 来启动传输的错误信息，请验证是否已安装在 Linux 实例 scp 上。

使用 Windows Subsystem for Linux 从 Windows 连接到 Linux 实例

启动您的实例之后，您可以连接到该实例，然后像使用您面前的计算机一样来使用它。

以下说明介绍如何使用 Windows Subsystem for Linux (WSL) 上的 Linux 发行版来连接到您的实例。可以免费下载 WSL，可用于在 Windows 上直接将本机 Linux 命令行工具与传统 Windows 桌面一起运行，而不会产生虚拟机开销。

通过安装 WSL，您可以使用本机 Linux 环境连接到 Linux EC2 实例，而不是使用 PuTTY 或 PuTTYgen。Linux 环境让连接到 Linux 实例变得更轻松，因为它附带一个本机 SSH 客户端，可用于连接到 Linux 实例并更改 .pem 密钥文件的权限。Amazon EC2 控制台提供用于连接到 Linux 实例的 SSH 命令，并且您可以获得 SSH 命令中的详细输出以进行故障排除。有关更多信息，请参阅 Windows Subsystem for Linux 文档。

> Note
>
> 在安装 WSL 后，所有先决条件和步骤都相同（如使用 SSH 连接到 Linux 实例 (p. 649)中所述），并且体验与使用本机 Linux 的体验类似。

如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

目录

- 先决条件 (p. 649)
- 使用 WSL 连接到 Linux 实例 (p. 670)
- 使用 SCP 将文件从 Linux 传输到 Linux 实例 (p. 671)
- 卸载 WSL (p. 672)

先决条件

在连接到 Linux 实例之前，请先完成以下先决条件：

验证该实例是否就绪

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查。您可以在实例页面的状态检查列中查看此信息。

验证有关连接到您的实例的常规先决条件

要查找实例的公有 DNS 名称或 IP 地址以及您在连接到实例时应使用的用户名，请参阅设置以连接到实例 (p. 645)。

在本地计算机上安装 Windows Subsystem for Linux (WSL) 和 Linux 发行版

按照 Windows 10 安装指南中的说明执行操作来安装 WSL 和 Linux 发行版。说明中的示例安装的是 Linux 的 Ubuntu 发行版，但您可以安装任意发行版。系统会提示您重新启动计算机以使更改生效。

将私有密钥从 Windows 复制到 WSL

在 WSL 终端窗口中，将 .pem 文件（适用于您在启动实例时指定的密钥对）从 Windows 复制到 WSL。记下在连接到实例时要使用的 WSL 上的 .pem 文件的完全限定路径。有关如何指定 Windows 硬盘的路径的信息，请参阅如何访问我的 C 驱动器？。有关密钥对和 Windows 实例的更多信息，请参阅 Amazon EC2 密钥对和 Windows 实例。

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

使用 WSL 连接到 Linux 实例

通过以下过程使用 Windows Subsystem for Linux (WSL) 连接到 Linux 实例。如果您在尝试连接到实例时收到错误，请参阅 排查实例的连接问题。 (p. 1684)。

使用 SSH 连接到您的实例

1. 在终端窗口中，使用 ssh 命令连接到该实例。您指定私有密钥的路径和文件名 (.pem)、实例的用户名以及实例的公有 DNS 名称或 IPv6 地址。有关如何查找私有密钥、实例的用户名以及实例的 DNS 名称或 IPv6 地址的更多信息，请参阅查找私有密钥并设置权限 (p. 648)和获取有关您的实例的信息 (p. 645)。要连接到实例，请使用以下命令之一。
   - （公有 DNS）要使用实例的公有 DNS 名称进行连接，请输入以下命令。

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
     ```

   - (IPv6) 或者，如果实例具有 IPv6 地址，您可以使用其 IPv6 地址连接到该实例。请在 ssh 命令中指定私有密钥 (.pem) 文件路径、适当的用户名和 IPv6 地址。

     ```
     ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
     ```

   您会看到如下响应：

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```

2. (可选) 验证安全警报中的指纹是否与您之前在 （可选）获取实例指纹 (p. 649) 中获得的指纹相匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。
3. 输入 yes。

您会看到如下响应：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

使用 SCP 将文件从 Linux 传输到 Linux 实例

在您的本地计算机与 Linux 实例之间传输文件的一种方法是使用安全复制协议 (SCP)。本节介绍了如何使用 SCP 传输文件。该步骤与使用 SSH 连接到实例的步骤类似。

先决条件

- 验证有关将文件传输到您的实例的常规先决条件。

  将文件传输到实例的常规先决条件与连接到实例的常规先决条件相同。有关更多信息，请参阅设置以连接到实例 (p. 645)。
- 安装 SCP 客户端

  默认情况下，大多数 Linux、Unix 和 Apple 计算机都包含 SCP 客户端。如果您的计算机不含 SSH 客户端，OpenSSH 项目提供了整套 SSH 工具免费使用的功能，包括 SCP 客户端。有关更多信息，请参阅 https://www.openssh.com。

以下步骤将引导您使用 SCP 来传输文件。如果您已经使用 SSH 连接到实例，且已确认实例指纹，您可以从包含 SCP 命令的步骤 (步骤 4) 开始。

使用 SCP 来传输文件

1. 使用实例的公有 DNS 名称将文件传输到您的实例。例如，如果私有密钥文件的名称为 `key-pair-name`，要传输的文件为 `SampleFile.txt`，用户名为 `instance-user-name`，实例的公有 DNS 名称为 `my-instance-public-dns-name` 或 IPv6 地址为 `my-instance-IPv6-address`，请使用以下命令之一将该文件复制到 `instance-user-name` 主目录中。
   - （公有 DNS）要使用实例的公有 DNS 名称传输文件，请输入以下命令。

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
     ```
   - (IPv6) 或者，如果实例具有 IPv6 地址，您可以使用实例的 IPv6 地址传输文件。IPv6 地址必须用方括号 ([ ]) 括起来，并且必须对方括号进行转义 (\)。

     ```
     scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@\[my-instance-IPv6-address\]:~
     ```

   您会看到如下响应：

   ```
   The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
   can't be established.
   RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
   Are you sure you want to continue connecting (yes/no)?
   ```
2. (可选) 验证安全警报中的指纹是否与您之前在（可选）获取实例指纹 (p. 649)中获得的指纹相匹配。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果匹配，请继续到下一步。
3. 输入 **yes**。

   您会看到如下响应：

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
Sending file modes: C0644 20 SampleFile.txt
Sink: C0644 20 SampleFile.txt
SampleFile.txt                                100%   20     0.0KB/s   00:00
```

如果您收到“bash: scp: command not found (bash: scp: 命令未找到)”错误，您必须先在 Linux 实例上安装 scp。对于某些操作系统，该命令会位于 `openssh-clients` 程序包中。对于 Amazon Linux 变体（如经 Amazon ECS 优化的 AMI），使用以下命令安装 scp：

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

4. 要在另一个方向上传输文件（从 Amazon EC2 实例中传输到本地计算机），请颠倒主机参数的顺序。例如，要将 `SampleFile.txt` 文件从 EC2 实例传回到本地计算机上的主目录并保存为 `SampleFile2.txt`，请在本地计算机上使用以下命令之一。
   - （公有 DNS）要使用实例的公有 DNS 名称传输文件，请输入以下命令。

     ```
     scp -i /path/key-pair-name.pem instance-user-
     name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/SampleFile2.txt
     ```

   - (IPv6) 或者，如果实例具有 IPv6 地址，要使用实例的 IPv6 地址在另一个方向上传输文件，请输入以下命令。

     ```
     scp -i /path/key-pair-name.pem instance-user-name@
     \[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
     ```

卸载 WSL

有关卸载 Windows Subsystem for Linux 的信息，请参阅如何卸载 WSL 发行版？

使用会话管理器连接到 Linux 实例

会话管理器是一项完全托管的 Amazon Systems Manager 功能，可让您通过基于浏览器的交互一键式 Shell 或通过 Amazon CLI 管理 Amazon EC2 实例。您可以使用会话管理器通过您账户中的实例来启动会话。启动会话后，您可以像通过任何其他连接类型一样运行 bash 命令。有关会话管理器的更多信息，请参阅 Amazon Systems Manager 用户指南 中的 Amazon Systems Manager 会话管理器。

在尝试使用会话管理器连接到实例之前，请确保已完成必要的设置步骤。有关更多信息和说明，请参阅设置会话管理器。

使用 Amazon EC2 控制台通过会话管理器连接到 Linux 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例，然后选择连接。
4. 对于 Connection method (连接方法)，请选择 Session Manager (会话管理器)。
5. 选择 Connect。

问题排查

如果您收到一个错误，该错误指示您无权执行一个或多个 Systems Manager 操作 (`ssm:command-name`)，则必须更新您的策略以允许您从 Amazon EC2 控制台开启会话。有关更多信息，请参阅 Amazon Systems Manager 用户指南中的会话管理器的 Quickstart 默认 IAM policy。

将 EC2 实例连接到 Amazon 资源

在您启动实例之后，您可以将其连接到一个或多个 Amazon 资源。

此部分介绍如何将 Amazon EC2 实例自动连接到 Amazon RDS 数据库。

将 EC2 实例自动连接到 RDS 数据库

您可以使用 Amazon EC2 控制台中的自动连接功能将一个或多个 EC2 实例快速连接到 RDS 数据库，以允许它们之间的流量。

有关更多信息，请参阅如何自动配置连接 (p. 675)。有关详细演练（包括连接 EC2 实例和 RDS 数据库的其他方法），请参阅 Tutorial: Connect an Amazon EC2 instance to an Amazon RDS database（教程：将 Amazon EC2 实例连接到 Amazon RDS 数据库） (p. 675)。

主题

- 成本 (p. 673)
- 先决条件 (p. 673)
- 自动连接实例和数据库 (p. 673)
- 如何自动配置连接 (p. 675)

成本

虽然将 EC2 实例自动连接到 RDS 数据库不收取任何费用，但您需要为基础服务付费。如果 EC2 实例和 RDS 数据库位于不同的可用区中，则将收取数据传输费。有关数据传输费的信息，请参阅“Amazon EC2 On-Demand Pricing”（Amazon EC2 按需定价）页面上的 Data Transfer（数据传输）。

先决条件

请检查以下各项，然后才能将 EC2 实例自动连接到 RDS 数据库：

- EC2 实例必须处于 Running（正在运行）状态。如果 EC2 实例处于其他状态，则您无法连接该实例。
- EC2 实例和 RDS 数据库必须位于同一虚拟私有云（VPC）中。如果 EC2 实例和 RDS 数据库位于不同的 VPC 中，则不支持自动连接功能。

自动连接实例和数据库

您可以在启动实例后立即或稍后将 EC2 实例自动连接到 RDS 数据库。

启动后立即自动连接

在您启动 EC2 实例后，使用以下步骤立即将 EC2 实例自动连接到 RDS 数据库。

要查看这些步骤的动画，请参阅 观看动画：将新启动的 EC2 实例自动连接到 RDS 数据库 (p. 674)。

使用 EC2 控制台将新启动的 EC2 实例自动连接到 RDS 数据库

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制台控制面板中，选择 Launch instances（启动实例），然后按照步骤启动实例 (p. 576)。
3. 在实例启动确认页面上，选择 Connect an RDS database（连接 RDS 数据库）。
4. 在 Connect RDS Database（连接 RDS 数据库）对话框中，执行以下操作：

    a. 对于 Database role（数据库角色），选择 Cluster（集群）或 Instance（实例）。

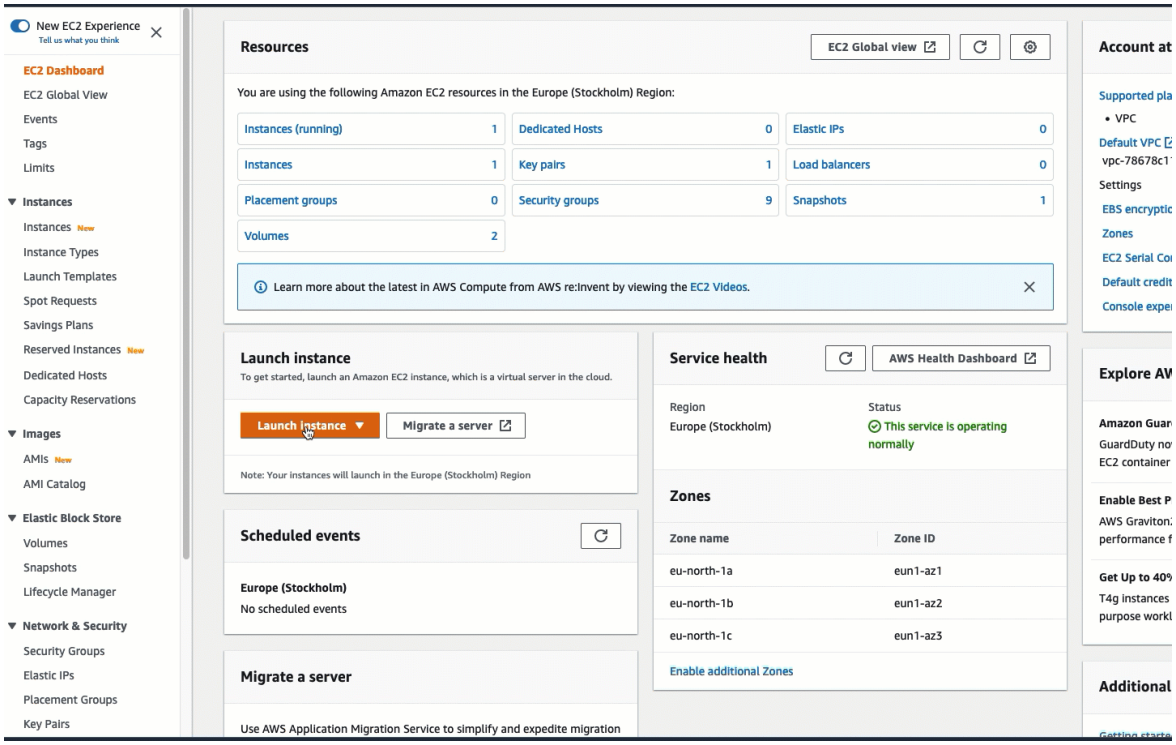
b. 对于 RDS database（RDS 数据库），选择要连接的数据库。

Note

EC2 实例和 RDS 数据库必须位于同一 VPC 中，以便相互连接。

c. 选择 Connect（连接）。

观看动画：将新启动的 EC2 实例自动连接到 RDS 数据库



自动连接现有实例

使用以下步骤将现有 EC2 实例自动连接到 RDS 数据库。

要查看这些步骤的动画，请参阅 观看动画：将现有 EC2 实例自动连接到 RDS 数据库 (p. 675)。

使用 EC2 控制台将现有 EC2 实例自动连接到 RDS 数据库

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择一个或多个要连接到 RDS 数据库的 EC2 实例，然后选择 Actions（操作）、Networking（联网）、Connect RDS database（连接 RDS 数据库）。

   如果 Connect RDS database（连接 RDS 数据库）不可用，请检查 EC2 实例是否处于 Running（正在运行）状态，以及它们是否位于同一 VPC 中。
4. 在 Connect RDS Database（连接 RDS 数据库）对话框中，执行以下操作：

   a. 对于 Database role（数据库角色），选择 Cluster（集群）或 Instance（实例）。

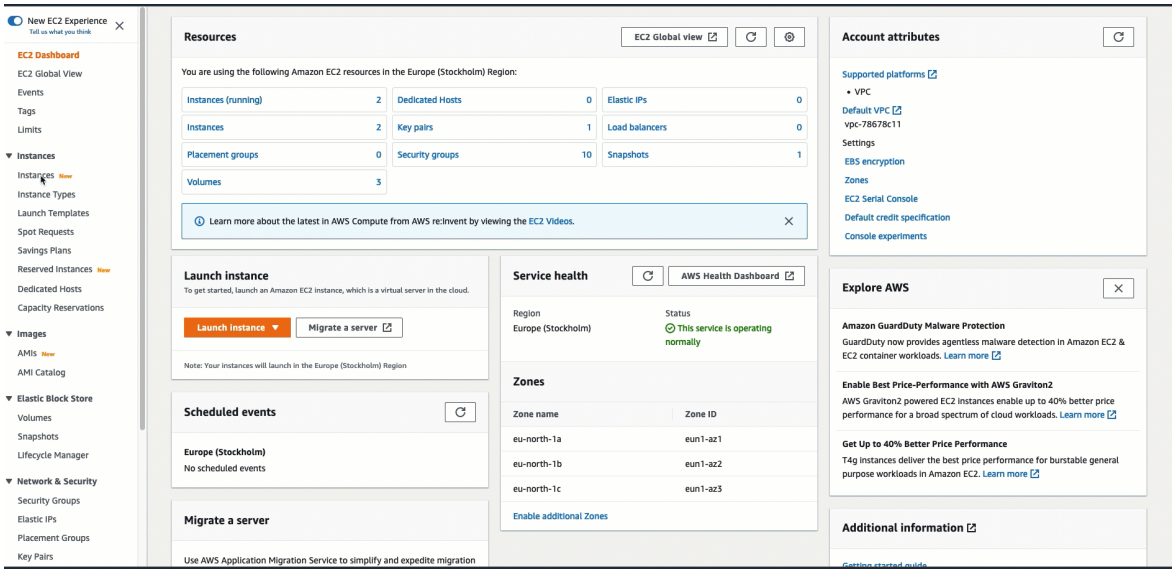
   b. 对于 RDS database（RDS 数据库），选择要连接的数据库。

   Note

   EC2 实例和 RDS 数据库必须位于同一 VPC 中，以便相互连接。

c. 选择 Connect（连接）。

观看动画：将现有 EC2 实例自动连接到 RDS 数据库



有关如何使用 Amazon RDS 控制台将 EC2 实例自动连接到 RDS 数据库的信息，请参阅《Amazon RDS 用户指南》中的配置与 EC2 实例的自动网络连接。

如何自动配置连接

当您使用 EC2 控制台自动配置 EC2 实例与 RDS 数据库之间的连接以允许它们之间的流量时，该连接将由安全组 (p. 1303)配置。

将自动创建安全组，并将其添加到 EC2 实例和 RDS 数据库中，如下所示：

- Amazon EC2 将创建一个名为 ec2-rds-*x* 的安全组，并将其添加到 EC2 实例中。它包含一条出站规则，通过将 rds-ec2-*x*（数据库安全组）指定为目标，以允许流向数据库的流量。
- Amazon RDS 将创建了一个名为 rds-ec2-*x* 的安全组，并将其添加到数据库中。它包含一条入站规则，通过将 ec2-rds-*x*（EC2 实例安全组）指定为其来源，以允许来自 EC2 实例的流量。

这些安全组相互引用作为目标和来源，并且只允许数据库端口上的流量。您可以重复使用这些安全组，这样任何具有 rds-ec2-*x* 安全组的数据库都可以与任何具有 ec2-rds-*x* 安全组的 EC2 实例通信。

安全组名称遵循某种模式。对于由 Amazon EC2 创建的安全组，该模式为 ec2-rds-*x*；对于由 Amazon RDS 创建的安全组，该模式为 rds-ec2-*x*。*x* 是一个数字，每次自动创建一个新的安全组时，该数字会增加 1。

Tutorial: Connect an Amazon EC2 instance to an Amazon RDS database（教程：将 Amazon EC2 实例连接到 Amazon RDS 数据库）

教程目标

本教程的目标是学习如何使用 Amazon Web Services Management Console 配置 Amazon EC2 实例与 Amazon RDS 数据库之间的安全连接。

有不同的选项用于配置连接。在本教程中，我们将探讨以下三个选项：

- 选项 1：使用 EC2 控制台将 EC2 实例自动连接到 RDS 数据库 (p. 678)

  使用 EC2 控制台中的自动连接功能自动配置 EC2 实例与 RDS 数据库之间的连接，以允许 EC2 实例与 RDS 数据库之间的流量。
- 选项 2：使用 RDS 控制台将 EC2 实例自动连接到 RDS 数据库 (p. 686)

  使用 RDS 控制台中的自动连接功能自动配置 EC2 实例与 RDS 数据库之间的连接，以允许 EC2 实例与 RDS 数据库之间的流量。
- 选项 3：通过模仿自动连接功能，将 EC2 实例手动连接到 RDS 数据库 (p. 692)

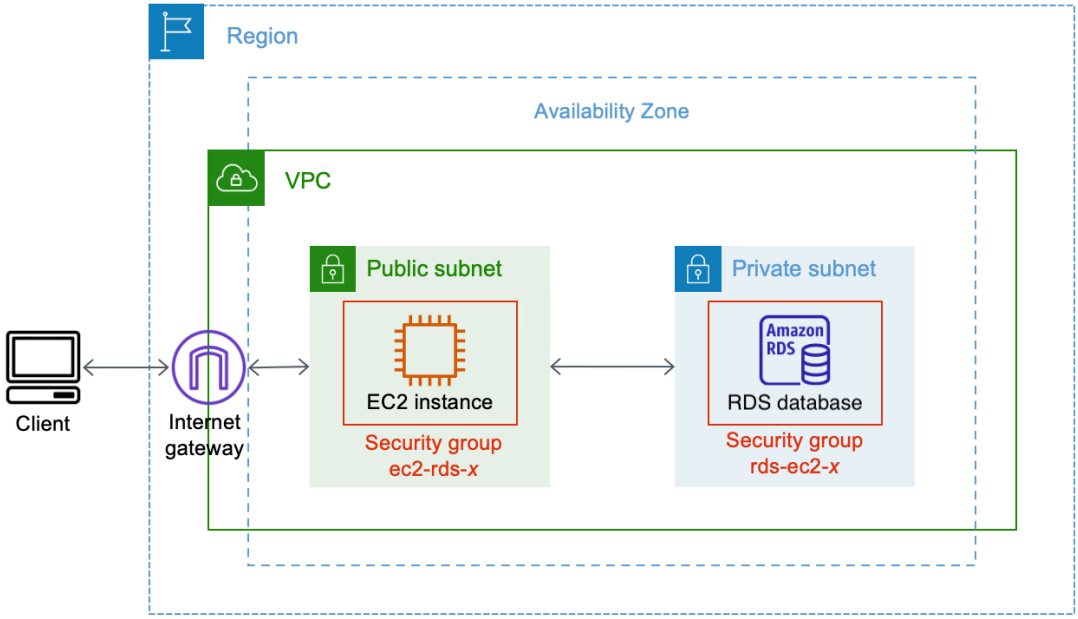
  通过手动配置和分配安全组来配置 EC2 实例与 RDS 数据库之间的连接，以重现由“选项 1”和“选项 2”中的自动连接功能自动创建的配置。

上下文

作为您为何要在 EC2 实例与 RDS 数据库之间配置连接的背景，让我们考虑以下场景：您的网站向您的用户提供一份表单以供填写。您需要在数据库中捕获表单数据。您可以在已配置为 Web 服务器的 EC2 实例上托管您的网站，也可以在 RDS 数据库中捕获该表单数据。EC2 实例和 RDS 数据库需要相互连接，以便表单数据可以从 EC2 实例传输到 RDS 数据库。本教程介绍如何配置该连接。请注意，这只是连接 EC2 实例与 RDS 数据库的使用案例的一个示例。

架构

下图显示了创建的资源以及完成本教程中的所有步骤后生成的架构配置。



该图说明了您将创建的以下资源：

- 您将在同一 Amazon Web Services 区域、VPC 和可用区中创建 EC2 实例及 RDS 数据库。
- 您将在公有子网中创建 EC2 实例。
- 您将在私有子网中创建 RDS 数据库。

  当您使用 RDS 控制台创建 RDS 数据库并自动连接 EC2 实例时，将自动选择数据库的 VPC、数据库（DB）子网组和公有访问设置。将在与 EC2 实例相同的 VPC 内的私有子网中自动创建 RDS 数据库。
- 互联网用户可以通过互联网网关使用 SSH 或 HTTP/HTTPS 连接到 EC2 实例。

- 互联网用户无法直接连接到 RDS 数据库；只有 EC2 实例连接到 RDS 数据库。
- 当您使用自动连接功能允许 EC2 实例与 RDS 数据库之间的流量时，将自动创建并添加以下安全组：
  - 将创建安全组 ec2-rds-*x* 并将其添加到 EC2 实例中。它包含一条出站规则，引用 rds-ec2-*x* 安全组作为其目标。这将允许来自 EC2 实例的流量通过 rds-ec2-*x* 安全组到达 RDS 数据库。
  - 将创建安全组 rds-ec2-*x* 并将其添加到 RDS 数据库中。它包含一条入站规则，引用 ec2-rds-*x* 安全组作为其来源。这将允许来自 EC2 实例（具有 ec2-rds-*x* 安全组）的流量到达 RDS 数据库。

  通过使用独立的安全组（一个用于 EC2 实例，一个用于 RDS 数据库），您可以更好地控制实例和数据库的安全性。如果您要在实例和数据库上使用同一安全组，然后将该安全组修改为仅适合（比如）数据库，则该修改将同时影响实例和数据库。换言之，如果您要使用一个安全组，则可能会无意中修改资源（实例或数据库）的安全性，因为您忘记了该安全组已连接到该资源。

  自动创建的安全组也遵循最低权限，因为它们仅允许通过创建特定于工作负载的安全组对，在数据库端口上为此工作负载建立相互连接。

注意事项

在完成本教程中的任务时，请注意以下几点：

- 两个控制台 - 在本教程中，您将使用以下两个控制台：
  - Amazon EC2 控制台 - 您将使用 EC2 控制台启动实例，将 EC2 实例自动连接到 RDS 数据库，以及使用手动选项通过创建安全组来配置连接。
  - Amazon RDS 控制台 - 您将使用 RDS 控制台创建 RDS 数据库，然后将 EC2 实例自动连接到 RDS 数据库。
- 一个 VPC - 要使用自动连接功能，EC2 实例和 RDS 数据库必须位于同一 VPC 中。

  如果您要手动配置 EC2 实例与 RDS 数据库之间的连接，可以在一个 VPC 中启动 EC2 实例，在另一个 VPC 中启动 RDS 数据库；但是，您需要设置额外的路由和 VPC 配置。本教程中未涵盖此场景。
- 一个 Amazon Web Services 区域 - EC2 实例和 RDS 数据库必须位于同一区域中。
- 两个安全组 - EC2 实例与 RDS 数据库之间的连接由两个安全组配置 - 一个安全组用于 EC2 实例，一个安全组用于 RDS 数据库。

  当您使用 EC2 控制台或 RDS 控制台中的自动连接功能配置连接（本教程的“选项 1”和“选项 2”）时，将自动创建安全组并将其分配给 EC2 实例和 RDS 数据库。

  如果您不使用自动连接功能，则需要手动创建和分配安全组。您可以在本教程的“选项 3”中执行此操作。

完成教程所需的时间

30 分钟

您可以一口气完成整个教程，也可以一次完成一项任务。

成本

您在完成本教程过程中创建的 Amazon 资源可能会产生费用。

您可以在 Free tier（免费套餐）下使用 Amazon EC2，前提是您的 Amazon 账户创建不到 12 个月，并且您根据免费套餐要求配置资源。

如果 EC2 实例和 RDS 数据库位于不同的可用区中，则需要支付数据传输费。为了避免产生这些费用，EC2 实例和 RDS 数据库必须位于同一可用区中。有关数据传输费的信息，请参阅“Amazon EC2 On-Demand Pricing”（Amazon EC2 按需定价）页面上的 Data Transfer（数据传输）。

为了防止在您完成教程后产生费用，请确保在不再需要资源时将其删除。有关删除资源的步骤，请参阅清除 (p. 698)。

选项 1：使用 EC2 控制台将 EC2 实例自动连接到 RDS 数据库

目标

“选项 1”的目标是探索 EC2 控制台中的自动连接功能，该功能可自动配置 EC2 实例与 RDS 数据库之间的连接，以允许从 EC2 实例到 RDS 数据库的流量。在“选项 3”中，您将学习如何手动配置连接。

开始前的准备工作

完成本教程需要做好以下准备：

- 与 EC2 实例位于同一 VPC 中的 RDS 数据库。您可以使用现有的 RDS 数据库，也可以按照“任务 1”中的步骤创建新的 RDS 数据库。
- 与 RDS 数据库位于同一 VPC 中的 EC2 实例。您可以使用现有的 EC2 实例，也可以按照“任务 2”中的步骤创建新的 EC2 实例。
- 调用以下操作的权限：
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

完成“选项 1”所需的任务

- 任务 1：创建 RDS 数据库 - 可选 (p. 678)
- 任务 2：启动 EC2 实例 - 可选 (p. 680)
- 任务 3：将 EC2 实例自动连接到 RDS 数据库 (p. 683)
- 任务 4：验证连接配置 (p. 684)

任务 1：创建 RDS 数据库 - 可选

> **Note**
>
> 创建 Amazon RDS 数据库不是本教程的重点。如果您已拥有 RDS 数据库并希望在本教程中使用它，则可跳过此任务。

任务目标

此任务的目标是创建 RDS 数据库，以便您可以完成“任务 3”，在该任务中，您将配置 EC2 实例与 RDS 数据库之间的连接。如果您拥有可以使用的 RDS 数据库，则可跳过此任务。

> **Important**
>
> 如果您使用现有的 RDS 数据库，请确保它与 EC2 实例位于同一 VPC 中，以便您可以使用自动连接功能。

创建 RDS 数据库的步骤

使用以下步骤创建 RDS 数据库。

要查看这些步骤的动画，请参阅 观看动画：创建 RDS 数据库 (p. 680)。

RDS 数据库配置

此任务中的步骤将按以下方式配置 RDS 数据库：

- 引擎类型：MySQL
- 模板：免费套餐
- 数据库实例标识符：**`tutorial-database-1`**
- 数据库实例类：`db.t3.micro`

> **Important**
>
> 在生产环境中，您应该配置数据库，以满足您的特定需求。

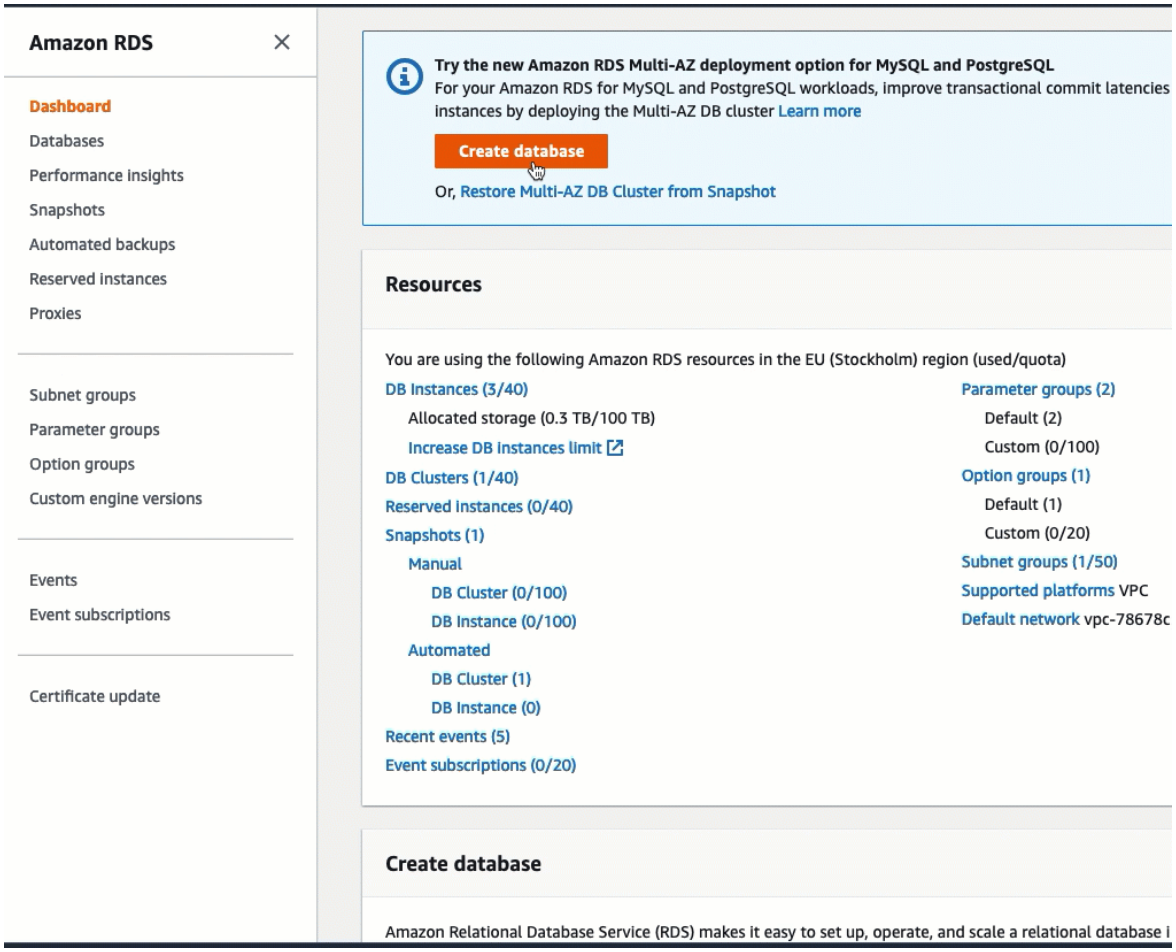
创建 MySQL RDS 数据库

1. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
2. 从“Region selector”（区域选择器）（位于右上角）中选择一个 Amazon Web Services 区域。数据库和 EC2 实例必须位于同一区域中，才能使用 EC2 控制台中的自动连接功能。
3. 在控制面板中，选择 Create database（创建数据库）。
4. 在 Choose a database creation method（选择数据库创建方法）下，检查并确保选择 Standard create（标准创建）。如果您选择 Easy create（轻松创建），则 VPC 选择器将不可用。您必须确保您的数据库与 EC2 实例位于同一 VPC 中，才能使用 EC2 控制台中的自动连接功能。
5. 在 Engine options（引擎选项）下，对于 Engine type（引擎类型），选择 MySQL。
6. 在 Templates（模板）下，选择一个满足您需求的示例模板。对于本教程，选择 Free tier（免费套餐）以免费创建数据库。但请注意，仅当您的账户创建不到 12 个月时，免费套餐才可用。其他限制适用。您可以通过选择 Free tier（免费套餐）框中的 Info（信息）链接来阅读更多内容。
7. 在 Settings (设置) 下，执行下列操作：
   a. 对于 DB instance identifier（数据库实例标识符），输入数据库的名称。在本教程中，请输入 **`tutorial-database-1`**。
   b. 对于 Master username（主用户名），保留默认名称，即 **`admin`**。
   c. 对于 Master password（主密码），输入您在本教程中可以记住的密码，然后对于 Confirm password（确认密码），再次输入该密码。
8. 在 Instance configuration（实例配置）下，对于 DB instance class（数据库实例类），保留默认值，即 db.t3.micro。如果您的账户创建不到 12 个月，则可以免费使用此数据库类。其他限制适用。有关更多信息，请参阅 Amazon Free Tier（免费套餐）。
9. 在 Connectivity（连接）下，对于 Compute resource（计算资源），选择 Don't connect to an EC2 compute resource（不连接到 EC2 计算资源），因为您稍后将在“任务 3”中连接 EC2 实例和 RDS 数据库。

   （稍后，在本教程的“选项 2”中，您将通过选择 Connect to an EC2 compute resource（连接到 EC2 计算资源），以试用 RDS 控制台中的自动连接功能。）
10. 对于 Virtual private cloud (VPC)（虚拟私有云（VPC）），选择一个 VPC。该 VPC 必须具有一个数据库子网组。要使用自动连接功能，EC2 实例和 RDS 数据库必须位于同一 VPC 中。
11. 对于此窗格中的其他字段，请保留所有默认值。
12. 选择 Create database（创建数据库）。

在 Databases（数据库）屏幕上，在数据库准备就绪可供使用之前，新数据库的 Status（状态）为 Creating（正在创建）。当状态变为 Available（可用）时，您便可以连接到该数据库。根据数据库类和存储量，新数据库可能需要等待多达 20 分钟时间才可用。

观看动画：创建 RDS 数据库



您现在已准备好任务 2：启动 EC2 实例 - 可选 (p. 680)。

任务 2：启动 EC2 实例 - 可选

Note

启动实例不是本教程的重点。如果您已拥有 Amazon EC2 实例并希望在本教程中使用它，则可跳过此任务。

任务目标

此任务的目标是启动 EC2 实例，以便您可以完成“任务 3”，在该任务中，您将配置 EC2 实例与 Amazon RDS 数据库之间的连接。如果您拥有可以使用 EC2 实例，则可跳过此任务。

Important

如果您使用现有的 EC2 实例，请确保它与您的 RDS 数据库位于同一 VPC 中，以便您可以使用自动连接功能。

启动 EC2 实例的步骤

使用以下步骤启动本教程的 EC2 实例。

要查看这些步骤的动画，请参阅 观看动画：启动 EC2 实例 (p. 682)。

EC2 实例配置

此任务中的步骤将按以下方式配置 EC2 实例：

- 实例名称：**`tutorial-instance-1`**
- AMI：Amazon Linux 2
- 实例类型：`t2.micro`
- 自动分配公有 IP：已启用
- 具有以下三条规则的安全组：
  - 允许来自您的 IP 地址的 SSH
  - 允许来自任何地方的 HTTPS 流量
  - 允许来自任何地方的 HTTP 流量

> **Important**
>
> 在生产环境中，您应该配置实例，以满足您的特定需求。

启动 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从“Region selector”（区域选择器）（位于右上角）中选择一个 Amazon Web Services 区域。实例与 RDS 数据库必须位于同一区域中，才能使用 EC2 控制台中的自动连接功能。
3. 在 EC2 Dashboard（EC2 控制面板）上，选择 Launch instance（启动实例）。
4. 在 Name and tags（名称与标签）下，对于 Name（名称），输入名称以标识您的实例。对于本教程，请将该实例命名为 **`tutorial-instance-1`**。虽然实例名称不是必填项，但是当您在 EC2 控制台中选择实例时，该名称将帮助您轻松识别它。
5. 在 Application and OS Images（应用程序和操作系统映像）下，选择满足您的 Web 服务器需求的 AMI。本教程使用 Amazon Linux 2。
6. 在 Instance type（实例类型）下，对于 Instance type（实例类型），选择满足您的 Web 服务器需求的实例类型。本教程使用的是 `t2.micro`。

   > **Note**
   >
   > 您可以在 Free tier（免费套餐）下使用 Amazon EC2，前提是您的 Amazon 账户创建不到 12 个月，并且您选择了 `t2.micro` 实例类型（或在 `t2.micro` 不可用的区域中选择 `t3.micro`）。
7. 在 Key pair (login)（密钥对（登录））下，对于 Key pair name（密钥对名称），选择您的密钥对。
8. 在 Network settings（网络设置）下，执行以下操作：

   a. 对于 Network（网络）和 Subnet（子网），如果您尚未更改默认 VPC 或子网，则可以保留默认设置。

      如果您对默认 VPC 或子网进行了更改，请检查以下各项：

      i. 实例必须与 RDS 数据库位于同一 VPC 中，才能使用自动连接功能。默认情况下，您只有一个 VPC。

      ii. 您要将实例启动到其中的 VPC 必须连接互联网网关，以便您能从互联网访问您的 Web 服务器。您的默认 VPC 将自动设置互联网网关。

iii. 为了确保您的实例收到公有 IP 地址，对于 Auto-assign public IP（自动分配公有 IP），请检查并确保选择 Enable（启用）。如果选择 Disable（禁用），请选择 Edit（编辑）（位于 Network Settings（网络设置）右侧），然后对于 Auto-assign public IP（自动分配公有 IP），选择 Enable（启用）。

b. 要使用 SSH 连接到您的实例，您需要一条安全组规则，授权来自您计算机的公有 IPv4 地址的 SSH (Linux) 或 RDP (Windows) 流量。默认情况下，当您启动实例时，将使用允许来自任何地方的入站 SSH 流量的规则创建新的安全组。

要确保只有您的 IP 地址才能连接到您的实例，请在 Firewall (security groups)（防火墙（安全组））下，从 Allow SSH traffic from（允许入站 SSH 流量）复选框旁边的下拉列表中，选择 My IP（我的 IP）。

c. 要允许流量从互联网流向您的实例，请选中以下复选框：

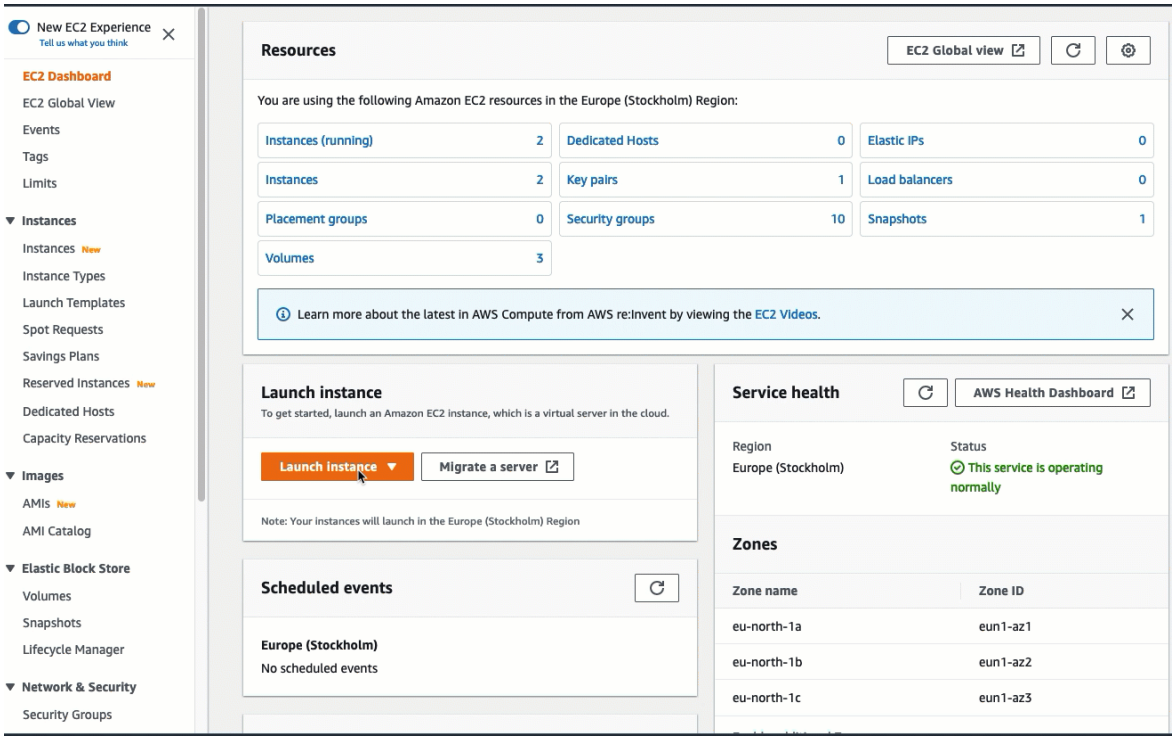
- Allow HTTPs traffic from the internet（允许来自互联网的 HTTPs 流量）
- Allow HTTP traffic from the internet（允许来自互联网的 HTTP 流量）

9. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。
10. 保持确认页面处于打开状态。对于下一个任务，当您将实例自动连接到数据库时，您将需要该页面。

如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

有关启动实例的更多信息，请参阅 使用新启动实例向导启动实例 (p. 575)。

观看动画：启动 EC2 实例



您现在已准备好任务 3：将 EC2 实例自动连接到 RDS 数据库 (p. 683)。

任务 3：将 EC2 实例自动连接到 RDS 数据库

任务目标

此任务的目标是使用 EC2 控制台中的自动连接功能自动配置 EC2 实例与 RDS 数据库之间的连接。

连接 EC2 实例和 RDS 数据库的步骤

使用以下步骤，使用 EC2 控制台中的自动功能连接 EC2 实例和 RDS 数据库。

要查看这些步骤的动画，请参阅 观看动画：将新启动的 EC2 实例自动连接到 RDS 数据库 (p. 684)。

使用 EC2 控制台将 EC2 实例自动连接到 RDS 数据库

1. 在实例启动确认页面（它应从上一个任务中打开）上，选择 Connect an RDS database（连接 RDS 数据库）。

   如果您关闭了该确认页面，请按以下步骤操作：

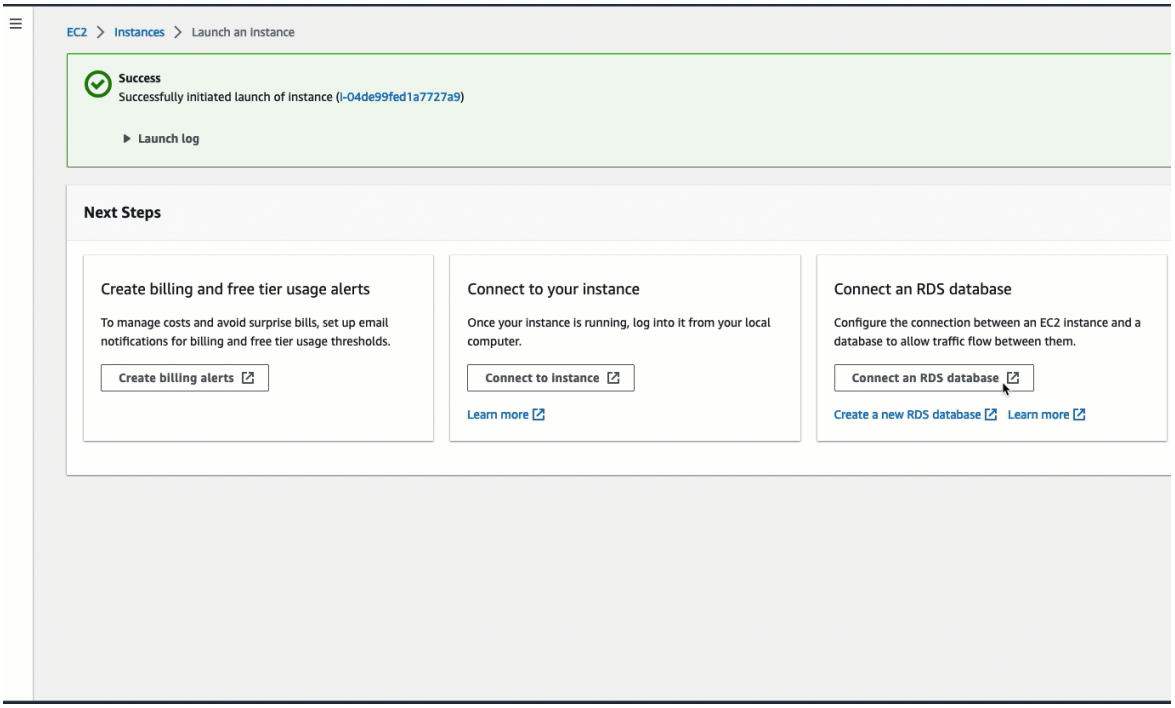
   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 在导航窗格中，选择实例。
   c. 选择您刚刚创建的 EC2 实例，然后选择 Actions（操作）、Networking（联网）、Connect RDS database（连接 RDS 数据库）。

      如果 Connect RDS database（连接 RDS 数据库）不可用，请检查该 EC2 实例是否处于 Running（正在运行）状态。
2. 对于 Database role（数据库角色），选择 Instance（实例）。本例中的实例是指数据库实例。
3. 对于 RDS database（RDS 数据库），选择您在“任务 1”中创建的 RDS 数据库。

   Note

   EC2 实例和 RDS 数据库必须位于同一 VPC 中，以便相互连接。
4. 选择 Connect（连接）。

观看动画：将新启动的 EC2 实例自动连接到 RDS 数据库



您现在已准备好任务 4：验证连接配置 (p. 684)。

任务 4：验证连接配置

任务目标

此任务的目标是验证两个安全组是否已创建并分配给实例和数据库。

当您使用 EC2 控制台中的自动连接功能配置连接时，将自动创建安全组并将其分配给实例和数据库，如下所示：

- 将创建安全组 rds-ec2-*x* 并将其添加到 RDS 数据库中。它包含一条入站规则，引用 ec2-rds-*x* 安全组作为其来源。这将允许来自 EC2 实例（具有 ec2-rds-*x* 安全组）的流量到达 RDS 数据库。
- 将创建安全组 ec2-rds-*x* 并将其添加到 EC2 实例中。它包含一条出站规则，引用 rds-ec2-*x* 安全组作为其目标。这将允许来自 EC2 实例的流量通过 rds-ec2-*x* 安全组到达 RDS 数据库。

验证连接配置的步骤

使用以下步骤验证连接配置。

要查看这些步骤的动画，请参阅 观看动画：验证连接配置 (p. 685)。

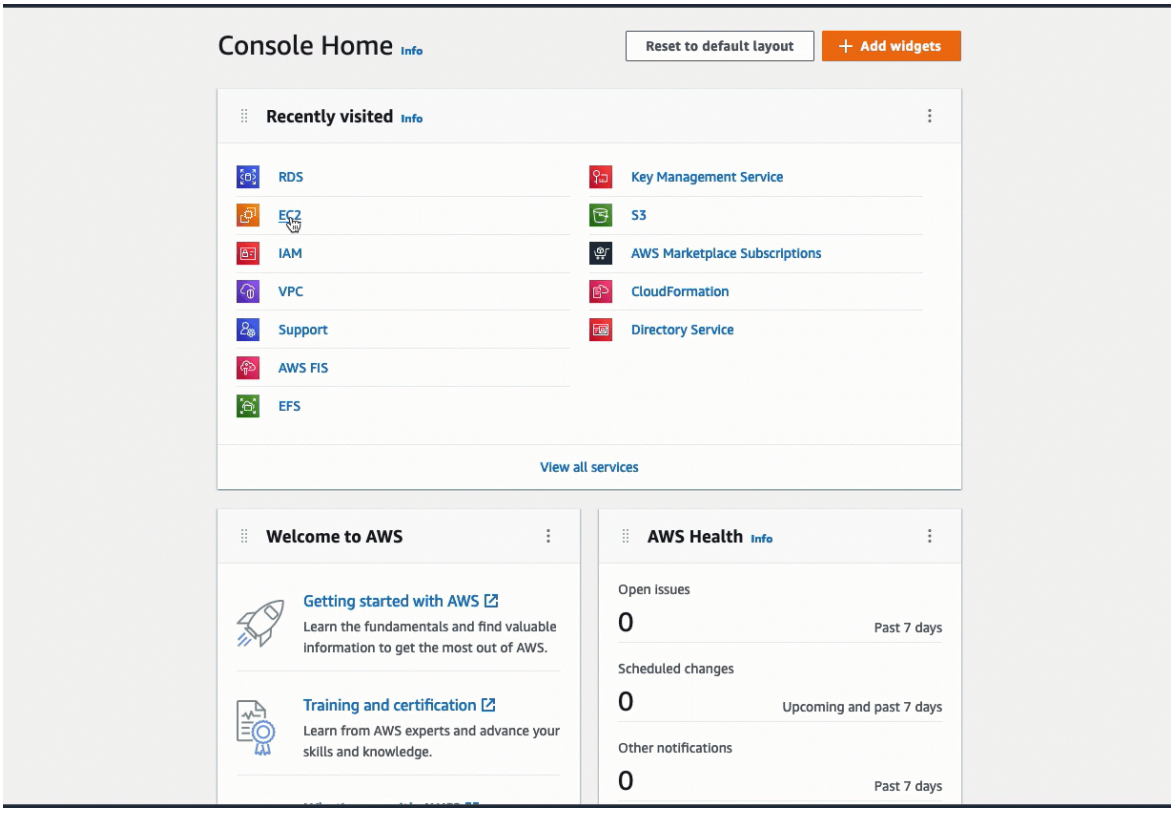
使用控制台验证连接配置

1. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
2. 在导航窗格中，选择 Databases（数据库）。
3. 选择您为本教程创建的 RDS 数据库。
4. 在 Connectivity & security（连接和安全性）选项卡的 Security（安全性）、VPC security groups（VPC 安全组）下，验证并确保显示名为 rds-ec2-*x* 的安全组。
5. 选择 rds-ec2-*x* 安全组。EC2 控制台中的 Security Groups（安全组）屏幕打开。
6. 选择 rds-ec2-*x* 安全组以打开它。

7. 选择 Inbound rules（入站规则）选项卡。
8. 验证并确保以下安全组规则存在，如下所示：
   - 类型：MYSQL/Aurora
   - 端口范围：3306
   - 来源：***sg-0987654321example*** / ec2-rds-***x*** - 这是分配给您在前面的步骤中验证的 EC2 实例的安全组。
   - 描述：允许来自 EC2 实例的连接的规则，附有 ***sg-1234567890example***
9. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
10. 在导航窗格中，选择实例。
11. 选择您在上一个任务中选择要连接到 RDS 数据库的 EC2 实例，然后选择 Security（安全性）选项卡。
12. 在 Security details（安全详细信息）的 Security groups（安全组）下，验证并确保列表中有名为 ec2-rds-***x*** 的安全组。*x* 是一个数字。
13. 选择 ec2-rds-***x*** 安全组以打开它。
14. 选择 Outbound rules（出站规则）选项卡。
15. 验证并确保以下安全组规则存在，如下所示：
    - 类型：MYSQL/Aurora
    - 端口范围：3306
    - 目标：***sg-1234567890example*** / rds-ec2-***x***
    - 描述：允许从此安全组所连接的任何实例到 **`database-tutorial`** 的连接的规则

通过验证这些安全组和安全组规则是否存在，以及它们是否已按照此过程中所述分配给 RDS 数据库和 EC2 实例，您可以使用自动连接功能验证是否已自动配置连接。

观看动画：验证连接配置



您已完成本教程的“选项 1”。现在，您可以完成“选项 2”，它将介绍如何使用 RDS 控制台将 EC2 实例自动连接到 RDS 数据库；您也可以完成“选项 3”，它将介绍如何手动配置在“选项 1”中自动创建的安全组。

选项 2：使用 RDS 控制台将 EC2 实例自动连接到 RDS 数据库

目标

“选项 2”的目标是探索 RDS 控制台中的自动连接功能，该功能可自动配置 EC2 实例与 RDS 数据库之间的连接，以允许从 EC2 实例到 RDS 数据库的流量。在“选项 3”中，您将学习如何手动配置连接。

开始前的准备工作

完成本教程需要做好以下准备：

- 与 RDS 数据库位于同一 VPC 中的 EC2 实例。您可以使用现有的 EC2 实例，也可以按照“任务 1”中的步骤创建新实例。
- 调用以下操作的权限：
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

完成“选项 2”所需的任务

- 任务 1：启动 EC2 实例 - 可选 (p. 686)
- 任务 2：创建 RDS 数据库并将其自动连接到 EC2 实例 (p. 688)
- 任务 3：验证连接配置 (p. 690)

任务 1：启动 EC2 实例 - 可选

> **Note**
>
> 启动实例不是本教程的重点。如果您已拥有 Amazon EC2 实例并希望在本教程中使用它，则可跳过此任务。

任务目标

此任务的目标是启动 EC2 实例，以便您可以完成“任务 2”，在该任务中，您将配置 EC2 实例与 Amazon RDS 数据库之间的连接。如果您拥有可以使用 EC2 实例，则可跳过此任务。

启动 EC2 实例的步骤

使用以下步骤启动本教程的 EC2 实例。

要查看这些步骤的动画，请参阅 观看动画：启动 EC2 实例 (p. 688)。

EC2 实例配置

此任务中的步骤将按以下方式配置 EC2 实例：

- 实例名称：**`tutorial-instance-2`**
- AMI：Amazon Linux 2
- 实例类型：`t2.micro`
- 自动分配公有 IP：已启用
- 具有以下三条规则的安全组：
  - 允许来自您的 IP 地址的 SSH
  - 允许来自任何地方的 HTTPS 流量
  - 允许来自任何地方的 HTTP 流量

> **Important**
>
> 在生产环境中，您应该配置实例，以满足您的特定需求。

启动 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 EC2 Dashboard（EC2 控制面板）上，选择 Launch instance（启动实例）。
3. 在 Name and tags（名称与标签）下，对于 Name（名称），输入名称以标识您的实例。对于本教程，请将该实例命名为 **`tutorial-instance-2`**。虽然实例名称不是必填项，但是当您在 RDS 控制台中选择实例时，该名称将帮助您轻松识别它。
4. 在 Application and OS Images（应用程序和操作系统映像）下，选择满足您的 Web 服务器需求的 AMI。本教程使用 Amazon Linux。
5. 在 Instance type（实例类型）下，对于 Instance type（实例类型），选择满足您的 Web 服务器需求的实例类型。本教程使用的是 `t2.micro`。

   > **Note**
   >
   > 您可以在 Free tier（免费套餐）下使用 Amazon EC2，前提是您的 Amazon 账户创建不到 12 个月，并且您选择了 `t2.micro` 实例类型（或在 `t2.micro` 不可用的区域中选择 `t3.micro`）。
6. 在 Key pair (login)（密钥对（登录））下，对于 Key pair name（密钥对名称），选择您的密钥对。
7. 在 Network settings（网络设置）下，执行以下操作：

   a. 对于 Network（网络）和 Subnet（子网），如果您尚未更改默认 VPC 或子网，则可以保留默认设置。

      如果您对默认 VPC 或子网进行了更改，请检查以下各项：

      i. 实例必须与 RDS 数据库位于同一 VPC 中，才能使用自动连接配置。默认情况下，您只有一个 VPC。

      ii. 您要将实例启动到其中的 VPC 必须连接互联网网关，以便您能从互联网访问您的 Web 服务器。您的默认 VPC 将自动设置互联网网关。

      iii. 为了确保您的实例收到公有 IP 地址，对于 Auto-assign public IP（自动分配公有 IP），请检查并确保选择 Enable（启用）。如果选择 Disable（禁用），请选择 Edit（编辑）（位于 Network Settings（网络设置）右侧），然后对于 Auto-assign public IP（自动分配公有 IP），选择 Enable（启用）。

   b. 要使用 SSH 连接到您的实例，您需要一条安全组规则，授权来自您计算机的公有 IPv4 地址的 SSH (Linux) 或 RDP (Windows) 流量。默认情况下，当您启动实例时，将使用允许来自任何地方的入站 SSH 流量的规则创建新的安全组。

要确保只有您的 IP 地址才能连接到您的实例，请在 Firewall (security groups)（防火墙（安全组））下，从 Allow SSH traffic from（允许入站 SSH 流量）复选框旁边的下拉列表中，选择 My IP（我的 IP）。

c. 要允许流量从互联网流向您的实例，请选中以下复选框：

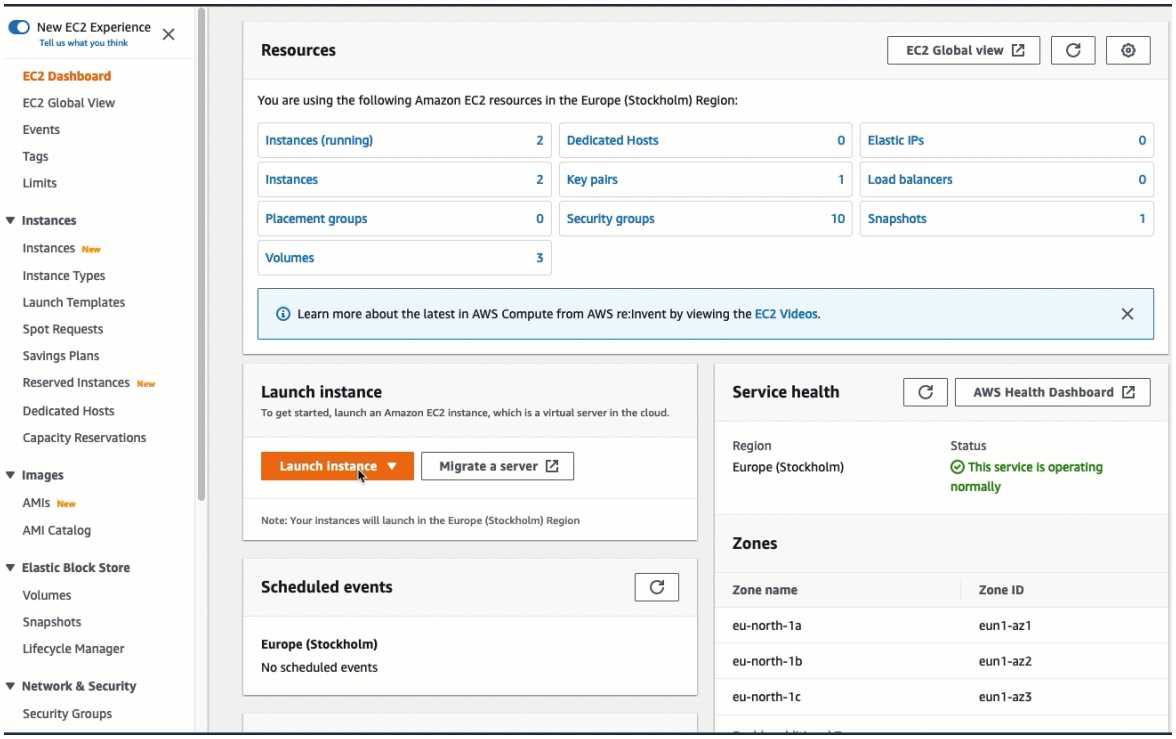
- Allow HTTPs traffic from the internet（允许来自互联网的 HTTPs 流量）
- Allow HTTP traffic from the internet（允许来自互联网的 HTTP 流量）

8. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。
9. 选择 View all instances（查看所有实例）以关闭确认页面并返回控制台。实例将首先处于 `pending` 状态，然后进入 `running` 状态。

   如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

有关启动实例的更多信息，请参阅 使用新启动实例向导启动实例 (p. 575)。

观看动画：启动 EC2 实例



您现在已准备好任务 2：创建 RDS 数据库并将其自动连接到 EC2 实例 (p. 688)。

任务 2：创建 RDS 数据库并将其自动连接到 EC2 实例

任务目标

此任务的目标是创建 RDS 数据库，然后使用 RDS 控制台中的自动连接功能自动配置 EC2 实例与 RDS 数据库之间的连接。

创建 RDS 数据库的步骤

使用以下步骤创建 RDS 数据库，然后使用 RDS 控制台中的自动功能将其连接到 EC2 实例。

要查看这些步骤的动画，请参阅 观看动画：创建 RDS 数据库并将其自动连接到 EC2 实例 (p. 690)。

数据库实例配置

此任务中的步骤将按以下方式配置数据库实例：

- 引擎类型：MySQL
- 模板：免费套餐
- 数据库实例标识符：**tutorial-database**
- 数据库实例类：db.t3.micro

> **Important**
>
> 在生产环境中，您应该配置实例，以满足您的特定需求。

创建 RDS 数据库并将其自动连接到 EC2 实例

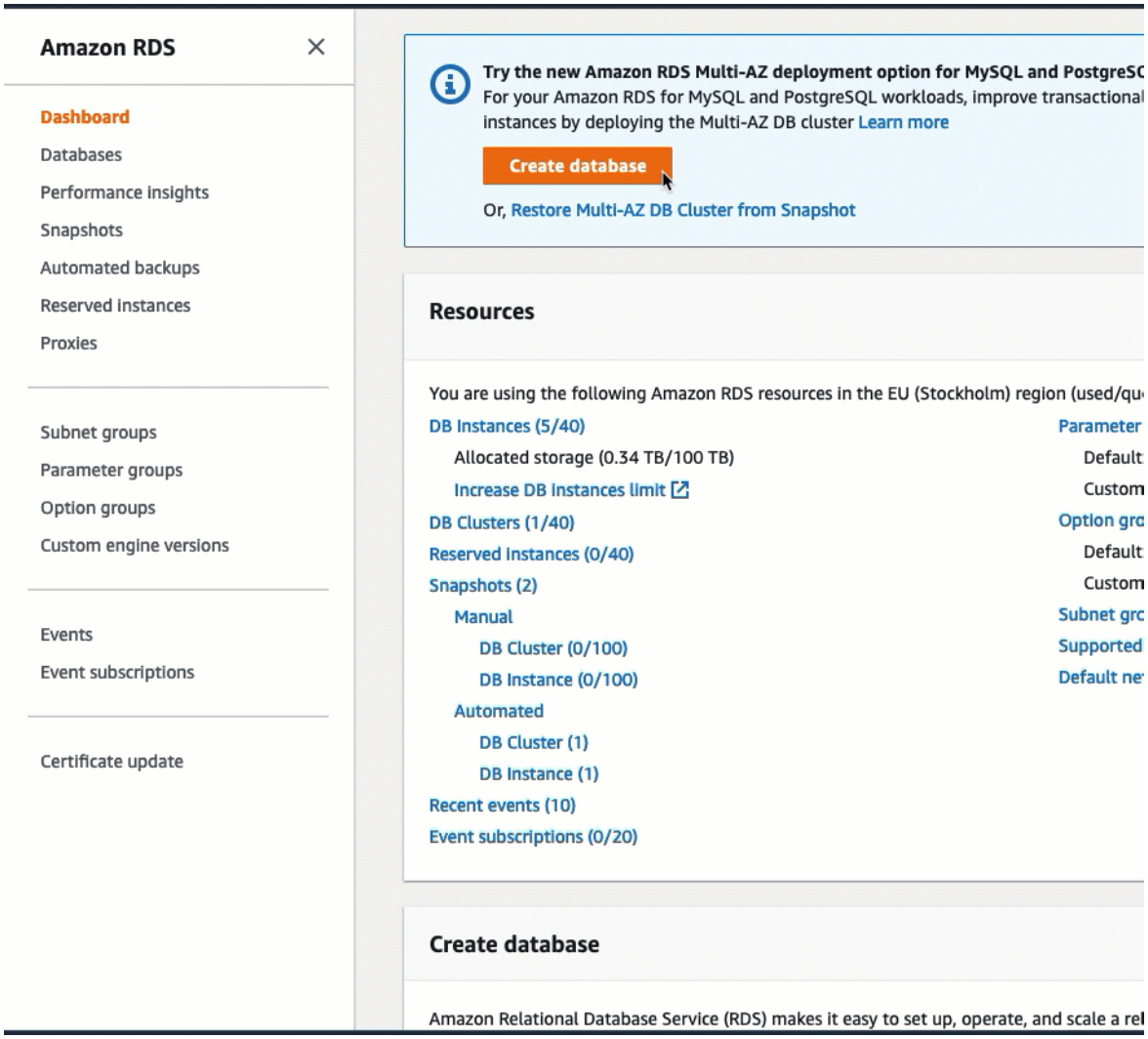
1. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
2. 从“Region selector”（区域选择器）（位于右上角）中，选择您在其中创建 EC2 实例的 Amazon Web Services 区域。EC2 实例和 RDS 数据库必须位于同一区域中。
3. 在控制面板中，选择 Create database（创建数据库）。
4. 在 Choose a database creation method（选择数据库创建方法）下，检查并确保选择 Standard create（标准创建）。如果选择 Easy create（轻松创建），则自动连接功能不可用。
5. 在 Engine options（引擎选项）下，对于 Engine type（引擎类型），选择 MySQL。
6. 在 Templates（模板）下，选择一个满足您需求的示例模板。对于本教程，选择 Free tier（免费套餐）以免费创建 RDS 数据库。但请注意，仅当您的账户创建不到 12 个月时，免费套餐才可用。其他限制适用。您可以通过选择 Free tier（免费套餐）框中的 Info（信息）链接来阅读更多内容。
7. 在 Settings (设置) 下，执行下列操作：
   a. 对于 DB instance identifier（数据库实例标识符），输入数据库的名称。在本教程中，请输入 **tutorial-database**。
   b. 对于 Master username（主用户名），保留默认名称，即 **admin**。
   c. 对于 Master password（主密码），输入您在本教程中可以记住的密码，然后对于 Confirm password（确认密码），再次输入该密码。
8. 在 Instance configuration（实例配置）下，对于 DB instance class（数据库实例类），保留默认值，即 db.t3.micro。如果您的账户创建不到 12 个月，则可以免费使用此实例。其他限制适用。有关更多信息，请参阅 AmazonFree Tier（免费套餐）。
9. 在 Connectivity（连接）下，对于 Compute resource（计算资源），选择 Connect to an EC2 compute resource（连接到 EC2 计算资源）。这是 RDS 控制台中的自动连接功能。
10. 对于 EC2 instance（EC2 实例），选择您要连接到的 EC2 实例。出于本教程的目的，您可以选择您在上一个任务中创建的实例（您已将其命名为 **tutorial-instance**），也可以选择另一个现有实例。如果您未在列表中看到您的实例，请选择 Connectivity（连接）右侧的刷新图标。

    当您使用自动连接功能时，将向此 EC2 实例中添加一个安全组，并将另一个安全组添加到 RDS 数据库中。会将这些安全组自动配置为允许 EC2 实例与 RDS 数据库之间的流量。在下一个任务中，您将验证安全组是否已创建并分配给 EC2 实例和 RDS 数据库。
11. 选择 Create database（创建数据库）。

    在 Databases（数据库）屏幕上，在数据库准备就绪可供使用之前，新数据库的 Status（状态）为 Creating（正在创建）。当状态变为 Available（可用）时，您便可以连接到该数据库。根据数据库类和存储量，新数据库可能需要等待多达 20 分钟时间才可用。

要了解更多信息，请参阅《Amazon RDS 用户指南》中的配置与 EC2 实例的自动网络连接。

观看动画：创建 RDS 数据库并将其自动连接到 EC2 实例



您现在已准备好任务 3：验证连接配置 (p. 690)。

任务 3：验证连接配置

任务目标

此任务的目标是验证两个安全组是否已创建并分配给实例和数据库。

当您使用 RDS 控制台中的自动连接功能配置连接时，将自动创建安全组并将其分配给实例和数据库，如下所示：

- 将创建安全组 rds-ec2-*x* 并将其添加到 RDS 数据库中。它包含一条入站规则，引用 ec2-rds-*x* 安全组作为其来源。这将允许来自 EC2 实例（具有 ec2-rds-*x* 安全组）的流量到达 RDS 数据库。
- 将创建安全组 ec2-rds-*x* 并将其添加到 EC2 实例中。它包含一条出站规则，引用 rds-ec2-*x* 安全组作为其目标。这将允许来自 EC2 实例的流量通过 rds-ec2-*x* 安全组到达 RDS 数据库。

验证连接配置的步骤

使用以下步骤验证连接配置。

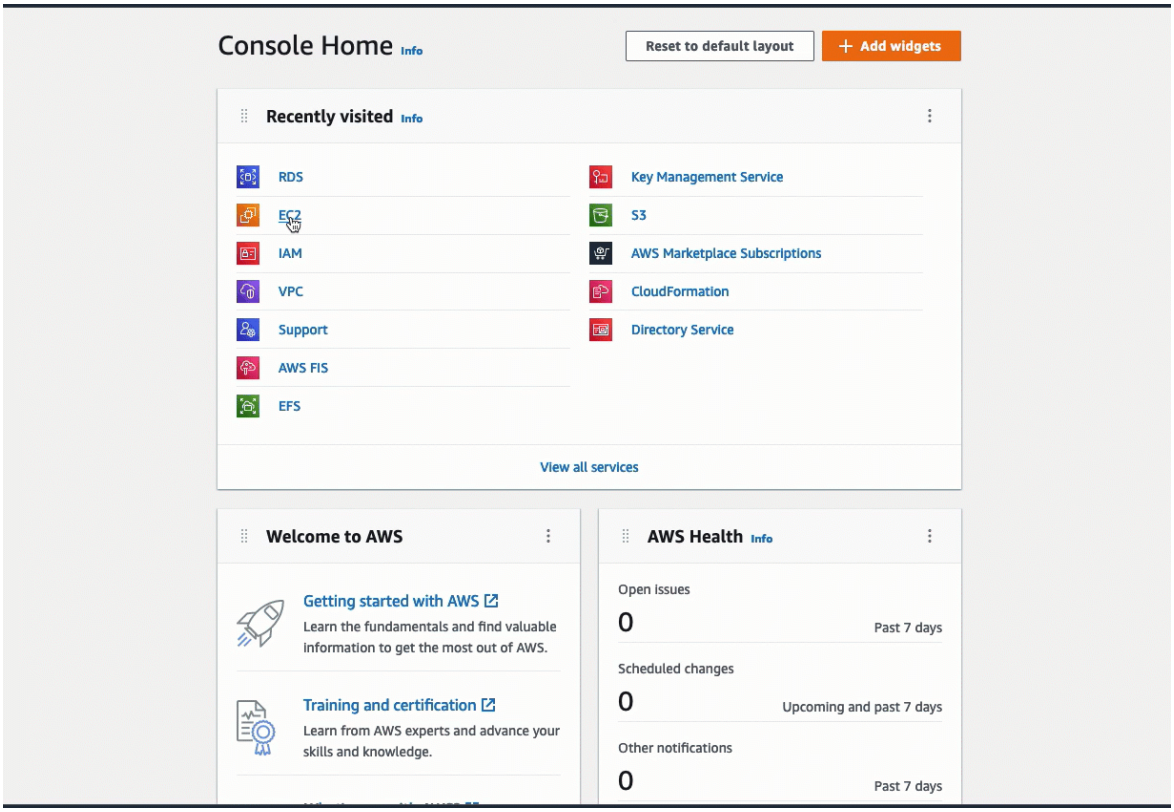
要查看这些步骤的动画，请参阅 观看动画：验证连接配置 (p. 692)。

使用控制台验证连接配置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您在上一个任务中选择要连接到 RDS 数据库的 EC2 实例，然后选择 Security（安全性）选项卡。
4. 在 Security details（安全详细信息）的 Security groups（安全组）下，验证并确保列表中有名为 ec2-rds-***x*** 的安全组。*x* 是一个数字。
5. 选择 ec2-rds-***x*** 安全组以打开它。
6. 选择 Outbound rules（出站规则）选项卡。
7. 验证并确保以下安全组规则存在，如下所示：
   - 类型：MYSQL/Aurora
   - 端口范围：3306
   - 目标：***sg-1234567890example*** / rds-ec2-***x***
   - 描述：允许从此安全组所连接的任何实例到 **database-tutorial** 的连接的规则
8. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
9. 在导航窗格中，选择 Databases（数据库）。
10. 选择您为本教程创建的 RDS 数据库。
11. 在 Connectivity & security（连接和安全性）选项卡的 Security（安全性）、VPC security groups（VPC 安全组）下，验证并确保显示名为 rds-ec2-***x*** 的安全组。
12. 选择 rds-ec2-***x*** 安全组。EC2 控制台中的 Security Groups（安全组）屏幕将打开。
13. 选择 rds-ec2-***x*** 安全组以打开它。
14. 选择 Inbound rules（入站规则）选项卡。
15. 验证并确保以下安全组规则存在，如下所示：
    - 类型：MYSQL/Aurora
    - 端口范围：3306
    - 来源：***sg-0987654321example*** / ec2-rds-***x*** - 这是分配给您在前面的步骤中验证的 EC2 实例的安全组。
    - 描述：允许来自 EC2 实例的连接的规则，附有 ***sg-1234567890example***

    通过验证这些安全组和安全组规则是否存在，以及它们是否已按照此过程中所述分配给 EC2 实例和 RDS 数据库，您可以使用自动连接功能验证是否已自动配置连接。

观看动画：验证连接配置



您已完成本教程的“选项 2”。现在，您可以完成“选项 3”，它将介绍如何手动配置在“选项 2”中自动创建的安全组。

选项 3：通过模仿自动连接功能，将 EC2 实例手动连接到 RDS 数据库

目标

“选项 3”的目标是学习如何通过手动重现自动连接功能的配置，手动配置 EC2 实例与 RDS 数据库之间的连接。

开始前的准备工作

完成本教程需要做好以下准备：

- 与 RDS 数据库位于同一 VPC 中的 EC2 实例。您可以使用现有的 EC2 实例，也可以按照“任务 1”中的步骤创建新实例。
- 与 EC2 实例位于同一 VPC 中的 RDS 数据库。您可以使用现有的 RDS 数据库，也可以按照“任务 2”中的步骤创建新数据库。
- 调用以下操作的权限。如果您已完成本教程的“选项 1”，则您已经拥有这些权限。
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`

- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:RevokeSecurityGroupEgress`

完成“选项 3”所需的任务

- 任务 1：启动 EC2 实例 - 可选 (p. 693)
- 任务 2：创建 RDS 数据库 - 可选 (p. 695)
- 任务 3：通过创建安全组并将它们分配给实例，将 EC2 实例手动连接到 RDS 数据库 (p. 697)

任务 1：启动 EC2 实例 - 可选

> **Note**
>
> 启动实例不是本教程的重点。如果您已拥有 Amazon EC2 实例并希望在本教程中使用它，则可跳过此任务。

任务目标

此任务的目标是启动 EC2 实例，以便您可以完成“任务 3”，在该任务中，您将配置 EC2 实例与 Amazon RDS 数据库之间的连接。

启动 EC2 实例的步骤

使用以下步骤启动本教程的 EC2 实例。

要查看这些步骤的动画，请参阅 观看动画：启动 EC2 实例 (p. 695)。

EC2 实例配置

此任务中的步骤将按以下方式配置 EC2 实例：

- 实例名称：**`tutorial-instance`**
- AMI：Amazon Linux 2
- 实例类型：`t2.micro`
- 自动分配公有 IP：已启用
- 具有以下三条规则的安全组：
  - 允许来自您的 IP 地址的 SSH
  - 允许来自任何地方的 HTTPS 流量
  - 允许来自任何地方的 HTTP 流量

> **Important**
>
> 在生产环境中，您应该配置实例，以满足您的特定需求。

启动 EC2 实例

1. 登录 Amazon Web Services Management Console，打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在 EC2 Dashboard（EC2 控制面板）上，选择 Launch instance（启动实例）。
3. 在 Name and tags（名称与标签）下，对于 Name（名称），输入名称以标识您的实例。对于本教程，请将该实例命名为 **`tutorial-instance-manual-1`**。虽然实例名称不是必填项，但该名称将帮助您轻松识别它。
4. 在 Application and OS Images（应用程序和操作系统映像）下，选择满足您的 Web 服务器需求的 AMI。本教程使用 Amazon Linux。
5. 在 Instance type（实例类型）下，对于 Instance type（实例类型），选择满足您的 Web 服务器需求的实例类型。本教程使用的是 `t2.micro`。

   Note

   您可以在 Free tier（免费套餐）下使用 Amazon EC2，前提是您的 Amazon 账户创建不到 12 个月，并且您选择了 `t2.micro` 实例类型（或在 `t2.micro` 不可用的区域中选择 `t3.micro`）。
6. 在 Key pair (login)（密钥对（登录））下，对于 Key pair name（密钥对名称），选择您的密钥对。
7. 在 Network settings（网络设置）下，执行以下操作：

   a. 对于 Network（网络）和 Subnet（子网），如果您尚未更改默认 VPC 或子网，则可以保留默认设置。

      如果您对默认 VPC 或子网进行了更改，请检查以下各项：

      i. 实例必须与 RDS 数据库位于同一 VPC 中。默认情况下，您只有一个 VPC。
      ii. 您要将实例启动到其中的 VPC 必须连接互联网网关，以便您能从互联网访问您的 Web 服务器。您的默认 VPC 将自动设置互联网网关。
      iii. 为了确保您的实例收到公有 IP 地址，对于 Auto-assign public IP（自动分配公有 IP），请检查并确保选择 Enable（启用）。如果选择 Disable（禁用），请选择 Edit（编辑）（位于 Network Settings（网络设置）右侧），然后对于 Auto-assign public IP（自动分配公有 IP），选择 Enable（启用）。

   b. 要使用 SSH 连接到您的实例，您需要一条安全组规则，授权来自您计算机的公有 IPv4 地址的 SSH (Linux) 或 RDP (Windows) 流量。默认情况下，当您启动实例时，将使用允许来自任何地方的入站 SSH 流量的规则创建新的安全组。

      要确保只有您的 IP 地址才能连接到您的实例，请在 Firewall (security groups)（防火墙（安全组））下，从 Allow SSH traffic from（允许入站 SSH 流量）复选框旁边的下拉列表中，选择 My IP（我的 IP）。

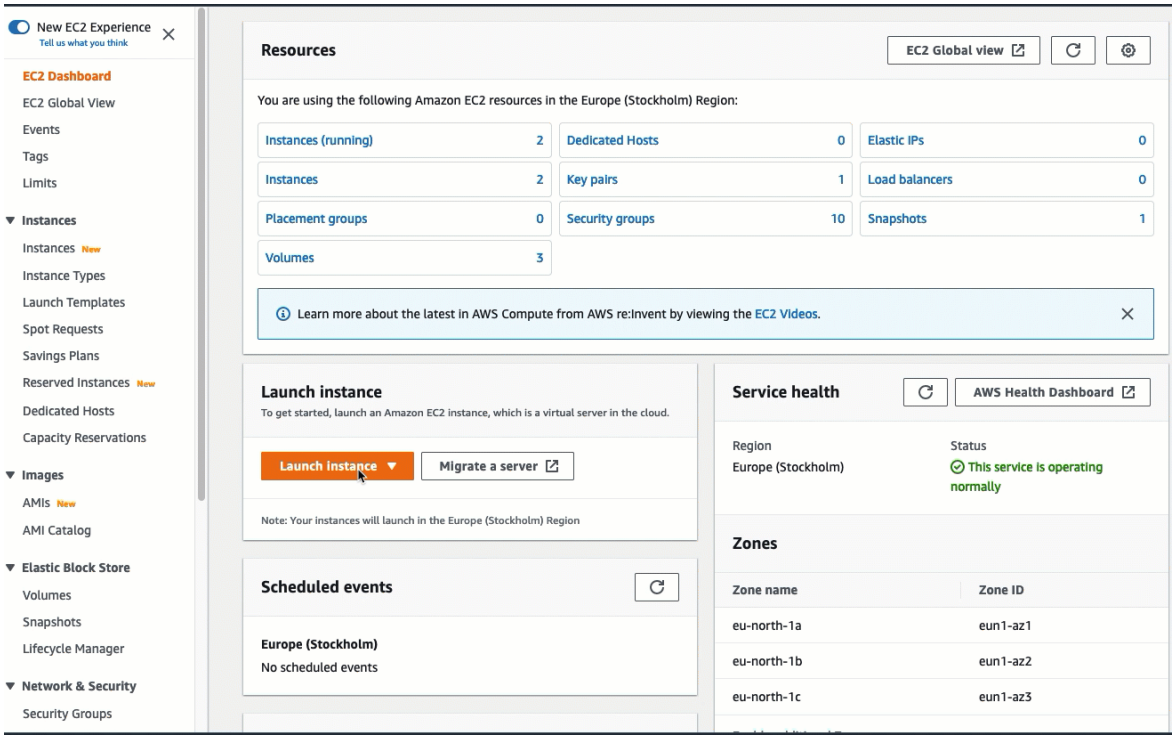
   c. 要允许流量从互联网流向您的实例，请选中以下复选框：

      - Allow HTTPs traffic from the internet（允许来自互联网的 HTTPs 流量）
      - Allow HTTP traffic from the internet（允许来自互联网的 HTTP 流量）
8. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。
9. 选择 View all instances（查看所有实例）以关闭确认页面并返回控制台。实例将首先处于 `pending` 状态，然后进入 `running` 状态。

   如果实例无法启动或状态立即转至 `terminated` 而非 `running`，请参阅 排查实例启动问题 (p. 1681)。

有关启动实例的更多信息，请参阅 使用新启动实例向导启动实例 (p. 575)。

观看动画：启动 EC2 实例



您现在已准备好任务 2：创建 RDS 数据库 - 可选 (p. 695)。

任务 2：创建 RDS 数据库 - 可选

> **Note**
>
> 创建 RDS 数据库不是该教程这一部分的重点。如果您已拥有 RDS 数据库并希望将其用于本教程，则可跳过此任务。

任务目标

此任务的目标是创建 RDS 数据库。在“任务 3”中，当您将此实例连接到 EC2 实例时，您将使用此实例。

创建 RDS 数据库的步骤

使用以下步骤为本教程的“选项 3”创建 RDS 数据库。

要查看这些步骤的动画，请参阅观看动画：创建数据库实例 (p. 696)。

RDS 数据库配置

此任务中的步骤将按以下方式配置 RDS 数据库：

- 引擎类型：MySQL
- 模板：免费套餐
- 数据库实例标识符：**`tutorial-database-manual`**
- 数据库实例类：`db.t3.micro`

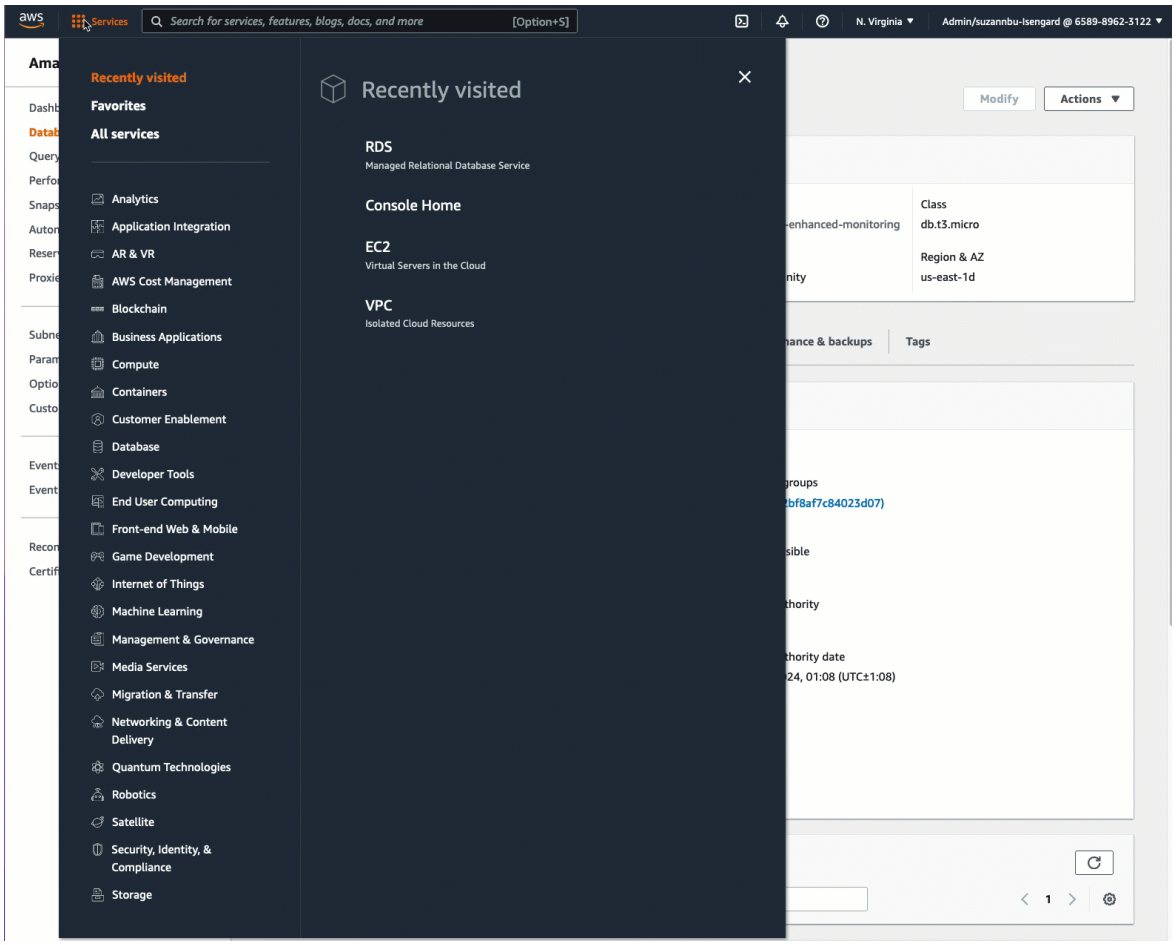
> **Important**
>
> 在生产环境中，您应该配置实例，以满足您的特定需求。

创建 MySQL 数据库实例

1. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
2. 从“Region selector”（区域选择器）（位于右上角）中，选择您在其中创建 EC2 实例的 Amazon Web Services 区域。EC2 实例和数据库实例必须位于同一区域中。
3. 在控制面板中，选择 Create database（创建数据库）。
4. 在 Choose a database creation method（选择数据库创建方法）下，选择 Easy create（轻松创建）。当您选择此选项时，用于自动配置连接的自动连接功能将不可用。
5. 在 Engine options（引擎选项）下，对于 Engine type（引擎类型），选择 MySQL。
6. 对于 数据库实例大小，选择 免费套餐。
7. 对于 DB instance identifier（数据库实例标识符），输入 RDS 数据库的名称。在本教程中，请输入 **`tutorial-database-manual`**。
8. 对于 Master username（主用户名），保留默认名称，即 **`admin`**。
9. 对于 Master password（主密码），输入您在本教程中可以记住的密码，然后对于 Confirm password（确认密码），再次输入该密码。
10. 选择 Create database（创建数据库）。

    在 Databases（数据库）屏幕上，在数据库实例准备就绪可供使用之前，新数据库实例的 Status（状态）为 Creating（正在创建）。当状态变为 Available（可用）时，您便可以连接到该数据库实例。根据数据库实例类和存储量，新实例可能需要等待 20 分钟时间才可用。

观看动画：创建数据库实例



您现在已准备好任务 3：通过创建安全组并将它们分配给实例，将 EC2 实例手动连接到 RDS 数据库 (p. 697)。

任务 3：通过创建安全组并将它们分配给实例，将 EC2 实例手动连接到 RDS 数据库

任务目标

此任务的目标是通过手动执行以下操作以重现自动连接功能的连接配置：创建两个新安全组，然后分别向 EC2 实例和 RDS 数据库添加一个安全组。

创建新安全组并将它们添加到实例的步骤

使用以下步骤，通过创建两个新安全组，将 EC2 实例连接到 RDS 数据库。然后分别向 EC2 实例和 RDS 数据库添加一个安全组。

创建两个新安全组，然后分别向 EC2 实例和 RDS 数据库分配一个安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 首先创建要添加到 EC2 实例的安全组，如下所示：
   a. 在导航窗格中，选择 Security Groups（安全组）。
   b. 选择Create security group（创建安全组）。
   c. 对于 Security group name（安全组名称），请输入一个描述性的安全组名称。在本教程中，请输入 **ec2-rds-manual-configuration**。
   d. 对于 Description（描述），请输入一段简短描述。在本教程中，请输入 **EC2 instance security group to allow EC2 instance to securely connect to RDS database**。
   e. 选择Create security group（创建安全组）。在创建 RDS 数据库安全组后，您将返回此安全组以添加出站规则。
3. 现在，创建要添加到 RDS 数据库的安全组，如下所示：
   a. 在导航窗格中，选择 Security Groups（安全组）。
   b. 选择Create security group（创建安全组）。
   c. 对于 Security group name（安全组名称），请输入一个描述性的安全组名称。在本教程中，请输入 **rds-ec2-manual-configuration**。
   d. 对于 Description（描述），请输入一段简短描述。在本教程中，请输入 **RDS database security group to allow EC2 instance to securely connect to RDS database**。
   e. 在 Inbound rules（入站规则）下，选择 Add rule（添加规则），然后执行以下操作：
      i. 对于 Type（类型），选择 MYSQL/Aurora。
      ii. 对于 Source（来源），选择您在此过程的“步骤 2”中创建的 EC2 实例安全组 ec2-rds-manual-configuration。
   f. 选择Create security group（创建安全组）。
4. 编辑 EC2 实例安全组以添加出站规则，如下所示：
   a. 在导航窗格中，选择 Security Groups（安全组）。
   b. 选择 EC2 实例安全组（您已将其命名为 **ec2-rds-manual-configuration**），然后选择 Outbound rules（出站规则）选项卡。
   c. 选择 Edit outbound rules（编辑出站规则）。
   d. 选择 Add rule（添加规则），然后执行以下操作：
      i. 对于 Type（类型），选择 MYSQL/Aurora。
      ii. 对于 Source（来源），选择您在此过程的“步骤 3”中创建的 RDS 数据库安全组 rds-ec2-manual-configuration。

iii. 选择 Save rules（保存规则）。

5. 将 EC2 实例安全组添加到 EC2 实例中，如下所示：

   a. 在导航窗格中，选择实例。
   b. 选择您的 EC2 实例，然后依次选择 Actions（操作）、Security（安全性）和 Change security groups（更改安全组）。
   c. 在 Associated security groups（关联安全组）下，选择 Select security groups（选择安全组）字段，选择您之前创建的 ec2-rds-manual-configuration，然后选择 Add security group（添加安全组）。
   d. 选择 Save（保存）。

6. 将 RDS 数据库安全组添加到 RDS 数据库，如下所示：

   a. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
   b. 在导航窗格中，选择 Databases（数据库），然后选择您的数据库。
   c. 选择 Modify（修改）。
   d. 在 Connectivity（连接）下，对于 Security group（安全组），选择您之前创建的 rds-ec2-manual-configuration，然后选择 Continue（继续）。
   e. 在 Scheduling of modifications（修改计划）下，选择 Apply immediately（立即应用）。
   f. 选择修改数据库实例。

   现在，您已完成模仿在使用自动连接功能时出现的自动步骤的手动步骤。

您已完成本教程的“选项 3”。如果您已完成“选项 1”、“选项 2”和“选项 3”，并且不再需要在本教程中创建的资源，则应删除这些资源，以防止产生不必要的成本。有关更多信息，请参阅清除 (p. 698)。

清除

现在您已完成该教程，最好清理（删除）所有您不再需要使用的资源。清理 Amazon 资源可以防止您的账户产生任何进一步的费用。

主题

- 终止 EC2 实例 (p. 698)
- 删除 RDS 数据库 (p. 698)

终止 EC2 实例

如果您专门为本教程启动了 EC2 实例，则可以将其终止，以停止产生任何与之相关的费用。

使用控制台终止实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您为本教程创建的实例，然后依次选择 Instance state（实例状态）、Terminate instance（终止实例）。
4. 当系统提示您确认时，选择终止。

删除 RDS 数据库

如果您专门为本教程创建了 RDS 数据库，则可以将其删除，以停止产生任何与之相关的费用。

使用控制台删除 RDS 数据库

1. 通过以下网址打开 Amazon RDS 控制台：https://console.aws.amazon.com/rds/。
2. 在导航窗格中，选择 Databases (数据库)。
3. 选择您为本教程创建的 RDS 数据库，然后依次选择 Actions（操作）、Delete（删除）。
4. 在方框中输入 **`delete me`**，然后选择 Delete（删除）。

配置您的 Amazon Linux 实例

在成功启动和登录您的 Amazon Linux 实例之后，您可以对其进行修改。可以通过许多不同方式配置实例以满足特定应用程序的需求。下面是一些可帮助您入门的常见任务。

目录

- 常见配置方案 (p. 699)
- 在 Amazon Linux 实例上管理软件 (p. 699)
- 管理 Linux 实例上的用户 (p. 705)
- 您的 EC2 实例的处理器状态控制 (p. 707)
- 输入/输出调度器 (p. 713)
- 为 Linux 实例设置时间 (p. 714)
- 优化 CPU 选项 (p. 721)
- 更改 Amazon Linux 实例的主机名 (p. 744)
- 在 Amazon Linux 实例上设置动态 DNS (p. 747)
- 启动时在 Linux 实例上运行命令 (p. 748)
- 实例元数据和用户数据 (p. 754)

常见配置方案

Amazon Linux 的基本发行版包含基本服务器操作所需的许多软件包和实用工具。但是，各种软件存储库还提供许多软件包，还有更多软件包可供您从源代码进行构建。有关从这些位置安装和构建软件的更多信息，请参阅在 Amazon Linux 实例上管理软件 (p. 699)。

Amazon Linux 实例预配置有 `ec2-user`，但是，您可能需要添加没有超级用户权限的其他用户。有关添加和删除用户的更多信息，请参阅 管理 Linux 实例上的用户 (p. 705)。

Amazon Linux 实例的默认时间配置使用 Amazon Time Sync Service 在实例上设置系统时间。默认时区为 UTC。有关设置实例的时区或使用自有时间服务器的更多信息，请参阅为 Linux 实例设置时间 (p. 714)。

如果您自己有注册了域名的网络，则可以更改实例的主机名，将它自身标识为该域名的一部分。您还可以在不更改主机名设置的情况下更改系统提示，以显示更有意义的名称。有关更多信息，请参阅更改 Amazon Linux 实例的主机名 (p. 744)。您可以将实例配置成使用动态 DNS 服务提供商。有关更多信息，请参阅在 Amazon Linux 实例上设置动态 DNS (p. 747)。

当您在 Amazon EC2 中启动实例时，可以选择将用户数据传递到可用于执行常见配置任务甚至在实例启动后运行脚本的实例。您可以将两类用户数据传递到 Amazon EC2：cloud-init 指令和 Shell 脚本。有关更多信息，请参阅启动时在 Linux 实例上运行命令 (p. 748)。

在 Amazon Linux 实例上管理软件

Amazon Linux 的基本发行版包含基本服务器操作所需的许多软件包和实用工具。各种软件存储库还提供许多软件包，还有更多软件包可供您从源代码进行构建。

目录

- 更新 Amazon Linux 实例上的实例软件 (p. 700)
- 在 Amazon Linux 实例上添加存储库 (p. 701)
- 在 Amazon Linux 实例上查找软件包 (p. 702)
- 在 Amazon Linux 实例上安装软件包 (p. 703)
- 准备在 Amazon Linux 实例上编译软件 (p. 704)

使软件保持最新非常重要。Linux 发行版中的许多程序包会经常更新，以修复错误、添加功能，以及防止安全漏洞。有关更多信息，请参阅更新 Amazon Linux 实例上的实例软件 (p. 700)。

默认情况下，Amazon Linux 实例启动时启用以下存储库：

- Amazon Linux 2：`amzn2-core` 和 `amzn2extra-docker`
- Amazon Linux AMI：`amzn-main` 和 `amzn-updates`

尽管在 Amazon Web Services 更新的这些存储库中有许多程序包，但是您需要安装的程序包可能在其他存储库中。有关更多信息，请参阅在 Amazon Linux 实例上添加存储库 (p. 701)。有关在启用的存储库中查找程序包的帮助，请参阅在 Amazon Linux 实例上查找软件包 (p. 702)。有关在 Amazon Linux 实例上安装软件的信息，请参阅在 Amazon Linux 实例上安装软件包 (p. 703)。

并非所有软件均可在存储库中存储的软件包中获得；有些软件必须在实例上从其源代码进行编译。有关更多信息，请参阅准备在 Amazon Linux 实例上编译软件 (p. 704)。

Amazon Linux 实例使用 yum 程序包管理器管理其软件。yum 程序包管理器可安装、删除和更新软件，以及管理每个包的所有依赖关系。基于 Debian 的 Linux 发行版（如 Ubuntu）使用 apt-get 命令和 dpkg 程序包管理器，因此，下面几部分中的 yum 示例不适用于这些发行版。

更新 Amazon Linux 实例上的实例软件

使软件保持最新非常重要。Linux 发行版中的许多程序包会经常更新，以修复错误、添加功能，以及防止安全漏洞。当您首次启动并连接到 Amazon Linux 实例时，您可能会看到出于安全目的要求您更新软件包的消息。本节介绍如何更新整个系统或仅更新单个程序包。

有关 Amazon Linux 2 变更和更新的信息，请参阅 Amazon Linux 2 发布说明。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

> **Important**
>
> 如果您在仅 IPv6 的子网中启动了使用 Amazon Linux 2 AMI 的 EC2 实例，则必须连接到该实例并运行 `sudo amazon-linux-https disable`。这样，您的 AL2 实例才可以使用 http 补丁服务通过 IPv6 连接到 S3 中的 yum 存储库。

更新 Amazon Linux 实例上的所有程序包

1. （可选）在 Shell 窗口中启动 screen 会话。有时您可能会遇到网络中断，这样会断开到实例的 SSH 连接。如果在较长的软件更新期间发生这种情况，实例处于混乱、但可恢复的状态。即使连接中断，通过 screen 会话也可继续运行更新，您稍后可重新连接到此会话，不会有问题。

   a. 执行 screen 命令以开始会话。

   ```
   [ec2-user ~]$ screen
   ```

   b. 如果会话中断，请再次登录实例并列出可用屏幕。

```
[ec2-user ~]$ screen -ls
There is a screen on:
 17793.pts-0.ip-12-34-56-78 (Detached)
1 Socket in /var/run/screen/S-ec2-user.
```

c. 使用 screen -r 命令和前一命令的进程 ID 重新连接到屏幕。

```
[ec2-user ~]$ screen -r 17793
```

d. 使用 screen 完成操作后，使用 exit 命令关闭会话。

```
[ec2-user ~]$ exit
[screen is terminating]
```

2. 运行 yum update 命令。您可以选择添加 `--security` 标记，这样仅应用安全更新。

```
[ec2-user ~]$ sudo yum update
```

3. 查看所列的程序包，输入 **y** 并按 Enter 接受更新。更新系统上的所有程序包可能需要几分钟。yum 输出显示更新运行状态。
4. (可选) 重启实例以确保您使用的是来自更新的最新程序包和库；重启发生前不会加载内核更新。更新任何 `glibc` 库后也应进行重启。对于用来控制服务的程序包的更新，重新启动服务可能就足以使更新生效，但系统重启可确保所有之前的程序包和库更新都是完整的。

更新 Amazon Linux 实例上的单个程序包

使用此过程可更新单个程序包 (及其依赖关系)，而非整个系统。

1. 使用要更新的程序包的名称运行 yum update 命令。

```
[ec2-user ~]$ sudo yum update openssl
```

2. 查看所列的程序包信息，输入 **y** 并按 Enter 接受更新。如果存在必须解析的程序包依赖关系，有时会列出多个数据包。yum 输出显示更新运行状态。
3. (可选) 重启实例以确保您使用的是来自更新的最新程序包和库；重启发生前不会加载内核更新。更新任何 `glibc` 库后也应进行重启。对于用来控制服务的程序包的更新，重新启动服务可能就足以使更新生效，但系统重启可确保所有之前的程序包和库更新都是完整的。

在 Amazon Linux 实例上添加存储库

默认情况下，Amazon Linux 实例启动时启用以下存储库：

- Amazon Linux 2：`amzn2-core` 和 `amzn2extra-docker`
- Amazon Linux AMI：`amzn-main` 和 `amzn-updates`

尽管在 Amazon Web Services 更新的这些存储库中有许多程序包，但是您需要安装的程序包可能在其他存储库中。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

要使用 yum 从不同存储库安装程序包，您需要将存储库信息添加到 `/etc/yum.conf` 文件中，或者添加到 *`repository`*`.repo` 目录中它自己的 `/etc/yum.repos.d` 文件中。您可以手动执行此操作，但大多数 yum 存储库在其存储库 URL 提供各自的 *`repository`*`.repo` 文件。

确定已安装的 yum 存储库

- 使用以下命令列出已安装的 yum 存储库：

```
[ec2-user ~]$ yum repolist all
```

输出结果会列出已安装的存储库，并报告每个存储库的状态。启用的存储库会显示其中包含的程序包数量。

将 yum 存储库添加到 /etc/yum.repos.d

1. 查找 .repo 文件的位置。这随要添加的存储库而异。在本示例中，.repo 文件位于 https://www.*example*.com/*repository*.repo。
2. 使用 yum-config-manager 命令添加存储库。

```
[ec2-user ~]$ sudo yum-config-manager --add-repo https://
www.example.com/repository.repo
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
grabbing file https://www.example.com/repository.repo to /etc/
yum.repos.d/repository.repo
repository.repo                                          | 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

安装存储库后，必须按照以下过程启用存储库。

在 /etc/yum.repos.d 中启用 yum 存储库

- 使用带 yum-config-manager 标志的 --enable *repository* 命令。以下命令从 Fedora 项目启用 Extra Packages for Enterprise Linux (EPEL) 存储库。默认情况下，此存储库显示在 Amazon Linux AMI 实例上的 /etc/yum.repos.d 中，但未启用。

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

> **Note**
>
> 要在 Amazon Linux 2 上启用 EPEL 存储库，请使用以下命令：
>
> ```
> [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-
> release-latest-7.noarch.rpm
> ```
>
> 有关在其他发行版（如 Red Hat 和 CentOS）上启用 EPEL 存储库的信息，请参阅 https://fedoraproject.org/wiki/EPEL 上的 EPEL 文档。

在 Amazon Linux 实例上查找软件包

您可以使用 yum search 命令搜索在您配置的存储库中可用的程序包的描述。如果不知道要安装的程序包的确切名称，这尤其有帮助。只需将关键字搜索附加到该命令；对于多字词搜索，请使用引号括起搜索查询。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

```
[ec2-user ~]$ sudo yum search "find"
```

下面是 Amazon Linux 2 的示例输出。

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
============================== N/S matched: find ==============================
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
gedit-plugin-findinfiles.x86_64 : gedit findinfiles plugin
ocaml-findlib-devel.x86_64 : Development files for ocaml-findlib
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
 File::Find
robotfindskitten.x86_64 : A game/zen simulation. You are robot. Your job is to find kitten.
mlocate.x86_64 : An utility for finding files by name
ocaml-findlib.x86_64 : Objective CAML package manager and build helper
perl-Devel-Cycle.noarch : Find memory cycles in objects
perl-Devel-EnforceEncapsulation.noarch : Find access violations to blessed objects
perl-File-Find-Rule-Perl.noarch : Common rules for searching for Perl things
perl-File-HomeDir.noarch : Find your home and other directories on any platform
perl-IPC-Cmd.noarch : Finding and running system commands made easy
perl-Perl-MinimumVersion.noarch : Find a minimum required version of perl for Perl code
texlive-xesearch.noarch : A string finder for XeTeX
valgrind.x86_64 : Tool for finding memory management bugs in programs
valgrind.i686 : Tool for finding memory management bugs in programs
```

下面是 Amazon Linux 的示例输出。

```
Loaded plugins: priorities, security, update-motd, upgrade-helper
============================== N/S Matched: find ==============================
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
 File::Find
perl-Module-Find.noarch : Find and use installed modules in a (sub)category
libpuzzle.i686 : Library to quickly find visually similar images (gif, png, jpg)
libpuzzle.x86_64 : Library to quickly find visually similar images (gif, png, jpg)
mlocate.x86_64 : An utility for finding files by name
```

引号中的多个字词搜索查询仅返回符合确切查询的结果。如果您没有看到需要的程序包，请将搜索简化为一个关键字，然后扫描结果。您还可以尝试使用关键字同义词来扩大搜索范围。

有关 Amazon Linux 2 和 Amazon Linux 软件包的更多信息，请参阅以下文件：

- 程序包存储库 (p. 211)
- Extras 库 (Amazon Linux 2) (p. 213)

在 Amazon Linux 实例上安装软件包

yum 程序包管理器是出色的安装软件工具，因为它可以搜索您针对不同软件包启用的所有存储库，还可以处理软件安装过程中的任何依赖关系。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

从存储库安装软件包

使用 yum install ***package*** 命令，将 *package* 替换为要安装的软件的名称。例如，若要安装 links 基于文本的 Web 浏览器，请输入以下命令。

```
[ec2-user ~]$ sudo yum install links
```

安装您已下载的 RPM 软件包文件

您还可使用 yum install 安装您已经从互联网下载的 RPM 程序包文件。为此，将 RPM 文件的路径名称而不是存储库程序包名称附加到安装命令。

```
[ec2-user ~]$ sudo yum install my-package.rpm
```

列出已安装软件包

要查看实例上已安装的软件包的列表，请使用以下命令。

```
[ec2-user ~]$ yum list installed
```

准备在 Amazon Linux 实例上编译软件

互联网上有大量开源软件，这些软件尚未预编译，可从程序包存储库下载。您可能最终会发现需要您亲自从源代码编译的软件包。要使系统能够编译软件，您需要安装几个开发工具，如 make、gcc 和 autoconf。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

因为软件编译不是每个 Amazon EC2 实例都需要的任务，所以在默认情况下不安装这些工具，不过，称为“开发工具”的程序包组中包含这些工具，而这个程序包组可通过 yum groupinstall 命令方便地添加到实例。

```
[ec2-user ~]$ sudo yum groupinstall "Development Tools"
```

软件源代码包通常以压缩存档文件（称为 tarball）的形式提供下载（从 https://github.com/ 和 http://sourceforge.net/ 等网站）。这些 tarball 的文件扩展名通常为 `.tar.gz`。您可以使用 tar 命令解压缩这些存档。

```
[ec2-user ~]$ tar -xzf software.tar.gz
```

将源代码包解压并解档后，应在源代码目录中查找 `README` 或 `INSTALL` 文件，这些文件包含有关编译和安装源代码的进一步说明。

检索 Amazon Linux 程序包的源代码

Amazon Web Services 提供所维护的程序包的源代码。您可以使用 yumdownloader --source 命令下载已安装的任何程序包的源代码。

- 运行 yumdownloader --source ***package*** 命令可下载 *package* 的源代码。例如，若要下载 `htop` 程序包的源代码，请输入以下命令。

```
[ec2-user ~]$ yumdownloader --source htop

Loaded plugins: priorities, update-motd, upgrade-helper
Enabling amzn-updates-source repository
Enabling amzn-main-source repository
amzn-main-source
                        | 1.9 kB  00:00:00
amzn-updates-source
                        | 1.9 kB  00:00:00
(1/2): amzn-updates-source/latest/primary_db
                        |  52 kB  00:00:00
```

```
(2/2): amzn-main-source/latest/primary_db
                        | 734 kB  00:00:00
htop-1.0.1-2.3.amzn1.src.rpm
```

源 RPM 的位置位于您运行命令的目录中。

管理 Linux 实例上的用户

每个 Linux 实例均以默认的 Linux 系统用户启动。您可以向实例添加用户，也可以删除用户。

对于默认用户，默认用户名 (p. 705)由您在启动实例时指定的 AMI 决定。

Note

默认情况下，密码身份验证和根用户登录将被禁用，而 sudo 将会启用。要登录您的实例，必须使用密钥对。有关日志记录的更多信息，请参阅 连接到您的 Linux 实例 (p. 644)。
您可以允许对您的实例进行密码身份验证和根用户登录。有关更多信息，请参阅您的操作系统文档。

Note

Linux 系统用户不应与 IAM 用户混淆。有关更多信息，请参阅 IAM 用户指南中的 IAM 用户。

目录

- 默认用户名 (p. 705)
- 注意事项 (p. 705)
- 创建用户 (p. 706)
- 删除用户 (p. 707)

默认用户名

EC2 实例的默认用户名由您在启动实例时指定的 AMI 决定。

默认用户名为：

- 对于 Amazon Linux 2022、Amazon Linux 2 或 Amazon Linux AMI，用户名是 `ec2-user`。
- 对于 CentOS AMI，用户名是 `centos` 或 `ec2-user`。
- 对于 Debian AMI，用户名称是 `admin`。
- 对于 Fedora AMI，用户名是 `fedora` 或 `ec2-user`。
- 对于 RHEL AMI，用户名是 `ec2-user` 或 `root`。
- 对于 SUSE AMI，用户名是 `ec2-user` 或 `root`。
- 对于 Ubuntu AMI，用户名称是 `ubuntu`。
- 对于 Oracle AMI，用户名是 `ec2-user`。
- 对于 Bitnami AMI，用户名称是 `bitnami`。
- 否则，检查 AMI 提供程序。

注意事项

对于许多应用程序来说，使用默认用户是适当的。但是，您可以选择添加用户，以便个人能够拥有自己的文件和工作区。此外，为新用户创建用户比向多个（可能缺乏经验的）用户授予对默认用户的访问权限更安

全，因为如果使用不当，该默认用户可能对系统造成严重破坏。有关更多信息，请参阅有关保护您的 EC2 实例的提示。

要使用 Linux 系统用户启用对 EC2 实例的用户 SSH 访问，您必须与用户分享 SSH 密钥。此外，您可以使用 EC2 实例连接来向用户提供访问权限而无需共享和管理 SSH 密钥。有关更多信息，请参阅使用 EC2 Instance Connect 连接到 Linux 实例 (p. 652)。

创建用户

先创建用户，然后添加允许用户连接并登录实例的 SSH 公有密钥。

创建用户

1. 创建新的密钥对 (p. 1290)。您必须将 .pem 文件提供给要为其创建用户的用户。他们必须使用此文件来连接到实例。
2. 从您在上一步中创建的密钥对中检索公有密钥。

   ```
   $  ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   该命令返回公有密钥，如以下示例所示。

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/
   cQk+0FzZqaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. 连接到实例。
4. 使用 adduser 命令创建用户并将其添加到系统（/etc/passwd 文件中会有一个条目）。该命令还可以为用户创建一个组和一个主目录。在此示例中，用户名为 *newuser*。

   - Amazon Linux 和 Amazon Linux 2

     对于 Amazon Linux 和 Amazon Linux 2，创建用户时将默认禁用密码身份验证。

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     添加 --disabled-password 参数以创建用户并禁用密码身份验证。

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. 切换到新用户，以便所创建的目录和文件具有适当的所有权。

   ```
   [ec2-user ~]$ sudo su - newuser
   ```

   如果提示从 ec2-user 变为 *newuser*，则表示您已将 Shell 会话切换到新用户。
6. 将 SSH 公有密钥添加到用户。首先在 SSH 密钥文件对应的用户主目录中创建一个目录，然后创建密钥文件，最后将公有密钥粘贴到该密钥文件中，如以下分步说明中所述。

   a. 在 .ssh 主目录中创建一个 *newuser* 目录，并将其权限更改为 700 (只有文件所有者能够读取、写入或打开该目录。)

      ```
      [newuser ~]$ mkdir .ssh
      ```

```
[newuser ~]$ chmod 700 .ssh
```

Important

如果没有这些确切的文件权限，用户将无法登录。

b. 在 authorized_keys 目录中创建名为 .ssh 的文件并将其权限更改为 600 (只有文件所有者能够读取或写入此文件)。

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

Important

如果没有这些确切的文件权限，用户将无法登录。

c. 使用您常用的文本编辑器 (如 vim 或 nano) 打开 authorized_keys 文件。

```
[newuser ~]$ nano .ssh/authorized_keys
```

将您在步骤 2 中检索到的公有密钥粘贴到文件中并保存更改。

Important

确保将公有密钥粘贴到一个连续行中。不得将公有密钥拆分为多行。

用户现在能够使用添加到 *newuser* 文件的公有密钥所对应的私有密钥登录实例上的 authorized_keys 用户。有关连接到 Linux 实例的不同方法的更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

删除用户

如果不再需要某个用户，可以将其删除，使它不再可用。

使用 userdel 命令从系统中删除用户。当您指定 -r 参数时，用户的主目录和邮件后台打印将被删除。要保留用户的主目录和邮件后台打印，请省略 -r 参数。

```
[ec2-user ~]$ sudo userdel -r olduser
```

您的 EC2 实例的处理器状态控制

C 状态控制当核心处于空闲状态时可以进入的睡眠级别。C 状态从 C0 (最浅空闲状态，此时核心完全唤醒并在执行指令) 开始编号，一直增进到 C6 (最深空闲状态，此时核心关闭)。

P 状态控制核心的所需性能 (以 CPU 频率的形式)。P 状态从 P0 (最高性能设置，此时核心可以使用 Intel 睿频加速技术提高频率) 开始编号，然后从 P1 (请求最大基准频率的 P 状态) 一直增加到 P15 (可能最低的频率)。

以下实例类型为操作系统提供了控制处理器 C 状态和 P 状态的功能：

- 通用：m4.10xlarge |m4.16xlarge |m5.metal |m5d.metal |m5n.metal |m5zn.metal |m6i.metal |m6id.metal
- 计算优化：c4.8xlarge | c5.metal | c5n.metal | c6i.metal | c6id.metal

- 内存优化型：r4.8xlarge | r4.16xlarge | r5.metal | r5b.metal | r5d.metal | r6i.metal | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | x1.16xlarge | x1.32xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | z1d.metal
- 存储优化：d2.8xlarge |i3.8xlarge |i3.16xlarge |i3.metal |i3en.metal |h1.8xlarge |h1.16xlarge
- 加速计算：f1.16xlarge |g3.16xlarge |g4dn.metal |p2.16xlarge |p3.16xlarge

以下实例类型为操作系统提供了控制处理器 C 状态的功能：

- 通用型：m5.12xlarge | m5.24xlarge | m5d.12xlarge | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge | m6a.24xlarge | m6a.48xlarge | m6i.16xlarge | m6i.32xlarge
- 计算优化型：c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge | c6a.24xlarge | c6a.32xlarge | c6a.48xlarge | c6i.16xlarge | c6i.32xlarge
- 内存优化型：r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge | u-12tb1.112xlarge | z1d.6xlarge | z1d.12xlarge
- 存储优化型：d3en.12xlarge | dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.metal | r5b.12xlarge | r5b.24xlarge | i4i.16xlarge
- 加速计算型：dl1.24xlarge | g5.24xlarge | g5.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | vt1.24xlarge

Amazon Graviton 处理器具有内置的节能模式，并以固定频率运行。因此，它们不提供操作系统控制 C 状态和 P 状态的能力。

改变 C 状态或 P 状态设置可以增加处理器性能一致性，减少延迟，还可以针对特定工作负载对实例进行调校。默认 C 状态和 P 状态设置可提供最大性能，是大多数工作负载的最佳选择。但是，如果您的应用程序更适合以牺牲较高的单核或双核频率的方式来降低延迟，或需要在较低频率下保持稳定性能 (而不适合使用突发式睿频加速频率)，那么可以考虑运用对这些实例可用的 C 状态或 P 状态设置。

以下部分介绍了不同的处理器状态配置以及如何监控配置效果。这些步骤专为 Amazon Linux 编写并供其使用，但也适用于搭载 Linux 内核版本 3.9 及更高版本的其他 Linux 发行版。有关其他 Linux 发行版和处理器状态控制的更多信息，请参阅您系统的特定文档。

> **Note**
>
> 本页上的示例使用以下内容：
>
> - 显示处理器频率和 C 状态信息的 turbostat 实用程序。默认情况下，turbostat 实用程序在 Amazon Linux 上提供。
> - 模拟工作负载的 stress 命令。若要安装 stress，首先通过运行 sudo amazon-linux-extras install epel 启用 EPEL 存储库，然后运行 sudo yum install -y stress。
>
> 如果输出不显示 C 状态信息，请在命令中加入 --debug 选项 (sudo turbostat --debug stress ***<options>***)。

目录

- 具有最大睿频加速频率的最高性能 (p. 709)
- 通过限制深层 C 状态实现高性能和低延迟 (p. 710)

- 变化最少的基准性能 (p. 711)

具有最大睿频加速频率的最高性能

这是 Amazon Linux AMI 的默认处理器状态控制配置，推荐大多数工作负载使用。此配置可提供最高性能，且变化更少。允许非活动核心进入深层睡眠状态可提供单核或双核进程所需的热空间，以达到最大睿频加速潜能。

以下示例显示了具有两个有效执行工作且达到其最大处理器睿频加速频率的核心的 c4.8xlarge 实例。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30680] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
 Pkg_W RAM_W PKG_% RAM_%
            5.54 3.44 2.90   0   9.18   0.00  85.28   0.00   0.00   0.00   0.00   0.00
 94.04 32.70 54.18  0.00
 0   0   0   0.12 3.26 2.90   0   3.61   0.00  96.27   0.00   0.00   0.00   0.00   0.00
 48.12 18.88 26.02  0.00
 0   0  18   0.12 3.26 2.90   0   3.61
 0   1   1   0.12 3.26 2.90   0   4.11   0.00  95.77   0.00
 0   1  19   0.13 3.27 2.90   0   4.11
 0   2   2   0.13 3.28 2.90   0   4.45   0.00  95.42   0.00
 0   2  20   0.11 3.27 2.90   0   4.47
 0   3   3   0.05 3.42 2.90   0  99.91   0.00   0.05   0.00
 0   3  21  97.84 3.45 2.90   0   2.11
...
 1   1  10   0.06 3.33 2.90   0  99.88   0.01   0.06   0.00
 1   1  28  97.61 3.44 2.90   0   2.32
...
10.002556 sec
```

在此示例中，vCPU 21 和 vCPU 28 均以其最大睿频加速频率运行，因为其他内核已进入 C6 睡眠状态以节省性能，并为正在工作的内核提供性能和热空间。vCPU 3 和 vCPU 10（分别与 vCPU 21 和 vCPU 28 共享一个处理器内核）均处于等待指令的 C1 状态。

在以下示例中，所有 18 个核心均在有效执行工作，因此没有达到最大睿频加速频率的空间，但这些核心都在以 3.2 GHz 的“所有核心睿频加速”速度运行。

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
 Pkg_W RAM_W PKG_% RAM_%
           99.27 3.20 2.90   0   0.26   0.00   0.47   0.00   0.00   0.00   0.00   0.00
 228.59 31.33 199.26  0.00
 0   0   0  99.08 3.20 2.90   0   0.27   0.01   0.64   0.00   0.00   0.00   0.00   0.00
 114.69 18.55 99.32  0.00
 0   0  18  98.74 3.20 2.90   0   0.62
 0   1   1  99.14 3.20 2.90   0   0.09   0.00   0.76   0.00
 0   1  19  98.75 3.20 2.90   0   0.49
 0   2   2  99.07 3.20 2.90   0   0.10   0.02   0.81   0.00
 0   2  20  98.73 3.20 2.90   0   0.44
 0   3   3  99.02 3.20 2.90   0   0.24   0.00   0.74   0.00
 0   3  21  99.13 3.20 2.90   0   0.13
 0   4   4  99.26 3.20 2.90   0   0.09   0.00   0.65   0.00
 0   4  22  98.68 3.20 2.90   0   0.67
 0   5   5  99.19 3.20 2.90   0   0.08   0.00   0.73   0.00
 0   5  23  98.58 3.20 2.90   0   0.69
 0   6   6  99.01 3.20 2.90   0   0.11   0.00   0.89   0.00
 0   6  24  98.72 3.20 2.90   0   0.39
```

```
...
```

通过限制深层 C 状态实现高性能和低延迟

C 状态控制当核心处于非活动状态时可能进入的睡眠级别。您可能需要控制 C 状态来调校系统的延迟与性能。将核心置于睡眠状态需要时间，尽管睡眠中的核心可为其他核心提供更多空间以加速至更高频率，但该睡眠中的核心也需要时间来重新唤醒并执行工作。例如，如果某个负责处理网络数据包中断的核心处于睡眠状态，那么在处理此类中断时可能会出现延迟。您可以将系统配置为不使用深层 C 状态，这可以降低处理器的反应延迟，但反过来也会减少其他核心达到睿频加速频率可用的空间。

禁用深层睡眠状态的常见情形是 Redis 数据库应用程序，该应用程序将数据库存储在系统内存中，以实现最快速的查询响应。

限制 Amazon Linux 2 上的深层睡眠状态

1. 使用所选编辑器打开 `/etc/default/grub` 文件。

   ```
   [ec2-user ~]$ sudo vim /etc/default/grub
   ```

2. 编辑 `GRUB_CMDLINE_LINUX_DEFAULT` 行并添加 `intel_idle.max_cstate=1` 和 `processor.max_cstate=1` 选项，以将 C1 设置为空闲内核的最深层 C 状态。

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1
    processor.max_cstate=1"
   GRUB_TIMEOUT=0
   ```

   `intel_idle.max_cstate=1` 选项用于为基于英特尔处理器的实例配置 C 状态限制，`processor.max_cstate=1` 选项用于为基于 AMD 处理器的实例配置 C 状态限制。您可以放心将这两个选项添加到配置中。这可实现通过单个配置在英特尔和 AMD 处理器上设置所需的行为。

3. 保存文件并退出您的编辑器。
4. 运行以下命令重新构建启动配置。

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

5. 重启实例以启用新的内核选项。

   ```
   [ec2-user ~]$ sudo reboot
   ```

限制 Amazon Linux AMI 上的深层睡眠状态

1. 使用所选编辑器打开 `/boot/grub/grub.conf` 文件。

   ```
   [ec2-user ~]$ sudo vim /boot/grub/grub.conf
   ```

2. 编辑第一个条目的 `kernel` 行并添加 `intel_idle.max_cstate=1` 和 `processor.max_cstate=1` 选项，以将 C1 设置为空闲内核的最深层 C 状态。

   ```
   # created by imagebuilder
   default=0
   timeout=1
   hiddenmenu

   title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
   ```

```
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
 intel_idle.max_cstate=1  processor.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

`intel_idle.max_cstate=1` 选项用于为基于英特尔处理器的实例配置 C 状态限制，`processor.max_cstate=1` 选项用于为基于 AMD 处理器的实例配置 C 状态限制。您可以放心将这两个选项添加到配置中。这可实现通过单个配置在英特尔和 AMD 处理器上设置所需的行为。

3. 保存文件并退出您的编辑器。
4. 重启实例以启用新的内核选项。

```
[ec2-user ~]$ sudo reboot
```

以下示例显示的 `c4.8xlarge` 实例具有两个以“所有核心睿频加速”核心频率有效执行工作的核心。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5322] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5322] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
 Pkg_W RAM_W PKG_% RAM_%
            5.56 3.20 2.90   0  94.44   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 131.90 31.11 199.47  0.00
 0   0   0   0.03 2.08 2.90   0  99.97   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 67.23 17.11 99.76  0.00
 0   0  18   0.01 1.93 2.90   0  99.99
 0   1   1   0.02 1.96 2.90   0  99.98   0.00   0.00   0.00
 0   1  19  99.70 3.20 2.90   0   0.30
...
 1   1  10   0.02 1.97 2.90   0  99.98   0.00   0.00   0.00
 1   1  28  99.67 3.20 2.90   0   0.33
 1   2  11   0.04 2.63 2.90   0  99.96   0.00   0.00   0.00
 1   2  29   0.02 2.11 2.90   0  99.98
...
```

在此示例中，vCPU 19 和 vCPU 28 的核心均以 3.2 GHz 的频率运行，而其他核心处于等待指令的 C1 C 状态。虽然运行中的核心没有达到其最大睿频加速频率，但非活动核心对新请求的响应速度将比其处于深层 C6 C 状态时快得多。

变化最少的基准性能

您可以通过 P 状态减少处理器频率的变化。P 状态控制核心的所需性能 (以 CPU 频率的形式)。大多数工作负载在 P0 状态下性能更好，该状态要求采用睿频加速频率。但是，您可能需要调校系统以获得稳定性能而非突发式性能，而突发式性能可能会在启用睿频加速频率后出现。

Intel 高级矢量扩展 (AVX 或 AVX2) 工作负载能够以较低的频率较好地运行，而 AVX 指令也可以使用更多性能。通过禁用睿频加速来以较低的频率运行处理器，可以降低所使用的性能并保持更稳定的速度。有关优化您的实例配置和 AVX 工作负载的更多信息，请参阅 http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/performance-xeon-e5-v3-advanced-vector-extensions-paper.pdf。

CPU 空闲驱动程序用于控制 P 状态。较新一代的 CPU 需要更新与内核级别对应的 CPU 空闲驱动程序，如下所示：

- Linux 内核 5.6 及更高版本（例如 m6i）– 支持英特尔 Icelake。
- Linux 内核 5.10 及更高版本（例如 m6a）– 支持 AMD Milan。

要检测正在运行的系统的内核是否识别 CPU，请运行以下命令。

```
if [ -d /sys/devices/system/cpu/cpu0/cpuidle ]; then echo "C-state control enabled"; else
 echo "Kernel cpuidle driver does not recognize this CPU generation"; fi
```

如果此命令的输出指示不支持，则建议您升级内核。

此部分介绍了如何限制深层睡眠状态以及禁用睿频加速 (通过请求 P1 P 状态)，从而为这些类型的工作负载提供低延迟和最少的处理器速度变化。

限制 Amazon Linux 2 上的深层睡眠状态并禁用睿频加速

1. 使用所选编辑器打开 /etc/default/grub 文件。

   ```
   [ec2-user ~]$ sudo vim /etc/default/grub
   ```

2. 编辑 GRUB_CMDLINE_LINUX_DEFAULT 行并添加 intel_idle.max_cstate=1 和 processor.max_cstate=1 选项，以将 C1 设置为空闲内核的最深层 C 状态。

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1
    processor.max_cstate=1"
   GRUB_TIMEOUT=0
   ```

   intel_idle.max_cstate=1 选项用于为基于英特尔处理器的实例配置 C 状态限制，processor.max_cstate=1 选项用于为基于 AMD 处理器的实例配置 C 状态限制。您可以放心将这两个选项添加到配置中。这可实现通过单个配置在英特尔和 AMD 处理器上设置所需的行为。
3. 保存文件并退出您的编辑器。
4. 运行以下命令重新构建启动配置。

   ```
   [ec2-user ~]$ grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

5. 重启实例以启用新的内核选项。

   ```
   [ec2-user ~]$ sudo reboot
   ```

6. 如果您需要 P1 P 状态提供的较少处理器速度变化，请运行以下命令禁用睿频加速。

   ```
   [ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
   ```

7. 在工作负载完成后，您可以使用以下命令重新启用睿频加速。

   ```
   [ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
   ```

限制 Amazon Linux AMI 上的深层睡眠状态并禁用睿频加速

1. 使用所选编辑器打开 /boot/grub/grub.conf 文件。

   ```
   [ec2-user ~]$ sudo vim /boot/grub/grub.conf
   ```

2. 编辑第一个条目的 kernel 行并添加 intel_idle.max_cstate=1 和 processor.max_cstate=1 选项，以将 C1 设置为空闲内核的最深层 C 状态。

   ```
   # created by imagebuilder
   default=0
   timeout=1
   hiddenmenu
   ```

```
title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
 intel_idle.max_cstate=1 processor.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

`intel_idle.max_cstate=1` 选项用于为基于英特尔处理器的实例配置 C 状态限制，`processor.max_cstate=1` 选项用于为基于 AMD 处理器的实例配置 C 状态限制。您可以放心将这两个选项添加到配置中。这可实现通过单个配置在英特尔和 AMD 处理器上设置所需的行为。

3. 保存文件并退出您的编辑器。
4. 重启实例以启用新的内核选项。

```
[ec2-user ~]$ sudo reboot
```

5. 如果您需要 P1 P 状态提供的较少处理器速度变化，请运行以下命令禁用睿频加速。

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

6. 在工作负载完成后，您可以使用以下命令重新启用睿频加速。

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

以下示例显示的 `c4.8xlarge` 实例具有两个以基准核心频率有效执行工作的 vCPU，这两个 vCPU 均没有启用睿频加速。

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5389] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
 Pkg_W RAM_W PKG_% RAM_%
            5.59 2.90 2.90   0  94.41   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 128.48 33.54 200.00  0.00
 0   0   0   0.04 2.90 2.90   0  99.96   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 65.33 19.02 100.00  0.00
 0   0  18   0.04 2.90 2.90   0  99.96
 0   1   1   0.05 2.90 2.90   0  99.95   0.00   0.00   0.00
 0   1  19   0.04 2.90 2.90   0  99.96
 0   2   2   0.04 2.90 2.90   0  99.96   0.00   0.00   0.00
 0   2  20   0.04 2.90 2.90   0  99.96
 0   3   3   0.05 2.90 2.90   0  99.95   0.00   0.00   0.00
 0   3  21  99.95 2.90 2.90   0   0.05
...
 1   1  28  99.92 2.90 2.90   0   0.08
 1   2  11   0.06 2.90 2.90   0  99.94   0.00   0.00   0.00
 1   2  29   0.05 2.90 2.90   0  99.95
```

vCPU 21 和 vCPU 28 的核心以 2.9 GHz 的基准处理器速度有效执行工作，而所有非活动核心也在 C1 C 状态下以基准速度运行，准备接受指令。

输入/输出调度器

输入/输出调度器位于 Linux 操作系统中，用于排序和合并输入/输出请求，并决定这些请求的处理顺序。

输入/输出调度器尤其适用于磁盘驱动器等设备，因为此类设备可能需要在查找时间上花费非常昂贵的成本，并且其最适合合并同地协作的请求。输入/输出调度器对固态设备和虚拟化环境的影响较小。这是因为对于固态设备而言，顺序访问与随机访问没有区别，而对于虚拟化环境，则由主机提供自定义的调度层。

本主题将就 Amazon Linux 输入/输出调度器进行讨论。有关其它 Linux 发行版使用的输入/输出调度器的更多信息，请参阅其文档。

主题

- 支持的调度器 (p. 714)
- 默认调度器 (p. 714)
- 更改调度器 (p. 714)

支持的调度器

Amazon Linux 支持以下输入/输出调度器：

- `deadline` – 截止日期输入/输出调度器会对输入/输出请求进行排序，并以最有效的顺序进行处理。其保证了每个输入/输出请求的开始时间。其还会为等待时间过长的输入/输出请求提供更高的优先级。
- `cfq` – 完全公平队列 (CFQ) 输入/输出调度器会试图在进程之间公平分配输入/输出资源。其会对输入/输出请求进行排序并将其插入到每个进程队列之中。
- noop – 无操作 (noop) 输入/输出调度器会将所有输入/输出请求插入到 FIFO 队列之中，然后将其合并至单个请求。此调度器不会排序任何请求。

默认调度器

无操作 (noop) 是 Amazon Linux 的默认输入/输出调度器。使用此调度器的原因如下：

- 许多实例类型都使用虚拟化设备，其中底层主机会为实例执行调度。
- 许多实例类型都使用固态设备，而输入/输出调度器的不会在此情况下体现出明显优势。
- 该调度器是侵入性最小的输入/输出调度器，且可以根据需要进行自定义设置。

更改调度器

根据调度器能否在给定时间内完成更多或更少的输入/输出请求，更改输入/输出请求者可以提高或降低性能。这在很大程度上取决于您的工作负载、正在使用的实例类型的生成以及正在访问的设备的类型。若要更改正在使用的输入/输出调度器，我们建议您使用工具（例如 iotop）来衡量输入/输出的性能并确定此更改是否有益于您的使用场景。

您可以使用以下命令来查看设备的输入/输出调度器，例如 `nvme0n1`。将以下命令中的 `nvme0n1` 替换为您实例上的 `/sys/block` 中列出的设备。

```
$  cat /sys/block/nvme0n1/queue/scheduler
```

请使用以下命令为设备设置输入/输出调度器。

```
$  echo cfq|deadline|noop > /sys/block/nvme0n1/queue/scheduler
```

例如，要将 *xvda* 设备的输入/输出调度器设置为从 noop 到 `cfq`，请使用以下命令。

```
$  echo cfq > /sys/block/xvda/queue/scheduler
```

为 Linux 实例设置时间

对于许多服务器任务和进程来说，准确一致的时间参考是非常重要的。大多数系统日志包含时间戳，您可以用来确定问题发生的时间以及事件发生的顺序。如果您使用 Amazon CLI 或 Amazon 开发工具包从您的实例

发送请求，这些工具会以您的名义签署请求。如果您的实例的日期和时间设置不正确，签名中的日期可能与请求的日期不匹配，进而导致 Amazon 拒绝请求。

Amazon 提供 Amazon Time Sync Service，该服务可从所有 EC2 实例访问，同样由其他 Amazon Web Services 使用。该服务在每个 Amazon Web Services 区域 中使用一组与卫星连接的原子参考时钟，以通过网络时间协议（NTP）提供准确的当前协调世界时（UTC）全球标准时间读数。Amazon Time Sync Service 自动消除在 UTC 中添加的任何闰秒。

Amazon Time Sync Service 是通过 NTP（IPv4 地址为 `169.254.169.123` 或 IPv6 地址为 `fd00:ec2::123`）为 VPC 中运行的任何实例提供的。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。您的实例不需要访问互联网，并且您不必配置安全组规则或网络 ACL 规则以允许进行访问。最新版本的 Amazon Linux 2 和 Amazon Linux AMI 默认情况下与 Amazon Time Sync Service 同步。

可以使用以下步骤通过 `chrony` 客户端在实例上配置 Amazon Time Sync Service。或者，您也可以使用外部 NTP 源。有关 NTP 和公共时间源的更多信息，请访问 http://www.ntp.org/。实例需要访问 Internet，外部 NTP 时间源才能正常工作。

对于 Windows 实例，请参阅为 Windows 实例设置时间。

要备份到 Amazon Time Sync 链路本地服务，以及将 Amazon EC2 之外的资源连接到 Amazon Time Sync Service，您可以使用位于 time.aws.com 的 Amazon Time Sync Public NTP 池。与 Amazon Time Sync Service 一样，Amazon Time Sync Public NTP 会自动消除在 UTC 中添加的任何闰秒。Amazon Time Sync Service Public NTP 由每个 Amazon Web Services 区域 中一组与卫星连接的原子参考时钟在全球范围内提供支持。有关配置说明，请参阅 使用 Amazon Time Sync Public NTP 为客户端配置时间 (p. 715)。

主题

- 使用 Amazon Time Sync Public NTP 为客户端配置时间 (p. 715)
- 配置具有 IPv4 地址的 EC2 实例的时间 (p. 716)
- 配置具有 IPv6 地址的 EC2 实例的时间 (p. 719)
- 在 Amazon Linux 上更改时区 (p. 719)
- 比较时间戳 (p. 721)

使用 Amazon Time Sync Public NTP 为客户端配置时间

您可以将客户端计算机配置为使用 Amazon Time Sync。

为 Apple macOS 配置 Amazon Time Sync Public NTP

1. 在客户端计算机上，打开 System Preferences（系统偏好设置）。
2. 选择 Date & Time（日期和时间），然后选择 Date & Time（日期和时间）选项卡。
3. 要进行更改，请选择锁定图标，并在出现提示时输入密码。
4. 对于 Set date and time automatically（自动设置日期和时间），请输入 **`time.aws.com`**。

为 Linux:chrony 或 ntpd 配置 Amazon Time Sync Public NTP

1. 使用常用的文本编辑器编辑 `/etc/chrony/chrony.conf`（如您使用 chrony）或 `/etc/ntp.conf`（如您使用 ntpd）。

   请勿编辑 `server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4` 行，以确保 EC2 实例与本地 Amazon Time Sync Service 保持连接。

   删除或注释掉以 `server` 开头的其他行，以防计算机尝试混用已涂抹和未涂抹的服务器。

   添加 `pool time.aws.com iburst` 行。
2. 选择 NAME（名称）。

3. 使用 `sudo service chrony force-reload`（适用于 chrony）或 `sudo service ntp reload`（适用于 ntpd）重启进程守护程序

   systemd-timesyncd

   在同一个配置文件中，将 `[Time]` 块的内容设置为 `[Time] NTP=FallbackNTP=time.aws.com`。

   这样可以防止计算机在已涂抹和未涂抹的时间服务器之间无意地移动。将 Amazon Time Sync Service Public NTP 配置为备用服务器会使其被选为唯一的 NTP 服务器。

   - 以具有适当权限的用户身份，使用 `systemctl restart systemd-timesyncd.service` 命令重启 `systemd-timesyncd`

   验证您的系统是否正在使用具有 `timedatectl show-timesync | grep` *`ServerName`* 的 Amazon Time Sync Public NTP 池。如果配置成功，输出将会显示 *`ServerName`*`=time.aws.com`。

配置具有 IPv4 地址的 EC2 实例的时间

此部分介绍如何根据 Linux 分发版的类型，为具有 IPv4 地址的 EC2 实例设置时间。

主题

- 在 Amazon Linux AMI 上配置 Amazon Time Sync Service (p. 716)
- 在 Ubuntu 上配置 Amazon Time Sync Service (p. 717)
- 在 SUSE Linux 上配置 Amazon Time Sync Service (p. 719)

在 Amazon Linux AMI 上配置 Amazon Time Sync Service

Note

在 Amazon Linux 2 上，`chrony` 已安装并配置为使用 Amazon Time Sync Service IP 地址。

对于 Amazon Linux AMI，您必须编辑 `chrony` 配置文件以添加 Amazon Time Sync Service 的服务器条目。

配置 实例以使用 Amazon Time Sync Service

1. 连接到您的实例并卸载 NTP 服务。

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. 安装 `chrony` 软件包。

```
[ec2-user ~]$ sudo yum install chrony
```

3. 使用任何文本编辑器（如 `/etc/chrony.conf` 或 vim）打开 nano 文件。确认该文件包含以下行：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

   如果该行存在，则已配置 Amazon Time Sync Service，您可以转到下一步。如果不存在，请在该文件中已包含的任何其他 `server` 或 `pool` 语句后面添加该行，然后保存您的更改。

4. 重启 `chrony` 守护程序 (`chronyd`)。

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

Note

在 RHEL 和 CentOS (最高版本为 6) 上，服务名称是 chrony 而不是 chronyd。

5. 使用 chkconfig 命令可将 chronyd 配置为在每次系统启动时启动。

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. 确认 chrony 使用 169.254.169.123 IP 地址同步时间。

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-  287us
^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-   11ms
^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/- 1959us
^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-    0ns
^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-    0ns
^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-    0ns
^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-    0ns
```

在返回的输出中，^* 指示首选的时间源。

7. 验证 chrony 报告的时间同步指标。

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
        Stratum         : 4
        Ref time (UTC)  : Wed Nov 22 13:18:34 2017
        System time     : 0.000000626 seconds slow of NTP time
        Last offset     : +0.002852759 seconds
        RMS offset      : 0.002852759 seconds
        Frequency       : 1.187 ppm fast
        Residual freq   : +0.020 ppm
        Skew            : 24.388 ppm
        Root delay      : 0.000504752 seconds
        Root dispersion : 0.001112565 seconds
        Update interval : 64.4 seconds
        Leap status     : Normal
```

在 Ubuntu 上配置 Amazon Time Sync Service

您必须编辑 chrony 配置文件以添加 Amazon Time Sync Service 的服务器条目。

配置 实例以使用 Amazon Time Sync Service

1. 连接到您的实例并使用 apt 安装 chrony 软件包。

```
ubuntu:~$ sudo apt install chrony
```

   Note

   如有必要，请先运行 sudo apt update 以更新您的实例。

2. 使用任何文本编辑器（如 /etc/chrony/chrony.conf 或 vim）打开 nano 文件。在该文件中已包含的任何其他 server 或 pool 语句前面添加以下行，然后保存您的更改：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. 重新启动 chrony 服务。

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. 确认 chrony 使用 169.254.169.123 IP 地址同步时间。

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

             .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
           ||                                                 .- xxxx [ yyyy ] +/-
zzzz
           ||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
           ||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
           ||                                \     |          |  zzzz = estimated
error.
           ||                                 |    |           \
           MS Name/IP address         Stratum Poll Reach LastRx Last sample

===============================================================================
           ^* 169.254.169.123               3   6    17    12    +15us[  +57us] +/-
320us
           ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us] +/-
1779us
           ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us] +/-
7710us
           ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns] +/-
0ns
           ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns] +/-
0ns
           ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns] +/-
0ns
           ^? bray.walcz.net                0   6     0   10y     +0ns[   +0ns] +/-
0ns
```

在返回的输出中，以 ^* 开始的行会指示首选的时间源。

5. 验证 chrony 报告的时间同步指标。

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
           Stratum         : 4
           Ref time (UTC)  : Wed Nov 29 07:41:57 2017
           System time     : 0.000000011 seconds slow of NTP time
           Last offset     : +0.000041659 seconds
           RMS offset      : 0.000041659 seconds
           Frequency       : 10.141 ppm slow
           Residual freq   : +7.557 ppm
           Skew            : 2.329 ppm
           Root delay      : 0.000544 seconds
           Root dispersion : 0.000631 seconds
           Update interval : 2.0 seconds
           Leap status     : Normal
```

在 SUSE Linux 上配置 Amazon Time Sync Service

从 https://software.opensuse.org/package/chrony 安装 chrony。

使用任何文本编辑器（如 /etc/chrony.conf 或 vim）打开 nano 文件。确认该文件包含以下行：

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

如果此行不存在，请添加它。注释掉任何其他服务器或池行。打开 yaST 并启用 chrony 服务。

配置具有 IPv6 地址的 EC2 实例的时间

此部分介绍了如果您为使用 IPv6 地址的 EC2 实例配置 Amazon Time Sync Service，在 配置具有 IPv4 地址的 EC2 实例的时间 (p. 716) 中介绍的流程有何不同。它没有解释整个 Amazon Time Sync Service 配置流程。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

Note

我们不建议在您的 chrony.conf 文件中同时使用 IPv4 地址和 IPv6 地址条目。IPv4 和 IPv6 NTP 数据包来自您的实例的同一个本地服务器。如果同时使用来自 IPv4 端点的一些数据包和来自 IPv6 端点的一些数据包，则很可能会得到混合的结果。

根据您使用的 Linux 发行版，当您到达编辑 chrony.conf 文件的步骤时，您将使用 Amazon Time Sync Service的 IPv6 端点 (fd00:ec2::123) 而不是 IPv4 端点 (169.254.169.123)：

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

保存文件并确认 chrony 使用 fd00:ec2::123 IPv6 地址同步时间：

```
[ec2-user ~]$ chronyc sources -v
```

在输出中，如果您看到 fd00:ec2::123 IPv6 地址，则配置完成。

在 Amazon Linux 上更改时区

Amazon Linux 实例默认设置为 UTC（协调世界时）时区。您可以将实例上的时间更改为本地时间或网络中的其他时区。

Important

此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

要更改 Amazon Linux 2 实例上的时区

1. 查看系统的当前时区设置。

```
[ec2-user ~]$ timedatectl
```

2. 列出可用的时区。

```
[ec2-user ~]$ timedatectl list-timezones
```

3. 设置选定的时区。

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. （可选）通过运行 timedatectl 命令，确认当前时区已更新为新时区。

```
[ec2-user ~]$ timedatectl
```

要更改 Amazon Linux 实例上的时区

1. 确定将在实例上使用的时区。/usr/share/zoneinfo 目录包含时区数据文件的层次结构。浏览该位置的目录结构，查找针对您的时区的文件。

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile    GB         Indian       Mideast   posixrules  US
America     CST6CDT  GB-Eire    Iran         MST       PRC         UTC
Antarctica  Cuba     GMT        iso3166.tab  MST7MDT   PST8PDT     WET
Arctic      EET      GMT0       Israel       Navajo    right       W-SU
...
```

   该位置的部分条目是目录 (如 America)，这些目录包含针对特定城市的时区文件。查找要用于实例的城市 (或时区中的一个城市)。

2. 使用新时区更新 /etc/sysconfig/clock 文件。在此示例中，我们使用洛杉矶的时区数据文件 /usr/share/zoneinfo/America/Los_Angeles。

   a. 使用您常用的文本编辑器（如 /etc/sysconfig/clock 或 vim）打开 nano 文件。您需要在编辑器命令中使用 sudo，因为 /etc/sysconfig/clock 归 root 所有。

```
[ec2-user ~]$ sudo nano /etc/sysconfig/clock
```

   b. 查找 ZONE 条目，将其更改为时区文件 (忽略路径的 /usr/share/zoneinfo 部分)。例如，要更改为洛杉矶时区，请将 ZONE 条目更改为以下内容：

```
ZONE="America/Los_Angeles"
```

      Note

      请勿将 UTC=true 条目更改为其他值。此条目用于硬件时钟；如果您在实例上设置了其他时区，则无需调整此条目。

   c. 保存文件，退出文本编辑器。

3. 在 /etc/localtime 与时区文件之间创建一个符号链接，以便实例在引用本地时间信息时找到此时区文件。

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. 重启系统，以便所有服务和应用程序接受新时区信息。

```
[ec2-user ~]$ sudo reboot
```

5. （可选）使用 date 命令确认当前时区已更新为新时区。当前时区将显示在输出中。在下面的示例中，当前时区是 PDT，它指的是洛杉矶时区。

```
[ec2-user ~]$ date
Sun Aug 16 05:45:16 PDT 2020
```

比较时间戳

如果您使用的是 Amazon Time Sync Service，就可以将 Amazon EC2 实例上的时间戳与 ClockBound 进行比较，以确定事件的真实时间。ClockBound 可以测定 EC2 实例的时钟的准确性，并允许您检查一个给定的时间戳是早于还是晚于实例的当前时钟。在确定整个 EC2 实例中的事件与事务的顺序和一致性方面，这些信息十分重要，并且不会收到各个实例的地理位置的影响。

ClockBound 是一个开源守护进程和开源库。要了解关于 ClockBound 的详情，包括安装说明，请参阅 GitHub 上的 ClockBound。

优化 CPU 选项

Amazon EC2 实例支持多线程技术，该技术可使多个线程在一个 CPU 核心上并发运行。每个线程都表示为实例上的一个虚拟 CPU (vCPU)。实例具有默认数量的 CPU 核心，根据实例类型而异。例如，默认情况下，m5.xlarge 实例类型有两个 CPU 内核，每个内核有两个线程—，共四个 vCPU。

> **Note**
>
> 每个 vCPU 都是 CPU 核心的线程，但 T2 实例和由 Amazon Graviton2 处理器提供支持的实例除外。

在大多数情况下，都有一个 Amazon EC2 实例类型，它具有适合您工作负载的内存和 vCPU 数量组合。但是，您可以指定以下 CPU 选项来针对特定工作负载或业务需求优化实例：

- CPU 核心数：您可以自定义实例的 CPU 核心数。也许可以通过这种方式让实例拥有适合内存密集型工作负载的充足 RAM，同时减少 CPU 核心数，从而优化您的软件的许可成本。
- 每内核线程数：您可以通过为每个 CPU 内核指定一个线程来禁用多线程技术。也许可以为特定工作负载（例如高性能计算 (HPC) 工作负载）执行该操作。

可以在实例启动期间指定上述 CPU 选项。指定 CPU 选项不会增加或减少费用。收费标准与使用默认 CPU 选项启动的实例相同。

目录

- 指定 CPU 选项的规则 (p. 722)
- 每种实例类型的 CPU 核心数和每 CPU 核心的线程数 (p. 722)
- 指定实例的 CPU 选项 (p. 741)
- 查看实例的 CPU 选项 (p. 743)

指定 CPU 选项的规则

要为您的实例指定 CPU 选项，请注意以下规则：

- CPU 选项只能在实例启动期间指定，启动后无法修改。
- 启动实例时，必须在请求中指定 CPU 核心数和每核心线程数。有关示例请求，请参阅指定实例的 CPU 选项 (p. 741)。
- 实例的 vCPU 总数等于 CPU 内核数乘以每内核线程数。要指定自定义数量的 vCPU，必须为实例类型指定有效的 CPU 核心数和每核心线程数。不能超出实例的默认 vCPU 数量。有关更多信息，请参阅每种实例类型的 CPU 核心数和每 CPU 核心的线程数 (p. 722)。
- 要禁用多线程技术，请为每个内核指定一个线程。
- 更改现有实例的实例类型 (p. 399)时，CPU 选项会自动更改为新实例类型的默认 CPU 选项。
- 停止、启动或重启实例后，仍将保留指定的 CPU 选项。

每种实例类型的 CPU 核心数和每 CPU 核心的线程数

下表列出了支持指定 CPU 选项的实例类型。

目录

- 通用实例 (p. 722)
- 计算优化型实例 (p. 727)
- 内存优化型实例 (p. 731)
- 存储优化型实例 (p. 737)
- 加速计算实例 (p. 739)

通用实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m2.xlarge	2	2	1	1、2	1
m2.2xlarge	4	4	1	1、2、3、4	1
m2.4xlarge	8	8	1	1、2、3、4、5、6、7、8	1
m3.large	2	1	2	1	1、2
m3.xlarge	4	2	2	1、2	1、2
m3.2xlarge	8	4	2	1、2、3、4	1、2
m4.large	2	1	2	1	1、2
m4.xlarge	4	2	2	1、2	1、2
m4.2xlarge	8	4	2	1、2、3、4	1、2
m4.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
m4.10xlarge	40	20	2	2、4、6、8、10、12、14、16、18、20	1、2
m4.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m5.large	2	1	2	1	1、2
m5.xlarge	4	2	2	2	1、2
m5.2xlarge	8	4	2	2、4	1、2
m5.4xlarge	16	8	2	2、4、6、8	1、2
m5.8xlarge	32	16	2	2、4、6、8、10、12	1、2 14、16
m5.12xlarge	48	24	2	2、4、6、8、10、12	1、2 14、16、18、20、22、2
m5.16xlarge	64	32	2	2、4、6、8、10、12	1、2 14、16、18、20、22、2
m5.24xlarge	96	48	2	4、6、8、10、12、14	1、2 16、18、20、22、24、
m5a.large	2	1	2	1	1、2
m5a.xlarge	4	2	2	2	1、2
m5a.2xlarge	8	4	2	2、4	1、2
m5a.4xlarge	16	8	2	2、4、6、8	1、2
m5a.8xlarge	32	16	2	4、6、8、10、12、14	1、2 16
m5a.12xlarge	48	24	2	6、12、18、24	1、2
m5a.16xlarge	64	32	2	8、10、12、14、16	1、2 18、20、22、24、26、2
m5a.24xlarge	96	48	2	12、18、24、36、48	1、2
m5ad.large	2	1	2	1	1、2
m5ad.xlarge	4	2	2	2	1、2
m5ad.2xlarge	8	4	2	2、4	1、2
m5ad.4xlarge	16	8	2	2、4、6、8	1、2
m5ad.8xlarge	32	16	2	4、6、8、10、12、14	1、2 16
m5ad.12xlarge	48	24	2	6、12、18、24	1、2
m5ad.16xlarge	64	32	2	8、10、12、14、16	1、2 18、20、22、24、26、2
m5ad.24xlarge	96	48	2	12、18、24、36、48	1、2
m5d.large	2	1	2	1	1、2
m5d.xlarge	4	2	2	2	1、2
m5d.2xlarge	8	4	2	2、4	1、2
m5d.4xlarge	16	8	2	2、4、6、8	1、2
m5d.8xlarge	32	16	2	2、4、6、8、10、12	1、2 14、16
m5d.12xlarge	48	24	2	2、4、6、8、10、12	1、2 14、16、18、20、22、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m5d.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5d.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	
m5dn.large	2	1	2	1	1、2
m5dn.xlarge	4	2	2	1、2	1、2
m5dn.2xlarge	8	4	2	2、4	1、2
m5dn.4xlarge	16	8	2	2、4、6、8	1、2
m5dn.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
m5dn.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5dn.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5dn.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5n.large	2	1	2	1	1、2
m5n.xlarge	4	2	2	1、2	1、2
m5n.2xlarge	8	4	2	2、4	1、2
m5n.4xlarge	16	8	2	2、4、6、8	1、2
m5n.8xlarge	32	16	2	2、4、6、8、10、12、14、16	
m5n.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5n.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5n.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	
m5zn.large	2	1	2	1	1、2
m5zn.xlarge	4	2	2	1、2	1、2
m5zn.2xlarge	8	4	2	2、4	1、2
m5zn.3xlarge	12	6	2	2、4、6	1、2
m5zn.6xlarge	24	12	2	2、4、6、8、10、12	
m5zn.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	
m6a.large	2	1	2	1	1、2
m6a.xlarge	4	2	2	1、2	1、2
m6a.2xlarge	8	4	2	1、2、3、4	1、2
m6a.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
m6a.8xlarge	32	16	2	1、2、3、4、5、6、7、8、10、12、14、16	1、2
m6a.12xlarge	48	24	2	1、2、3、4、5、6、7、8、10、12、14、16、18、20、22、24	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m6a.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	1、2
m6a.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48	1、2
m6a.32xlarge	128	64	2	4、8、12、16、20、24、28、32、36、40、44、48、52、56、60、64	1、2
m6a.48xlarge	192	96	2	4、8、12、16、20、24、28、32、36、40、44、48、52、56、60、64、68、72、76、80、84、88、92、96	1、2
m6g.large	2	2	1	1、2	1
m6g.xlarge	4	4	1	1、2、3、4	1
m6g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
m6g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16	1
m6g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32	1
m6g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39、40、41、42、43、44、45、46、47、48	1
m6g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39、40、41、42、43、44、45、46、47、48、49、50、51、52、53、54、55、56、57、58、59、60、61、62、63、64	1
m6gd.large	2	2	1	1、2	1
m6gd.xlarge	4	4	1	1、2、3、4	1
m6gd.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
m6gd.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16	1
m6gd.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32	1
m6gd.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39、40、41、42、43、44、45、46、47、48	1
m6gd.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32、33、34、35、36、37、38、39、40、41、42、43、44、45、46、47、48、49、50、51、52、53、54、55、56、57、58、59、60、61、62、63、64	1
m6i.large	2	1	2	1	1、2
m6i.xlarge	4	2	2	1、2	1、2
m6i.2xlarge	8	4	2	2、4	1、2
m6i.4xlarge	16	8	2	2、4、6、8	1、2
m6i.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
m6i.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	1、2
m6i.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	1、2
m6i.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48	1、2
m6i.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48、50、52、54、56、58、60、62、64	1、2
m6id.large	2	1	2	1	1、2
m6id.xlarge	4	2	2	1、2	1、2
m6id.2xlarge	8	4	2	2、4	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m6id.4xlarge	16	8	2	2、4、6、8	1、2
m6id.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
m6id.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
m6id.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
m6id.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
m6id.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
m6idn.large	2	1	2	1	1、2
m6idn.xlarge	4	2	2	1、2	1、2
m6idn.2xlarge	8	4	2	1、2、3、4	1、2
m6idn.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
m6idn.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6idn.12xlarge	48	24	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6idn.16xlarge	64	32	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6idn.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
m6idn.32xlarge	128	64	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
m6in.large	2	1	2	1	1、2
m6in.xlarge	4	2	2	1、2	1、2
m6in.2xlarge	8	4	2	1、2、3、4	1、2
m6in.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
m6in.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6in.12xlarge	48	24	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6in.16xlarge	64	32	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
m6in.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
m6in.32xlarge	128	64	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
m7g.large	2	2	1	1、2	1
m7g.xlarge	4	4	1	1、2、3、4	1
m7g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
m7g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
m7g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
m7g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
m7g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
t3.nano	2	1	2	1	1、2
t3.micro	2	1	2	1	1、2
t3.small	2	1	2	1	1、2
t3.medium	2	1	2	1	1、2
t3.large	2	1	2	1	1、2
t3.xlarge	4	2	2	2	1、2
t3.2xlarge	8	4	2	2、4	1、2
t3a.nano	2	1	2	1	1、2
t3a.micro	2	1	2	1	1、2
t3a.small	2	1	2	1	1、2
t3a.medium	2	1	2	1	1、2
t3a.large	2	1	2	1	1、2
t3a.xlarge	4	2	2	2	1、2
t3a.2xlarge	8	4	2	2、4	1、2
t4g.nano	2	2	1	1、2	1
t4g.micro	2	2	1	1、2	1
t4g.small	2	2	1	1、2	1
t4g.medium	2	2	1	1、2	1
t4g.large	2	2	1	1、2	1
t4g.xlarge	4	4	1	1、2、3、4	1
t4g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1

计算优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
c3.large	2	1	2	1	1、2
c3.xlarge	4	2	2	1、2	1、2
c3.2xlarge	8	4	2	1、2、3、4	1、2
c3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
c3.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
c4.large	2	1	2	1	1、2
c4.xlarge	4	2	2	1、2	1、2
c4.2xlarge	8	4	2	1、2、3、4	1、2
c4.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
c4.8xlarge	36	18	2	2、4、6、8、10、12、14、16、18	1、2
c5.large	2	1	2	1	1、2
c5.xlarge	4	2	2	2	1、2
c5.2xlarge	8	4	2	2、4	1、2
c5.4xlarge	16	8	2	2、4、6、8	1、2
c5.9xlarge	36	18	2	2、4、6、8、10、12、14、16、18	1、2
c5.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
c5.18xlarge	72	36	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
c5.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
c5a.large	2	1	2	1	1、2
c5a.xlarge	4	2	2	1、2	1、2
c5a.2xlarge	8	4	2	1、2、3、4	1、2
c5a.4xlarge	16	8	2	1、2、3、4、8	1、2
c5a.8xlarge	32	16	2	1、2、3、4、8、12、16	1、2
c5a.12xlarge	48	24	2	1、2、3、4、8、12、16、20、24	1、2
c5a.16xlarge	64	32	2	1、2、3、4、8、12、16、20、24、28、32	1、2
c5a.24xlarge	96	48	2	1、2、3、4、8、12、16、20、24、28、32、36	1、2
c5ad.large	2	1	2	1	1、2
c5ad.xlarge	4	2	2	1、2	1、2
c5ad.2xlarge	8	4	2	1、2、3、4	1、2
c5ad.4xlarge	16	8	2	1、2、3、4、8	1、2
c5ad.8xlarge	32	16	2	1、2、3、4、8、12、16	1、2
c5ad.12xlarge	48	24	2	1、2、3、4、8、12、16、20、24	1、2
c5ad.16xlarge	64	32	2	1、2、3、4、8、12、16、20、24、28、32	1、2
c5ad.24xlarge	96	48	2	1、2、3、4、8、12、16、20、24、28、32、36	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
c5d.large	2	1	2	1	1、2
c5d.xlarge	4	2	2	2	1、2
c5d.2xlarge	8	4	2	2、4	1、2
c5d.4xlarge	16	8	2	2、4、6、8	1、2
c5d.9xlarge	36	18	2	2、4、6、8、10、11、12	1、2
c5d.12xlarge	48	24	2	2、4、6、8、10、11、12	1、2
c5d.18xlarge	72	36	2	4、6、8、10、12、14、16	1、2
c5d.24xlarge	96	48	2	2、4、6、8、10、11、12	1、2
c5n.large	2	1	2	1	1、2
c5n.xlarge	4	2	2	2	1、2
c5n.2xlarge	8	4	2	2、4	1、2
c5n.4xlarge	16	8	2	2、4、6、8	1、2
c5n.9xlarge	36	18	2	2、4、6、8、10、11、12	1、2
c5n.18xlarge	72	36	2	4、6、8、10、12、14、16	1、2
c6a.large	2	1	2	1	1、2
c6a.xlarge	4	2	2	1、2	1、2
c6a.2xlarge	8	4	2	1、2、3、4	1、2
c6a.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
c6a.8xlarge	32	16	2	1、2、3、4、5、6、7、8、16	1、2
c6a.12xlarge	48	24	2	1、2、3、4、5、6、7、8、16、24	1、2
c6a.16xlarge	64	32	2	2、4、6、8、10、11、12	1、2
c6a.24xlarge	96	48	2	2、4、6、8、10、11、12	1、2
c6a.32xlarge	128	64	2	4、8、12、16、20、24、28、32、64	1、2
c6a.48xlarge	192	96	2	4、8、12、16、20、24、28、32、64、96	1、2
c6g.large	2	2	1	1、2	1
c6g.xlarge	4	4	1	1、2、3、4	1
c6g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
c6g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
c6g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
c6g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
c6g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gd.large	2	2	1	1、2	1
c6gd.xlarge	4	4	1	1、2、3、4	1
c6gd.2xlarge	8	8	1	1、2、3、4、5、6、7、8	
c6gd.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gd.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gd.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gd.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1、2	1
c6gn.xlarge	4	4	1	1、2、3、4	1
c6gn.2xlarge	8	8	1	1、2、3、4、5、6、7、8	
c6gn.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gn.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gn.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6gn.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6i.large	2	1	2	1	1、2
c6i.xlarge	4	2	2	1、2	1、2
c6i.2xlarge	8	4	2	2、4	1、2
c6i.4xlarge	16	8	2	2、4、6、8	1、2
c6i.8xlarge	32	16	2	2、4、6、8、10、12	1、2、14、16
c6i.12xlarge	48	24	2	2、4、6、8、10、12	1、2、14、16、18、20、22、2
c6i.16xlarge	64	32	2	2、4、6、8、10、12	1、2、14、16、18、20、22、2
c6i.24xlarge	96	48	2	2、4、6、8、10、12	1、2、14、16、18、20、22、2
c6i.32xlarge	128	64	2	2、4、6、8、10、12	1、2、14、16、18、20、22、2
c6id.large	2	1	2	1	1、2
c6id.xlarge	4	2	2	1、2	1、2
c6id.2xlarge	8	4	2	2、4	1、2
c6id.4xlarge	16	8	2	2、4、6、8	1、2
c6id.8xlarge	32	16	2	2、4、6、8、10、12	1、2、14、16

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
c6id.12xlarge	48	24	2	2、4、6、8、10、11、12、14、16、18、20、22、2	
c6id.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、2	
c6id.24xlarge	96	48	2	2、4、6、8、10、11、12、14、16、18、20、22、2	
c6id.32xlarge	128	64	2	2、4、6、8、10、11、12、14、16、18、20、22、2	
c6in.large	2	1	2	1	1、2
c6in.xlarge	4	2	2	1、2	1、2
c6in.2xlarge	8	4	2	1、2、3、4	1、2
c6in.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
c6in.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6in.12xlarge	48	24	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6in.16xlarge	64	32	2	1、2、3、4、5、6、7、8、9、10、11、12、13	
c6in.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	
c6in.32xlarge	128	64	2	4、6、8、10、12、14、16、18、20、22、24、	
c7g.large	2	2	1	1、2	1
c7g.xlarge	4	4	1	1、2、3、4	1
c7g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	
c7g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c7g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c7g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
c7g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	

内存优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
hpc6id.32xlarge	64	64	1	4、6、8、10、12、14、16、18、20、22、24、	
r3.large	2	1	2	1	1、2
r3.xlarge	4	2	2	1、2	1、2
r3.2xlarge	8	4	2	1、2、3、4	1、2
r3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	
r3.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
r4.large	2	1	2	1	1、2
r4.xlarge	4	2	2	1、2	1、2
r4.2xlarge	8	4	2	1、2、3、4	1、2
r4.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
r4.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
r4.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
r5.large	2	1	2	1	1、2
r5.xlarge	4	2	2	2	1、2
r5.2xlarge	8	4	2	2、4	1、2
r5.4xlarge	16	8	2	2、4、6、8	1、2
r5.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
r5.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
r5.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
r5.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
r5a.large	2	1	2	1	1、2
r5a.xlarge	4	2	2	2	1、2
r5a.2xlarge	8	4	2	2、4	1、2
r5a.4xlarge	16	8	2	2、4、6、8	1、2
r5a.8xlarge	32	16	2	4、6、8、10、12、14、16	1、2
r5a.12xlarge	48	24	2	6、12、18、24	1、2
r5a.16xlarge	64	32	2	8、10、12、14、16、18、20、22、24、26、28	1、2
r5a.24xlarge	96	48	2	12、18、24、36、48	1、2
r5ad.large	2	1	2	1	1、2
r5ad.xlarge	4	2	2	2	1、2
r5ad.2xlarge	8	4	2	2、4	1、2
r5ad.4xlarge	16	8	2	2、4、6、8	1、2
r5ad.8xlarge	32	16	2	4、6、8、10、12、14、16	1、2
r5ad.12xlarge	48	24	2	6、12、18、24	1、2
r5ad.16xlarge	64	32	2	8、10、12、14、16、18、20、22、24、26、28	1、2
r5ad.24xlarge	96	48	2	12、18、24、36、48	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
r5b.large	2	1	2	1	1、2
r5b.xlarge	4	2	2	1、2	1、2
r5b.2xlarge	8	4	2	2、4	1、2
r5b.4xlarge	16	8	2	2、4、6、8	1、2
r5b.8xlarge	32	16	2	2、4、6、8、10、12	1、2
r5b.12xlarge	48	24	2	2、4、6、8、10、12	1、2
r5b.16xlarge	64	32	2	2、4、6、8、10、12	1、2
r5b.24xlarge	96	48	2	2、4、6、8、10、12	1、2
r5d.large	2	1	2	1	1、2
r5d.xlarge	4	2	2	2	1、2
r5d.2xlarge	8	4	2	2、4	1、2
r5d.4xlarge	16	8	2	2、4、6、8	1、2
r5d.8xlarge	32	16	2	2、4、6、8、10、12	1、2
r5d.12xlarge	48	24	2	2、4、6、8、10、12	1、2
r5d.16xlarge	64	32	2	2、4、6、8、10、12	1、2
r5d.24xlarge	96	48	2	4、6、8、10、12、14	1、2
r5dn.large	2	1	2	1	1、2
r5dn.xlarge	4	2	2	1、2	1、2
r5dn.2xlarge	8	4	2	2、4	1、2
r5dn.4xlarge	16	8	2	2、4、6、8	1、2
r5dn.8xlarge	32	16	2	2、4、6、8、10、12	1、2
r5dn.12xlarge	48	24	2	2、4、6、8、10、12	1、2
r5dn.16xlarge	64	32	2	2、4、6、8、10、12	1、2
r5dn.24xlarge	96	48	2	2、4、6、8、10、12	1、2
r5n.large	2	1	2	1	1、2
r5n.xlarge	4	2	2	1、2	1、2
r5n.2xlarge	8	4	2	2、4	1、2
r5n.4xlarge	16	8	2	2、4、6、8	1、2
r5n.8xlarge	32	16	2	2、4、6、8、10、12	1、2
r5n.12xlarge	48	24	2	2、4、6、8、10、12	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
r5n.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
r5n.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
r6a.large	2	1	2	1	1、2
r6a.xlarge	4	2	2	1、2	1、2
r6a.2xlarge	8	4	2	1、2、3、4	1、2
r6a.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
r6a.8xlarge	32	16	2	1、2、3、4、5、6、7、8、16	1、2
r6a.12xlarge	48	24	2	1、2、3、4、5、6、7、8、16、24	1、2
r6a.16xlarge	64	32	2	2、4、6、8、10、12、14、16、32	1、2
r6a.24xlarge	96	48	2	2、4、6、8、10、12、14、16、32、48	1、2
r6a.32xlarge	128	64	2	4、8、12、16、20、24、28、32、64	1、2
r6a.48xlarge	192	96	2	4、8、12、16、20、24、28、32、64、96	1、2
r6g.large	2	2	1	1、2	1
r6g.xlarge	4	4	1	1、2、3、4	1
r6g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
r6g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6gd.large	2	2	1	1、2	1
r6gd.xlarge	4	4	1	1、2、3、4	1
r6gd.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
r6gd.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6gd.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6gd.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6gd.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
r6i.large	2	1	2	1	1、2
r6i.xlarge	4	2	2	1、2	1、2
r6i.2xlarge	8	4	2	2、4	1、2
r6i.4xlarge	16	8	2	2、4、6、8	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
r6i.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
r6i.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	1、2
r6i.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	1、2
r6i.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48	1、2
r6i.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48、50、52、54、56、58、60、62、64	1、2
r6idn.large	2	1	2	1	1、2
r6idn.xlarge	4	2	2	1、2	1、2
r6idn.2xlarge	8	4	2	1、2、3、4	1、2
r6idn.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
r6idn.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16	1、2
r6idn.12xlarge	48	24	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24	1、2
r6idn.16xlarge	64	32	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32	1、2
r6idn.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48	1、2
r6idn.32xlarge	128	64	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48、50、52、54、56、58、60、62、64	1、2
r6in.large	2	1	2	1	1、2
r6in.xlarge	4	2	2	1、2	1、2
r6in.2xlarge	8	4	2	1、2、3、4	1、2
r6in.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
r6in.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16	1、2
r6in.12xlarge	48	24	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24	1、2
r6in.16xlarge	64	32	2	1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26、27、28、29、30、31、32	1、2
r6in.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48	1、2
r6in.32xlarge	128	64	2	4、6、8、10、12、14、16、18、20、22、24、26、28、30、32、34、36、38、40、42、44、46、48、50、52、54、56、58、60、62、64	1、2
r6id.large	2	1	2	1	1、2
r6id.xlarge	4	2	2	1、2	1、2
r6id.2xlarge	8	4	2	2、4	1、2
r6id.4xlarge	16	8	2	2、4、6、8	1、2
r6id.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
r6id.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、24	1、2
r6id.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、24、26、28、30、32	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
r6id.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	
r6id.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	
r7g.large	2	2	1	1、2	1
r7g.xlarge	4	4	1	1、2、3、4	1
r7g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	
r7g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
r7g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
r7g.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
r7g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
u-3tb1.56xlarge	224	112	2	4、8、12、16、20、24、28、32、36、40、44	
u-6tb1.56xlarge	224	224	1	8、16、24、32、40、48、56、64、72、80、88	
u-6tb1.112xlarge	448	224	2	8、16、24、32、40、48、56、64、72、80、88	
u-9tb1.112xlarge	448	224	2	8、16、24、32、40、48、56、64、72、80、88	
u-12tb1.112xlarge	448	224	2	8、16、24、32、40、48、56、64、72、80、88	
x1.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	
x1.32xlarge	128	64	2	4、8、12、16、20、24、28、32、36、40、44	
x2gd.large	2	2	1	1、2	1
x2gd.xlarge	4	4	1	1、2、3、4	1
x2gd.2xlarge	8	8	1	1、2、3、4、5、6、7、8	
x2gd.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
x2gd.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
x2gd.12xlarge	48	48	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
x2gd.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	
x2idn.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	
x2idn.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	
x2idn.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	
x2iedn.xlarge	4	2	2	1、2	1、2
x2iedn.2xlarge	8	4	2	2、4	1、2
x2iedn.4xlarge	16	8	2	2、4、6、8	1、2
x2iedn.8xlarge	32	16	2	2、4、6、8、10、12、14、16	

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
x2iedn.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
x2iedn.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
x2iedn.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
x2iezn.2xlarge	8	4	2	2、4	1、2
x2iezn.4xlarge	16	8	2	2、4、6、8	1、2
x2iezn.6xlarge	24	12	2	2、4、6、8、10、12	1、2
x2iezn.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
x2iezn.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
x1e.xlarge	4	2	2	1、2	1、2
x1e.2xlarge	8	4	2	1、2、3、4	1、2
x1e.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
x1e.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
x1e.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
x1e.32xlarge	128	64	2	4、8、12、16、20、24、28、32、36、40、44	1、2
z1d.large	2	1	2	1	1、2
z1d.xlarge	4	2	2	1、2	1、2
z1d.2xlarge	8	4	2	2、4	1、2
z1d.3xlarge	12	6	2	2、4、6	1、2
z1d.6xlarge	24	12	2	2、4、6、8、10、12	1、2
z1d.12xlarge	48	24	2	4、6、8、10、12、14、16、18、20、22、24	1、2

存储优化型实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
d2.xlarge	4	2	2	1、2	1、2
d2.2xlarge	8	4	2	1、2、3、4	1、2
d2.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
d2.8xlarge	36	18	2	2、4、6、8、10、12、14、16、18	1、2
d3.xlarge	4	2	2	1、2	1、2
d3.2xlarge	8	4	2	2、4	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
d3.4xlarge	16	8	2	2、4、6、8	1、2
d3.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	1、2
d3en.xlarge	4	2	2	1、2	1、2
d3en.2xlarge	8	4	2	2、4	1、2
d3en.4xlarge	16	8	2	2、4、6、8	1、2
d3en.6xlarge	24	12	2	2、4、6、8、10、11、12	1、2
d3en.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	1、2
d3en.12xlarge	48	24	2	2、4、6、8、10、11、12、14、16、18、20、22、2	1、2
h1.2xlarge	8	4	2	1、2、3、4	1、2
h1.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
h1.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
h1.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、2	1、2
i2.xlarge	4	2	2	1、2	1、2
i2.2xlarge	8	4	2	1、2、3、4	1、2
i2.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
i2.8xlarge	32	16	2	2、4、6、8、10、11、12、14、16	1、2
i3.large	2	1	2	1	1、2
i3.xlarge	4	2	2	1、2	1、2
i3.2xlarge	8	4	2	1、2、3、4	1、2
i3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
i3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
i3.16xlarge	64	32	2	2、4、6、8、10、11、12、14、16、18、20、22、2	1、2
i3en.large	2	1	2	1	1、2
i3en.xlarge	4	2	2	1、2	1、2
i3en.2xlarge	8	4	2	2、4	1、2
i3en.3xlarge	12	6	2	2、4、6	1、2
i3en.6xlarge	24	12	2	2、4、6、8、10、11、12	1、2
i3en.12xlarge	48	24	2	2、4、6、8、10、11、12、14、16、18、20、22、2	1、2
i3en.24xlarge	96	48	2	2、4、6、8、10、11、12、14、16、18、20、22、2	1、2
i4i.large	2	1	2	1	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
i4i.xlarge	4	2	2	1、2	1、2
i4i.2xlarge	8	4	2	1、2、3、4	1、2
i4i.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
i4i.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
i4i.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
i4i.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
im4gn.large	2	2	1	1、2	1
im4gn.xlarge	4	4	1	1、2、3、4	1
im4gn.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
im4gn.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
im4gn.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
im4gn.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1、2	1
is4gen.xlarge	4	4	1	1、2、3、4	1
is4gen.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
is4gen.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
is4gen.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1

加速计算实例

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
dl1.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
f1.2xlarge	8	4	2	1、2、3、4	1、2
f1.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
f1.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
g2.2xlarge	8	4	2	1、2、3、4	1、2
g2.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
g3.4xlarge	16	8	2	1、2、3、4、5、6、7、8	1、2
g3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
g3.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
g4ad.xlarge	4	2	2	2	1、2
g4ad.2xlarge	8	4	2	2、4	1、2
g4ad.4xlarge	16	8	2	2、4、8	1、2
g4ad.8xlarge	32	16	2	2、4、8、16	1、2
g4ad.16xlarge	64	32	2	2、4、8、16、32	1、2
g4dn.xlarge	4	2	2	2	1、2
g4dn.2xlarge	8	4	2	2、4	1、2
g4dn.4xlarge	16	8	2	2、4、6、8	1、2
g4dn.8xlarge	32	16	2	2、4、6、8、10、12、14、16	1、2
g4dn.12xlarge	48	24	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
g4dn.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
g5g.xlarge	4	4	1	1、2、3、4	1
g5g.2xlarge	8	8	1	1、2、3、4、5、6、7、8	1
g5g.4xlarge	16	16	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
g5g.8xlarge	32	32	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
g5g.16xlarge	64	64	1	1、2、3、4、5、6、7、8、9、10、11、12、13	1
inf1.xlarge	4	2	2	2	1、2
inf1.2xlarge	8	4	2	2、4	1、2
inf1.6xlarge	24	12	2	2、4、6、8、10、12	1
inf1.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
p2.xlarge	4	2	2	1、2	1、2
p2.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
p2.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
p3.2xlarge	8	4	2	1、2、3、4	1、2
p3.8xlarge	32	16	2	1、2、3、4、5、6、7、8、9、10、11、12、13	1、2
p3.16xlarge	64	32	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
p3dn.24xlarge	96	48	2	4、6、8、10、12、14、16、18、20、22、24、	1、2
p4d.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
p4de.24xlarge	96	48	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2

实例类型	默认 vCPU	默认 CPU 核心数	默认每核心线程数	有效的 CPU 核心	每个核心的有效线程
trn1.2xlarge	8	4	2	2、4	1、2
trn1.32xlarge	128	64	2	2、4、6、8、10、12、14、16、18、20、22、2	1、2
vt1.3xlarge	12	6	2	6	1、2
vt1.6xlarge	24	12	2	6、12	1、2
vt1.24xlarge	96	48	2	6、12、48	1、2

指定实例的 CPU 选项

可以在实例启动期间指定 CPU 选项。

以下示例介绍了如何在使用启动实例向导和 run-instances Amazon CLI 命令时指定 CPU 选项。您还可以使用启动模板 (p. 588)来指定 CPU 选项。如果使用 Amazon EC2 控制台，启动模板屏幕当前不提供用于指定 CPU 选项的字段，但是您可以使用 create-launch-template Amazon CLI 命令指定 CPU 选项。对于 EC2 机群或竞价型实例集，您必须在启动模板中指定 CPU 选项。

以下示例适用于 r4.4xlarge 实例类型，该实例类型具有以下默认值 (p. 731)：

- 默认 CPU 核心数：8
- 默认每核心线程数：2
- 默认 vCPU：16 (8 * 2)
- 有效的 CPU 核心数：1、2、3、4、5、6、7、8
- 有效的每核心线程数：1、2

禁用多线程

要禁用多线程技术，请为每个内核指定一个线程。

New console

在实例启动期间禁用多线程技术

1. 按照 快速启动实例 (p. 576) 程序进行操作并根据需要配置实例。
2. 展开高级详细信息，然后选中指定 CPU 选项复选框。
3. 对于 Core count (内核数)，选择所需的 CPU 内核数量。在此示例中，要为 r4.4xlarge 实例指定默认 CPU 内核数，请选择 8。
4. 要禁用多线程技术，请为每内核线程数选择 1。
5. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

Old console

在实例启动期间禁用多线程技术

1. 按照使用旧的启动实例向导启动实例 (p. 583)过程操作。
2. 在 Configure Instance Details (配置实例详细信息) 页面上，为 CPU options (CPU 选项) 选择 Specify CPU options (指定 CPU 选项)。

3. 对于 Core count (内核数)，选择所需的 CPU 内核数量。在此示例中，要为 r4.4xlarge 实例指定默认 CPU 内核数，请选择 8。
4. 要禁用多线程技术，请为每内核线程数选择 1。
5. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。

Amazon CLI

在实例启动期间禁用多线程技术

使用 run-instances Amazon CLI 命令，并将 1 参数的 ThreadsPerCore 值指定为 --cpu-options。对于 CoreCount，请指定 CPU 内核的数量。在此示例中，要为 r4.4xlarge 实例指定默认 CPU 内核数，请指定值 8。

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r4.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

指定自定义 vCPU 数量

您可以为实例自定义 CPU 内核数和每个内核的线程数。

以下示例启动一个具有六个 vCPU 的 r4.4xlarge 实例。

New console

在实例启动期间指定自定义 vCPU 数量

1. 按照 快速启动实例 (p. 576) 程序进行操作并根据需要配置实例。
2. 展开高级详细信息，然后选中指定 CPU 选项复选框。
3. 要获得六个 vCPU，请指定三个 CPU 内核并为每个内核指定两个线程，如下所示：
   - 对于 Core count (内核数)，选择 3。
   - 对于 Threads per core (每内核线程数)，选择 2。
4. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。有关更多信息，请参阅使用新启动实例向导启动实例 (p. 575)。

Old console

在实例启动期间指定自定义 vCPU 数量

1. 按照使用旧的启动实例向导启动实例 (p. 583)过程操作。
2. 在 Configure Instance Details (配置实例详细信息) 页面上，为 CPU options (CPU 选项) 选择 Specify CPU options (指定 CPU 选项)。
3. 要获得六个 vCPU，请指定三个 CPU 内核并为每个内核指定两个线程，如下所示：
   - 对于 Core count (内核数)，选择 3。
   - 对于 Threads per core (每内核线程数)，选择 2。
4. 根据向导的提示继续。检查完核查实例启动页面上的选项后，选择启动。有关更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。

Amazon CLI

在实例启动期间指定自定义 vCPU 数量

使用 run-instances Amazon CLI 命令，并在 `--cpu-options` 参数中指定 CPU 内核数和线程数。可以指定三个 CPU 核心并为每个核心指定两个线程，从而获得六个 vCPU。

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r4.4xlarge \
    --cpu-options "CoreCount=3,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

或者，也可以通过指定六个 CPU 核心和为每个核心指定一个线程（禁用多线程技术）来获得六个 vCPU：

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r4.4xlarge \
    --cpu-options "CoreCount=6,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

查看实例的 CPU 选项

您可以在 Amazon EC2 控制台中查看现有实例的 CPU 选项，也可以通过使用 Amazon CLI 描述实例来查看。

Console

使用控制台查看实例的 CPU 选项

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择实例，然后选择实例。
3. 在详细信息选项卡中的主机和置放群组下，找到 vCPU 数量。

Amazon CLI

查看实例的 CPU 选项 (Amazon CLI)

可以使用 describe-instances 命令。

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
```

```
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

在返回的输出中，CoreCount 字段指示实例的核心数。ThreadsPerCore 字段指示每核心线程数。

或者，也可以连接实例并使用工具（例如 lscpu）查看实例的 CPU 信息。

可以使用 Amazon Config 记录、评估、审计实例的配置更改，包括终止的实例。有关更多信息，请参阅 Amazon Config 开发人员指南中的 Amazon Config 入门

更改 Amazon Linux 实例的主机名

当您将实例启动到私有 VPC 中时，Amazon EC2 会分配一个来宾操作系统主机名。Amazon EC2 分配的主机名类型取决于您的子网设置。有关 EC2 主机名的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。

配置为使用 IPv4 地址的基于 IP 的命名的 EC2 实例的典型的 Amazon EC2 私有 DNS 名称如下所示：ip-12-34-56-78.us-west-2.compute.internal，其中包含内部域、服务（在此示例中为 compute）、区域和某种形式的私有 IPv4 地址。当您登录实例时，Shell 提示符处显示此主机名的一部分 (例如，ip-12-34-56-78)。每次停止和重新启动 Amazon EC2 实例时 (除非您使用的是弹性 IP 地址)，公有 IPv4 地址都会改变，而且公有 DNS 名称、系统主机名和 Shell 提示符也会改变。

Important

此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

更改系统主机名

如果为实例的 IP 地址注册了公用 DNS 名称 (如 webserver.mydomain.com)，则可以设置系统主机名，以便实例将自己标识为该域的一部分。这还会更改 Shell 提示符，以便它显示此名称的第一部分，而不是 Amazon 提供的主机名（例如，ip-12-34-56-78）。如果没有注册公用 DNS 名，还是可以更改主机名，但过程略有差异。

为使主机名持续更新，您必须确认 preserve_hostname cloud-init 设置已设为 true。您可以运行以下命令来编辑或添加此设置：

```
sudo vi /etc/cloud/cloud.cfg
```

如果未列出 preserve_hostname 设置，请在文件末尾添加以下文本行：

```
preserve_hostname: true
```

将系统主机名更改为公用 DNS 名称

如果已注册了公用 DNS 名称，请执行此过程。

1. • 对于 Amazon Linux 2：使用 hostnamectl 命令设置主机名以反映完全限定域名（例如 **webserver.mydomain.com**）。

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.mydomain.com
```

- 对于 Amazon Linux AMI：在您的实例上，使用常用的文本编辑器打开 /etc/sysconfig/network 配置文件，更改 HOSTNAME 条目以反映完全限定域名（例如 **webserver.mydomain.com**）。

```
HOSTNAME=webserver.mydomain.com
```

2. 重启实例以接受新主机名。

```
[ec2-user ~]$ sudo reboot
```

或者，您也可以使用 Amazon EC2 控制台重启（在实例页面上，选择实例，然后依次选择实例状态、重启实例）。

3. 登录实例，验证主机名是否已更新。提示符应显示新主机名（直到第一个“.”），hostname 命令应显示完全限定域名。

```
[ec2-user@webserver ~]$ hostname
webserver.mydomain.com
```

在无公用 DNS 名称的情况下更改系统主机名

1. - 对于 Amazon Linux 2：使用 hostnamectl 命令设置主机名以反映所需的系统主机名（例如 **webserver**）。

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.localdomain
```

- 对于 Amazon Linux AMI：在您的实例上，使用常用的文本编辑器打开 /etc/sysconfig/network 配置文件，更改 HOSTNAME 条目以反映所需的系统主机名（例如 **webserver**）。

```
HOSTNAME=webserver.localdomain
```

2. 在您常用的文本编辑器中打开 /etc/hosts 文件，更改以 **127.0.0.1** 开始的条目，以匹配以下示例，替换为您自己的主机名。

```
127.0.0.1 webserver.localdomain webserver localhost4 localhost4.localdomain4
```

3. 重启实例以接受新主机名。

```
[ec2-user ~]$ sudo reboot
```

或者，您也可以使用 Amazon EC2 控制台重启（在实例页面上，选择实例，然后依次选择实例状态、重启实例）。

4. 登录实例，验证主机名是否已更新。提示符应显示新主机名（直到第一个“.”），hostname 命令应显示完全限定域名。

```
[ec2-user@webserver ~]$ hostname
webserver.localdomain
```

您还可以实施更多的编程解决方案，例如指定用户数据以配置您的实例。如果您的实例是自动扩缩组的一部分，您可以使用生命周期挂钩定义用户数据。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的启动时在 Linux 实例上运行命令和用于实例启动的生命周期挂钩。

在不影响主机名的情况下更改 Shell 提示符

如果不需要修改实例的主机名，但是希望显示比 **webserver** 提供的专用名称（例如 Amazon）更有用的系统名称（如 ip-12-34-56-78），您可以编辑 Shell 提示符配置文件，以显示系统别名，而不是主机名。

将 Shell 提示符更改为主机别名

1. 在 /etc/profile.d 中创建一个文件，用于将称为 NICKNAME 的环境变量设置为要在 Shell 提示符中显示的值。例如，若要将系统别名设置为 **webserver**，请运行以下命令。

   ```
   [ec2-user ~]$ sudo sh -c 'echo "export NICKNAME=webserver" > /etc/profile.d/prompt.sh'
   ```

2. 使用您常用的文本编辑器（例如 /etc/bashrc 或 /etc/bash.bashrc）打开 vim (Red Hat) 或 nano (Debian/Ubuntu) 文件。您需要在编辑器命令中使用 sudo，因为 /etc/bashrc 和 /etc/bash.bashrc 归 root 所有。
3. 编辑文件，将 Shell 提示符变量 (PS1) 更改为显示别名而不是主机名。在 /etc/bashrc 或 /etc/bash.bashrc 中查找以下设置 Shell 提示符的行（为了上下文需要，下面多显示了几行；查找以 ["$PS1" 开头的行）：

   ```
   # Turn on checkwinsize
   shopt -s checkwinsize
   [ "$PS1" = "\\s-\\v\\$ " ] && PS1="[\u@\h \W]\\$ "
   # You might want to have e.g. tty in prompt (e.g. more virtual machines)
   # and console windows
   ```

   将该行中的 \h (hostname 的符号) 更改为 NICKNAME 变量的值。

   ```
   # Turn on checkwinsize
   shopt -s checkwinsize
   [ "$PS1" = "\\s-\\v\\$ " ] && PS1="[\u@$NICKNAME \W]\\$ "
   # You might want to have e.g. tty in prompt (e.g. more virtual machines)
   # and console windows
   ```

4. (可选) 要将 Shell 窗口上的标题设置为新别名，请完成以下步骤。

   a. 创建一个名为的文件 /etc/sysconfig/bash-prompt-xterm。

      ```
      [ec2-user ~]$ sudo touch /etc/sysconfig/bash-prompt-xterm
      ```

   b. 使用以下命令使该文件可执行。

      ```
      [ec2-user ~]$ sudo chmod +x /etc/sysconfig/bash-prompt-xterm
      ```

   c. 在您常用的文本编辑器（如 /etc/sysconfig/bash-prompt-xterm 或 vim）中打开 nano 文件。您需要在编辑器命令中使用 sudo，因为 /etc/sysconfig/bash-prompt-xterm 归 root 所有。

   d. 将以下行添加到该文件。

      ```
      echo -ne "\033]0;${USER}@${NICKNAME}:${PWD/#$HOME/~}\007"
      ```

5. 注销，再重新登录，以接受新别名值。

在其他 Linux 发行版上更改主机名

此页面上的过程仅适用于 Amazon Linux。有关其他 Linux 发行版的更多信息，请参阅其特定文档和下列文章：

- 如何为运行 RHEL 7 或 Centos 7 的私有 Amazon EC2 实例分配静态主机名？

在 Amazon Linux 实例上设置动态 DNS

当您启动 EC2 实例时，系统会为其分配公有 IP 地址和公有域名系统（DNS）名称，您可以通过互联网访问这些地址和名称。因为 Amazon Web Services 域中有非常多主机，所以这些公用名称必须足够长才能使每个名称保持唯一。典型的 Amazon EC2 公用 DNS 名称如下所示：`ec2-12-34-56-78.us-west-2.compute.amazonaws.com`，其中名称由 Amazon Web Services 域、服务（在此示例中为 `compute`）、Amazon Web Services 区域 和公有 IP 地址的形式组成。

动态 DNS 服务在其域区域中提供自定义主机名，这些主机名便于记忆，也与主机的使用案例更为相关。其中一些服务也是免费的。您可以对 Amazon EC2 使用动态 DNS 提供商，可以将实例配置为每次实例启动时都更新与公用 DNS 名称关联的 IP 地址。有许多不同的提供商可以选择，本指南不介绍有关如何选择提供商以及如何向它们注册名称的具体详细信息。

> **Important**
>
> 此信息适用于 Amazon Linux。有关其他发布版本的信息，请参阅特定于该版本的文档。

对 Amazon EC2 使用动态 DNS

1. 向动态 DNS 服务提供商注册并利用其服务注册公用 DNS 名称。这个过程使用来自 noip.com/free 的免费服务作为示例。
2. 配置动态 DNS 更新客户端。有了动态 DNS 服务提供商并且使用其服务注册了公用 DNS 名称后，将 DNS 名称指向实例的 IP 地址。很多提供商（包括 noip.com）允许您从您在其网站上的账户页手动执行此操作，不过很多也支持软件更新客户端。如果更新客户端正在 EC2 实例上运行，则每次 IP 地址更改（如关机和重启后）都会更新动态 DNS 记录。在本例中，将安装 noip2 客户端，该客户端利用 noip.com 提供的服务。

   a. 启用 Extra Packages for Enterprise Linux (EPEL) 存储库，以获取对 noip2 客户端的访问权。

      > **Note**
      >
      > 默认情况下，Amazon Linux 实例安装有 EPEL 存储库的 GPG 密钥和存储库信息；但是，Red Hat 和 CentOS 实例必须先安装 `epel-release` 软件包，然后您才能启用 EPEL 存储库。有关更多信息以及要下载此软件包的最新版本，请参阅 https://fedoraproject.org/wiki/EPEL。

      - 对于 Amazon Linux 2

        ```
        [ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
        ```

      - 对于 Amazon Linux AMI

        ```
        [ec2-user ~]$ sudo yum-config-manager --enable epel
        ```

   b. 安装 `noip` 软件包。

      ```
      [ec2-user ~]$ sudo yum install -y noip
      ```

   c. 创建配置文件。在提示时输入登录名和密码信息，并回答后续问题以配置客户端。

      ```
      [ec2-user ~]$ sudo noip2 -C
      ```

3. 启用 noip 服务。

   - 对于 Amazon Linux 2

```
[ec2-user ~]$ sudo systemctl enable noip.service
```

- 对于 Amazon Linux AMI

```
[ec2-user ~]$ sudo chkconfig noip on
```

4. 启动 noip 服务。

   - 对于 Amazon Linux 2

   ```
   [ec2-user ~]$ sudo systemctl start noip.service
   ```

   - 对于 Amazon Linux AMI

   ```
   [ec2-user ~]$ sudo service noip start
   ```

   该命令启动客户端，读取先前创建的配置文件 (`/etc/no-ip2.conf`)，并且更新您选择的公用 DNS 名称的 IP 地址。

5. 验证更新客户端是否已为动态 DNS 名称设置了正确的 IP 地址。等待几分钟使 DNS 记录进行更新，然后尝试使用您在此过程中配置的公有 DNS 名称通过 SSH 连接到实例。

启动时在 Linux 实例上运行命令

当您在 Amazon EC2 中启动实例时，您可以选择将用户数据传递到可用于执行常见自动配置任务甚至在实例启动后运行脚本的实例。您可以将两类用户数据传递到 Amazon EC2：Shell 脚本和 cloud-init 指令。您还可以将此数据以纯文本、文件（这非常适合通过命令行工具启动实例）或者 base64 编码文本（用于 API 调用）的形式传递到启动实例向导中。

如果您对更复杂的自动化方案感兴趣，可以考虑使用 Amazon CloudFormation 或 Amazon OpsWorks。有关更多信息，请参阅下列内容：

- 《Amazon CloudFormation 用户指南》中的使用 Amazon CloudFormation 在 Amazon EC2 上部署应用程序。
- Amazon OpsWorks 用户指南。

有关在启动时在 Windows 实例上运行命令的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的启动时在您的 Windows 实例上运行命令和管理 Windows 实例配置。

在以下示例中，在 Amazon Linux 2 上安装 LAMP Web 服务器 (p. 24)中的命令转换成了 Shell 脚本和一组在实例启动时运行的 cloud-init 指令。在每个示例中，以下任务都根据用户数据执行：

- 更新发行版软件包。
- 安装必要的 Web 服务器、php 和 `mariadb` 程序包。
- 通过 `httpd` 启动和打开 systemctl 服务。
- `ec2-user` 将添加到 apache 组。
- 为 Web 目录以及其中的文件设置适当的所有权和文件权限。
- 创建简单网页来测试 Web 服务器和 PHP 引擎。

目录

- 先决条件 (p. 749)

- 用户数据和 Shell 脚本 (p. 749)
- 用户数据和控制台 (p. 749)
- 用户数据和 cloud-init 指令 (p. 751)
- 用户数据和 Amazon CLI (p. 752)
- 将 Shell 脚本和 cloud-init 指令组合使用 (p. 753)

先决条件

本主题中的示例假定以下内容：

- 您的实例具有可从互联网访问的公用 DNS 名称。有关更多信息，请参阅 Network settings (网络设置) (p. 579) 部分和 创建安全组 (p. 6) 中的Auto-assign Public IP（自动分配公有 IP）。
- 与您的实例关联的安全组将被配置为允许 SSH（端口 22）流量，以便您可以连接到该实例，以查看输出日志文件。有关更多信息，请参阅创建安全组 (p. 6)。
- 您的实例将使用 Amazon Linux 2 AMI 启动。这些指令适合与 Amazon Linux 2 一起使用，这些命令和指令可能不适用于其他 Linux 发行版。有关其他发行版的更多信息，如它们对 cloud-init 的支持，请参阅各自的具体文档。

用户数据和 Shell 脚本

如果您熟悉 Shell 脚本编写，要在启动时将指令发送到实例，这是最简单、最完整的方式。在启动时添加这些任务会增加启动实例所需的时间。您应多等待几分钟让这些任务完成，然后测试用户脚本是否已成功完成。

> **Important**
>
> 默认情况下，用户数据脚本和 cloud-init 指令仅在首次启动实例时在引导周期内运行。您可以更新您的配置，以确保您的用户数据脚本和 cloud-init 指令在每次重新启动实例时都会运行。有关更多信息，请参阅Amazon知识中心中的如何利用用户数据在每次重新启动 Amazon EC2 Linux 实例时自动运行脚本？。

用户数据 Shell 脚本必须以 #! 字符以及要读取脚本的解释器的路径（通常为 /bin/bash））开始。有关 Shell 脚本的精彩介绍，请参阅 Linux 文档项目 (tldp.org) 中的 BASH 编程操作方法。

作为用户数据输入的脚本是作为根用户加以运行的，因此在脚本中不使用 sudo 命令。请注意，您创建的任何文件都将归根用户所有；如果您需要非根用户具有文件访问权限，应在脚本中相应地修改权限。此外，这是因为脚本不交互运行，所以无法包含要求用户反馈的命令（如 yum update，无 -y 标志）。

如果您使用 Amazon API（包括 Amazon CLI），则在启动实例时必须使用实例配置文件。实例配置文件提供用户数据脚本发出 API 调用所需的适当 Amazon 凭证。有关更多信息，请参阅 IAM 用户指南 中的使用实例配置文件。您分配给 IAM 角色的权限取决于您使用 API 调用的服务。有关更多信息，请参阅 Amazon EC2 的 IAM 角色。

cloud-init 输出日志文件捕获控制台输出，因此，如果实例的行为不符合您的预期，可在启动后方便地调试脚本。要查看日志文件，请连接到实例 (p. 644)并打开 `/var/log/cloud-init-output.log`。

在处理用户数据脚本时，该脚本将复制到 `/var/lib/cloud/instances/instance-id/` 目录并从该目录运行。脚本在运行后无法删除。请在从实例创建 AMI 之前务必删除 `/var/lib/cloud/instances/instance-id/` 中的用户数据脚本。否则，该脚本将存在于从 AMI 启动的任何实例上的此目录中。

用户数据和控制台

您可在启动实例时指定实例用户数据。如果实例的根卷是 EBS 卷，您还可以停止实例并更新其用户数据。

启动时指定实例用户数据

按照启动实例 (p. 577)的程序进行操作。User data（用户数据）字段位于启动实例向导的 高级详细信息 (p. 581) 部分。在 User data（用户数据）字段中输入您的 Shell 脚本，然后完成实例启动程序。

在下面的示例脚本中，脚本将创建并配置我们的 Web 服务器。

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

让实例有足够的时间启动和执行脚本中的命令，然后查看脚本是否完成了预期的任务。

对于我们的示例，在 Web 浏览器中输入脚本创建的 PHP 测试文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

您应该会看到 PHP 信息页面。如果您无法看到 PHP 信息页，请检查所用的安全组是否包含允许 HTTP (端口 80) 通信的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

（可选）如果您的脚本没有完成您期望的任务，或者如果您只是想验证您的脚本是否已完成且没有错误，请连接到实例 (p. 644)，检查 cloud-init 输出日志文件 (`/var/log/cloud-init-output.log`)，然后查找输出中的错误消息。

对于其他调试信息，您可以使用以下指令创建包含 cloud-init 数据部分的 Mime 分段存档：

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

此指令将您脚本的命令输出发送到 `/var/log/cloud-init-output.log`。有关 cloud-init 数据格式以及创建 Mime 分段存档的更多信息，请参阅 cloud-init 格式。

查看和更新实例用户数据

要更新实例用户数据，您必须先停止实例。如果实例正在运行，那么您可以查看用户数据，但不能进行修改。

> Warning
>
> 当您停止某个实例时，任何实例存储卷上的数据都将被擦除。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

修改实例用户数据

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择实例状态、停止实例。如果此选项处于禁用状态，则表示实例已停止，或者其根设备是实例存储卷。
4. 当系统提示您确认时，选择 Stop。停止实例可能需要几分钟时间。
5. 在实例仍被选中的情况下，依次选择操作、实例设置和编辑用户数据。

6. 根据需要修改用户数据，然后选择保存。
7. 开启实例。开启实例后，新的用户数据将在实例上可见；但不会运行用户数据脚本。

用户数据和 cloud-init 指令

cloud-init 程序包在启动时配置新 Amazon Linux 实例的特定方面；最值得注意的是，它为 ec2-user 配置 `.ssh/authorized_keys` 文件，以便您使用自己的私有密钥登录。有关 cloud-init 软件包为 Amazon Linux 实例执行的配置任务的更多信息，请参阅 cloud-init (p. 215)。

可在启动时将 cloud-init 用户指令传递给实例，方式与传递脚本相同，只是语法不同。有关 cloud-init 的更多信息，请参阅 http://cloudinit.readthedocs.org/en/latest/index.html。

> **Important**
>
> 默认情况下，用户数据脚本和 cloud-init 指令仅在首次启动实例时在引导周期内运行。您可以更新您的配置，以确保您的用户数据脚本和 cloud-init 指令在每次重新启动实例时都会运行。有关更多信息，请参阅Amazon知识中心中的如何利用用户数据在每次重新启动 Amazon EC2 Linux 实例时自动运行脚本？。

在启动时添加这些任务会增加启动实例所需的时间。您应多等待几分钟让这些任务完成，然后测试用户数据指令是否已完成。

使用用户数据将 cloud-init 指令传递给实例

1. 按照启动实例 (p. 577)的程序进行操作。User data（用户数据）字段位于启动实例向导的 高级详细信息 (p. 581) 部分。在 User data（用户数据）字段中输入您的 cloud-init 指令文本，然后完成实例启动程序。

   在以下示例中，这些指令在 Amazon Linux 2 上创建并配置 Web 服务器。要将命令标识为 cloud-init 指令，顶部的 `#cloud-config` 行是必需的。

   ```
   #cloud-config
   repo_update: true
   repo_upgrade: all

   packages:
    - httpd
    - mariadb-server

   runcmd:
    - [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
    - systemctl start httpd
    - sudo systemctl enable httpd
    - [ sh, -c, "usermod -a -G apache ec2-user" ]
    - [ sh, -c, "chown -R ec2-user:apache /var/www" ]
    - chmod 2775 /var/www
    - [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
    - [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
    - [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
   ```

2. 让实例有足够的时间启动和运行用户数据中的指令，然后查看指令是否完成了预期的任务。

   对于此示例，在 Web 浏览器中输入指令创建的 PHP 测试文件的 URL。此 URL 是实例的公用 DNS 地址，后接正斜杠和文件名。

   ```
   http://my.public.dns.amazonaws.com/phpinfo.php
   ```

   您应该会看到 PHP 信息页面。如果您无法看到 PHP 信息页，请检查所用的安全组是否包含允许 HTTP (端口 80) 通信的规则。有关更多信息，请参阅向安全组添加规则 (p. 1311)。

3. （可选）如果您的指令没有完成您期望的任务，或者如果您只是想验证您的指令是否已完成且没有错误，请连接到实例 (p. 644)，检查输出日志文件 (/var/log/cloud-init-output.log)，然后查找输出中的错误消息。对于其他调试信息，您可以将以下行添加到指令：

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

此指令将 runcmd 输出发送到 /var/log/cloud-init-output.log。

用户数据和 Amazon CLI

您可以使用 Amazon CLI 指定、修改和查看实例的用户数据。有关使用实例元数据从实例查看用户数据的信息，请参阅检索实例用户数据 (p. 775)。

在 Windows 上，您可以使用 Amazon Tools for Windows PowerShell 而不是使用 Amazon CLI。有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的用户数据和 Tools for Windows PowerShell。

示例：启动时指定用户数据

要在启动实例时指定用户数据，请结合使用 run-instances 命令与 --user-data 参数。使用 run-instances，Amazon CLI 将对您的用户数据执行 base64 编码。

以下示例显示如何在命令行上指定字符串形式的脚本：

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data echo user data
```

以下示例显示如何使用文本文件指定脚本。请务必使用 file:// 前缀指定该文件。

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data file://my_script.txt
```

以下是具有 Shell 脚本的示例文本文件。

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

示例：修改停止的实例的用户数据

您可以使用 modify-instance-attribute 命令修改已停止的实例的用户数据。使用 modify-instance-attribute，Amazon CLI 不会对用户数据执行 base64 编码。

- 在 Linux 计算机上，使用 base64 命令对用户数据进行编码。

```
base64 my_script.txt >my_script_base64.txt
```

- 在 Windows 计算机上，使用 certutil 命令可对用户数据进行编码。您必须先删除第一行 (BEGIN CERTIFICATE) 和最后一行 (END CERTIFICATE)，然后才能将此文件用于 Amazon CLI。

```
certutil -encode my_script.txt my_script_base64.txt
notepad my_script_base64.txt
```

使用 --attribute 和 --value 参数可通过编码的文本文件指定用户数据。请务必使用 file:// 前缀指定该文件。

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData --
value file://my_script_base64.txt
```

示例：清除停止的实例的用户数据

要删除现有的用户数据，请按以下方式使用 modify-instance-attribute 命令：

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

示例：查看用户数据

要检索实例的用户数据，请使用 describe-instance-attribute 命令。使用 describe-instance-attribute，Amazon CLI 不会对用户数据执行 base64 解码。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData
```

以下是具有已进行 base64 编码的用户数据的示例输出。

```
{
    "UserData": {
        "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
    },
    "InstanceId": "i-1234567890abcdef0"
}
```

- 在 Linux 计算机上，使用 --query 选项获取已编码的用户数据和用于对该数据进行解码的 base64 命令。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" | base64 --decode
```

- 在 Windows 计算机上，使用 --query 选项获取已编码的用户数据和用于对该数据进行解码的 certutil 命令。请注意，编码的输出存储在一个文件中，解码的输出存储在另一个文件中。

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --output text --query "UserData.Value" >my_output.txt
certutil -decode my_output.txt my_output_decoded.txt
type my_output_decoded.txt
```

下面是示例输出。

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

将 Shell 脚本和 cloud-init 指令组合使用

默认情况下，一次只能在用户数据中包含一个内容类型。不过，您可以在 mime-multi part 文件中使用 text/cloud-config 和 text/x-shellscript，以便在用户数据中同时包含 Shell 脚本和 cloud-init 指令。

下面显示了 mime-multi part 的格式。

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
cloud-init directives

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
shell script commands
--//--
```

例如，以下用户数据包含了 cloud-init 指令和 bash Shell 脚本。cloud-init 指令会创建一个文件（`/test-cloudinit/cloud-init.txt`），然后将 `Created by cloud-init` 写入该文件。bash Shell 脚本会创建一个文件（`/test-userscript/userscript.txt`），然后将 `Created by bash shell script` 写入该文件。

```
Content-Type: multipart/mixed; boundary="//"
MIME-Version: 1.0

--//
Content-Type: text/cloud-config; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config
runcmd:
 - [ mkdir, /test-cloudinit ]
write_files:
 - path: /test-cloudinit/cloud-init.txt
   content: Created by cloud-init

--//
Content-Type: text/x-shellscript; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash
  mkdir test-userscript
  touch /test-userscript/userscript.txt
  echo "Created by bash shell script" >> /test-userscript/userscript.txt
--//--
```

实例元数据和用户数据

实例元数据 是有关您的实例的数据，可以用来配置或管理正在运行的实例。实例元数据分为[几类 (p. 776)]，例如，主机名、事件和安全组。

您也可以使用实例元数据访问您启动实例时指定的用户数据。例如，您可以指定参数以配置实例，或者包含简单的脚本。您可以构建通用 AMI，并使用用户数据修改启动时提供的配置文件。例如，如果您为各种小型

企业运行 Web 服务器，则这些企业可以使用相同的通用 AMI，并在启动时从您在用户数据中指定的 Amazon S3 存储桶中检索其内容。要随时添加新客户，请为客户创建一个存储桶，添加其内容，并使用在用户数据中为您的代码提供的唯一存储桶名称启动 AMI。如果您同时启动多个实例，则用户数据可供该预留中的所有实例使用。属于同一保留的每个实例具有唯一的 `ami-launch-index` 编号，从而允许您编写代码以控制要执行的操作。例如，第一台主机可能会选择将自己作为集群中的原始节点。有关详细的 AMI 启动示例，请参阅示例：AMI 启动索引值 (p. 783)。

EC2 实例还可包括动态数据，例如启动实例时生成的实例身份文档。有关更多信息，请参阅动态数据类别 (p. 783)。

> **Important**
>
> 虽然您只能从实例本身中访问实例元数据和用户数据，但并未使用身份验证或加密方法对数据进行保护。任何可以直接访问实例的人以及可能在实例上运行的任何软件都可以查看其元数据。因此，您不应将敏感数据（例如密码或长期保存的加密密钥）存储为用户数据。

> **Note**
>
> 本主题中的示例使用实例元数据服务（IMDS）的 IPv4 地址：`169.254.169.254`。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：`fd00:ec2::254`。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

目录

- 使用 IMDSv2 (p. 755)
- 配置实例元数据选项 (p. 760)
- 检索实例元数据 (p. 766)
- 处理实例用户数据 (p. 774)
- 检索动态数据 (p. 776)
- 实例元数据类别 (p. 776)
- 示例：AMI 启动索引值 (p. 783)
- 实例身份文档 (p. 786)
- 实例身份角色 (p. 808)

使用 IMDSv2

您可以使用以下其中一种方法，从正在运行的实例中访问实例元数据：

- 实例元数据服务版本 1 (IMDSv1) – 一种请求/响应方法
- 实例元数据服务版本 2 (IMDSv2) – 一种面向会话的方法

默认情况下，您可以使用 IMDSv1 和/或 IMDSv2。实例元数据服务根据以下条件区分 IMDSv1 和 IMDSv2 请求：对于任何给定请求，`PUT` 或 `GET` 标头（对于 IMDSv2 是唯一的）在该请求中是否存在。

您可以在每个实例上配置实例元数据服务（IMDS），以确保本地代码或用户必须使用 IMDSv2。在指定必须使用 IMDSv2 时，IMDSv1 不再起作用。有关如何配置实例以使用 IMDSv2 的信息，请参阅 配置实例元数据选项 (p. 760)。

有关 IMDSv2 的详细回顾，请参阅借助 EC2 实例元数据服务的增强功能，为开放式防火墙、反向代理和 SSRF 漏洞增加深度防御。

要检索实例元数据，请参阅检索实例元数据 (p. 766)。

主题

- 实例元数据服务版本 2 的工作原理 (p. 756)
- 转换为使用 实例元数据服务版本 2 (p. 757)
- 使用支持的 Amazon 开发工具包 (p. 759)

实例元数据服务版本 2 的工作原理

IMDSv2 使用面向会话的请求。对于面向会话的请求，您创建一个会话令牌以定义会话持续时间，该时间最少为 1 秒，最多为 6 小时。在指定的持续时间内，您可以将相同的会话令牌用于后续请求。在指定的持续时间到期后，您必须创建新的会话令牌以用于将来的请求。

> **Note**
>
> 本部分中的示例使用实例元数据服务（IMDS）的 IPv4 地址：`169.254.169.254`。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：`fd00:ec2::254`。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

以下示例使用 Linux Shell 脚本和 IMDSv2 检索顶级实例元数据项。示例：

- 使用 PUT 请求创建持续 6 小时（21600 秒）的会话令牌
- 将会话令牌标头存储在名为 TOKEN 的变量中
- 使用令牌请求顶级元数据项

您可以运行两个单独的命令，也可以将它们组合使用。

单独的命令

首先，使用以下命令生成令牌。

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"`
```

然后，通过令牌使用以下命令生成顶级元数据项。

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
meta-data/
```

组合命令

您可以存储令牌并组合命令。以下示例将上述两个命令组合在一起，并将会话令牌标头存储在名为 TOKEN 的变量中。

> **Note**
>
> 如果创建令牌时发生错误，则不会生成有效令牌，而会在变量中存储一条错误消息，该命令将不起作用。

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

在创建令牌后，您可以重复使用令牌，直到令牌过期。在以下示例命令（获取用于启动实例的 AMI 的 ID）中，将重复使用上一示例中的令牌（存储在 $TOKEN 中）。

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
meta-data/ami-id
```

在使用 IMDSv2 请求实例元数据时，请求必须包含以下内容：

1. 使用 PUT 请求启动到实例元数据服务的会话。PUT 请求返回一个令牌，该令牌必须包含在对实例元数据服务的后续 GET 请求中。需要具有该令牌才能使用 IMDSv2 访问元数据。
2. 将该令牌包含在对 IMDS 的所有 GET 请求中。如果将令牌使用设置为 `required`，没有有效令牌或令牌过期的请求将显示 `401 - Unauthorized` HTTP 错误代码。

- 令牌是实例特定的密钥。令牌在其他 EC2 实例上无效，如果尝试在生成令牌的实例外部使用，令牌将会被拒绝。
- PUT 请求必须包含一个标头，它以秒为单位指定令牌的生存时间 (TTL)，最多为 6 小时（21600 秒）。令牌表示一个逻辑会话。TTL 指定令牌的有效时间长度，因而指定会话的持续时间。
- 在令牌过期后，要继续访问实例元数据，您必须使用另一 PUT 创建新会话。
- 您可以选择在每个请求中重复使用令牌或创建新的令牌。对于少量请求，每次需要访问 IMDS 时生成令牌并立即使用可能会更容易。但为了提高效率，您可以为令牌指定更长的持续时间并重复使用令牌，而不必在每次需要请求实例元数据时都编写 PUT 请求。对并发令牌数量没有实际限制，每个令牌表示自己的会话。不过，IMDSv2 仍然受到正常 IMDS 连接和节流限制的制约。有关更多信息，请参阅查询限制 (p. 773)。

允许在 IMDSv2 实例元数据请求中使用 HTTP GET 和 HEAD 方法。如果 PUT 请求包含 X-Forwarded-For 标头，则会被拒绝。

默认情况下，PUT 请求的响应在 IP 协议级别的响应跃点数限制（生存时间）为 1。如果需要更大的跃点数限制，可使用 modify-instance-metadata-options Amazon CLI 命令进行调整。例如，您可能需要使用更大的跃点数限制，以便与实例上运行的容器服务保持向后兼容。有关更多信息，请参阅为现有实例修改实例元数据选项 (p. 763)。

转换为使用 实例元数据服务版本 2

如果迁移到 IMDSv2，我们建议您使用以下工具和转换途径。

主题

- 帮助转换为 IMDSv2 的工具 (p. 757)
- 要求 IMDSv2 的建议途径 (p. 758)

帮助转换为 IMDSv2 的工具

如果您的软件使用 IMDSv1，请使用以下工具帮助重新配置软件，以使用 IMDSv2。

Amazon 软件

最新版本的 Amazon CLI 和 Amazon SDK 均支持 IMDSv2。要使用 IMDSv2，请确保您的 EC2 实例具有最新版本的 CLI 和 SDK。有关更新 CLI 的信息，请参阅 Amazon Command Line Interface 用户指南中的安装、更新和卸载 Amazon CLI。

所有的 Amazon Linux 2 软件包都支持 IMDSv2。

有关支持 IMDSv2 的最低 Amazon 开发工具包版本，请参阅 使用支持的 Amazon 开发工具包 (p. 759)。

CloudWatch

IMDSv2 使用由令牌支持的会话，而 IMDSv1 不使用。MetadataNoToken CloudWatch 指标跟踪对使用 IMDSv1 的实例元数据服务（IMDS）的调用次数。通过查看该指标是否为零，您可以确定是否以及何时将所有软件升级为使用 IMDSv2。有关更多信息，请参阅实例指标 (p. 1003)。

EC2 API 和 CLI 更新

对于新实例，您可以使用 RunInstances API 以启动要求使用 IMDSv2 的新实例。有关更多信息，请参阅为新实例配置实例元数据选项 (p. 760)。

对于现有实例，您可以使用 ModifyInstanceMetadataOptions API 以要求使用 IMDSv2。有关更多信息，请参阅为现有实例修改实例元数据选项 (p. 763)。

为了要求在 Auto Scaling 组启动的所有新实例上使用 IMDSv2，您的 Auto Scaling 组可以使用启动模板或启动配置。当您创建启动模板或创建启动配置时，必须配置 MetadataOptions 参数以要求使

用 IMDSv2。自动扩缩组将使用新的启动模板或启动配置来启动新实例，但现有实例不受影响。对于自动扩缩组中的现有实例，您可以使用 ModifyInstanceMetadataOptions API 以要求在现有实例上使用 IMDSv2，或者终止实例，自动扩缩组将使用在新的启动模板或启动配置中定义的实例元数据选项设置启动新的替换实例。

使用默认配置 IMDSv2 的 AMI

启动实例时，您可以使用将 `ImdsSupport` 参数设置为 `v2.0` 的 AMI 启动该实例，从而自动将其配置为默认使用 IMDSv2（将 `HttpTokens` 参数设置为 `required`）。您可以在使用 register-image CLI 命令注册 AMI 时将 `ImdsSupport` 参数设置为 `v2.0`，也可以使用 modify-image-attribute CLI 命令修改现有的 AMI。有关更多信息，请参阅配置 AMI (p. 762)。

IAM policy 和 SCP

您可以使用 IAM policy 或 Amazon Organizations 服务控制策略（SCP）来控制用户，具体如下所示：

- 除非将实例配置为使用 IMDSv2，否则无法使用 RunInstances API 启动实例。
- 无法使用 ModifyInstanceMetadataOptions API 修改正在运行的实例以重新启用 IMDSv1。

IAM policy 或 SCP 必须包含以下 IAM 条件键：

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

如果 API 或 CLI 调用中的参数与包含该条件键的策略中指定的状态不一致，则 API 或 CLI 调用将失败并显示 `UnauthorizedOperation` 响应。

此外，您还可以选择额外的保护层以强制从 IMDSv1 更改为 IMDSv2。在与通过 EC2 角色凭证调用的 API 相关的访问管理层上，您可以在 IAM policy 或 Amazon Organizations 服务控制策略 (SCP) 中使用新的条件键。具体来说，通过在 IAM policy 中使用值为 `ec2:RoleDelivery` 的条件键 `2.0`，使用从 IMDSv1 获取的 EC2 角色凭证进行的 API 调用将会收到 `UnauthorizedOperation` 响应。通过使用 SCP 所需的该条件，可以更广泛地实现相同的效果。这会确保通过 IMDSv1 提供的凭证不能实际用于调用 API，因为任何不符合指定条件的 API 调用将会收到 `UnauthorizedOperation` 错误。

有关示例 IAM policies，请参阅 使用实例元数据 (p. 1266)。有关 SCP 的更多信息，请参阅《Amazon Organizations 用户指南》中的 服务控制策略。

要求 IMDSv2 的建议途径

在使用上述工具时，我们建议您按照以下途径转换为 IMDSv2。

步骤 1：在开始时

将在 EC2 实例上使用角色凭证的 SDK、CLI 和软件更新为与 IMDSv2 兼容的版本。有关更新 CLI 的信息，请参阅 Amazon Command Line Interface 用户指南中的升级到最新版本的 Amazon CLI。

然后，使用 IMDSv2 请求更改直接访问实例元数据的软件（换句话说，不使用开发工具包）。

第 2 步：跟踪转换进度

使用 CloudWatch 指标 `MetadataNoToken` 跟踪您的转换进度。此指标显示对实例上 IMDS 的 IMDSv1 调用次数。有关更多信息，请参阅实例指标 (p. 1003)。

第 3 步：当 IMDSv1 的使用量为零时

当 CloudWatch 指标 `MetadataNoToken` 记录的 IMDSv1 使用量为零时，表明您的实例已准备好完全转换到使用 IMDSv2。在此阶段，您可以执行以下操作：

- 新实例

  启动新实例时，您可以执行以下操作：

  - Amazon EC2 控制台：在启动实例向导中，将 Metadata accessible（可访问元数据）设置为 Enabled（已启用），将 Metadata version（元数据版本）设置为 V2 only (token required) [仅 V2（必须使用令牌）]。有关更多信息，请参阅在启动时配置实例 (p. 761)。
  - Amazon CLI：使用 run-instances CLI 命令指定仅使用 IMDSv2。
- 现有实例

  对于现有实例，您可以执行以下操作：
  - Amazon EC2 控制台：在实例页面上选择实例，然后依次选择操作、实例设置、修改实例元数据选项，对于 IMDSv2，选择必需。有关更多信息，请参阅要求使用 IMDSv2 (p. 764)。
  - Amazon CLI：使用 modify-instance-metadata-options CLI 命令指定仅使用 IMDSv2。

  您可以在正在运行的实例上修改实例元数据选项，并且修改后无需重新启动实例。

步骤 4：检查实例是否切换为 IMDSv2

您可以检查是否有任何实例尚未配置为要求使用 IMDSv2，换言之，IMDSv2 仍配置为 `optional`。如果仍有实例配置为 `optional`，则可通过重复上述步骤 3 (p. 758) 来修改实例元数据选项，以将 IMDSv2 配置为 `required`。

筛选实例：

- Amazon EC2 控制台：在实例页面，使用 IMDSv2 = 可选筛选条件来筛选实例。有关筛选的更多信息，请参阅 使用控制台筛选资源 (p. 1657)。您还可以查看 IMDSv2 对每个实例是必需的还是可选的：在首选项窗口中，打开 IMDSv2，以将 IMDSv2 列添加到实例表中。
- Amazon CLI：使用 describe-instances CLI 命令并按 `metadata-options.http-tokens = optional` 进行筛选，如下所示：

```
aws ec2 describe-instances --filters "Name=metadata-options.http-tokens,Values=optional"
 --query "Reservations[*].Instances[*].[InstanceId]" --output text
```

步骤 5：当所有实例已切换为 IMDSv2

`ec2:MetadataHttpTokens`、`ec2:MetadataHttpPutResponseHopLimit` 和 `ec2:MetadataHttpEndpoint` IAM 条件键可用于控制 RunInstances 和 ModifyInstanceMetadataOptions API 及相应 CLI 的使用。如果创建了策略，并且 API 调用中的参数与使用条件键的策略中指定的状态不匹配，API 或 CLI 调用将失败并显示 `UnauthorizedOperation` 响应。有关示例 IAM policies，请参阅 使用实例元数据 (p. 1266)。

使用支持的 Amazon 开发工具包

要使用 IMDSv2，EC2 实例必须使用支持 IMDSv2 的 Amazon 开发工具包版本。所有 Amazon 开发工具包的最新版本均支持使用 IMDSv2。

> **Important**
>
> 我们建议您及时了解开发工具包版本，以了解其最新功能、安全更新和底层依赖项。不建议继续使用不受支持的开发工具包版本，但是否继续使用由您自行决定。有关更多信息，请参阅《Amazon SDK 和工具参考指南》中的 Amazon SDK 和工具维护策略。

以下是支持使用 IMDSv2 的最低版本：

- Amazon CLI – 1.13.23
- Amazon SDK for .NET – 3.3.634.1
- Amazon SDK for C++ – 1.7.229
- Amazon SDK for Go – 1.25.38

- Amazon SDK for Go v2 – 0.19.0
- Amazon SDK for Java – 1.11.678
- Amazon SDK for Java 2.x – 2.10.21
- 适用于 Node.js 中 JavaScript 的 Amazon 开发工具包 – 2.722.0
- Amazon SDK for PHP – 3.147.7
- Amazon SDK for Python (Boto) – 1.13.23
- Amazon SDK for Python (Boto3) – 1.12.6
- Amazon SDK for Ruby – 3.79.0

配置实例元数据选项

通过实例元数据选项，您可以通过配置新实例或现有实例来执行以下操作：

- 在请求实例元数据时要求使用 IMDSv2
- 指定 PUT 响应跃点限制
- 关闭对实例元数据的访问

您还可以在 IAM policy 或 SCP 中使用 IAM 条件键执行以下操作：

- 仅在实例配置为要求使用 IMDSv2 时允许实例启动
- 限制允许的跃点数
- 关闭对实例元数据的访问

> **Note**
>
> 在进行任何更改之前，您应谨慎执行操作并进行仔细的测试。记录以下内容：
>
> - 如果您强制使用 IMDSv2，则使用 IMDSv1 访问实例元数据的应用程序或代理将会中断。
> - 如果禁用对实例元数据的所有访问，则依赖于实例元数据访问才能正常工作的应用程序或代理将会中断。
> - 对于 IMDSv2，在检索令牌时必须使用 `/latest/api/token`。

主题

- 为新实例配置实例元数据选项 (p. 760)
- 为现有实例修改实例元数据选项 (p. 763)

为新实例配置实例元数据选项

主题

- 要求使用 IMDSv2 (p. 760)
- 配置 IPv4 和 IPv6 端点 (p. 762)
- 关闭对实例元数据的访问 (p. 763)

要求使用 IMDSv2

您可以通过多种方式要求在启动时在实例上使用 IMDSv2，如下所示：

- 在启动时配置实例 (p. 761)
- 配置 AMI (p. 762)

- 使用 IAM policy (p. 762)

在启动时配置实例

当您 启动实例 (p. 576) 时，您可以通过配置以下字段，从而将实例配置为要求使用 IMDSv2：

- Amazon EC2 控制台：将 Metadata version（元数据版本）设置为 V2 only (token required) [仅 V2（必须使用令牌）]。
- Amazon CLI：将 `HttpTokens` 设置为 `required`。

当您指定必须使用 IMDSv2 时，还必须将可访问元数据设置为已启用（控制台），或将 `HttpEndpoint` 设置为 `enabled`（Amazon CLI），以启用实例元数据服务（IMDS）端点。

New console

要求在新实例上使用 IMDSv2

- 在 Amazon EC2 控制台中启动新实例时，展开 Advanced details（高级详细信息），然后执行以下操作：
  - 对于 Metadata accessible（可访问的元数据），选择 Enabled（已启用）。
  - 对于 Metadata version（元数据版本），选择 V2 only (token required)（仅限 V2（需要令牌））。

  有关更多信息，请参阅高级详细信息 (p. 581)。

Old console

要求在新实例上使用 IMDSv2

- 在 Amazon EC2 控制台中启动新实例时，请在配置实例详细信息页面上选择以下选项：
  - 在高级详细信息下，对于可访问的元数据，选择已启用。
  - 对于元数据版本，选择 V2 (令牌必填)。

有关更多信息，请参阅步骤 3：配置实例详细信息 (p. 585)。

Amazon CLI

要求在新实例上使用 IMDSv2

以下 run-instances 示例会启动 `c3.large` 设置为 `--metadata-options` 的 `HttpTokens=required` 实例。在为 `HttpTokens` 指定值时，还必须将 `HttpEndpoint` 设置为 `enabled`。由于元数据检索请求的安全令牌标头设置为 `required`，这会在请求实例元数据时要求实例使用 IMDSv2。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
 ...
    --metadata-options "HttpEndpoint=enabled,HttpTokens=required"
```

Amazon CloudFormation

要使用 Amazon CloudFormation 指定实例的元数据选项，请参阅 Amazon CloudFormation 用户指南中的 亚马逊云科技::EC2::LaunchTemplate MetadataOptions 属性。

配置 AMI

注册新 AMI 或修改现有 AMI 时，可将 `imds-support` 参数设置为 `v2.0`。从此 AMI 启动的实例会将 Metadata version（元数据版本）设置为 V2 only (token required) [仅 V2（必须使用令牌）]（控制台），或将 `HttpTokens` 设置为 `required`（Amazon CLI）。借助这些设置，实例将要求在请求实例元数据时使用 IMDSv2。

请注意，如果您将 `imds-support` 设置为 `v2.0`，从此 AMI 启动的实例还会将 Metadata response hop limit（元数据响应跃点限制）（控制台）或 `http-put-response-hop-limit`（Amazon CLI）将设置为 2。

> **Important**
>
> 除非 AMI 软件支持 IMDSv2，否则不要使用该参数。将值设置为 `v2.0` 后，无法撤消。“重置”AMI 的唯一方法是从底层快照创建新的 AMI。

为 IMDSv2 配置新的 AMI

下面的 register-image 示例将使用某个 EBS 根卷的指定快照的 AMI 注册为设备 `/dev/xvda`。为 `imds-support` 参数指定 `v2.0`，以便从此 AMI 启动的实例要求在请求实例元数据时使用 IMDSv2。

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snap-0123456789example} \
    --imds-support v2.0
```

为 IMDSv2 配置现有 AMI

以下 modify-image-attribute 示例仅为 IMDSv2 修改现有 AMI。为 `imds-support` 参数指定 `v2.0`，以便从此 AMI 启动的实例要求在请求实例元数据时使用 IMDSv2。

```
aws ec2 modify-image-attribute \
    --image-id ami-0123456789example \
    --imds-support v2.0
```

使用 IAM policy

您可以创建 IAM policy 来阻止用户启动新实例，除非他们要求在新实例上使用 IMDSv2。

使用 IAM policy 强制要求在所有新实例上使用 IMDSv2

要确保用户只能启动要求在请求实例元数据时使用 IMDSv2 的实例，您可以指定在启动实例之前要求 IMDSv2 必须满足的条件。有关示例 IAM policy，请参阅 使用实例元数据 (p. 1266)。

配置 IPv4 和 IPv6 端点

默认禁用 IPv6 端点。即使在仅 IPv6 子网中启动实例，也是如此。您可以在使用 Amazon CLI 启动实例时选择启用 IPv6 端点。此选项在 Amazon EC2 控制台中不可用。

IMDS 的 IPv6 端点仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

配置 IPv4 和 IPv6 端点

下方 run-instances 示例会启动一个 `t3.large` 实例并为 IMDS 启用 IP6 端点。要启用 IPv6 端点，请将 `--metadata-options` 参数指定为 `HttpProtocolIpv6=enabled`。在为 `HttpProtocolIpv6` 指定值时，还必须将 `HttpEndpoint` 设置为 `enabled`。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t3.large \
    ...
```

```
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

关闭对实例元数据的访问

您可以确保关闭对实例元数据的访问权限，无论您使用的是哪个版本的 IMDS。您可以稍后开启访问权限。有关更多信息，请参阅开启对实例元数据的访问权限 (p. 765)。

New console

关闭对实例元数据的访问

- 在 Amazon EC2 控制台中 启动实例 (p. 576)，并在 Advanced details（高级详细信息）下指定以下参数：
  - 对于 Metadata accessible（可访问的元数据），选择 Disabled（已禁用）。

有关更多信息，请参阅高级详细信息 (p. 581)。

Old console

关闭对实例元数据的访问

- 在 Amazon EC2 控制台中启动实例，并在 Configure Instance Details（配置实例详细信息）页面上选择以下选项：
  - 在高级详细信息下，对于可访问的元数据，选择已禁用。

有关更多信息，请参阅步骤 3：配置实例详细信息 (p. 585)。

Amazon CLI

关闭对实例元数据的访问

启动实例并将 `--metadata-options` 设置为 `HttpEndpoint=disabled`。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

Amazon CloudFormation

要使用 Amazon CloudFormation 指定实例的元数据选项，请参阅 Amazon CloudFormation 用户指南中的 AWS::EC2::LaunchTemplate MetadataOptions 属性。

为现有实例修改实例元数据选项

您可以修改现有实例的实例元数据选项。

您还可以创建 IAM policy，以阻止用户修改现有实例上的实例元数据选项。要控制哪些用户可以修改实例元数据选项，请指定一个策略，阻止除具有指定角色的用户以外的所有用户使用 ModifyInstanceMetadataOptions API。有关示例 IAM policy，请参阅 使用实例元数据 (p. 1266)。

您可以修改现有实例的下列元数据选项：

- 要求使用 IMDSv2 (p. 764)
- 恢复使用 imdsv1 (p. 764)
- 更改 PUT 响应跃点限制 (p. 765)

- 为实例启用 IPv6 端点 (p. 765)
- 开启对实例元数据的访问权限 (p. 765)
- 关闭对实例元数据的访问 (p. 766)

要求使用 IMDSv2

使用以下方法之一修改现有实例上的实例元数据选项，以要求在请求实例元数据时使用 IMDSv2。如果 IMDSv2 是必需的，则无法使用 IMDSv1。

Console

要求在现有实例上使用 IMDSv2

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 依次选择操作、实例设置、修改实例元数据选项。
5. 在修改实例元数据选项对话框中，执行以下操作：
   a. 对于实例元数据服务，选择启用。
   b. 对于IMDSv2，选择必需。
   c. 选择 Save（保存）。

Amazon CLI

要求在现有实例上使用 IMDSv2

请使用 modify-instance-metadata-options CLI 命令，并将 `http-tokens` 参数设置为 `required`。在为 `http-tokens` 指定值时，还必须将 `http-endpoint` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

恢复使用 imdsv1

如果 IMDSv2 是必需的，则 IMDSv1 在请求实例元数据时无法正常工作。如果 IMDSv2 是可选的，则 IMDSv2 和 IMDSv1 都将正常工作。因此，要恢复 IMDSv1，请使用以下方法之一将 IMDSv2 设为可选。

Console

恢复在实例上使用 IMDSv1

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 依次选择操作、实例设置、修改实例元数据选项。
5. 在修改实例元数据选项对话框中，执行以下操作：
   a. 对于实例元数据服务，请确保选择启用。
   b. 对于 IMDSv2，选择可选。
   c. 选择 Save（保存）。

Amazon CLI

恢复在实例上使用 IMDSv1

您可以使用 modify-instance-metadata-options CLI 命令并将 `http-tokens` 设置为 `optional`，以在请求实例元数据时恢复使用 IMDSv1。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

更改 PUT 响应跃点限制

对于现有的实例，您可以更改 PUT 响应跃点数限制设置。

目前仅 Amazon CLI 和 Amazon SDK 支持更改 PUT 响应跃点限制。

更改 PUT 响应跃点限制

请使用 modify-instance-metadata-options CLI 命令，并将 `http-put-response-hop-limit` 参数设置为所需的跃点数。在以下示例中，跃点数限制设置为 3。请注意，在为 `http-put-response-hop-limit` 指定值时，还必须将 `http-endpoint` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

为实例启用 IPv6 端点

默认禁用 IPv6 端点。即使您已在仅 IPv6 子网中启动了实例，也是如此。IMDS 的 IPv6 端点仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

目前，仅 Amazon CLI 和 Amazon SDK 支持为实例启用 IPv6 端点。

为实例启用 IPv6 端点

请使用 modify-instance-metadata-options CLI 命令，并将 `http-protocol-ipv6` 参数设置为 `enabled`。请注意，在为 `http-protocol-ipv6` 指定值时，还必须将 `http-endpoint` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

开启对实例元数据的访问权限

您可以通过启用实例上 IMDS 的 HTTP 端点来开启对实例元数据的访问权限，无论您使用的是哪个版本的 IMDS。您可以随时通过禁用 HTTP 端点来撤消该更改。

使用以下方法之一，即可开启对实例上实例元数据的访问权限。

Console

开启对实例元数据的访问权限

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。

4. 依次选择操作、实例设置、修改实例元数据选项。
5. 在修改实例元数据选项对话框中，执行以下操作：
   a. 对于实例元数据服务，选择启用。
   b. 选择 Save（保存）。

Amazon CLI

开启对实例元数据的访问权限

请使用 modify-instance-metadata-options CLI 命令，并将 `http-endpoint` 参数设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

关闭对实例元数据的访问

您可以通过禁用实例上 IMDS 的 HTTP 端点来关闭对实例元数据的访问权限，无论您使用的是哪个版本的 IMDS。您可以随时启用 HTTP 终端节点以撤消该更改。

使用以下方法之一，即可关闭对实例上实例元数据的访问权限。

Console

关闭对实例元数据的访问

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 依次选择操作、实例设置、修改实例元数据选项。
5. 在修改实例元数据选项对话框中，执行以下操作：
   a. 对于实例元数据服务，清除启用。
   b. 选择 Save（保存）。

Amazon CLI

关闭对实例元数据的访问

请使用 modify-instance-metadata-options CLI 命令，并将 `http-endpoint` 参数设置为 `disabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

检索实例元数据

由于您的正在运行的实例存在实例元数据，因此您无需使用 Amazon EC2 控制台或 Amazon CLI。这在您编写脚本以实现从实例运行时非常有用。例如，您可从实例元数据访问您的实例的本地 IP 地址来以管理与外部应用程序的连接。

实例元数据可划分成不同类别。有关每个实例元数据类别的描述，请参阅实例元数据类别 (p. 776)。

要查看正在运行的实例内所有类别的实例元数据，请使用以下 IPv4 或 IPv6 URI。

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

IP 地址是链路本地地址，仅从该实例访问时有效。有关更多信息，请参阅 Wikipedia 上的链路本地地址。

> **Note**
>
> 本部分中的示例使用 IMDS 的 IPv4 地址：169.254.169.254。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：fd00:ec2::254。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

根据您使用的是 IMDSv1 还是 IMDSv2，命令格式会有所不同。默认情况下，可以使用 IMDS 的两个版本。要要求使用 IMDSv2，请参阅使用 IMDSv2 (p. 755)。

您可以使用 cURL 等工具，如以下示例中所示。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

有关从 Windows 实例检索实例元数据的命令，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的检索实例元数据。

成本

您无需为用于检索实例元数据和用户数据的 HTTP 请求付费。

注意事项

为避免实例元数据检索出现问题，请考虑以下事项：

- 默认情况下，Amazon开发工具包使用 IMDSv2 调用。如果 IMDSv2 调用没有收到任何响应，SDK 将重新调用，如果仍然不成功，则使用 IMDSv1。这可能会导致延迟。在容器环境中，如果跃点限制为 1，则 IMDSv2 响应不会返回，因为转到容器被视为额外的网络跃点。为避免出现回退到 IMDSv1 的流程以及由此产生的延迟，在容器环境中，我们建议您将跃数限制设置为 2。有关更多信息，请参阅配置实例元数据选项 (p. 760)。
- 对于 IMDSv2，在检索令牌时必须使用 /latest/api/token。将 PUT 请求发放到任何版本特定的路径（例如 /2021-03-23/api/token）将导致元数据服务返回 403 禁止错误。这是预期行为。

响应和错误消息

所有实例元数据以文本形式返回（HTTP 内容类型 text/plain）。

特定元数据资源的请求返回相应的值；如果资源不可用，则返回 HTTP 错误代码 404 - Not Found。

对通用元数据资源的请求 (以 / 结尾的 URI) 会返回一个可用资源列表，如果此类资源不存在，则会返回 HTTP 错误代码 `404 - Not Found`。列表中的各个项目位于被换行符 (ASCII 10) 终止的不同的行上。

对于使用 实例元数据服务版本 2 发出的请求，可能会返回以下 HTTP 错误代码：

- `400 - Missing or Invalid Parameters` – PUT 请求无效。
- `401 - Unauthorized` – GET 请求使用无效的令牌。建议的措施是生成新的令牌。
- `403 - Forbidden` – 该请求不被允许，或者 IMDS 已关闭。

检索实例元数据的示例

以下示例提供了可以在 Linux 实例上使用的命令。有关从 Windows 实例检索实例元数据的命令，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的检索实例元数据。

示例

- 获取实例元数据的可用版本 (p. 768)
- 获取顶级元数据项 (p. 769)
- 获取可用的公有密钥列表 (p. 771)
- 显示可以使用公有密钥 0 的格式 (p. 771)
- 获取公有密钥 0（采用 OpenSSH 密钥格式）(p. 772)
- 获取实例的子网 ID (p. 772)
- 获取实例的实例标签 (p. 773)

获取实例元数据的可用版本

此示例可以获取实例元数据的可用版本。当有新的实例元数据类别发布时，每个版本都引用一个实例元数据构建。实例元数据构建版本与 Amazon EC2 API 版本不相关。如果您有依赖于以前版本中所存在的结构和信息的脚本，则您可使用早期版本。

> **Note**
>
> 为避免每次 Amazon EC2 发布新的实例元数据构建时都必须更新您的代码，我们建议您在路径中使用 `latest`，而不是版本号。例如，如下所示使用 `latest`：
> `curl http://169.254.169.254/latest/meta-data/ami-id`

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
```

```
latest
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

获取顶级元数据项

此示例获得顶级元数据项目。有关更多信息，请参阅实例元数据类别 (p. 776)。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

以下示例获取在前面的示例中获取的某些顶级元数据项的值。IMDSv2 请求使用在前面的示例命令中创建和存储的令牌，并假设该令牌尚未过期。

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/reservation-id
r-0efghijk987654321
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/local-hostname
```

```
ip-10-251-50-12.ec2.internal
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

获取可用的公有密钥列表

此示例获得可用公有密钥的列表。

IMDSv2

```
[ec2-user ~]$ `curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

显示可以使用公有密钥 0 的格式

此示例显示了可以使用公有密钥 0 的格式。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/public-keys/0/
openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

获取公有密钥 0（采用 OpenSSH 密钥格式）

此示例获得公有密钥 0 (以 OpenSSH 密钥格式)。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

获取实例的子网 ID

此示例获取实例的子网 ID。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

获取实例的实例标签

在以下示例中，示例实例具有启用实例元数据上的标签 (p. 1676)和实例标签 Name=MyInstance 和 Environment=Dev。

此示例获取实例的所有实例标签键。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

以下示例获取在上述示例中获取的 Name 密钥的值。IMDSv2 请求使用在前面的示例命令中创建和存储的令牌，并假设该令牌尚未过期。

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

查询限制

我们基于每个实例来限制对 IMDS 的查询，并且对从实例到 IMDS 的同时连接数进行限制。

如果您使用 IMDS 检索 Amazon 安全凭证，请避免在每个事务期间查询凭证或从大量线程或进程中并发查询凭证，因为这可能会导致节流。相反，我们建议您缓存凭证，直到凭证开始接近其到期时间。有关 IAM 角色以及与其关联的安全凭证的更多信息，请参阅 从实例元数据中检索安全凭证 (p. 1278)。

如果在访问 IMDS 时受到限制，请使用指数回退策略重试查询。

限制 IMDS 访问权限

您可以考虑使用本地防火墙规则，以禁止从某些进程或所有进程中访问 IMDS。

> **Note**
>
> 对于 基于 Nitro 系统构建的实例 (p. 246)，如果 VPC 内的网络设备（例如虚拟路由器）将数据包转发到 IMDS 地址，且实例的原定设置 source/destination check（源/目标检查）被禁用，则可以从您自己的网络访问 IMDS。要防止源从 VPC 外部到达 IMDS，我们建议您修改网络设备的配置，以丢弃目标 IPv4 地址为 IMDS 169.254.169.254 的数据包，并且如果您启用 IPv6 端点，则丢弃目标 IPv6 地址为 IMDS fd00:ec2::254 的数据包。

使用 iptables 限制访问

以下示例使用 Linux iptables 及其 owner 模块禁止 Apache Web 服务器（基于其默认安装用户 ID apache）访问 169.254.169.254。它使用拒绝规则 拒绝来自以该用户身份运行的任何进程的所有实例元数据请求（无论是 IMDSv1 还是 IMDSv2）。

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner --uid-owner apache --jump REJECT
```

或者，您可以考虑使用允许规则 以仅允许特定用户或组进行访问。从安全的角度看，允许规则可能更易于管理，因为它们要求您决定哪种软件需要访问实例元数据。如果使用允许规则，在您以后更改实例上的软件或配置时，不太可能会意外允许软件访问元数据服务（您不打算让该软件进行访问）。您还可以将组与允许规则结合使用，以便您可以在允许的组中添加和删除用户，而无需更改防火墙规则。

以下示例禁止所有进程访问 IMDS，但在用户账户 trustworthy-user 中运行的进程除外。

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner trustworthy-user --jump REJECT
```

Note

- 要使用本地防火墙规则，您需要修改前面的示例命令以符合您的需求。
- 默认情况下，不会在系统重新引导之间持久保留 iptables 规则。可以使用此处未介绍的操作系统功能持久保留这些规则。
- 只有在组是给定本地用户的主要组时，iptables owner 模块才会匹配组成员资格。不会匹配其他组。

使用 PF 或 IPFW 限制访问

如果使用 FreeBSD 或 OpenBSD，您也可以考虑使用 PF 或 IPFW。以下示例将 IMDS 访问限制为仅根用户。

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

Note

PF 和 IPFW 命令的顺序至关重要。PF 默认为最后一个匹配规则，而 IPFW 默认为第一个匹配规则。

处理实例用户数据

与实例用户数据配合使用时，请注意以下内容：

- 用户数据必须采用 base64 编码。Amazon EC2 控制台可以为您执行 base64 编码或接受 base64 编码的输入。

- 用户数据在进行 base64 编码之前的原始格式的大小限制为 16 KB。长度为 n 的字符串在进行 base64 编码之后的大小为 ceil(n/3)*4。
- 在检索用户数据时，必须对其进行 base64 解码。如果您使用实例元数据或控制台检索数据，则会自动对数据进行解码。
- 用户数据会被视为非透明数据；您提供什么数据您就会得到什么数据。由实例对其进行解释。
- 如果您停止实例，修改用户数据，然后启动实例，则在启动实例时，不会更新后的用户数据。

启动时指定实例用户数据

您可在启动实例时指定用户数据。您可以指定用户数据在启动时运行一次，或者在每次重新引导或启动实例时运行。有关更多信息，请参阅启动时在 Linux 实例上运行命令 (p. 748)。

修改实例用户数据

如果根卷是 EBS 卷，则可以修改处于停止状态的实例的用户数据。有关更多信息，请参阅查看和更新实例用户数据 (p. 750)。

检索实例用户数据

> **Note**
>
> 本部分中的示例使用 IMDS 的 IPv4 地址：169.254.169.254。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：fd00:ec2::254。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

要从正在运行的实例中检索用户数据，请使用以下 URI。

```
http://169.254.169.254/latest/user-data
```

请求用户数据时，按原样返回数据 (内容类型 application/octet-stream)。

该示例返回以逗号分隔文本形式提供的用户数据。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/user-
data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

该示例返回以脚本形式提供的用户数据。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
```

```
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

要从您自己的计算机检索实例的用户数据，请参阅 用户数据和 Amazon CLI (p. 752)。

检索动态数据

要从正在运行的实例中检索动态数据，请使用以下 URI。

```
http://169.254.169.254/latest/dynamic/
```

> **Note**
>
> 本部分中的示例使用 IMDS 的 IPv4 地址：169.254.169.254。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：fd00:ec2::254。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

该示例说明了如何检索简要的实例身份类别。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/dynamic/
instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

有关动态数据的详细信息和如何对其进行检索的示例，请参阅 实例身份文档 (p. 786)。

实例元数据类别

实例元数据可划分成不同类别。要检索实例元数据，请在请求中指定类别，然后响应中会返回元数据。

有新类别发布时，系统会使用新版本号创建新的实例元数据构建。在下表中，Version when category was released（类别发布时的版本）列指定实例元数据类别发布时的构建版本。为避免每次 Amazon EC2 发布

新的实例元数据构建时都必须更新您的代码，请在元数据请求中使用 `latest`，而不是版本号。有关更多信息，请参阅获取实例元数据的可用版本 (p. 768)。

当 Amazon EC2 发布新的实例元数据类别时，新类别的实例元数据可能不适用于现有实例。对于基于 Nitro 系统 (p. 246)的实例，只能检索启动时可用的类别的实例元数据。对于具有 Xen 虚拟机管理程序的实例，可以停止然后启动 (p. 610)实例以更新可用于实例的类别。

下表列举了实例元数据的类别。一些类别名称包括实例独有的数据的占位符。例如，*mac* 表示网络接口的 MAC 地址。在检索实例元数据时，您必须使用实际值替换占位符。

类别	描述	类别发布时的版本
`ami-id`	用于启动实例的 AMI ID。	1.0
`ami-launch-index`	如果您同时启动了多个实例，此值表示实例启动的顺序。第一个启动的实例的值是 0。	1.0
`ami-manifest-path`	指向 Amazon S3 中的 AMI 清单文件的路径。如果您使用 Amazon EBS-backed AMI 来启动实例，则返回的结果为 `unknown`。	1.0
`ancestor-ami-ids`	为创建此 AMI 而重新绑定的任何实例的 AMI ID。仅当 AMI 清单文件包含一个 `ancestor-amis` 密钥时，此值才存在。	2007-10-10
`autoscaling/target-lifecycle-state`	显示 Auto Scaling 实例正在转换到的目标 Auto Scaling 生命周期状态的值。当实例在 2022 年 3 月 10 日之后转换到目标生命周期状态之一时显示。可能的值：`Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated`。有关更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的通过实例元数据检索目标生命周期状态。	2021-07-15
`block-device-mapping/ami`	包含根/启动文件系统的虚拟设备。	2007-12-15
`block-device-mapping/ebs` 否	与任何 Amazon EBS 卷关联的虚拟设备。仅当 Amazon EBS 卷在启动时存在或者在上一次启动该实例时存在时，这些卷才在元数据中可用。N 表示 Amazon EBS 卷的索引（例如 `ebs1` 或 `ebs2`）。	2007-12-15
`block-device-mapping/ephemeral` 否	任何非 NVMe 实例存储卷的虚拟设备。N 表示每个卷的索引。块储存设备映射中的实例存储卷数可能与实例的实际实例存储卷数不匹配。实例类型将决定对实例可用的实例存储卷的数量。如果块储存设备映射中的实例存储卷数超	2007-12-15

类别	描述	类别发布时的版本
	过了对实例可用的实例存储卷数，则其他实例存储卷将被忽略。	
block-device-mapping/root	与根设备关联的虚拟设备或分区或虚拟设备上的分区，其中根（/ 或 C:）文件系统与给定实例相关联。	2007-12-15
block-device-mapping/swap	与 swap 关联的虚拟设备。并不总是存在。	2007-12-15
elastic-gpus/associations/*elastic-gpu-id*	如果有 Elastic GPU 附加到实例，在有关 Elastic GPU 的信息中包含 JSON 字符串，包括其 ID 和连接信息。	2016-11-30
elastic-inference/associations/*eia-id*	如果有 Elastic Inference 加速器附加到实例，则在有关Elastic Inference 加速器的信息中包含一个 JSON 字符串，包括其 ID 和类型。	2018-11-29
events/maintenance/history	如果实例存在已完成或已取消的维护事件，则包含一个 JSON 字符串，其中包含有关事件的信息。有关更多信息，请参阅查看有关已完成或已取消的事件的事件历史记录 (p. 984)。	2018-08-17
events/maintenance/scheduled	如果实例存在活动的维护事件，则包含一个 JSON 字符串，其中包含有关事件的信息。有关更多信息，请参阅查看计划的事件 (p. 982)。	2018-08-17
events/recommendations/rebalance	为实例发出 EC2 实例再平衡建议通知的大致时间 (UTC)。下面是此类别的元数据示例：{"noticeTime": "2020-11-05T08:22:00Z"}。此类别仅在发出通知后可用。有关更多信息，请参阅EC2 实例再平衡建议 (p. 480)。	2020-10-27
hostname	如果 EC2 实例使用的是基于 IP 的命名 (IPBN)，则此为实例的私有 IPv4 DNS 主机名。如果 EC2 实例使用的是基于资源的命名 (RBN)，则此为 RBN。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。有关 IPBN 和 RBN 的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。	1.0
iam/info	如果存在与实例关联的 IAM 角色，则包含有关实例配置文件上次更新时间的信息 (包括实例的 LastUpdated 日期、InstanceProfileArn 和 InstanceProfileId)。如果没有，则不显示。	2012-01-12

类别	描述	类别发布时的版本
iam/security-credentials/role-name	如果存在与实例关联的 IAM 角色，则 *role-name* 为角色的名称，并且 *role-name* 包含与角色关联的临时安全凭证 (有关更多信息，请参阅 从实例元数据中检索安全凭证 (p. 1278))。如果没有，则不显示。	2012-01-12
identity-credentials/ec2/info	identity-credentials/ec2/security-credentials/ec2-instance 中凭证的相关信息。	2018-05-23
identity-credentials/ec2/security-credentials/ec2-instance	允许实例软件向 Amazon 确认自身身份，以支持 EC2 实例连接及 Amazon Systems Manager 默认主机管理配置等功能的实例身份角色凭证。这些凭证并未附加策略，因此除了将实例标识为 Amazon 功能外，它们没有其他 Amazon API 权限。有关更多信息，请参阅实例身份角色 (p. 808)。	2018-05-23
instance-action	通知实例在准备打包时重新启动。有效值：none | shutdown | bundle-pending。	2008-09-01
instance-id	此实例的 ID。	1.0
instance-life-cycle	此实例的采购选项。有关更多信息，请参阅实例购买选项 (p. 404)。	2019-10-01
instance-type	实例的类型。有关更多信息，请参阅实例类型 (p. 238)。	2007-08-29
ipv6	实例的 IPv6 地址。在存在多个网络接口的情况下，其指的是 eth0 设备（设备号为 0 的设备）的网络接口和第一个分配的 IPv6 地址。若网络接口 [0] 上不存在 IPv6 地址，则不会设置此项目且会导致 HTTP 404 响应。	2021-01-03
kernel-id	此实例启动的内核的 ID，如果适用的话。	2008-02-01
local-hostname	在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。如果 EC2 实例使用的是基于 IP 的命名 (IPBN)，则此为实例的私有 IPv4 DNS 主机名。如果 EC2 实例使用的是基于资源的命名 (RBN)，则此为 RBN。有关 IPBN、RBN 和 EC2 实例命名的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。	2007-01-19
local-ipv4	实例的私有 IPv4 地址。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。若此为仅 IPv6 的实例，则不会设置此项目且会导致 HTTP 404 响应。	1.0

类别	描述	类别发布时的版本
mac	实例的媒体访问控制 (MAC) 地址。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。	2011 年 1 月 1 日
metrics/vhostmd	不再可用。	2011-05-01
network/interfaces/macs/mac/device-number	与该接口关联的唯一设备号。设备号与设备名称对应；例如，device-number 为 2 对应于 eth2 设备。此类别对应的是 Amazon CLI 的 Amazon EC2 API 和 EC2 命令使用的 DeviceIndex 和 device-index 字段。	2011 年 1 月 1 日
network/interfaces/macs/mac/interface-id	网络接口的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/ipv4-associations/public-ip	与每个公用 IP 地址相关联并被分配到该接口的私有 IPv4 地址。	2011 年 1 月 1 日
network/interfaces/macs/mac/ipv6s	与接口关联的 IPv6 地址。仅对启动至 VPC 的实例返回。	2016-06-30
network/interfaces/macs/mac/local-hostname	实例的私有 IPv4 DNS 主机名。在存在多个网络接口的情况下，其指的是 eth0 设备 (设备号为 0 的设备)。若此为仅 IPv6 的实例，则此为基于资源的名称。有关 IPBN 和 RBN 的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。	2007-01-19
network/interfaces/macs/mac/local-ipv4s	与接口关联的私有 IPv4 地址。若此为仅 IPv6 的网络接口，则不会设置此项目且会导致 HTTP 404 响应。	2011 年 1 月 1 日
network/interfaces/macs/mac/mac	该实例的 MAC 地址。	2011 年 1 月 1 日
network/interfaces/macs/*mac*/network-card-index	网卡的索引。有些实例类型支持多个网卡。	2020-11-01
network/interfaces/macs/mac/owner-id	网络接口拥有者的 ID。在多个接口的环境中，接口可由第三方连接，如 Elastic Load Balancing。接口拥有者需为接口上的流量付费。	2011 年 1 月 1 日
network/interfaces/macs/mac/public-hostname	接口的公有 DNS (IPv4)。仅当 enableDnsHostnames 属性设置为 true 时，才返回此类别。有关更多信息，请参阅 Amazon VPC 用户指南中的在您的 VPC 中使用 DNS。如果实例仅具有公有 IPv6 地址而没有公有 IPv4 地址，则不会设置此项目并导致 HTTP 404 响应。	2011 年 1 月 1 日

类别	描述	类别发布时的版本
network/interfaces/macs/mac/public-ipv4s	与接口关联的公有 IP 地址或弹性 IP 地址。一个实例上可能有多个 IPv4 地址。	2011 年 1 月 1 日
network/interfaces/macs/mac/security-groups	网络接口所属的安全组。	2011 年 1 月 1 日
network/interfaces/macs/mac/security-group-ids	网络接口所属的安全组的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-id	接口所驻留的子网的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-ipv4-cidr-block	接口所在子网的 IPv4 CIDR 块。	2011 年 1 月 1 日
network/interfaces/macs/mac/subnet-ipv6-cidr-blocks	接口所在子网的 IPv6 CIDR 块。	2016-06-30
network/interfaces/macs/mac/vpc-id	接口所驻留的 VPC 的 ID。	2011 年 1 月 1 日
network/interfaces/macs/mac/vpc-ipv4-cidr-block	VPC 的主 IPv4 CIDR 块。	2011 年 1 月 1 日
network/interfaces/macs/mac/vpc-ipv4-cidr-blocks	VPC 的 IPv4 CIDR 块。	2016-06-30
network/interfaces/macs/mac/vpc-ipv6-cidr-blocks	接口所在 VPC 的 IPv6 CIDR 块。	2016-06-30
placement/availability-zone	实例启动的可用区。	2008-02-01
placement/availability-zone-id	在其中启动实例的静态可用区 ID。可用区 ID 在账户之间保持一致。但是，它可能与可用区不同，后者可能因账户而异。	2019-10-01
placement/group-name	在其中启动实例的置放群组的名称。	2020-08-24
placement/host-id	启动实例的主机的 ID。仅适用于专用主机。	2020-08-24
placement/partition-number	在其中启动实例的分区编号。	2020-08-24
placement/region	在其中启动实例的 Amazon 区域。	2020-08-24
product-codes	Amazon Web Services Marketplace与实例相关联的 产品代码（如果有）。	2007-03-01

类别	描述	类别发布时的版本
public-hostname	实例的公有 DNS (IPv4)。仅当 enableDnsHostnames 属性设置为 true 时，才返回此类别。有关更多信息，请参阅 Amazon VPC 用户指南中的在您的 VPC 中使用 DNS。如果实例仅具有公有 IPv6 地址而没有公有 IPv4 地址，则不会设置此项目并导致 HTTP 404 响应。	2007-01-19
public-ipv4	公有 IPv4 地址。如果弹性 IP 地址与实例相关联，返回的值是弹性 IP 地址。	2007-01-19
public-keys/0/openssh-key	公有密钥。仅在实例启动时提供了公有密钥的情况下可用。	1.0
ramdisk-id	启动时指定的 RAM 磁盘 的 ID，如果适用的话。	2007-10-10
reservation-id	预留的 ID。	1.0
security-groups	应用到实例的安全组的名称。 在启动后，您可以更改实例的安全组。这些更改将体现在此处和 network/interfaces/macs/*mac*/security-groups 中。	1.0
services/domain	区域的 Amazon 资源所在的域。	2014-02-25
services/partition	资源所处的分区。对于标准 Amazon 区域，分区是 aws。如果资源位于其他分区，则分区是 aws-*partitionname*。例如，中国（北京）区域中的资源的分区为 aws-cn。	2015-10-20
spot/instance-action	操作（休眠、停止或终止）和操作发生的大致时间（用 UTC 表示）。仅在已将竞价型实例标记为休眠、停止或终止时才提供此项目。有关更多信息，请参阅instance-action (p. 491)。	2016-11-15
spot/termination-time	竞价型实例 操作系统将收到关闭信号的大致时间 (UTC)。仅当竞价型实例已由 Amazon EC2 标记为终止时，此项目才会出现并包含时间值（例如，2015-01-05T18:02:00Z）。如果您自己终止了竞价型实例，那么终止时间项目不会设置为时间。有关更多信息，请参阅termination-time (p. 492)。	2014-11-05
tags/instance	与实例关联的实例标签。只有明确允许访问实例元数据中的标签时才可用。有关更多信息，请参阅允许访问实例元数据中的标签 (p. 1676)。	2021-03-23

动态数据类别

下表列举了动态数据的类别。

类别	描述	类别发布时的版本
`fws/instance-monitoring`	显示客户是否在 CloudWatch 中启用了详细的一分钟监控的值。有效值：`enabled	disabled`	2009-04-04
`instance-identity/document`	包含实例属性 (如实例 ID、私有 IP 地址等) 的 JSON。请参阅 实例身份文档 (p. 786)。	2009-04-04
`instance-identity/pkcs7`	用于验证签名的文档的真实性和内容。请参阅 实例身份文档 (p. 786)。	2009-04-04
`instance-identity/signature`	可被其他各方用于验证来源和真实性的数据。请参阅 实例身份文档 (p. 786)。	2009-04-04

示例：AMI 启动索引值

本示例演示如何使用用户数据和实例元数据来配置实例。

> **Note**
>
> 本部分中的示例使用 IMDS 的 IPv4 地址：`169.254.169.254`。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：`fd00:ec2::254`。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

Alice 想要启动她最喜欢的数据库 AMI 的四个实例，第一个实例用作原始实例，其余三个用作副本。当她启动它们时，她想为每个副本添加有关复制策略的用户数据。她知道这些数据将对所有四个实例都可用，因此她所采用的用户数据构建方式必须能够让每个实例识别出哪些部分适用于自己。她可通过 `ami-launch-index` 实例元数据值来实现这一点，该值对每个实例都是唯一的。如果她同时启动多个实例，则 `ami-launch-index` 表示实例启动的顺序。第一个启动的实例的值是 `0`。

以下是 Alice 构建的用户数据。

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

`replicate-every=1min` 数据定义第一个副本的配置，`replicate-every=5min` 定义第二个副本的配置，以此类推。Alice 决定以 ASCII 字符串形式提供这些数据，用竖线符号 (`|`) 来分隔每个实例的数据。

Alice 使用 run-instances 命令启动 4 个实例，并指定用户数据。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

实例启动之后，所有实例都有以下用户数据和常用元数据的副本：

- AMI ID：ami-0abcdef1234567890
- 预留 ID：r-1234567890abcabc0
- 公有密钥：无
- 安全组名称：默认值

- 实例类型：t2.micro

然而，每个实例都包含某些特定的元数据。

实例 1

元数据	值
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

实例 2

元数据	值
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

实例 3

元数据	值
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

实例 4

元数据	值
instance-id	i-1234567890abcdef0

元数据	值
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice 可以使用 `ami-launch-index` 值确定用户数据的哪个部分适用于特定实例。

1. 她连接到其中一个实例并检索该实例的 `ami-launch-index`，以确保该实例是副本之一：

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token"
    -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
   data/ami-launch-index
   2
   ```

   对于以下步骤，IMDSv2 请求使用前面的 IMDSv2 命令中存储的令牌，并假设令牌尚未过期。

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. 她将 `ami-launch-index` 保存为一个变量。

   IMDSv2

   ```
   [ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v
    http://169.254.169.254/latest/meta-data/ami-launch-index`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
   launch-index`
   ```

3. 她将用户数据保存为一个变量。

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. 最后，Alice 使用 cut 命令提取适用于该实例的用户数据部分。

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   ```

```
replicate-every=5min
```

IMDSv1

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
replicate-every=5min
```

实例身份文档

您启动的每个实例都有一个实例身份文档，用于提供有关实例自身的信息。您可以使用实例身份文档验证实例的属性。

实例身份文档在实例停止并启动、重新启动或启动时生成。实例身份文档通过实例元数据服务（IMDS）公开（采用纯文本 JSON 格式）。IPv4 地址 169.254.169.254 是链路本地地址，仅从该实例有效。有关更多信息，请参阅 Wikipedia 上的链路本地地址。IPv6 地址 fd00:ec2::254 是唯一本地地址，仅从该实例有效。有关更多信息，请参阅 Wikipedia 上的 Unique local address（链路本地地址）。

Note

本部分中的示例使用 IMDS 的 IPv4 地址：169.254.169.254。如果要通过 IPv6 地址检索 EC2 实例的实例元数据，请确保启用并改用 IPv6 地址：fd00:ec2::254。IMDS 的 IPv6 地址与 IMDSv2 命令兼容。IPv6 地址仅可在 基于 Nitro 系统构建的实例 (p. 246) 上访问。

您可以随时从正在运行的实例中检索实例身份文档。实例身份文档 中包括以下信息：

数据	描述
accountId	启动实例的 Amazon 账户的 ID。
architecture	启动实例所用 AMI 的架构 (i386 | x86_64 | arm64)。
availabilityZone	实例在其中运行的可用区。
billingProducts	实例的计费产品。
devpayProductCodes	已淘汰。
imageId	用于启动实例的 AMI 的 ID。
instanceId	实例的 ID。
instanceType	实例的实例类型。
kernelId	与实例关联的内核的 ID（如果适用）。
marketplaceProductCodes	用于启动实例的 AMI 的 Amazon Web Services Marketplace 产品代码。
pendingTime	启动实例的日期和时间。
privateIp	实例的私有 IPv4 地址。
ramdiskId	与实例关联的 RAM 磁盘的 ID（如果适用）。
region	运行实例的区域。
version	实例身份文档格式的版本。

检索明文实例身份文档

检索明文实例身份文档

连接到实例，并根据实例使用的 IMDS 版本运行以下命令之一。

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

下面是示例输出。

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

验证 实例身份文档

如果您打算将实例身份文档的内容用于重要用途，则应在使用前验证其内容和真实性。

明文实例身份文档附有三个经哈希处理的加密签名。您可以使用这些签名验证实例身份文档的来源和真实性以及其中包含的信息。其中提供以下签名：

- Base64 编码的签名 — 这是实例身份文档的 Base64 编码 SHA256 哈希值，使用 RSA 密钥对进行加密。
- PKCS7 签名 — 这是实例身份文档的 SHA1 哈希值，使用 DSA 密钥对进行加密。
- RSA-2048 签名 — 这是实例身份文档的 SHA256 哈希值，使用 RSA-2048 密钥对进行加密。

每个签名在实例元数据中的不同终端节点上可用。您可以根据哈希和加密要求使用这些签名中的任何一个。要验证签名，您必须使用对应的 Amazon 公有证书。

以下主题提供了使用每个签名验证实例身份文档的详细步骤。

- 使用 PKCS7 签名验证 实例身份文档 (p. 788)
- 使用 base64 编码的签名验证 实例身份文档 (p. 792)
- 使用 RSA-2048 签名验证 实例身份文档 (p. 796)

使用 PKCS7 签名验证 实例身份文档

本主题说明如何使用 PKCS7 签名和 Amazon DSA 公有证书验证实例身份文档。

使用 PKCS7 签名和 Amazon DSA 公有证书验证实例身份文档

1. 连接到实例。
2. 从实例元数据中检索 PKCS7 签名，并将其连同所需的页眉和页脚添加到名为 pkcs7 的新文件。根据实例使用的 IMDS 版本，使用以下命令之一。

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

3. 将 Amazon DSA 公有证书添加到名为 certificate 的新文件。根据您的实例所在的地区，使用以下命令之一。

   Other Amazon Regions

   以下 Amazon 公有证书适用于除中国香港、巴林、开普敦、米兰、雅加达、中国和 GovCloud 之外的所有 Amazon 区域。

   ```
   $  echo "-----BEGIN CERTIFICATE-----
   MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
   FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
   VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
   ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
   IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
   cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
   ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
   VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
   hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
   k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
   hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
   lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
   MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
   MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
   vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
   7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
   -----END CERTIFICATE-----" >> certificate
   ```

   Asia Pacific (Hong Kong)

   亚太地区（香港）的 Amazon 公有证书如下所示。

   ```
   $  echo "-----BEGIN CERTIFICATE-----
   MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
   ```

```
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----" >> certificate
```

Middle East (Bahrain)

中东（巴林）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1Qli0OB
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----" >> certificate
```

Middle East (UAE)

中东（阿联酋）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMB4XDTIxMDQxNTIxNTM1MFoX
DTQ3MDQxNTIxNTM1MFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBtzCCASwGByqGSM44BAEwggEfAoGBAP1/U4EddRIpUt9K
nC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/xfW6MPbLm1Vs14E7gB00
b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E+4P208UewwI1VBNa
FpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/BYHPUCgYEA
9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCBgLRJ
FnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7
zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf
8moOhqCom9+0+ovuUFdpvCie86bpEZW5G8QbGebFr1F/TOZU568Ty1ff3dDWbdRz
eNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z+XGmzK
mgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----" >> certificate
```

Africa (Cape Town)

非洲（开普敦）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----" >> certificate
```

Europe (Milan)

欧洲地区（米兰）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----" >> certificate
```

Asia Pacific (Jakarta)

亚太地区（雅加达）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAe
BgNVBAoMF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMB4XDTIxMDEwNjAwMTUyMFoX
DTQ3MDEwNjAwMTUyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0
b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpvbiBXZWIg
U2VydmljZXMgTExDMIIBuDCCASwGByqGSM44BAEwggEfAoGBAP1/U4EddRIpUt9K
nC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/xfW6MPbLm1Vs14E7gB00
b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E+4P208UewwI1VBNa
FpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/BYHPUCgYEA
9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT+ZxBxCBgLRJ
```

```
FnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx+2J6ASQ7
zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3J
Q6cVwntJie67D8OuNo4jGRn+crEtL7YO0jSVB9zGE1ga+UgRPIaYETL293S8rTJT
VgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM+/52
g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIR
twK+9qnaTOBhvO/njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----" >> certificate
```

China

中国（北京）和中国（宁夏）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----" >> certificate
```

Amazon GovCloud (US)

Amazon GovCloud（美国东部）和 Amazon GovCloud（美国西部）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----" >> certificate
```

4. 使用 OpenSSL smime 命令来验证签名。包括 `-verify` 选项以指示需要验证签名，而包括 `-noverify` 选项则指示不需要验证证书。

```
$ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
 document
```

如果签名有效，则会显示 `Verification successful` 消息。

此命令还会将实例身份文档的内容写入一个名为 `document` 的新文件。您可以使用以下命令将来自实例元数据的实例身份文档内容与此文件的内容进行比较。

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document | openssl dgst -sha256
```

如果无法验证签名，请联系 Amazon Web Services Support。

使用 base64 编码的签名验证 实例身份文档

本主题说明如何使用 base64 编码的签名和 Amazon RSA 公有证书验证实例身份文档。

使用 base64 编码的签名和 Amazon RSA 公有证书验证实例身份文档

1. 连接到实例。
2. 从实例元数据中检索 base64 编码的签名，将其转换为二进制文件，然后将其添加到名为 `signature` 的文件。根据实例使用的 IMDS 版本，使用以下命令之一。

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   dynamic/instance-identity/signature | base64 -d >> signature
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
    base64 -d >> signature
   ```
3. 从实例元数据中检索明文 实例身份文档，并将其添加到名为 `document` 的文件。根据实例使用的 IMDS 版本，使用以下命令之一。

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```
4. 将 Amazon RSA 公有证书添加到名为 `certificate` 的新文件。根据您的实例所在的地区，使用以下命令之一。

Other Amazon Regions

以下 Amazon 公有证书适用于除中国香港、巴林、开普敦、米兰、雅加达、中国和 GovCloud 之外的所有 Amazon 区域。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIDIjCCAougAwIBAgIJAKnL4UEDMN/FMA0GCSqGSIb3DQEBBQUAMGoxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgw
FgYDVQQKEw9BbWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3Mu
Y29tMB4XDTE0MDYwNTE0MjgwMloXDTI0MDYwNTE0MjgwMlowajELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1NlYXR0bGUxGDAWBgNV
BAoTD0FtYXpvbi5jb20gSW5jLjEaMBgGA1UEAxMRZWMyLmFtYXpvbmF3cy5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIe9GN//SRK2knbjySG0ho3yqQM3
e2TDhWO8D2e8+XZqck754gFSo99AbT2RmXClambI7xsYHZFapbELC4H91ycihvrD
jbST1ZjkLQgga0NE1q43eS68ZeTDccScXQSNivSlzJZS8HJZjgqzBlXjZftjtdJL
XeE4hwvo0sD4f3j9AgMBAAGjgc8wgcwwHQYDVR0OBBYEFCXWzAgVyrbwnFncFFIs
77VBdlE4MIGcBgNVHSMEgZQwgZGAFCXWzAgVyrbwnFncFFIs77VBdlE4oW6kbDBq
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2Vh
dHRsZTEYMBYGA1UEChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1h
em9uYXdzLmNvbYIJAKnL4UEDMN/FMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEF
BQADgYEAFYcz1OgEhQBXIwIdsgCOS8vEtiJYF+j9uO6jz7VOmJqO+pRlAbRlvY8T
C1haGgSI/A1uZUKs/Zfnph0oEI0/hu1IIJ/SKBDtN5lvmZ/IzbOPIJWirslslQIQ
7zvWbGd9c9+Rm3p04oTvhup99la7kZqevJK0QRdD/6NpCKsqP/0=
-----END CERTIFICATE-----" >> certificate
```

Asia Pacific (Hong Kong)

亚太地区（香港）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----" >> certificate
```

Middle East (Bahrain)

中东（巴林）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
```

```
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----" >> certificate
```

Middle East (UAE)

中东（阿联酋）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYT
AlVTMRkwFwYDVQQIDBBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHDAdTZWF0dGxl
MSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMTA0MTQxODM5
MzNaGA8yMjAwMDQxNDE4MzkzM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdh
c2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpv
biBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDc
aTgW/KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C
3qzE4rIenmahvUplu9ZmLwL1idWXMRX2RlSvIt+d2SeoKOKQWoc2UOFZMHYxDue7
zkyk1CIRaBukTeY13/RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEB
BQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/Cnz5YaoUivRRdX2A83BHuBTvJE2+
WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
+OfK1bAcKTtfkkkP9r4RdwSjKzO5Zu/B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----" >> certificate
```

Africa (Cape Town)

非洲（开普敦）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----" >> certificate
```

Europe (Milan)

欧洲地区（米兰）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
```

```
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
-----END CERTIFICATE-----" >> certificate
```

Asia Pacific (Jakarta)

亚太地区（雅加达）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYT
AlVTMRkwFwYDVQQIDBBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHDAdTZWF0dGxl
MSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMTAxMDYwMDE1
MzBaGA8yMjAwMDEwNjAwMTUzMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdh
c2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYXR0bGUxIDAeBgNVBAoMF0FtYXpv
biBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCn
CS/Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf
1R9S3AUwLnsc7b+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2Qs
WBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV+OkP9ab5wIDAQABMA0GCSqGSIb3DQEB
BQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs6eo
fLTSGovrReX7MtVgrcJBZjmPIentw5dWUs+87w/g9lNwUnUt0ZHYyh2tuBG6hVJu
UEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----" >> certificate
```

China

中国（北京）和中国（宁夏）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQCQu97teKRD4zANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xMzA4MjExMzIyNDNaFw0yMzA4MjExMzIyNDNaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6GFQ2WoBl1xZYH85INUMaTc4D30QXM6f+
YmWZyJD9fC7Z0UlaZIKoQATqCO58KNCre+jECELYIX56Uq0lb8LRLP8tijrQ9Sp3
qJcXiH66kH0eQ44a5YdewcFOy+CSAYDUIaB6XhTQJ2r7bd4A2vw3ybbxTOWONKdO
WtgIe3M3iwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHzQC5XZVeuD9GTJTsbO5AyH
ZQvki/jfARNrD9dgBRYZzLC/NOkWG6M9wlrmks9RtdNxc53nLxKq4I2Dd73gI0yQ
wYu9YYwmM/LMgmPlI33Rg2Ohwq4DVgT3hO170PL6Fsgiq3dMvctSImJvjWktBQaT
bcAgaZLHGIpXPrWSA2d+
-----END CERTIFICATE-----" >> certificate
```

Amazon GovCloud (US)

Amazon GovCloud（美国东部）和 Amazon GovCloud（美国西部）的 Amazon 公有证书如下所示。

```
$  echo "-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJAIe9Hnq82O7UMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMTA3MTQx
NDI3NTdaFw0yNDA3MTMxNDI3NTdaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
qaIcGFFTx/SO1W5G91jHvyQdGP25n1Y91aXCuOOWAUTvSvNGpXrI4AXNrQF+CmIO
C4beBASnHCx082jYudWBBl9Wiza0psYc9flrczSzVLMmN8w/c78F/95NfiQdnUQP
pvgqcMeJo82cgHkLR7XoFWgMrZJqrcUK0gnsQcb6kakCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFNWV53gWJz72F5B1ZVY4O/dfFYBPMIGOBgNVHSME
gYYwgYOAFNWV53gWJz72F5B1ZVY4O/dfFYBPoWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQCHvR56vNju1DASBgNVHRMB
```

```
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBACrKjWj460GUPZCGm3/z0dIz
M2BPuH769wcOsqfFZcMKEysSFK91tVtUb1soFwH4/Lb/T0PqNrvtEwD1Nva5k0h2
xZhNNRmDuhOhW1K9wCcnHGRBwY5t4lYL6hNV6hcrqYwGMjTjcAjBG2yMgznSNFle
Rwi/S3BFXISixNx9cILu
-----END CERTIFICATE-----" >> certificate
```

5. 从 Amazon RSA 公有证书中提取公有密钥，并将其保存到名为 key 的文件。

```
$ openssl x509 -pubkey -noout -in certificate >> key
```

6. 使用 OpenSSL dgst 命令来验证实例身份文档。

```
$ openssl dgst -sha256 -verify key -signature signature document
```

如果签名有效，则会显示 Verification successful 消息。

此命令还会将实例身份文档的内容写入一个名为 document 的新文件。您可以使用以下命令将来自实例元数据的实例身份文档内容与此文件的内容进行比较。

```
$ openssl dgst -sha256 < document
```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document | openssl dgst -sha256
```

如果无法验证签名，请联系 Amazon Web Services Support。

使用 RSA-2048 签名验证 实例身份文档

本主题说明如何使用 RSA-2048 签名和 Amazon RSA-2048 公有证书验证实例身份文档。

使用 RSA-2048 签名和 Amazon RSA-2048 公有证书验证实例身份文档。

1. 连接到实例。
2. 从实例元数据中检索 RSA-2048 签名，并将其连同所需的页眉和页脚添加到名为 rsa2048 的文件。根据实例使用的 IMDS 版本，使用以下命令之一。

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   dynamic/instance-identity/rsa2048 >> rsa2048 \
   && echo "" >> rsa2048 \
   && echo "-----END PKCS7-----" >> rsa2048
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> rsa2048 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
    >> rsa2048 \
   && echo "" >> rsa2048 \
   && echo "-----END PKCS7-----" >> rsa2048
   ```

3. 将您所在区域的 Amazon RSA-2048 公有证书添加到名为 certificate 的新文件。根据您的实例所在的地区，使用以下命令之一。

North America Regions

- 美国东部（弗吉尼亚州北部）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----" >> certificate
```

- 美国东部（俄亥俄州）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----" >> certificate
```

- 美国西部（俄勒冈州）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
```

```
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----" >> certificate
```

- 美国西部（北加利福尼亚）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----" >> certificate
```

- 加拿大（中部）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
```

```
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----" >> certificate
```

South America Regions

- 南美洲（圣保罗）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----" >> certificate
```

Europe, Middle East, and Africa Regions

- 欧洲（法兰克福）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
```

```
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----" >> certificate
```

- 欧洲（伦敦）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Y1eec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----" >> certificate
```

- 欧洲（巴黎）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----" >> certificate
```

- 欧洲（爱尔兰）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
```

```
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----" >> certificate
```

- 欧洲（米兰）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----" >> certificate
```

- 欧洲（斯德哥尔摩）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----" >> certificate
```

- 中东（巴林）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
```

```
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQ1dd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----" >> certificate
```

- 中东（阿联酋）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----" >> certificate
```

- 非洲（开普敦）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
```

```
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----" >> certificate
```

Asia Pacific Regions

- 亚太地区（悉尼）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（东京）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61szi UAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区 (首尔)

```
$ echo "-----BEGIN CERTIFICATE-----
```

```
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（大阪）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（孟买）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
```

```
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（香港）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（新加坡）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----" >> certificate
```

- 亚太地区（雅加达）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyycgt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
```

```
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----" >> certificate
```

- 中国（宁夏）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----" >> certificate
```

- 中国（北京）

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----" >> certificate
```

Amazon GovCloud (US) Regions

- Amazon GovCloud（美国西部）区域

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----" >> certificate
```

- Amazon GovCloud（美国东部）区域

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----" >> certificate
```

4. 使用 OpenSSL smime 命令来验证签名。包括 `-verify` 选项以指示需要验证签名，而包括 `-noverify` 选项则指示不需要验证证书。

```
$ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify | tee
 document
```

如果签名有效，则会显示 `Verification successful` 消息。如果无法验证签名，请联系 Amazon Web Services Support。

实例身份角色

您启动的每个实例都有一个代表其身份的实例身份角色。实例身份角色是一种 IAM 角色。集成使用实例身份角色的 Amazon 服务和功能可以使用它来标识服务的实例。

实例身份角色凭证可通过 `/identity-credentials/ec2/security-credentials/ec2-instance` 的实例元数据服务（IMDS）访问。凭证由 Amazon 临时访问密钥对和会话令牌组成。它们用于对使用实例身份角色的 Amazon 服务签署 Amazon Sigv4 请求。无论实例上是否启用了使用实例身份角色的服务或功能，凭证都存在于实例元数据中。

实例身份角色会在实例启动时自动创建，没有 role-trust 策略文档，并且不受任何身份或资源策略的约束。

支持的服务

以下 Amazon 服务使用实例身份角色：

- Amazon Systems Manager – 使用默认主机管理配置时，Amazon Systems Manager 将使用实例身份角色提供的身份来注册 EC2 实例。标识实例后，Systems Manager 可将 `AWSSystemsManagerDefaultEC2InstanceManagementRole` IAM 角色传递给实例。
- Amazon EC2 – 通过实例身份角色更新 EC2 实例的主机密钥。
- Amazon Security Token Service（Amazon STS）– 实例身份角色凭证可与 Amazon STS `GetCallerIdentity` 操作结合使用。

实例身份角色不能与其他 Amazon 服务或功能结合使用，因为其并未与实例身份角色集成。

实例身份角色 ARN

实例身份角色 ARN 采用以下格式：

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

例如：

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

有关 ARN 的更多信息，请参阅《IAM 用户指南》中的 Amazon 资源名称（ARN）。

Amazon Elastic Inference

> **Note**
>
> 自 2023 年 4 月 15 日起，Amazon 不再允许新客户加入 Amazon Elastic Inference（EI），并将帮助现有客户将其工作负载迁移到价格更低廉且性能更出色的选项。2023 年 4 月 15 日之后，新客户将无法在 Amazon SageMaker、Amazon ECS 或Amazon EC2 中使用 Amazon EI 加速器启动实例。但是，在过去 30 天内至少使用过一次 Amazon EI 的客户将视为当前客户，可继续使用该服务。

Amazon Elastic Inference（EI）是一种资源，您可以将其附加到 Amazon EC2 CPU 实例以用于深度学习（DL）推导工作负载。

有关 Amazon EI 的更多信息，请参阅 Amazon Elastic Inference 开发人员指南。

识别 EC2 Linux 实例

您可能需要确定您的应用程序是否运行在 EC2 实例上。

有关识别 Windows 实例的信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的识别 EC2 Windows 实例。

检查 实例身份文档

对于标识 EC2 实例的明确且以加密方式验证的方法，请查看实例标识文档，包括其签名。这些文档适用于本地、不可路由地址 `http://169.254.169.254/latest/dynamic/instance-identity/` 处的每个 EC2 实例。有关更多信息，请参阅实例身份文档 (p. 786)。

检查系统 UUID

您可以获取系统 UUID 并检查 UUID 的起始 octet 中是否存在字符 “ec2”或 “EC2”。此确定系统是否为 EC2 实例的方法速度快，但可能不准确，因为不是 EC2 实例的系统也有很小的几率使用以这些字符开头的 UUID。此外，对于不使用 Amazon Linux 2 的 EC2 实例，发行版的 SMBIOS 实施可能表示 little-endian 格式的 UUID，因此“EC2”字符不显示在 UUID 的开头。

Example ：从 DMI 获取 UUID（仅限 HVM AMI）

通过以下命令使用桌面管理界面 (DMI) 获取 UUID：

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

在以下示例输出中，UUID 以“EC2”开头，表示该系统可能是 EC2 实例。

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

在以下示例输出中，UUID 以 little-endian 格式表示。

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

或者，对于在 Nitro 系统上构建的实例，您可以使用以下命令：

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

如果输出是实例 ID，如下面的示例输出所示，则说明系统是 EC2 实例：

```
i-0af01c0123456789a
```

Example ：从管理程序获取 UUID（仅限 PV AMI）

使用以下命令从管理程序获取 UUID：

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

在以下示例输出中，UUID 以“ec2”开头，表示该系统可能是 EC2 实例。

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

检查系统虚拟机生成标识符

虚拟机生成标识符由被解释为加密随机整数标识符的 128 位的唯一缓冲区组成。您可以检索虚拟机生成标识符来识别 Amazon Elastic Compute Cloud 实例。生成标识符通过 ACPI 表条目在实例的来宾操作系统中公开。如果您的计算机被克隆、复制或导入到 Amazon，例如使用 VM Import/Export，该值将改变。

Example ：从 Linux 中检索虚拟机生成标识符

您可以使用以下命令从运行 Linux 的实例中检索虚拟机生成标识符。

Amazon Linux 2

1. 根据需要，使用以下命令更新现有软件包：

```
sudo yum update
```

2. 如有必要，使用以下命令获取 busybox 软件包：

```
sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/b/
busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
```

3. 如有必要，使用以下命令安装必备软件包：

```
sudo yum install busybox.rpm iasl -y
```

4. 运行以下 `iasl` 命令从 ACPI 表中生成输出：

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. 运行以下命令以查看 `iasl` 命令的输出：

```
cat SSDT2.dsl
```

输出应该产生检索虚拟机生成标识符所需的地址空间：

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
 * Intel ACPI Component Architecture
 * AML/ASL+ Disassembler version 20190509 (64-bit version)
 * Copyright (c) 2000 - 2019 Intel Corporation
 *
 * Disassembling to symbolic ASL+ operators
 *
 * Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
 *
 * Original Table Header:
 *     Signature        "SSDT"
 *     Length           0x0000007B (123)
 *     Revision         0x01
 *     Checksum         0xB8
 *     OEM ID           "AMAZON"
 *     OEM Table ID     "AMZNSSDT"
```

```
 *     OEM Revision     0x00000001 (1)
 *     Compiler ID      "AMZN"
 *     Compiler Version 0x00000001 (1)
 */
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
    Scope (\_SB)
    {
        Device (VMGN)
        {
            Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
            Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
            Name (_HID, "AMZN0000")  // _HID: Hardware ID
            Name (ADDR, Package (0x02)
            {
                0xFED01000,
                Zero
            })
        }
    }
}
```

6. （可选）使用以下命令提升终端对剩余步骤的权限：

```
sudo -s
```

7. 使用以下命令存储以前收集的地址空间：

```
VMGN_ADDR=0xFED01000
```

8. 使用以下命令迭代地址空间并构建虚拟机生成标识符：

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. 使用以下命令从输出文件中检索虚拟机生成标识符：

```
cat vmgenid ; echo
```

您的输出应类似于以下内容：

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. 根据需要，使用以下命令更新现有软件包：

```
sudo apt update
```

2. 如有必要，使用以下命令安装必备软件包：

```
sudo apt install busybox iasl -y
```

3. 运行以下 `iasl` 命令从 ACPI 表中生成输出：

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. 运行以下命令以查看 `iasl` 命令的输出：

```
cat SSDT2.dsl
```

输出应该产生检索虚拟机生成标识符所需的地址空间：

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
 * Intel ACPI Component Architecture
 * AML/ASL+ Disassembler version 20190509 (64-bit version)
 * Copyright (c) 2000 - 2019 Intel Corporation
 *
 * Disassembling to symbolic ASL+ operators
 *
 * Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
 *
 * Original Table Header:
 *     Signature        "SSDT"
 *     Length           0x0000007B (123)
 *     Revision         0x01
 *     Checksum         0xB8
 *     OEM ID           "AMAZON"
 *     OEM Table ID     "AMZNSSDT"
 *     OEM Revision     0x00000001 (1)
 *     Compiler ID      "AMZN"
 *     Compiler Version 0x00000001 (1)
 */
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
    Scope (\_SB)
    {
        Device (VMGN)
        {
            Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
            Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
            Name (_HID, "AMZN0000")  // _HID: Hardware ID
            Name (ADDR, Package (0x02)
            {
                0xFED01000,
                Zero
            })
        }
    }
}
```

5. （可选）使用以下命令提升终端对剩余步骤的权限：

```
sudo -s
```

6. 使用以下命令存储以前收集的地址空间：

```
VMGN_ADDR=0xFED01000
```

7. 使用以下命令迭代地址空间并构建虚拟机生成标识符：

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. 使用以下命令从输出文件中检索虚拟机生成标识符：

```
cat vmgenid ; echo
```

您的输出应类似于以下内容：

```
EC2F335D979132C4165896753E72BD1C
```

EC2 队列和 Spot 队列

您可以使用 EC2 队列或 Spot 队列启动实例队列。在单个 API 调用中，队列可以同时使用按需型实例、预留实例和竞价型实例购买选项跨多个可用区启动多种实例类型。

主题

- EC2 Fleet (p. 814)
- Spot 队列 (p. 871)
- 使用 Amazon EventBridge 监控队列事件 (p. 920)
- EC2 队列和 Spot 队列教程 (p. 935)
- EC2 队列和 Spot 队列配置示例 (p. 945)
- 队列配额 (p. 970)

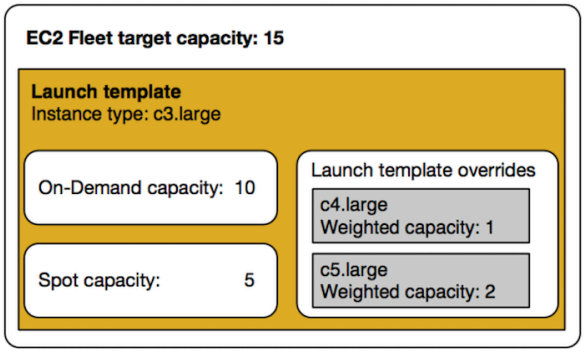
EC2 Fleet

EC2 队列 包含用于启动实例队列（或实例组）的配置信息。在单个 API 调用中，队列可以同时使用按需型实例、预留实例和竞价型实例购买选项跨多个可用区启动多种实例类型。通过使用 EC2 队列，您可以：

- 定义单独的按需和 Spot 容量目标以及您愿意每小时支付的最大金额
- 指定最适合您的应用程序的实例类型
- 指定 Amazon EC2 应如何在每个购买选项中分配您的队列容量

也可以设置您愿意为队列支付的每小时最大金额，EC2 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

EC2 队列会尝试启动适当数量的实例，以满足在您的请求中指定的目标容量要求。如果您指定了每小时最高总价，它将满足容量要求，直至达到您愿意支付的最大金额。如果竞价型实例中断，队列还可能会尝试保持其目标 Spot 容量。有关更多信息，请参阅竞价型实例的工作原理 (p. 453)。



您可以为每个 EC2 队列指定无限数量的实例类型。那些实例类型可以使用按需和 Spot 购买选项进行预配置。您也可以指定多个可用区，为每个实例指定不同的最高 Spot 价格，并为每个队列选择其他 Spot 选项。Amazon EC2 在队列启动时使用指定的选项来预置容量。

当队列运行时，如果 Amazon EC2 因价格上涨或实例失败而回收竞价型实例，EC2 实例集会尝试将实例替换为您指定的任何实例类型的实例。这使得可在 Spot 价格高峰期间更轻松地重新获取容量。您可以为每个

队列制定灵活的弹性资源配置策略。例如，在特定的队列中，您可以用成本较低的 Spot 容量 (如果可用) 按需补充主容量。

如果有预留实例，并且在队列中指定按需型实例，EC2 实例集会使用预留实例。例如，如果机群指定 `c4.large` 个按需型实例，而您有 `c4.large` 预留实例，则采用Reserved Instance定价。

使用 EC2 队列 不收取任何额外费用。您只需为队列为您启动的 EC2 实例付费。

目录

- EC2 队列限制 (p. 815)
- 可突增性能实例 (p. 815)
- EC2 队列请求类型 (p. 815)
- EC2 队列配置策略 (p. 832)
- 使用 EC2 队列 (p. 853)

EC2 队列限制

以下限制适用于 EC2 队列。

- EC2 实例集仅可通过 Amazon EC2 API、Amazon CLI、Amazon 开发工具包 和 Amazon CloudFormation 访问。
- EC2 队列请求不能跨 Amazon 区域。您需要为每个区域创建单独的 EC2 队列。
- EC2 队列请求不能跨同一可用区内的不同子网。

可突增性能实例

如果您使用可突增性能的实例类型 (p. 274)启动您的 Spot 实例，并打算立即并短时间使用可突增性能的 Spot 实例，且没有空闲时间来积累 CPU 积分，建议您以标准模式 (p. 288)启动实例，以避免支付更高的成本。如果您以无限模式 (p. 282)启动可突增性能的 Spot 实例并立即突增 CPU，您将会为突增花费超额积分。如果使用实例的时间很短，使得实例没有时间积累 CPU 积分来支付超额积分，则您将在终止实例时为超额积分付费。

仅当实例的运行时间较长，足以积累进行突增的 CPU 积分时，针对可突增性能的竞价型实例的无限模式才适用。否则，支付剩余积分会使可突增性能的竞价型实例比使用其他实例更加昂贵。有关更多信息，请参阅何时使用无限模式与固定 CPU (p. 283)。

通过提供足够的计算资源来配置实例，启动积分旨在为 T2 实例提供有成效的初始启动体验。不允许重复启动 T2 实例以访问新的启动积分。如果您需要持续的 CPU，您可以赚取积分（通过空转一段时间），将无限模式 (p. 282)用于 T2 Spot 实例，或将实例类型和专用 CPU 一起使用。

EC2 队列请求类型

EC2 队列请求有三种类型：

`instant`

如果您将请求类型配置为 `instant`，EC2 队列会针对所需容量发出同步一次性请求。在 API 响应中，它返回启动的实例以及那些无法启动实例的错误。有关更多信息，请参阅使用类型为 'instant' 的 EC2 队列 (p. 816)。

`request`

如果您将请求类型配置为 `request`，EC2 队列针对所需容量发出异步一次性请求。此后，如果由于 Spot 中断导致容量减少，队列不会尝试补充竞价型实例，也不会当容量不可用时在其他 Spot 容量池中提交请求。

`maintain`

（默认）如果您将请求类型配置为 `maintain`，EC2 队列针对所需容量发出异步请求，并自动补充任何中断的 Spot 实例 以保持容量。

所有三种请求类型都可通过分配策略获益。有关更多信息，请参阅竞价型实例的分配策略 (p. 833)。

使用类型为 'instant' 的 EC2 队列

instant 类型的 EC2 队列是同步一次性请求，该请求只尝试启动所需容量一次。API 响应列出已启动的实例，以及那些无法启动实例的错误。使用 instant 类型的 EC2 队列有几个益处，本文会对其进行介绍。本文末尾提供了配置示例。

对于需要仅启动 API 来启动 EC2 实例的工作负载，您可以使用 RunInstances API。但是，通过 RunInstances，您只能启动按需实例或 Spot 实例，但不能在同一请求中启动两者。此外，当您使用 RunInstances 启动 Spot 实例时，您的 Spot 实例请求仅限于一个实例类型和一个可用区。此操作针对单个 Spot 容量池（一组具有相同实例类型和可用区的未使用实例）。如果 Spot 容量池没有足够的 Spot 实例容量来满足您的请求，则 RunInstances 调用将失败。

相比使用 RunInstances 启动 Spot 实例，我们建议您使用具有设为 `instant` 的 `type` 参数的 CreateFleet API，以获得以下益处：

- 在一个请求中启动按需实例和 Spot 实例。EC2 队列可以启动按需实例和/或 Spot 实例。如果具有可用的容量，并且您的请求的每小时最高价格超过 Spot 价格，则会满足竞价型实例请求。
- 提高 Spot 实例的可用性。通过使用类型为 `instant` 的 EC2 阶段，您可以根据 Spot 最佳实践启动 Spot 实例，获得以下益处：
  - Spot 最佳实践：灵活地选择实例类型和可用区。

    益处：通过指定多个实例类型和可用区，您可以增加 Spot 容量池的数量。这让 Spot 服务有更好的机会查找和分配所需的 Spot 计算容量。一条很好的经验法则是，对于每种工作负载，灵活地在至少 10 种实例类型之间进行选择，并确保所有可用区配置为在 VPC 中使用。
  - Spot 最佳实践：使用容量优化的分配策略。

    益处：`capacity-optimized` 分配策略自动从最可用的 Spot 容量池中预置实例。由于 Spot 实例容量来自于具有最佳容量的池，因此，这会降低在 Amazon EC2 需要回收容量时，将中断 Spot 实例的可能性。
- 获得更广泛功能集的访问权限。对于需要仅启动 API 的工作负载，并且您希望管理实例的生命周期，而不是让 EC2 队列为您进行管理，请使用类型为 `instant` 的 EC2 队列，而不是 RunInstances API。EC2 队列提供相比 RunInstances 更广泛的功能组，如以下示例所示。对于所有其他工作负载，您应该使用 Amazon EC2 Auto Scaling，因为它为各种工作负载（如 ELB 支持的应用程序、容器化工作负载和队列处理作业）提供了更全面的功能集。

Amazon EC2 Auto Scaling 和 Amazon EMR 等 Amazon 服务使用类型为 instant 的 EC2 队列启动 EC2 实例。

类型为 instant 的 EC2 队列的先决条件

有关创建 EC2 队列的先决条件，请参阅 EC2 队列先决条件 (p. 854)。

instant EC2 队列如何工作

使用类型为 `instant` 的 EC2 队列时，事件序列如下所示：

1. 将 CreateFleet 请求类型配置为 `instant`。有关更多信息，请参阅创建 EC2 队列 (p. 860)。请注意，在进行 API 调用之后，您无法修改它。
2. 如果您进行 API 调用，EC2 队列会针对所需容量发出同步一次性请求。

3. API 响应列出已启动的实例，以及那些无法启动实例的错误。
4. 您可以描述 EC2 队列、列出与 EC2 队列关联的实例，以及查看 EC2 队列的历史记录。
5. 实例启动后，您可以删除实例集请求。删除实例集请求时，您还可以选择终止关联的实例，或使其运行。
6. 您可以随时终止实例。

示例

以下示例显示如何使用类型为 `instant` 的 EC2 队列，以获取不同使用案例。有关使用 EC2 CreateFleet API 参数的更多信息，请参阅 Amazon EC2 API 引用中的 CreateFleet。

示例

- 示例 1：使用容量优化的分配策略启动 Spot 实例 (p. 817)
- 示例 2：使用容量优化分配策略启动单个 Spot 实例 (p. 818)
- 示例 3：使用实例权重启动 Spot 实例 (p. 820)
- 示例 4：在单个可用区内启动 Spot 实例 (p. 821)
- 示例 5：在单个可用区内启动单个实例类型的 Spot 实例 (p. 822)
- 示例 6：仅当可以启动最小目标容量时才启动 Spot 实例 (p. 824)
- 示例 7：仅当可在单个可用区中启动相同实例类型的最低目标容量时，才能启动 Spot 实例 (p. 825)
- 示例 8：启动具有多个启动模板的实例 (p. 826)
- 示例 9：启动基于按需实例的 Spot 实例 (p. 828)
- 示例 10：基于使用容量预留和优先分配策略的按需实例，使用容量优化分配策略启动 Spot 实例 (p. 829)
- 示例 11：使用容量优化优先级分配策略启动 Spot 实例 (p. 831)

示例 1：使用容量优化的分配策略启动 Spot 实例

下面的示例指定了类型为 `instant` 的 EC2 队列中所需的参数：启动模板、目标容量、原定设置购买选项，并启动模板覆盖。

- 启动模板由其启动模板名称和版本号标识。
- 12 个启动模板覆盖指定了 4 个不同的实例类型和 3 个不同的子网，每个子网都位于单独的可用区中。每个实例类型和子网组合都定义了 Spot 容量池，从而生成 12 个 Spot 容量池。
- 队列的目标容量为 20 个实例。
- 原定设置购买选项为 `spot`，这会导致实例集尝试在 Spot 容量池中启动 20 个 Spot 实例，并为启动的实例数量提供最佳容量。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
```

```
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"c5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922"
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

示例 2：使用容量优化分配策略启动单个 Spot 实例

您可以通过进行类型为 `instant` 的多个 EC2 队列 API 调用，将 TotalTargetCapacity 设置为 1，以最佳方式一次启动一个 Spot 实例。

下面的示例指定了类型为 instant 的 EC2 队列中所需的参数：启动模板、目标容量、原定设置购买选项和启动模板覆盖。启动模板由其启动模板名称和版本号标识。12 个启动模板覆盖有 4 个不同的实例类型和 3 个不同的子网，每个子网位于单独的可用区域中。实例集的目标容量为 1 个实例，并且原定设置购买选项为 Spot，这导致实例集尝试根据容量优化分配策略，从 12 个 Spot 容量池之一启动 Spot 实例，从最可用的容量池启动 Spot 实例。

```
{
```

```
"SpotOptions": {
    "AllocationStrategy": "capacity-optimized"
},
"LaunchTemplateConfigs": [
  {
     "LaunchTemplateSpecification":{
        "LaunchTemplateName":"ec2-fleet-lt1",
        "Version":"$Latest"
     },
     "Overrides":[
        {
           "InstanceType":"c5.large",
           "SubnetId":"subnet-fae8c380"
        },
        {
           "InstanceType":"c5.large",
           "SubnetId":"subnet-e7188bab"
        },
        {
           "InstanceType":"c5.large",
           "SubnetId":"subnet-49e41922"
        },
        {
           "InstanceType":"c5d.large",
           "SubnetId":"subnet-fae8c380"
        },
        {
           "InstanceType":"c5d.large",
           "SubnetId":"subnet-e7188bab"
        },
        {
           "InstanceType":"c5d.large",
           "SubnetId":"subnet-49e41922"
        },
        {
           "InstanceType":"m5.large",
           "SubnetId":"subnet-fae8c380"
        },
        {
           "InstanceType":"m5.large",
           "SubnetId":"subnet-e7188bab"
        },
        {
           "InstanceType":"m5.large",
           "SubnetId":"subnet-49e41922"
        },
        {
           "InstanceType":"m5d.large",
           "SubnetId":"subnet-fae8c380"
        },
        {
           "InstanceType":"m5d.large",
           "SubnetId":"subnet-e7188bab"
        },
        {
           "InstanceType":"m5d.large",
           "SubnetId":"subnet-49e41922"
        }
     ]
  }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 1,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
```

```
}
```

示例 3：使用实例权重启动 Spot 实例

以下示例使用实例权重，这意味着价格是每单位小时价格，而不是每实例小时价格。假定一个工作负载单位需要 15 GB 内存和 4 个 vCPU，每个启动配置列出不同的实例类型和不同的权重，具体取决于实例上可以运行的工作负载单位数。例如，m5.xlarge（4 个 vCPU 和 16 GB 内存）可以运行 1 个单位且权重为 1，m5.2xlarge（8 个 vCPUs 和 32 GB 内存）可以运行 2 个单位，且权重为 2，依此类推。总目标容量设置为 40 个单位。原定设置购买选项为 Spot，并且分配策略为容量优化，这会导致 40 个 m5.xlarge（40 除以 1），20 个 m5.2xlarge（40 除以 2），10 个 m5.4xlarge（40 除以 4），5 个 m5.8xlarge（40 除以 8），或基于容量优化分配策略，权重相加达到所需容量的实例类型的混合。

有关更多信息，请参阅EC2 队列实例权重 (p. 852)。

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.2xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":2
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":4
```

```
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":4
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

示例 4：在单个可用区内启动 Spot 实例

您可以通过将 Spot 选项 SingleAvailabilityZone 设置为 true（真），将实例集配置为启动单个可用区中的所有实例。

12 个启动模板覆盖具有不同的实例类型和子网（每个都位于单独的可用区），但权重容量相同。总目标容量为 20 个实例，原定设置购买选项为 Spot，并且 Spot 分配策略为容量优化。EC2 队列使用启动规范，从具有最佳容量的 Spot 容量池启动全部在单个可用区中的 20 个 Spot 实例。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
```

```
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

示例 5：在单个可用区内启动单个实例类型的 Spot 实例

您可以通过将 SpotOptions SingleInstanceType 和 SingleAvailabilityZone 设置为 true（真），将队列配置为启动单个可用区中相同实例类型的所有实例。

12 个启动模板覆盖具有不同的实例类型和子网（每个都位于单独的可用区），但权重容量相同。总目标容量为 20 个实例，原定设置购买选项为 Spot，Spot 分配策略为容量优化。EC2 队列使用启动规范，从具有最佳容量的 Spot 容量池启动全部在单个可用区中相同实例类型的 20 个 Spot 实例。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
```

```
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
   "TargetCapacitySpecification": {
       "TotalTargetCapacity": 20,
       "DefaultTargetCapacityType": "spot"
   },
   "Type": "instant"
}
```

示例 6：仅当可以启动最小目标容量时才启动 Spot 实例

只有通过将 Spot 选项 MinTargetCapacity 设置为要同时启动的最小目标容量，以启动最小目标容量，您才可以将队列配置为启动实例。

12 个启动模板覆盖具有不同的实例类型和子网（每个都位于单独的可用区），但权重容量相同。总目标容量和最小目标容量均为 20 个实例，原定设置购买选项为 Spot，Spot 分配策略为容量优化。只有在能够同时启动所有 20 个实例时，EC2 队列才能使用启动模板覆盖，从具有最佳容量的 Spot 容量池启动 20 个 Spot 实例。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
```

```
                "SubnetId":"subnet-e7188bab"
            },
            {
                "InstanceType":"m5d.4xlarge",
                "SubnetId":"subnet-49e41922"
            }
        ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

示例 7：仅当可在单个可用区中启动相同实例类型的最低目标容量时，才能启动 Spot 实例

只有通过将 Spot 选项 MinTargetCapacity，以及 SingleInstanceType 和 SingleAvailabilityZone 选项设置为要同时启动的最小目标容量，以在单个可用区中，以单个实例类型启动最小目标容量，您才可以将队列配置为启动实例。

覆盖启动模板的 12 个启动规范具有不同的实例类型和子网（每个都位于单独的可用区），但权重容量相同。总目标容量和最小目标容量均为 20 个实例，原定设置购买选项为 Spot，Spot 分配策略为容量优化，SingleInstanceType 和 SingleAvailabilityZone 均为 true（真）。只有在能够同时启动所有 20 个实例时，EC2 队列才能使用启动规范，从具有最佳容量的 Spot 容量池，启动全部在单个可用区中相同实例类型的 20 个 Spot 实例。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.4xlarge",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.4xlarge",
              "SubnetId":"subnet-e7188bab"
           },
           {
```

```
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

示例 8：启动具有多个启动模板的实例

您可以通过指定多个启动模板来配置队列，以便为不同的实例类型或一组实例类型启动具有不同启动规范的实例。在此示例中，我们希望为不同实例类型提供不同的 EBS 卷大小，并且我们已经在启动模板 ec2-fleet-lt-4xl、ec2-fleet-lt-9xl 和 ec2-fleet-lt-18xl 中进行配置。

在此示例中，我们根据大小为 3 种实例类型使用了 3 种不同启动模板。所有启动模板上的启动规范覆盖使用基于实例类型上 vCPU 的实例权重。总目标容量为 144 个单位，原定设置购买选项为 Spot，并且 Spot 分配策略为容量优化。EC2 队列可以使用启动模板 ec2-fleet-4xl 启动 9 个 c5n.4xlarge（144 除以 16），或者使用启动模板 ec2-fleet-9xl 启动 4 个 c5n.9xlarge（144 除以 36），或者使用启动模板 ec2-fleet-18xl 启动 2 个 c5n.18xlarge（144 除以 72），或基于容量优化分配策略，权重相加达到所需容量的实例类型的混合。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5n.18xlarge",
               "SubnetId":"subnet-fae8c380",
```

```
            "WeightedCapacity":72
         },
         {
            "InstanceType":"c5n.18xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":72
         },
         {
            "InstanceType":"c5n.18xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":72
         }
      ]
   },
   {
      "LaunchTemplateSpecification":{
         "LaunchTemplateName":"ec2-fleet-lt-9xl",
         "Version":"$Latest"
      },
      "Overrides":[
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":36
         }
      ]
   },
   {
      "LaunchTemplateSpecification":{
         "LaunchTemplateName":"ec2-fleet-lt-4xl",
         "Version":"$Latest"
      },
      "Overrides":[
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":16
         },
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":16
         },
         {
            "InstanceType":"c5n.4xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":16
         }
      ]
   }
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 144,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
```

```
}
```

示例 9：启动基于按需实例的 Spot 实例

下面的示例为队列指定 20 个实例的总目标容量和 5 个按需实例的目标容量。原定设置购买选项为 Spot。队列按照指定的方式启动 5 个按需实例，但需要再启动 15 个实例以满足总目标容量要求。差值购买选项的计算公式为 TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType，这使得启动 15 个 Spot 实例的队列根据容量优化分配策略构成 12 个 Spot 容量池之一。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
          "LaunchTemplateSpecification":{
             "LaunchTemplateName":"ec2-fleet-lt1",
             "Version":"$Latest"
          },
          "Overrides":[
             {
                "InstanceType":"c5.large",
                "SubnetId":"subnet-fae8c380"
             },
             {
                "InstanceType":"c5.large",
                "SubnetId":"subnet-e7188bab"
             },
             {
                "InstanceType":"c5.large",
                "SubnetId":"subnet-49e41922"
             },
             {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-fae8c380"
             },
             {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-e7188bab"
             },
             {
                "InstanceType":"c5d.large",
                "SubnetId":"subnet-49e41922"
             },
             {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-fae8c380"
             },
             {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-e7188bab"
             },
             {
                "InstanceType":"m5.large",
                "SubnetId":"subnet-49e41922"
             },
             {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-fae8c380"
             },
             {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab"
             },
```

```
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

示例 10：基于使用容量预留和优先分配策略的按需实例，使用容量优化分配策略启动 Spot 实例

您可以通过将容量预留的使用策略配置为 use-capacity-reservations-first（首先使用容量预留），来将队列配置为在以原定设置目标容量类型作为 Spot 启动按需实例的基础时，首先使用按需容量预留。此外，如果多个实例池具有未使用的 容量预留，则应用选定的按需分配策略。在此示例中，按需分配策略为优先级。

在该示例中，有 6 个可用的未使用容量预留。此数目少于队列的 10 个按需实例的目标按需容量。

账户在 2 个池中有以下 6 个未使用的容量预留。每个池中的容量预留数由 AvailableInstanceCount 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

以下队列配置仅显示该示例的相关配置。按需分配策略为优先级，容量预留的使用策略为 use-capacity-reservations-first（首先使用容量预留）。Spot 分配策略为容量优化。总目标容量为 20，按需目标容量为 10，原定设置目标容量类型为 Spot。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
```

```
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 8.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 9.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 10.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 11.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 12.0
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

在使用上述配置创建 instant 队列后，将启动下面的 20 个实例来满足目标容量：

- us-east-1a 中的 7 个 c5.large 按需实例 – us-east-1a 中的 c5.large 的优先级第一，并且有 3 个可用的未使用 c5.large 容量预留。首先使用容量预留启动 3 个按需实例，并根据按需分配策略（此示例中为优先级）启动另 4 个按需实例。
- us-east-1a 中的 3 个 m5.large 按需实例 – us-east-1a 中的 m5.large 的优先级第二，并且有 3 个可用的未使用的 c3.large 容量预留。
- 来自 12 个 Spot 容量池之一的 10 个 Spot 实例，该容量池根据容量优化的分配策略具有最佳容量。

在启动队列后，您可以运行 describe-capacity-reservations 来查看保留的未使用的 容量预留 的数目。在此示例中，您该看到以下响应，该响应指示已使用所有 c5.large 和 m5.large 容量预留。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

示例 11：使用容量优化优先级分配策略启动 Spot 实例

下面的示例指定了类型为 instant 的 EC2 队列中所需的参数：启动模板、目标容量、原定设置购买选项和启动模板覆盖。启动模板由其启动模板名称和版本号标识。覆盖启动模板的 12 个启动规范具有分配了优先级的 4 个不同的实例类型，以及 3 个不同的子网（每个都位于单独的可用区）。队列的目标容量是 20 个实例，原定设置购买选项为 Spot，这导致队列尝试根据容量优化优先级的分配策略，从 12 个 Spot 容量池之一启动 20 个 Spot 实例，该策略会尽最大努力实施优先级，但首先会针对容量进行优化。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 4.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

EC2 队列配置策略

EC2 队列 是一组按需实例和 Spot 实例。

EC2 队列 尝试启动适当数量的实例，以满足您在队列请求中指定的目标容量要求。队列可能仅包含按需型实例，仅包含竞价型实例或包含按需型实例和竞价型实例的组合。如果具有可用的容量，并且您的请求的每小时最高价格超过 Spot 价格，则会满足竞价型实例请求。如果竞价型实例中断，队列还会尝试保持其目标容量。

也可以设置您愿意为队列支付的每小时最大金额，EC2 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

Spot 容量池是一组具有相同实例类型和可用区的未使用 EC2 实例。在您创建 EC2 队列时，可以指定多个启动规范 (因实例类型、可用区、子网以及最高价而异)。该队列会基于请求中包含的启动说明以及请求的配置来选择用于执行请求的 Spot 容量池。竞价型实例来自所选的池。

EC2 队列让您能基于核心或实例数量或内存量预配置适合于您的应用程序的大量 EC2 容量。例如，您可以指定 EC2 实例集启动 200 个实例的目标容量，其中 130 个是按需型实例，其余是竞价型实例。

使用适当的配置策略创建满足您的需求的EC2 队列。

目录

- 规划 EC2 队列 (p. 833)
- 竞价型实例的分配策略 (p. 833)
- EC2 机群的基于属性的实例类型选择 (p. 836)
- 配置 EC2 队列 以进行按需备份 (p. 848)
- 容量再平衡 (p. 849)
- 最高价覆盖 (p. 851)
- 控制支出 (p. 851)
- EC2 队列实例权重 (p. 852)

规划 EC2 队列

规划 EC2 队列时，建议执行以下操作：

- 确定您要创建的 EC2 队列是针对所需目标容量提交同步或异步一次性请求，还是随着时间推移保持目标容量。有关更多信息，请参阅EC2 队列请求类型 (p. 815)。
- 确定满足您的应用程序要求的实例类型。
- 如果计划在 EC2 队列中包含 Spot 实例，在创建队列之前，请查看 Spot 最佳实践。使用这些最佳实践规划您的队列，以便以可能的最低价预配置实例。
- 确定您的 EC2 队列的目标容量。您可以采用实例或自定义单位设置目标容量。有关更多信息，请参阅EC2 队列实例权重 (p. 852)。
- 确定 EC2 队列目标容量的多大部分必须是按需容量和 Spot 容量。您可以为按需容量和/或 Spot 容量指定 0。
- 确定您的每单位价格 (如果使用实例权重)。要计算每单位价格，请将每实例小时价格除以该实例表示的单位数 (或权重)。如果不使用实例权重，则默认每单位价格为每实例小时价格。
- 确定您愿意为队列支付的每小时最大金额。有关更多信息，请参阅控制支出 (p. 851)。
- 查看可用于您的 EC2 队列的可能选项。有关机群参数的信息，请参阅 Amazon CLI 命令参考中的 create-fleet。有关 EC2 队列配置示例，请参阅EC2 队列 示例配置 (p. 945)。

竞价型实例的分配策略

您的启动配置决定了 EC2 Fleet 可以从中启动竞价型实例的所有可能竞价型容量池（实例类型和可用区）。但在启动实例时，EC2 Fleet 将使用您指定的分配策略从所有可能的池中选择特定的池。

您可以指定下面的任何一种分配策略：

`price-capacity-optimized`（推荐）

EC2 实例集为正在启动的实例数识别具有最高可用容量的池。这意味着我们将从我们认为短期内中断概率最低的池中请求竞价型实例。然后，EC2 实例集从这些池中价格最低的池请求竞价型实例。

`price-capacity-optimized` 分配策略是大多数 Spot 工作负载的最佳选择，例如无状态容器化应用程序、微服务、Web 应用程序、数据和分析任务以及批处理。

`capacity-optimized`

EC2 实例集为正在启动的实例数识别具有最高可用容量的池。这意味着我们将从我们认为短期内中断概率最低的池中请求竞价型实例。您可以选择使用 `capacity-optimized-prioritized` 为队列中的每种实例类型设置优先级。EC2 队列首先会针对容量进行优化，但会尽最大努力遵循实例类型的优先级。

使用竞价型实例，定价会根据长期供需趋势缓慢发生变化，但容量会实时波动。`capacity-optimized` 策略通过查看实时容量数据并预测可用性最高的池，自动在可用性最高的池中启动 Spot 实例。这适用于因重启工作而导致中断成本更高的工作负载，例如长时间持续集成（CI）、图像和媒体渲染、深度学习以及高性能计算（HPC）工作负载，这些工作负载可能具有与重启工作相关的更高的中断成本。通过实现更低的中断可能性，`capacity-optimized` 策略可以降低您工作负载的整体成本。

或者，您也可以使用 `capacity-optimized-prioritized` 分配策略，该策略带有优先级参数，以便从最高到最低优先级对实例类型进行排序。您可以为不同的实例类型设置相同的优先级。EC2 队列首先会针对容量进行优化，但会尽最大努力遵循实例类型的优先级（例如，如果遵循优先级不会显著影响 EC2 队列预置最佳容量的能力）。对于必须最大限度地减少中断可能性，同时对某些实例类型的偏好也很重要的工作负载来说，这是一个不错的选择。仅当您的队列使用启动模板时，才支持使用优先级。请注意，当您为 `capacity-optimized-prioritized` 设置优先级时，如果按需 `AllocationStrategy` 设置为 `prioritized`，那么相同的优先级也会应用于您的按需型实例。

`diversified`

竞价型实例 分布在所有 Spot 容量池中。

`lowest-price`

竞价型实例来自价格最低并且具有可用容量的池。这是默认策略。然而，我们建议您通过指定 `price-capacity-optimized` 分配策略来覆盖默认值。

如果价格最低的池没有可用容量，则竞价型实例将来自价格次低且具有可用容量的池。

如果某个池在满足您所需的容量之前耗尽容量，则 EC2 实例集将继续从价格次低的池中提取实例，以满足您的请求。为确保达到所需容量，您可能会获得来自多个容量池的竞价型实例。

由于此策略仅考虑实例价格而不考虑容量可用性，因此可能会导致较高的中断率。

`InstancePoolsToUseCount`

在其中分配您的目标 Spot 容量的 Spot 池数量。仅当分配策略设置为 `lowest-price` 时有效。EC2 实例集选择价格最低的 Spot 池，并在指定数量的 Spot 池之间平均分配目标 Spot 容量。

请注意，EC2 实例集会尽力尝试根据您指定的池数量提取竞价型实例。如果池在满足您目标容量之前耗尽 Spot 容量，则 EC2 实例集将继续从价格次低的池中提取实例，以满足您的请求。为确保达到目标容量，您可能会从超过指定数量的池接收竞价型实例。同样，如果大多数池没有 Spot 容量，则您可能会从少于指定数量的池接收完整目标容量。

选择合适的分配策略

您可以选择适当的 Spot 分配策略，从而根据您的使用案例来优化实例集。对于按需型实例目标容量，EC2 实例集始终根据公开按需型价格选择价格最低的实例类型，同时对竞价型实例按照分配策略（`price-capacity-optimized`、`capacity-optimized`、`diversified` 或 `lowest-price`）执行分配。

平衡最低价格和可用容量

为了获得价格最低价格 Spot 容量池与具有最高可用容量的 Spot 容量池之间的平衡，我们建议您使用 price-capacity-optimized 分配策略。该策略根据池的价格以及这些池中竞价型实例的可用容量来决定向哪些池请求竞价型实例。这意味着将从我们认为短期内中断概率最低的池中请求竞价型实例，同时还要考虑价格。

如果您的实例集运行弹性和无状态的工作负载（包括容器化应用程序、微服务、Web 应用程序、数据和分析作业以及批量处理），则使用 price-capacity-optimized 分配策略以实现最大的成本节约和可用容量。

如果实例集运行的工作负载可能会因重启工作而导致更高的中断成本，则应设置检查点，以便应用程序中断时可从该点重启。通过使用检查点，可以使 price-capacity-optimized 分配策略变得非常适合这些工作负载，因其会从价格最低的池中分配容量，这些池同时还具有较低的竞价型实例中断率。

有关使用 price-capacity-optimized 分配策略的示例配置，请参阅 示例 11：在价格容量优化的实例集中启动竞价型实例 (p. 957)。

当工作负载拥有较高中断成本时

如果您运行的工作负载使用价格相似的实例类型，或中断成本非常高，以至于任何成本节约都不足以负担一个轻微中断，则可以选择使用 capacity-optimized 策略。此策略从可用容量最多的 Spot 容量池分配容量，这些容量池中断的可能性更低，从而可降低您工作负载的整体成本。有关使用 capacity-optimized 分配策略的示例配置，请参阅 示例 9：在容量优化的队列中启动竞价型实例 (p. 955)。

如果必须将中断的可能性降至最低，但某些实例类型的首选项又很紧要时，则您可以通过使用 capacity-optimized-prioritized 分配策略来表达您的池优先级，然后将要使用的实例类型的顺序设置为从最高到最低优先级。有关示例配置，请参阅 示例 10：在具有优先级的容量优化队列中启动竞价型实例 (p. 956)。

请注意，仅当您的实例集使用启动模板时，才支持使用优先级。还需注意，为 capacity-optimized-prioritized 设置优先级时，如果按需 AllocationStrategy 设置为 prioritized，那么相同的优先级也会应用于您的按需型实例。

当您的工作负载时间灵活且可用容量不是一个因素时

如果您的实例集较小或运行时间较短，则可以使用 price-capacity-optimized 来最大限度地节省成本，同时还要考虑可用容量。

如果您的工作负载时间灵活且可用容量不是一个因素，则可以选择使用 lowest-price 分配策略来最大限度地节省成本。然而请注意，由于 lowest-price 分配策略仅考虑实例价格而不考虑可用容量，因此可能会导致较高的竞价型实例中断率。

当您的实例集较大或运行时间较长时

如果队列较大或长时间运行，则可以通过使用 diversified 策略在多个池间分配 Spot 实例 来提高队列的可用性。例如，如果 EC2 实例集指定 10 个池，目标容量为 100 个实例，则队列会在每个池中启动 10 个竞价型实例。如果某个池的 Spot 价格超过您在该池中的最高价，您的队列仅 10% 受到影响。使用此策略还可降低您的队列对单个池的 Spot 价格随时间上涨的敏感度。使用 diversified 策略时，EC2 队列不在 Spot 价格等于或高于按需价格的任何池中启动 Spot 实例。

若要创建低成本且多元化的实例集，请将 lowest-price 策略与 InstancePoolsToUseCount 结合使用。例如，如果您的目标容量是 10 个竞价型实例，并且您（为 InstancePoolsToUseCount）指定了 2 个 Spot 容量池，则 EC2 实例集将从两个价格最低的池提取实例，以满足您的 Spot 容量。

您可以使用少量或大量的 Spot 容量池以在其中分配您的竞价型实例。例如，如果您运行批处理，我们建议指定少量的 Spot 容量池（例如，InstancePoolsToUseCount=2）以确保队列始终具有计算容量，同时尽可能节省成本。如果您运行 Web 服务，我们建议您指定大量 Spot 容量池（例如，InstancePoolsToUseCount=10）以尽可能减少某个 Spot 容量池临时不可用造成的影响。

请注意，EC2 实例集会尽力尝试根据您指定的池数量提取竞价型实例。如果池在满足您目标容量之前耗尽 Spot 容量，则 EC2 实例集将继续从价格次低的池中提取实例，以满足您的请求。为确保达到目标容量，您可能会从超过指定数量的池接收竞价型实例。同样，如果大多数池没有 Spot 容量，则您可能会从少于指定数量的池接收完整目标容量。

维持目标容量

在 Spot 实例 因 Spot 价格或 Spot 容量池的可用容量发生变化而终止之后，`maintain` 类型的 EC2 队列 会启动替换 Spot 实例。分配策略确定从哪个池启动替换实例，如下所示：

- 如果分配策略是 `price-capacity-optimized`，则实例集在具有最多竞价型实例容量的池中启动替换实例，同时还要考虑价格并确定价格最低且具有高可用容量的池。
- 如果分配策略是 `capacity-optimized`，则实例集在当前具有最多竞价型实例可用容量的池中启动替换实例。
- 如果分配策略是 `diversified`，则队列在其余池间分配替换 Spot 实例。
- 如果分配策略是 `lowest-price`，则 队列在当前具有最低 Spot 价格的池中启动替换实例。
- 如果分配策略是 `lowest-price` 与 `InstancePoolsToUseCount` 的组合，则队列选择具有最低价格的 Spot 容量池并跨您指定数量的 Spot 容量池启动 Spot 实例。

EC2 机群的基于属性的实例类型选择

创建 EC2 机群时，必须指定一种或多种实例类型以配置机群中的按需型实例和竞价型实例。除了手动指定实例类型外，还可以指定实例必须具有的属性，Amazon EC2 将使用这些属性标识所有实例类型。这称为基于属性的实例类型选择。例如，您可以指定实例所需的最小和最大 vCPU 数量，EC2 机群将使用满足这些 vCPU 要求的任何可用实例类型启动实例。

基于属性的实例类型选择是工作负载和框架的理想选择，这些工作负载和框架可以灵活地确定所用的实例类型，例如在运行容器或 Web 机群、处理大数据以及实施持续集成和部署 (CI/CD) 工具等情况下。

优点

基于属性的实例类型选择具有以下优势：

- 有如此多的实例类型可供使用，因此找到适用于您的工作负载的实例类型可能非常耗时。当您指定实例属性时，实例类型将自动具有工作负载所需的属性。
- 要为 EC2 机群手动指定多种实例类型，您必须为每种实例类型创建单独的启动模板覆盖。但是，借助基于属性的实例类型选择，要提供多种实例类型，您只需在启动模板或启动模板覆盖中指定实例属性即可。
- 当您指定实例属性而不是实例类型时，您的机群可以在新一代实例类型发布时使用这些实例类型，“满足未来”机群配置的需求。
- 当您指定实例属性而不是实例类型时，EC2 机群可以从各种实例类型中进行选择以启动竞价型实例，从而遵循灵活选择实例类型 Spot 最佳实践 (p. 451)。

主题

- 基于属性的实例类型选择的工作原理 (p. 836)
- 注意事项 (p. 838)
- 通过基于属性的实例类型选择创建 EC2 机群 (p. 838)
- 有效配置示例和无效配置示例 (p. 839)
- 预览具有指定属性的实例类型 (p. 845)

基于属性的实例类型选择的工作原理

要在机群配置中使用基于属性的实例类型选择，请将实例类型列表替换为实例所需的实例属性列表。EC2 机群将在具有指定实例属性的任何可用实例类型上启动实例。

主题

- 实例属性的类型 (p. 837)
- 在何处配置基于属性的实例类型选择 (p. 837)
- 预置机群时，EC2 机群如何使用基于属性的实例类型选择 (p. 837)
- 价格保护 (p. 837)

实例属性的类型

您可以指定几个实例属性来表示计算需求。有关每个属性和默认值的描述，请参阅 Amazon EC2 API 参考中的 InstanceRequirements。

在何处配置基于属性的实例类型选择

根据您使用的是控制台还是 Amazon CLI，可以按如下方式为基于属性的实例类型选择指定实例属性：

在控制台中，您可以在以下实例集配置组件中指定实例属性：

- 在启动模板中，并在实例集请求中引用启动模板

在 Amazon CLI 中，您可以在以下一个或全部机群配置组件中指定实例属性：

- 在启动模板中，并在实例集请求中引用启动模板
- 在启动模板覆盖中

  如果您想混合应用使用不同 AMI 的实例，则可以在多个启动模板覆盖中指定实例属性。例如，不同的实例类型可以使用 x86 和基于 ARM 的处理器。
- 在启动规范中

预置机群时，EC2 机群如何使用基于属性的实例类型选择

EC2 机群通过以下方式预置实例集：

- EC2 机群标识具有指定属性的实例类型。
- EC2 机群使用价格保护确定要排除的实例类型。
- EC2 机群根据具有匹配实例类型的Amazon区域或可用区确定将从中启动实例的容量池。
- EC2 机群应用指定的分配策略以确定从中启动实例的容量池。

  请注意，基于属性的实例类型选择不会选择从中预置机群的容量池；这是分配策略的任务。可能有大量具有指定属性的实例类型，其中一些类型可能成本高昂。竞价型和按需型的 `lowest-price` 默认分配策略可保证 EC2 机群将从成本最低的容量池启动实例。

  如果您指定分配策略，EC2 机群将根据指定的分配策略启动实例。
  - 对于竞价型实例，基于属性的实例类型选择支持 `price-capacity-optimized`、`capacity-optimized` 和 `lowest-price` 分配策略。
  - 对于按需型实例，基于属性的实例类型选择支持 `lowest-price` 分配策略。
- 如果没有适用于具有指定实例属性的实例类型的容量，则无法启动任何实例，并且机群返回错误。

价格保护

价格保护是一项功能，可以防止 EC2 机群使用您认为成本过高的实例类型，即使它们恰好适合您指定的属性。当您使用基于属性的实例类型选择创建机群时，默认情况下会启用价格保护，并为按需型实例和竞价型实例设置了单独的阈值。当 Amazon EC2 选择具有您的属性的实例类型时，会排除定价高于阈值的实例类

型。阈值表示您将支付的最大值，以高于具有指定属性的成本最低的最新一代 M、C 或 R 实例类型的百分比表示。

如果不指定阈值，默认情况下将使用以下阈值：

- 对于按需型实例，价格保护阈值设置为 20%。
- 对于竞价型实例，价格保护阈值设置为 100%。

指定价格保护阈值

创建 EC2 机群时，配置机群以使用基于属性的实例类型选择，然后执行以下操作：

- 若要指定按需型实例价格保护阈值，请在 JSON 配置文件的 `InstanceRequirements` 结构中，为 `OnDemandMaxPricePercentageOverLowestPrice` 输入以百分比表示的价格保护阈值。
- 若要指定竞价型实例价格保护阈值，请在 JSON 配置文件的 `InstanceRequirements` 结构中，为 `SpotMaxPricePercentageOverLowestPrice` 输入以百分比表示的价格保护阈值。

有关创建机群的更多信息，请参阅 通过基于属性的实例类型选择创建 EC2 机群 (p. 838)。

> **Note**
>
> 创建 EC2 机群时，如果您将 `TargetCapacityUnitType` 设置为 `vcpu` 或 `memory-mib`，价格保护阈值将基于每个 vCPU 或每个内存的价格应用，而不是基于每个实例的价格应用。

注意事项

- 您可以在 EC2 机群中指定实例类型或实例属性，但不能同时指定两者。

  使用 CLI 时，启动模板覆盖将覆盖启动模板。例如，如果启动模板包含实例类型，而启动模板覆盖包含实例属性，则由实例属性标识的实例将覆盖启动模板中的实例类型。
- 使用 CLI 时，如果将实例属性指定为覆盖，也无法指定权重或优先级。
- 在一个请求配置中，最多可以指定四个 `InstanceRequirements` 结构。

通过基于属性的实例类型选择创建 EC2 机群

您可以通过 Amazon CLI 将机群配置为使用基于属性的实例类型选择。

若要通过基于属性的实例类型选择创建 EC2 实例集（Amazon CLI）

使用 create-fleet（Amazon CLI）命令创建 EC2 实例集。在 JSON 文件中指定机群配置。

```
aws ec2 create-fleet \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

示例 *file_name*.json 文件

以下示例包含配置 EC2 实例集的参数，以使用基于属性的实例类型选择，后附文本说明。

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
```

```
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

基于属性的实例类型选择的属性在 InstanceRequirements 结构中指定。在此示例中，指定了两个属性：

- VCpuCount – 至少指定了 2 个 vCPU。由于未指定最大值，因此没有最大限制。
- MemoryMiB – 至少指定了 4 MiB 的内存。由于未指定最大值，因此没有最大限制。

将识别具有 2 个或更多 vCPU 和 4 MiB 或更大内存的任何实例类型。然而，当 EC2 实例集预置实例集 (p. 837)时，价格保护和分配策略可能会排除某些实例类型。

有关您可以指定的所有可能属性的列表和描述，请参阅 Amazon EC2 API Reference（《Amazon EC2 API 参考》）中的 InstanceRequirements。

> **Note**
>
> 当 InstanceRequirements 包含在机群配置中时，必须排除 InstanceType 和 WeightedCapacity；它们无法与实例属性同时确定机群配置。

JSON 还包含以下实例集配置：

- "AllocationStrategy": "*price-capacity-optimized*" – 实例集中竞价型实例的分配策略。
- "LaunchTemplateName": "*my-launch-template*", "Version": "*1*" – 启动模板包含一些实例配置信息，但如果指定了任何实例类型，则这些配置信息将被 InstanceRequirements 中指定的属性覆盖。
- "TotalTargetCapacity": *20* – 目标容量为 20 个竞价型实例。
- "DefaultTargetCapacityType": "*spot*" – 默认容量为竞价型实例。
- "Type": "*instant*" – 实例集的请求类型是 instant。

有效配置示例和无效配置示例

如果您使用 Amazon CLI 创建 EC2 机群，必须确保机群配置有效。以下示例展示了有效配置和无效配置。

如果配置包含以下项，则视为无效：

- 单个 Overrides 结构，但同时包含 InstanceRequirements 和 InstanceType
- 两个 Overrides 结构，其中一个包含 InstanceRequirements，而另一个包含 InstanceType
- 两个 InstanceRequirements 结构，但在同一 LaunchTemplateSpecification 中具有重叠的属性值

示例配置

- 有效配置：具有覆盖的单个启动模板 (p. 840)
- 有效配置：具有多个 InstanceRequirements 的单个启动模板 (p. 841)
- 有效配置：两个启动模板，每个都具有覆盖 (p. 841)
- 有效配置：仅指定 InstanceRequirements，且属性值不重叠 (p. 842)
- 配置无效：Overrides 包含 InstanceRequirements 和 InstanceType (p. 843)
- 配置无效：两个 Overrides 包含 InstanceRequirements 和 InstanceType (p. 844)
- 配置无效：属性值重叠 (p. 844)

有效配置：具有覆盖的单个启动模板

以下配置有效。包含一个启动模板和一个 `Overrides` 结构（包含一个 `InstanceRequirements` 结构）。下面是示例配置的文本说明。

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

要使用基于属性的实例选择，您必须在机群配置中包含 `InstanceRequirements` 结构，并为机群中的实例指定所需的属性。

在上述示例中，指定了以下实例属性：

- `VCpuCount` – 实例类型的 vCPU 数量必须最少为 2 个，最多为 8 个。
- `MemoryMiB` – 实例类型的最大内存必须为 10240MiB。最小值 0 表示没有最低限制。

- MemoryGiBPerVCpu – 实例类型的每个 vCPU 内存最大值必须为 10000GiB。Min 参数是可选的。省略此属性表示没有最低限制。

TargetCapacityUnitType

TargetCapacityUnitType 参数为目标容量指定单位。在该示例中，目标容量是 5000，目标容量单位类型是 vcpu，它们共同指定了所需的 5000 个 vCPU 目标容量。EC2 机群将启动足够多的实例，以便机群中的 vCPU 总数为 5000 个 vCPU。

有效配置：具有多个 InstanceRequirements 的单个启动模板

以下配置有效。包含一个启动模板和一个 Overrides 结构（包含两个 InstanceRequirements 结构）。InstanceRequirements 中指定的属性有效，因为值不重叠，第一个 InstanceRequirements 结构指定 VCpuCount 为 0-2 个 vCPU，而第二个 InstanceRequirements 结构指定 4-8 个 vCPU。

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

有效配置：两个启动模板，每个都具有覆盖

以下配置有效。包含两个启动模板，每个模板都有一个 Overrides 结构（包含一个 InstanceRequirements 结构）。此配置适用于在同一机群中支持 arm 和 x86 架构。

```
{
        "LaunchTemplateConfigs": [
```

```
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

有效配置：仅指定 InstanceRequirements，且属性值不重叠

以下配置有效。包含两个 LaunchTemplateSpecification 结构，每个结构都有一个启动模板和一个 Overrides 结构（包含一个 InstanceRequirements 结构）。InstanceRequirements 中指定的属性有效，因为值不重叠，第一个 InstanceRequirements 结构指定 VCpuCount 为 0-2 个 vCPU，而第二个 InstanceRequirements 结构指定 4-8 个 vCPU。

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
```

```
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
            ]
        },
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyOtherLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
            {
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 4,
                        "Max": 8
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                }
            }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
  }
}
```

配置无效：Overrides 包含 InstanceRequirements 和 InstanceType

以下配置无效。Overrides 结构同时包含 InstanceRequirements 和 InstanceType。对于 Overrides，可以指定 InstanceRequirements 或 InstanceType，但不能同时指定两者。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "MyLaunchTemplate",
                "Version": "1"
            },
            "Overrides": [
            {
                "InstanceRequirements": {
                    "VCpuCount": {
                        "Min": 0,
                        "Max": 2
                    },
                    "MemoryMiB": {
                        "Min": 0
                    }
                }
            },
            {
                "InstanceType": "m5.large"
            }
            ]
        }
```

```
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

配置无效：两个 Overrides 包含 InstanceRequirements 和 InstanceType

以下配置无效。Overrides 结构同时包含 InstanceRequirements 和 InstanceType。您可以指定 InstanceRequirements 或 InstanceType，但不能同时指定两者，即使采用不同的 Overrides 结构也是如此。

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

配置无效：属性值重叠

以下配置无效。两个 InstanceRequirements 结构，每个结构都包含 "VCpuCount": {"Min": 0, "Max": 2}。这些属性的值重叠，这将导致容量池重复。

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                    }
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

预览具有指定属性的实例类型

您可以使用 get-instance-types-from-instance-requirements Amazon CLI 命令预览与您指定的属性匹配的实例类型。这对于在不启动任何实例的情况下确定要在请求配置中指定的属性尤其有用。请注意，该命令不考虑可用容量。

通过使用 Amazon CLI 指定属性来预览实例类型列表

1. （可选）要生成所有可以指定的可能属性，请使用 get-instance-types-from-instance-requirements 命令和 `--generate-cli-skeleton` 参数。您可以选择使用 `input > attributes.json` 将输出定向到某个文件以将其保存。

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

预期输出

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
```

```
"InstanceRequirements": {
    "VCpuCount": {
        "Min": 0,
        "Max": 0
    },
    "MemoryMiB": {
        "Min": 0,
        "Max": 0
    },
    "CpuManufacturers": [
        "intel"
    ],
    "MemoryGiBPerVCpu": {
        "Min": 0.0,
        "Max": 0.0
    },
    "ExcludedInstanceTypes": [
        ""
    ],
    "InstanceGenerations": [
        "current"
    ],
    "SpotMaxPricePercentageOverLowestPrice": 0,
    "OnDemandMaxPricePercentageOverLowestPrice": 0,
    "BareMetal": "included",
    "BurstablePerformance": "included",
    "RequireHibernateSupport": true,
    "NetworkInterfaceCount": {
        "Min": 0,
        "Max": 0
    },
    "LocalStorage": "included",
    "LocalStorageTypes": [
        "hdd"
    ],
    "TotalLocalStorageGB": {
        "Min": 0.0,
        "Max": 0.0
    },
    "BaselineEbsBandwidthMbps": {
        "Min": 0,
        "Max": 0
    },
    "AcceleratorTypes": [
        "gpu"
    ],
    "AcceleratorCount": {
        "Min": 0,
        "Max": 0
    },
    "AcceleratorManufacturers": [
        "nvidia"
    ],
    "AcceleratorNames": [
        "a100"
    ],
    "AcceleratorTotalMemoryMiB": {
        "Min": 0,
        "Max": 0
    },
    "NetworkBandwidthGbps": {
        "Min": 0.0,
        "Max": 0.0
    },
    "AllowedInstanceTypes": [
        ""
```

```
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 使用上一步的输出创建 JSON 配置文件，然后按如下方式进行配置：

   Note

   您必须提供 ArchitectureTypes、VirtualizationTypes、VCpuCount 和 MemoryMiB 的值。您可以省略其它属性；如果省略，则使用默认值。
   有关每个属性及其默认值的描述，请参阅 Amazon EC2 命令行参考中的 get-instance-types-from-instance-requirements。

   a. 对于 ArchitectureTypes，请指定一个或多个处理器架构类型。
   b. 对于 VirtualizationTypes，请指定一个或多个虚拟化类型。
   c. 对于 VCpuCount，请指定最小和最大 vCPU 数量。要指定没有最低限制，对于 Min，请指定 0。要指定没有最大限制，请省略 Max 参数。
   d. 对于 MemoryMiB，请指定最小和最大内存量（以 MiB 为单位）。要指定没有最低限制，对于 Min，请指定 0。要指定没有最大限制，请省略 Max 参数。
   e. 您可以选择指定一个或多个其他属性来进一步限制返回的实例类型列表。

3. 要预览具有您在 JSON 文件中所指定属性的实例类型，请使用 get-instance-types-from-instance-requirements 命令，然后使用 --cli-input-json 参数指定 JSON 文件的名称和路径。您可以选择将输出格式设置为以表格格式显示。

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

示例 *attributes.json* 文件

在此示例中，JSON 文件包含所需属性。它们是 ArchitectureTypes、VirtualizationTypes、VCpuCount 和 MemoryMiB。此外，还包含可选属性 InstanceGenerations。请注意，对于 MemoryMiB，可以省略 Max 值，指示没有限制。

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

输出示例

```
----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||             InstanceTypes             ||
|+-------------------------------------+|
||             InstanceType              ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. 在确定满足您的需求的实例类型后，请记下您使用的实例属性，以便在配置机群请求时可以使用。

配置 EC2 队列 以进行按需备份

如果有紧急而不可预测的扩展需要，如在发生重大新闻事件或比赛期间必须扩展的新闻网站，建议为按需型实例指定备用实例类型，以备首选选项没有足够可用容量时所需。例如，您可能首选 `c5.2xlarge` 按需实例，但是如果没有足够的可用容量，在负载高峰期内，您会愿意使用一些 `c4.2xlarge` 实例。在这种情况下，EC2 队列尝试使用 `c5.2xlarge` 实例满足所有目标容量要求，但如果没有足够的容量，则会自动启动 `c4.2xlarge` 实例以满足目标容量要求。

主题

- 针对按需容量优化实例类型 (p. 848)
- 将 容量预留 用于 按需型实例 (p. 849)

针对按需容量优化实例类型

EC2 实例集尝试满足您的按需容量时，它会默认首先启动价格最低的实例类型。如果 `AllocationStrategy` 设置为 `prioritized`，EC2 队列使用优先级来确定首先使用什么实例类型来满足按需容量。优先级分配给启动模板覆盖，优先级最高的最先启动。

示例：确定实例类型的优先级

在本例中，您可以配置三个启动模板覆盖，每个覆盖具有不同的实例类型。

实例类型的按需价格在价格范围内。以下是本例中使用的实例类型，按价格顺序列出，从价格最低的实例类型开始：

- `m4.large` – 价格最低
- `m5.large`
- `m5a.large`

如果您不使用优先级来确定顺序，则实例集将从价格最低的实例类型开始满足按需容量。

但是，假设您有想要先使用的未用 `m5.large` 预留实例。您可以设置启动模板覆盖优先级，以便按优先级顺序使用实例类型，如下所示：

- `m5.large` – 优先级 1
- `m4.large` – 优先级 2
- `m5a.large` – 优先级 3

将 容量预留 用于 按需型实例

可以通过将 容量预留 的使用策略配置为 use-capacity-reservations-first 来将队列配置为在启动 按需实例 时首先使用 按需容量预留。可以将此设置与 按需实例 的分配策略（lowest-price 或 prioritized）结合使用。

在将未使用的容量预留用于实现按需容量时：

- 队列使用未使用的容量预留来实现按需容量，最多可达到目标按需容量。
- 如果多个实例池具有未使用的容量预留，则应用按需分配策略（lowest-price 或 prioritized）。
- 如果未使用的容量预留数少于按需目标容量，则将根据按需分配策略（lowest-price 或 prioritized）启动剩余的按需目标容量。

只能将未使用的 按需容量预留 用于 instant 类型的队列。

有关如何将队列配置为使用 容量预留 来实现按需容量的示例，请参阅 EC2 队列 示例配置 (p. 945)。有关更多信息，请参阅On-Demand Capacity Reservations (p. 538)和按需容量预留常见问题。

容量再平衡

您可以配置 EC2 实例集以在 Amazon EC2 发出再平衡建议以通知您竞价型实例处于较高的中断风险时启动替换竞价型实例。容量再平衡功能可在运行中的实例被 Amazon EC2 中断之前，主动使用新竞价型实例扩展您的队列，从而帮助您维护工作负载的可用性。有关更多信息，请参阅EC2 实例再平衡建议 (p. 480)。

要配置 EC2 实例集以启动替换竞价型实例，请使用 create-fleet（Amazon CLI）命令和 MaintenanceStrategies 结构中的相关参数。有关更多信息，请参阅示例启动配置 (p. 954)。

限制

- 容量再平衡仅适用于类型为 maintain 的机群。
- 队列运行时，您无法修改容量再平衡设置。要更改容量再平衡设置，您必须删除此队列并创建新队列。

配置选项

EC2 机群的 ReplacementStrategy 支持以下两个值：

launch-before-terminate

Amazon EC2 可以在新的替换竞价型实例启动后终止接收再平衡通知的竞价型实例。如果指定 launch-before-terminate，还必须为 termination-delay 指定值。启动新的替换实例后，Amazon EC2 将等待 termination-delay 的持续时间，然后终止旧实例。对于 termination-delay，最短为 120 秒（2 分钟），最长为 7200 秒（2 小时）。

建议仅当您可以预测实例关闭过程完成所需的时长时才使用 launch-before-terminate。这将确保只有在关闭过程完成后才终止旧实例。请注意，Amazon EC2 可能会在 termination-delay 之前中断旧实例，并发出两分钟警告。

我们强烈建议不要将 lowest-price 分配策略与 launch-before-terminate 结合使用，以避免替换竞价型实例也处于中断风险升高的状态。

launch

针对现有竞价型实例发出再平衡通知时，Amazon EC2 将启动替换竞价型实例。Amazon EC2 不会终止接收再平衡通知的实例。您可以终止旧实例，也可以使其保持运行状态。在实例运行期间，您需要为它们付费。

注意事项

如果为容量再平衡配置 EC2 队列，请考虑以下事项：

在请求中提供尽可能多的 Spot 容量池

将您的 EC2 队列 配置为使用多种实例类型和多个可用区。这提供了在各种 Spot 容量池中启动竞价型实例的灵活性。有关更多信息，请参阅灵活地选择实例类型和可用区 (p. 451)。

避免替换竞价型实例中断的风险升高

如果您使用 `lowest-price` 分配策略，替换竞价型实例可能会面临中断升高的风险。这是因为，即使替换竞价型实例可能在启动后不久中断，Amazon EC2 始终会在当时具有可用容量的价格最低池中启动实例。为避免中断风险升高，我们强烈建议不要使用 `lowest-price` 分配策略，而建议使用 `capacity-optimized` 或 `capacity-optimized-prioritized` 分配策略。这些策略确保替换竞价型实例在最佳的竞价型容量池中启动，因此在不久的将来不太可能被中断。有关更多信息，请参阅使用价格和容量优化分配策略 (p. 451)。

只有可用性相同或更好时，Amazon EC2 才会启动新实例

容量再平衡的目标之一是提高竞价型实例的可用性。如果现有竞价型实例收到再平衡建议，Amazon EC2 只有在新实例提供与现有实例相同或更好的可用性时才会启动新实例。如果新实例的中断风险比现有实例更高，那么 Amazon EC2 将不会启动新实例。但是，Amazon EC2 将继续评测 Spot 容量池，并在可用性改善时启动新实例。

如果 Amazon EC2 没有主动启动新实例，则您的现有实例可能会中断。发生这种情况时，无论新实例的中断风险是否较高，Amazon EC2 都会尝试启动新实例。

容量再平衡不会提高您的竞价型实例中断率

当您启用容量再平衡时，它不会提高您的竞价型实例中断率 (p. 484)（在 Amazon EC2 需要收回容量时回收的竞价型实例的数量）。然而，如果容量再平衡检测到实例存在中断风险，Amazon EC2 将立即尝试启动新实例。结果是，与存在风险的实例中断后等待 Amazon EC2 启动新实例相比，可能会替换更多实例。

虽然在启用了容量再平衡的情况下您可以更换更多实例，但在中断您的实例之前，您会有更多时间采取行动，从而因为处于主动而非被动地位而受益。使用 Spot Instance interruption notice (p. 490)（竞价型实例中断通知），您通常最多只有两分钟的时间来正常关闭您的实例。借助容量再平衡提前启动新实例，您可以使现有流程更有可能在存在风险的实例上完成，您可以启动实例关闭程序，并防止在存在风险的实例上安排新工作。您还可以开始准备新启动的实例，以接管应用程序。借助容量再平衡的主动替换，您可以因绝佳的连续性而受益。

作为演示使用容量再平衡的风险和优点的理论示例，请考虑以下场景：

- 下午 2:00 – 收到针对实例 A 的再平衡建议，Amazon EC2 立即开始尝试启动替换实例 B，让您有时间启动关闭程序。*
- 下午 2:30 - 收到针对实例 B 的再平衡建议，该实例将被替换为实例 C，让您有时间启动关闭程序。*
- 下午 2:32 - 如果未启用容量再平衡，并且如果在下午 2:32 收到针对实例 A 的竞价型实例中断通知，则您最多只有两分钟时间采取行动，但实例 A 将一直运行到此时。

* 如果指定了 `launch-before-terminate`，Amazon EC2 将在替换实例上线后终止存在风险的实例。

Amazon EC2 可以启动新替换竞价型实例，直到已执行容量达到目标容量的两倍

为容量再平衡配置 EC2 实例集 时，队列会尝试为接收再平衡建议的每个竞价型实例启动新的替换竞价型实例。在竞价型实例收到再平衡建议后，它不再统计为已执行容量的一部分。根据替换策略，Amazon EC2 将在预配置的终止延迟后终止实例，或使其保持运行状态。这使您有机会对实例执行再平衡操作 (p. 481)。

如果您的队列达到目标容量的两倍，即使替换实例本身收到再平衡建议，它也会停止启动新的替换实例。

例如，您创建的 EC2 实例集 目标容量为 100 个竞价型实例。所有竞价型实例都会收到再平衡建议，这将导致 Amazon EC2 启动 100 个替换竞价型实例。这使已执行的竞价型实例的数量增加到 200 个，是目标容量的两倍。一些替换实例会收到再平衡建议，但由于队列不能超过目标容量的两倍，因此不会再启动更多替换实例。

请注意，在实例运行期间，您需要为所有实例付费。

我们建议您将 EC2 机群配置为终止接收再平衡建议的竞价型实例

如果您将 EC2 机群配置为实现容量再平衡，我们建议仅当您可以预测实例关闭过程完成所需的时长时才选择 `launch-before-terminate` 和适当的终止延迟。这将确保只有在关闭过程完成后才终止旧实例。

如果您选择自行终止建议再平衡的实例，我们建议您监控机群中的竞价型实例接收的再平衡建议信号。通过监控信号，您可以在 Amazon EC2 中断受影响的实例之前快速对其执行再平衡操作 (p. 481)，然后您可以手动终止它们。如果您不终止实例，则需要在实例运行期间继续为其付费。Amazon EC2 不会自动终止接收再平衡建议的实例。

您可以使用 Amazon EventBridge 或实例元数据设置通知。有关更多信息，请参阅监控再平衡建议信号 (p. 481)。

在计算扩大或缩小规模期间的已执行容量时，EC2 队列 不计入收到再平衡建议的实例

如果您的 EC2 队列 针对容量再平衡进行了配置，并且您将目标容量更改为向内或向外扩展，则队列不会将标记为再平衡的实例计算为已执行容量的一部分，如下所示：

- 横向缩减 – 如果您降低所需的目标容量，Amazon EC2 将终止未标记为再平衡的实例，直到达到所需容量。标记为再平衡的实例不计入已执行容量。

  例如，您创建的 EC2 实例集目标容量为 100 个竞价型实例。10 个实例会收到再平衡建议，因此 Amazon EC2 会启动 10 个新的替换实例，从而获得 110 个实例的执行容量。然后，您将目标容量减少到 50 个（横向缩减），但已执行的容量实际上为 60 个实例，因为 Amazon EC2 不会终止标记为再平衡的 10 个实例。您需要手动终止这些实例，也可以让它们保持运行状态。
- 横向扩展 – 如果您增加所需的目标容量，Amazon EC2 将启动新实例，直到达到所需容量。标记为再平衡的实例不计入已执行容量。

  例如，您创建的 EC2 实例集目标容量为 100 个竞价型实例。10 个实例会收到再平衡建议，因此队列启动 10 个新的替换实例，从而获得 110 个实例的执行容量。然后，您将目标容量增加到 200（扩展），但已执行的容量实际上为 210 个实例，因为标记为再平衡的 10 个实例不被队列计入目标容量的一部分。您需要手动终止这些实例，也可以让它们保持运行状态。

最高价覆盖

每个 EC2 队列可以包含全局最高价格，或使用默认值（按需价格）。队列将该价格作为每个启动规范的默认最高价。

您可以选择在一个或多个启动规范中指定最高价。该价格是启动规范特有的。如果启动规范包含特定的价格，则EC2 队列使用该最高价以覆盖全局最高价。不包含特定最高价的任何其他启动规范仍使用全局最高价。

控制支出

在达到以下参数之一时，EC2 队列停止启动实例：`TotalTargetCapacity` 或 `MaxTotalPrice`（您愿意支付的最大金额）。要控制您每小时为队列支付的金额，您可以指定 `MaxTotalPrice`。在达到最高总价时，即使未达到目标容量，EC2 队列也会停止启动实例。

以下示例显示了两个不同的方案。在第一个方案中，在达到目标容量时，EC2 队列停止启动实例。在第二个方案中，在达到您愿意支付的最大金额 (`MaxTotalPrice`) 时，EC2 队列停止启动实例。

示例：在达到目标容量时，停止启动实例

假设发出 m4.large 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- OnDemandTargetCapacity: 10
- MaxTotalPrice：1.50 美元

EC2 队列启动 10 个按需实例，因为按需实例的总价 1.00 美元（10 个实例 x 0.10 美元）不超过 MaxTotalPrice（1.50 美元）。

示例：在达到最高总价时，停止启动实例

假设发出 m4.large 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- OnDemandTargetCapacity: 10
- MaxTotalPrice：0.80 美元

如果 EC2 实例集启动按需目标容量（10 个按需型实例），则每小时的总成本为 1.00 美元。这超过了为按需实例的 MaxTotalPrice 指定的金额（0.80 美元）。为了防止支出超过您愿意支付的金额，EC2 队列仅启动 8 个按需实例（低于按需目标容量），因为启动更多实例将超过按需实例的 MaxTotalPrice。

EC2 队列实例权重

在创建 EC2 队列时，您可以定义每种实例类型为应用程序性能贡献的容量单位。然后，您可以使用实例权重调整每个启动规范的最高价格。

默认情况下，您指定的价格是每实例小时 价格。在使用实例权重功能时，您指定的价格是每单位小时 价格。您可以将某种实例类型的价格除以它表示的单位数来计算每单位小时价格。EC2 队列通过将目标容量除以实例权重，计算出要启动的实例数。如果结果不是整数，则 队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。队列可以选择您在启动规范中指定的任意池，即使所启动实例的容量超过请求的目标容量也是如此。

下表中提供了用于为目标容量是 10 的 EC2 队列请求确定每单位出价的计算示例。

实例类型	实例权重	目标容量	启动的实例数	每实例小时价格	每单位小时价格
r3.xlarge	2	10	5 (10 除以 2)	0.05 美元	0.025 美元 (0.05 除以 2)
r3.8xlarge	8	10	2 (10 除以 8，结果向上舍入)	0.10 美元	0.0125 美元 (0.10 除以 8)

按如下所示使用 EC2 队列实例权重，在执行时具有每单位最低价格的池中预置所需的目标容量：

1. 采用实例 (默认设置) 或采用所选单位 (如虚拟 CPU、内存、存储或吞吐量) 为 EC2 队列设置目标容量。
2. 设置每单位价格。
3. 为每个启动规范指定权重，这是实例类型向目标容量提供的单位数。

实例权重示例

考虑一个具有以下配置的 EC2 队列请求：

- 目标容量为 24
- 一个实例类型为 r3.2xlarge 且权重为 6 的启动规范
- 一个实例类型为 c3.xlarge 且权重为 5 的启动规范

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动规范提供了最低的每单位价格（r3.2xlarge 每实例小时价格除以 6），则 EC2 队列会启动 4 个这样的实例（24 除以 6）。

如果第二个启动规范提供了最低的每单位价格（c3.xlarge 每实例小时价格除以 5），则 EC2 队列会启动 5 个这样的实例（24 除以 5，结果向上舍入）。

实例权重和分配策略

考虑一个具有以下配置的 EC2 队列请求：

- 目标容量为 30 个竞价型实例
- 一个实例类型为 c3.2xlarge 且权重为 8 的启动规范
- 一个实例类型为 m3.xlarge 且权重为 8 的启动规范
- 一个实例类型为 r3.xlarge 且权重为 8 的启动规范

EC2 队列会启动四个实例 (30 除以 8，结果向上舍入)。在使用 lowest-price 策略时，所有四个实例均来自提供最低每单位价格的池。使用 diversified 策略时，队列会在所有三个池中各启动一个实例，并在三个池中提供最低每单位价格的那个池中启动第四个实例。

使用 EC2 队列

要开始使用 EC2 队列，请创建一个请求，其中包括总目标容量、按需容量、Spot 容量、实例的一个或多个启动规范以及您愿意支付的最高价。队列请求必须包括队列启动实例所需信息 (例如 AMI、实例类型、子网或可用区、一个或多个安全组) 的启动模板。您可以为您愿意支付的实例类型、子网、可用区以及您愿意支付的最高价指定启动规范覆盖，而且，您可以为每个启动规范覆盖分配权重容量。

EC2 实例集在有可用容量时启动按需型实例，在最高价超过 Spot 价格并且有可用容量时启动竞价型实例。

如果队列包括竞价型实例，Amazon EC2 将尝试在 Spot 价格变化时保持队列的目标容量。

类型 maintain 或 request 的 EC2 队列 请求在过期或您删除它之前一直有效。在删除类型 maintain 或request 的队列时，您可以指定删除操作是否会终止该队列中的实例。否则，按需型实例持续运行至您将其终止，竞价型实例持续运行至遇到中断或您将其终止。

目录

- EC2 队列请求状态 (p. 854)
- EC2 队列先决条件 (p. 854)
- EC2 队列运行状况检查 (p. 857)
- 生成 EC2 队列 JSON 配置文件 (p. 857)
- 创建 EC2 队列 (p. 860)
- 标记 EC2 队列 (p. 862)
- 描述 EC2 机群 (p. 864)
- 修改 EC2 队列 (p. 866)
- 删除 EC2 队列 (p. 867)

EC2 队列请求状态

EC2 队列请求可以处于以下某种状态：

`submitted`

EC2 队列 正在接受评估，并且 Amazon EC2 正准备启动目标数量的实例。请求可包括 按需型实例、竞价型实例 或两者。

`active`

EC2 队列 请求已验证，并且 Amazon EC2 正在尝试使正在运行的实例保持目标数量。请求会保持这一状态，直到其被修改或删除。

`modifying`

正在修改 EC2 队列 请求。请求会保持这一状态，直到修改全部完成或请求被删除。只能修改 `maintain` 队列类型。此状态不适用于其他请求类型。

`deleted_running`

EC2 队列 请求已删除，且不启动其他实例。其现有实例将继续运行，直至中断或被手动终止。请求会保持此状态，直到所有实例都已中断或终止。删除 EC2 队列 请求后，只有类型 `maintain` 或 `request` 的 EC2 队列 才能有正在运行的实例。不支持包含正在运行实例的已删除 `instant` 队列。此状态不适用于 `instant` 队列。

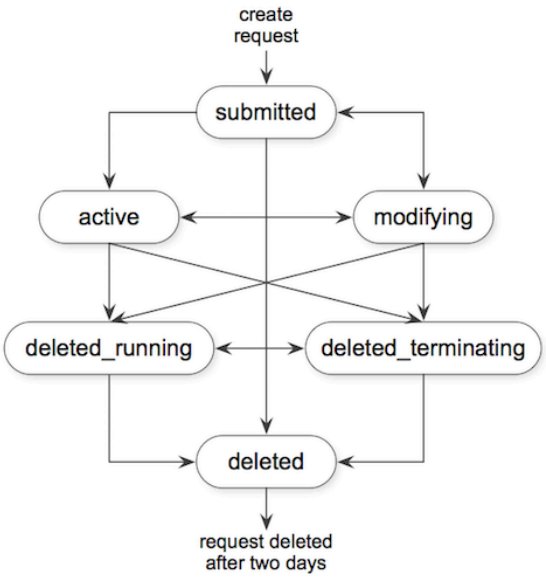
`deleted_terminating`

EC2 队列 请求已删除，正在终止其实例。请求会保持此状态，直到所有实例都已终止。

`deleted`

EC2 队列 已删除，没有正在运行的实例。请求将在其实例终止两天后被删除。

以下显示了 EC2 队列请求状态之间的转换。如果您超出队列限制，请求会立即被删除。



EC2 队列先决条件

要创建 EC2 队列，必须满足以下先决条件：

- 启动模板 (p. 855)

- EC2 队列的服务相关角色 (p. 855)
- 授予对用于加密的 AMI 和 EBS 快照的客户托管密钥的访问权限 (p. 855)
- EC2 实例集用户的权限 (p. 856)

启动模板

启动模板包含要启动的实例的有关信息，例如，实例类型、可用区以及您愿意支付的最高价。有关更多信息，请参阅通过启动模板启动实例 (p. 588)。

EC2 队列的服务相关角色

AWSServiceRoleForEC2Fleet 角色授予 EC2 实例集权限以代表您请求、启动、终止和标记实例。Amazon EC2 使用此服务相关角色来完成以下操作：

- ec2:RunInstances – 启动实例。
- ec2:RequestSpotInstances – 请求 Spot 实例。
- ec2:TerminateInstances – 终止实例。
- ec2:DescribeImages – 描述 Spot 实例 的 Amazon 系统映像 (AMI)。
- ec2:DescribeInstanceStatus – 描述 Spot 实例的状态。
- ec2:DescribeSubnets – 描述 Spot 实例的子网。
- ec2:CreateTags – 将标签添加到 EC2 队列、实例和卷中。

确保此角色存在，然后才使用 Amazon CLI 或 API 来创建 EC2 实例集。

> **Note**
>
> instant EC2 队列不需要此角色。

要创建该角色，请如下使用 IAM 控制台。

为 EC2 队列创建 AWSServiceRoleForEC2Fleet 角色

1. 访问：https://console.aws.amazon.com/iam/，打开 IAM 控制台。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 对于Select type of trusted entity（选择受信任实体的类型），选择 Amazon service（服务）。
4. 对于 Choose the service that will use this role (选择将使用此角色的服务)，选择 EC2 - Fleet (EC2 - 队列)，然后依次选择 Next: Permissions (下一步: 权限)、Next: Tags (下一步: 标签) 和 Next: Review (下一步: 审核)。
5. 在 Review (审核) 页面上，选择 Create role (创建角色)。

如果您不再需要使用 EC2 队列，我们建议您删除 AWSServiceRoleForEC2Fleet 角色。当此角色从您的账户中删除后，如果您创建其他队列，可再次创建此角色。

有关更多信息，请参阅 IAM 用户指南 中的使用服务相关角色。

授予对用于加密的 AMI 和 EBS 快照的客户托管密钥的访问权限

如果在 EC2 实例集中指定加密的 AMI (p. 196) 或加密的 Amazon EBS 快照 (p. 1504)，并且您使用 Amazon KMS 密钥进行加密，则必须授予 AWSServiceRoleForEC2Fleet 角色使用客户托管式密钥的权限，以便 Amazon EC2 可以代表您启动实例。为此，您必须在客户托管密钥中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用授权和在 Amazon KMS 中使用密钥策略。

为 AWSServiceRoleForEC2Fleet 角色授予使用客户托管密钥的权限

- 使用 create-grant 命令在客户托管密钥中添加授权，并指定授予权限的主体（AWSServiceRoleForEC2Fleet 服务相关角色），以执行授权允许的操作。客户托管密钥由 `key-id` 参数和客户托管密钥的 ARN 指定。委托人是由 `grantee-principal` 参数和 AWSServiceRoleForEC2Fleet 服务相关角色的 ARN 指定的。

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

EC2 实例集用户的权限

如果用户打算创建或管理 EC2 实例集，请确保为其授予所需权限。

为 EC2 实例集创建策略

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Policies (策略)。
3. 选择 Create policy。
4. 在创建策略页面上，选择 JSON 选项卡，将文本替换为以下内容，并选择查看策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*` 为用户授予调用所有 Amazon EC2 API 操作的权限。要将用户限制到特定 Amazon EC2 API 操作，请改为指定这些操作。

用户必须具有相应权限，可以调用 `iam:ListRoles` 操作以枚举现有 IAM 角色、调用 `iam:PassRole` 操作以指定 EC2 实例集角色以及调用 `iam:ListInstanceProfiles` 操作以枚举现有实例配置文件。

（可选）要允许用户使用 IAM 控制台创建角色或实例配置文件，还必须在策略中添加以下操作：

- `iam:AddRoleToInstanceProfile`

- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. 在查看策略页面上，输入策略名称和描述，然后选择创建策略。
6. 要提供访问权限，请为您的用户、组或角色添加权限：

   - 通过身份提供商在 IAM 中托管的用户：

     创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
   - IAM 用户：
     - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
     - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

EC2 队列运行状况检查

EC2 队列每 2 分钟检查一次队列中实例的运行状况。实例的运行状况为 `healthy` 或 `unhealthy`。

EC2 队列 将使用 Amazon EC2 提供的状态检查来确定实例的运行状况。如果在连续三次运行状况检查中，实例状态检查或系统状态检查的状态有任一项为 `unhealthy`，则确定该实例的运行状况为 `impaired`。有关更多信息，请参阅实例的状态检查 (p. 975)。

您可以配置您的队列以替换运行状况不佳的竞价型实例。将 `ReplaceUnhealthyInstances` 设置为 `true` 以后，若竞价型实例报告为 `unhealthy` 则将其替换。在替换运行状况不佳的竞价型实例时，队列可能在几分钟内降至其目标容量之下。

要求

- 仅对保持目标容量的 EC2 队列（类型 `maintain` 的队列）支持运行状况检查替换，不支持类型为 `request` 或 `instant` 的队列。
- 仅对竞价型实例支持运行状况检查替换。对于 按需型实例 不支持此功能。
- 您可以将 EC2 队列配置为仅在您创建它时替换运行状况不佳的实例。
- 用户仅在其有权调用 `ec2:DescribeInstanceStatus` 操作时才能使用运行状况检查替换。

配置 EC2 实例集 以替换运行状况不佳的竞价型实例

1. 按创建 EC2 队列 的步骤操作。有关更多信息，请参阅创建 EC2 队列 (p. 860)。
2. 要将队列配置为替换运行状况不佳的 Spot 实例，请在 JSON 文件中，对于 `ReplaceUnhealthyInstances` 输入 `true`。

生成 EC2 队列 JSON 配置文件

要查看 EC2 机群配置参数的完整列表，可以生成 JSON 文件。有关每个参数的说明，请参阅 Amazon CLI 命令参考中的 create-fleet。

通过命令行使用所有可能的 EC2 队列参数生成 JSON 文件

- 使用 create-fleet (Amazon CLI) 命令和 `--generate-cli-skeleton` 参数生成 EC2 机群 JSON 文件，并将输出定向到某个文件以将其保存。

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

输出示例

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
                        "MemoryGiBPerVCpu": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "ExcludedInstanceTypes": [
                            ""
                        ],
                        "InstanceGenerations": [
                            "previous"
                        ],
                        "SpotMaxPricePercentageOverLowestPrice": 0,
                        "OnDemandMaxPricePercentageOverLowestPrice": 0,
                        "BareMetal": "included",
                        "BurstablePerformance": "required",
                        "RequireHibernateSupport": true,
                        "NetworkInterfaceCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "LocalStorage": "excluded",
                        "LocalStorageTypes": [
                            "ssd"
                        ],
                        "TotalLocalStorageGB": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "BaselineEbsBandwidthMbps": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorTypes": [
                            "inference"
                        ],
                        "AcceleratorCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorManufacturers": [
                            "amd"
                        ],
                        "AcceleratorNames": [
                            "a100"
                        ],
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
```

```
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

创建 EC2 队列

要创建 EC2 机群，您只需指定以下参数：

- `LaunchTemplateId` 或 `LaunchTemplateName` – 指定要使用的启动模板（其中包含要启动的实例的参数，例如，实例类型、可用区以及您愿意支付的最高价）
- `TotalTargetCapacity` – 指定机群的总目标容量
- `DefaultTargetCapacityType` – 指定默认购买选项是按需型还是竞价型

您可以指定多个覆盖启动模板的启动规范。启动规范可以有不同的实例类型、可用区、子网和最高价，并且可以包含不同的权重容量。

如果不指定参数，机群将使用参数的默认值。

在 JSON 文件中指定机群参数。有关更多信息，请参阅生成 EC2 队列 JSON 配置文件 (p. 857)。

只能使用 Amazon CLI 创建 EC2 实例集。

创建 EC2 实例集（Amazon CLI）

- 使用 create-fleet (Amazon CLI) 命令创建 EC2 机群并指定包含机群配置参数的 JSON 文件。

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

有关示例配置文件，请参阅EC2 队列 示例配置 (p. 945)。

以下是 `request` 或 `maintain` 类型的队列的示例输出。

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

以下是启动了目标容量的 `instant` 类型队列的示例输出。

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
```

```
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

以下是启动了部分目标容量并且出现“无法启动实例”错误的 instant 类型队列的示例输出。

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
```

```
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

以下是未启动任何实例的 `instant` 类型队列的示例输出。

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

标记 EC2 队列

要对您的 EC2 队列 请求进行分类和管理，您可使用自定义元数据标记它们。您可以在创建 EC2 队列 请求时或之后为其分配标签。

在标记队列请求时，不会自动标记队列启动的实例和卷。您需要明确标记队列启动的实例和卷。您可以选择仅将标签分配给队列请求，仅分配给队列启动的实例，仅分配给附加到队列启动的实例的卷，或者分配给所有这三种内容。

Note

对于 instant 队列类型，您可以标记附加到按需实例和Spot 实例的卷。对于 request 或 maintain 队列类型，您只能标记附加到按需实例的卷。

有关标签的工作原理的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

先决条件

授予用户标记资源的权限。有关更多信息，请参阅示例：标记资源 (p. 1261)。

授予用户标记资源的权限

创建包含以下内容的 IAM policy：

- ec2:CreateTags 操作。这将授予用户创建标签的权限。
- ec2:CreateFleet 操作。这将授予用户创建 EC2 实例集请求的权限。
- 对于 Resource，我们建议您指定 "*"。这允许用户标记所有资源类型。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

对于 create-fleet 资源，我们目前不支持资源级权限。如果您指定 create-fleet 以作为资源，在您尝试标记队列时，将会发生未经授权异常。以下示例说明如何不 设置策略。

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

标记新的 EC2 队列 请求

要在创建时标记 EC2 队列请求，请在用于创建该队列的 JSON 文件 (p. 857)中指定键值对。ResourceType 的值必须为 fleet。如果指定其他值，队列请求失败。

标记 EC2 队列启动的实例和卷

要在队列启动实例和卷时标记它们，请在 EC2 队列请求中引用的启动模板 (p. 590)中指定标签。

Note

您无法标记附加到 request 或 maintain 队列类型启动的 Spot 实例的卷。

标记现有的 EC2 实例集请求、实例和卷（Amazon CLI）

使用 create-tags 命令标记现有的资源。

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

描述 EC2 机群

您可以描述 EC2 机群配置、EC2 机群中的实例，以及 EC2 机群的历史事件。

描述 EC2 机群 (Amazon CLI)

可以使用 describe-fleets 命令描述 EC2 队列。

```
aws ec2 describe-fleets
```

Important

如果机群是 instant 类型，则您必须指定机群 ID，否则其不会出现在响应中。按如下所示包含 --fleet-ids：

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

输出示例

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
```

```
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

可以使用 describe-fleet-instances 命令描述指定 EC2 队列的实例。正在运行的实例的返回列表将定期刷新，或可能过时。

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

输出示例

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

可以使用 describe-fleet-history 命令描述指定 EC2 队列在指定时间内的历史记录。

```
aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --
start-time 2018-04-10T00:00:00Z
```

输出示例

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
```

```
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```


修改 EC2 队列

您可以修改处于 submitted 或 active 状态的 EC2 队列。当您修改队列时，它会进入 modifying 状态。

您只能修改类型为 maintain 的EC2 队列。您不能修改类型为 request 或 instant 的 EC2 队列。

您可以修改 EC2 队列的以下参数：

- target-capacity-specification – 增加或减少 TotalTargetCapacity、OnDemandTargetCapacity 和 SpotTargetCapacity 的目标容量。
- excess-capacity-termination-policy – 当 EC2 队列的总目标容量降到队列的当前大小以下时是否应终止正在运行的实例。有效值为 no-termination 和 termination。

如果提升目标容量，EC2 队列会根据为 DefaultTargetCapacityType 指定的实例购买选项（按需实例或 Spot 实例）启动额外的实例。

如果 DefaultTargetCapacityType 为 spot，EC2 队列会根据其分配策略启动额外的 Spot 实例。如果分配策略为 lowest-price，实例集将从请求中价格最低的 Spot 容量池启动实例。如果分配策略为 diversified，队列将在请求中的池间分配实例。

在减少目标容量时，EC2 队列会删除超过新目标容量的任何打开的请求。您可以请求 队列终止 实例，直到队列的大小达到新目标容量。如果分配策略是 lowest-price，则 队列会终止每单位价格最高的实例。如果分配策略是 diversified，则 队列会在池间终止实例。或者，您可以请求 EC2 实例集保持队列当前的队列大小，而不替换已中断的竞价型实例或者您手动终止的任何实例。

当 EC2 实例集因目标容量下降而终止某个竞价型实例时，该实例将收到一条竞价型实例中断通知。

修改 EC2 实例集（Amazon CLI）

可以使用 modify-fleet 命令更新指定 EC2 队列的目标容量。

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

如果要减少目标容量，但希望保持队列的当前大小，您可以按如下方式修改上面的命令。

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

删除 EC2 队列

如果您不再需要某一 EC2 队列，可以将其删除。删除实例集后，将取消与实例集关联的所有竞价型实例请求，从而不会启动任何新的竞价型实例。

删除 EC2 实例集后，您还必须指定是否要终止其所有实例。包括按需型实例和竞价型实例。

如果您指定在实例集删除后必须终止实例，实例集会进入 deleted_terminating 状态。否则，队列会进入 deleted_running 状态，并且实例会继续运行，直到遇到中断或您手动将其终止。

限制

- 在单个请求中，您可以删除最多 25 个 instant 队列。如果超过此数量，则不删除任何 instant 队列，并会返回错误。对于类型为 maintain 或 request 的队列，在单个请求中可删除的数量没有限制。
- 单次删除 instant 队列的请求最多可终止 1000 个实例。

删除 EC2 实例集并终止其实例（Amazon CLI）

使用 delete-fleets 命令和 --terminate-instances 参数来删除指定的 EC2 实例集并终止其关联实例。

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

输出示例

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

删除 EC2 实例集而不终止其实例（Amazon CLI）

您可以使用 --no-terminate-instances 参数修改上一个命令，以删除指定的 EC2 实例集而不终止其关联实例。

Note

--no-terminate-instances 队列不支持 instant。

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

输出示例

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

队列无法删除时进行故障排除

如果 EC2 队列 无法删除，则 UnsuccessfulFleetDeletions 将返回 EC2 队列 的 ID、错误代码和错误消息。

错误代码为：

- ExceededInstantFleetNumForDeletion
- fleetIdDoesNotExist
- fleetIdMalformed
- fleetNotInDeletableState
- NoTerminateInstancesNotSupported
- UnauthorizedOperation
- unexpectedError

ExceededInstantFleetNumForDeletion 故障排除

如果您尝试在单个请求中删除超过 25 个 instant 队列，则会返回 ExceededInstantFleetNumForDeletion 错误。下面是此错误的示例输出。

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                  "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                  "Code": "ExceededInstantFleetNumForDeletion"
```

```
            }
      }
      .
      .
      .
      ],
      "SuccessfulFleetDeletions": []
}
```

NoTerminateInstancesNotSupported 问题排查

如果您指定在删除 instant 队列时不得终止该队列中的实例，则会返回 NoTerminateInstancesNotSupported 错误。--no-terminate-instances 队列不支持 instant。下面是此错误的示例输出。

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                         "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                         "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
```

UnauthorizedOperation 问题排查

如果您没有终止实例的权限，则在删除必须终止其实例的队列时会收到 UnauthorizedOperation 错误。下面是错误响应。

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized
 to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7N63SKlwe
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76H9ytg2zP
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7XAfdPMP_
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC9YPGMLK9
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</RequestID></
Response>
```

为了解决错误，您必须将 ec2:TerminateInstances 操作添加到 IAM policy，如下例中所示。

```
{
       "Version": "2012-10-17",
       "Statement": [
            {
                "Sid": "DeleteFleetsAndTerminateInstances",
                "Effect": "Allow",
                "Action": [
                       "ec2:DeleteFleets"
                       "ec2:TerminateInstances"
                ],
                "Resource": "*"
            }
```

```
        ]
    }
```

Spot 队列

竞价型实例集是竞价型实例及根据您指定的条件启动的可选按需型实例的集合。竞价型实例集选择满足您的需要的 Spot 容量池，并启动竞价型实例以满足队列的目标容量。默认情况下，在队列中的 Spot 实例 终止之后，系统会启动替换实例以保持 Spot 队列 的目标容量。您可以将 Spot 队列作为一次性请求来提交，这种请求在实例终止后不会被保留。您可以在竞价型实例集请求中包含按需型实例请求。

主题

- Spot 队列请求类型 (p. 871)
- Spot 实例集配置策略 (p. 871)
- 使用 Spot 队列 (p. 892)
- Spot 队列的 CloudWatch 指标 (p. 912)
- Spot 队列的自动扩展 (p. 914)

Spot 队列请求类型

有两种类型的 Spot 队列请求：

`request`

如果您将请求类型配置为 `request`，Spot 队列针对所需容量发出异步一次性请求。此后，如果由于 Spot 中断导致容量减少，队列不会尝试补充竞价型实例，也不会当容量不可用时在其他 Spot 容量池中提交请求。

`maintain`

如果您将请求类型配置为 `maintain`，Spot 实例集针对所需容量发出异步请求，并自动补充任何中断的 Spot 实例以保持容量。

要在 Amazon EC2 控制台中指定请求的类型，请在创建 Spot队列请求时执行以下操作：

- 要创建类型为 `request` 的 Spot 队列，清除 Maintain target capacity（维持目标容量）复选框。
- 要创建类型为 `maintain` 的 Spot 队列，选择 Maintain target capacity（维持目标容量）复选框。

有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台） (p. 901)。

两种请求类型都可以受益于分配策略。有关更多信息，请参阅竞价型实例的分配策略 (p. 872)。

Spot 实例集配置策略

Spot 队列是 Spot 实例和可选的按需实例的集合或队列。

竞价型实例集尝试启动一定数量的竞价型实例和按需型实例以满足您在竞价型实例集请求中指定的目标容量。如果具有可用的容量，并且在竞价型实例请求中指定的最高价格超过当前 Spot 价格，则会完成该请求。如果竞价型实例中断，竞价型实例集还可能会尝试保持其目标容量队列。

也可以设置您愿意为队列支付的每小时最大金额，Spot 队列将启动实例，直至达到最大金额。在达到您愿意支付的最大金额时，即使队列未达到目标容量，队列也会停止启动实例。

Spot 容量池 是一组未使用的 EC2 实例，具有相同的实例类型（例如 `m5.large`）、操作系统、可用区和网络平台。在您发出 Spot 队列请求时，您可以指定多个启动规范（因实例类型、AMI、可用区或子网而异）。Spot 队列会基于 Spot 队列请求中包含的启动说明以及 Spot 队列请求的配置来选择用于执行请求的 Spot 容量池。竞价型实例来自所选的池。

目录

- 规划 Spot 队列请求 (p. 872)
- 竞价型实例的分配策略 (p. 872)
- 竞价型实例集的基于属性的实例类型选择 (p. 874)
- Spot 队列中的按需实例 (p. 888)
- 容量再平衡 (p. 888)
- Spot 价格覆盖 (p. 891)
- 控制支出 (p. 891)
- Spot 队列实例权重 (p. 891)

规划 Spot 队列请求

在创建 Spot 队列请求前，请查看 Spot 最佳实践。使用这些最佳实践规划您的 Spot 队列请求，以便以可能的最低价格预置需要的实例类型。还建议执行以下操作：

- 确定您是要创建一个 Spot 队列来提交对所需目标容量的一次性请求，还是随着时间推移维持目标容量。
- 确定满足您的应用程序要求的实例类型。
- 确定您的 Spot 队列请求的目标容量。您可以采用实例或自定义单位设置目标容量。有关更多信息，请参阅Spot 队列实例权重 (p. 891)。
- 确定 Spot 队列目标容量的多大部分必须是按需容量。可以将按需容量指定为 0。
- 确定您的每单位价格 (如果使用实例权重)。要计算每单位价格，请将每实例小时价格除以该实例表示的单位数 (或权重)。如果不使用实例权重，则默认每单位价格为每实例小时价格。
- 查看用于您的 Spot 队列请求的可能选项。关于更多信息，请参阅 Amazon CLI Command Reference 中的 request-spot-fleet 命令。有关其他示例，请参阅 Spot 队列示例配置 (p. 958)。

竞价型实例的分配策略

您的启动配置决定了竞价型实例集可以从中启动竞价型实例的所有可能竞价型容量池（实例类型和可用区）。但在启动实例时，竞价型实例集将使用您指定的分配策略从所有可能的池中选择特定的池。

您可以指定下面的任何一种分配策略：

`priceCapacityOptimized`（推荐）

竞价型实例集为正在启动的实例数识别具有最高可用容量的池。这意味着我们将从我们认为短期内中断概率最低的池中请求竞价型实例。然后，竞价型实例集从这些池中价格最低的请求竞价型实例。

`priceCapacityOptimized` 分配策略是大多数 Spot 工作负载的最佳选择，例如无状态容器化应用程序、微服务、Web 应用程序、数据和分析任务以及批处理。

`capacityOptimized`

竞价型实例集为正在启动的实例数识别具有最高可用容量的池。这意味着我们将从我们认为短期内中断概率最低的池中请求竞价型实例。您可以选择使用 `capacityOptimizedPrioritized` 为队列中的每种实例类型设置优先级。Spot 队列首先会针对容量进行优化，但会尽最大努力遵循实例类型的优先级。

使用竞价型实例，定价会根据长期供需趋势缓慢发生变化，但容量会实时波动。`capacityOptimized` 策略通过查看实时容量数据并预测可用性最高的池，自动在可用性最高的池中启动 Spot 实例。这适用于因重启工作而导致中断成本更高的工作负载，例如长时间持续集成（CI）、图像和媒体渲染、深度学习以及高性能计算（HPC）工作负载，这些工作负载可能具有与重启工作相关的更高的中断成本。通过实现更低的中断可能性，`capacityOptimized` 策略可以降低您工作负载的整体成本。

或者，您也可以使用 `capacityOptimizedPrioritized` 分配策略，该策略带有优先级参数，以便从最高到最低优先级对实例类型进行排序。您可以为不同的实例类型设置相同的优先级。Spot 队列首

先会针对容量进行优化，但会尽最大努力遵循实例类型的优先级（例如，如果遵循优先级不会显著影响 Spot 队列预置最佳容量的能力）。对于必须最大限度地减少中断可能性，同时对某些实例类型的偏好也很重要的工作负载来说，这是一个不错的选择。仅当您的队列使用启动模板时，才支持使用优先级。请注意，当您为 `capacityOptimizedPrioritized` 设置优先级时，如果按需 `AllocationStrategy` 设置为 `prioritized`，那么相同的优先级也会应用于您的按需型实例。

`diversified`

竞价型实例分布在所有池中。

`lowestPrice`

竞价型实例来自价格最低并且具有可用容量的池。这是默认策略。然而，我们建议您通过指定 `priceCapacityOptimized` 分配策略来覆盖默认值。

如果价格最低的池没有可用容量，则竞价型实例将来自价格次低且具有可用容量的池。

如果某个池在满足您所需的容量之前耗尽容量，竞价型实例集将继续从价格次低的池中提取，以满足您的请求。为确保达到所需容量，您可能会获得来自多个容量池的竞价型实例。

由于此策略仅考虑实例价格而不考虑容量可用性，因此可能会导致较高的中断率。

`InstancePoolsToUseCount`

在其中分配您的目标 Spot 容量的 Spot 池数量。仅当分配策略设置为 `lowestPrice` 时有效。竞价型实例集选择价格最低的 Spot 池，并在指定数量的 Spot 池之间平均分配目标 Spot 容量。

请注意，竞价型实例集会尽力尝试根据您指定的池数量提取竞价型实例。如果某个池在满足您所需的容量之前耗尽 Spot 容量，则竞价型实例集将继续从价格次低的池中提取实例，以满足您的请求。为确保达到目标容量，您可能会从超过指定数量的池接收竞价型实例。同样，如果大多数池没有 Spot 容量，则您可能会从少于指定数量的池接收完整目标容量。

选择合适的分配策略

您可以选择适当的 Spot 分配策略，从而根据您的使用案例来优化实例集。对于按需型实例目标容量，竞价型实例集始终根据公开按需型价格选择价格最低的实例类型，同时对竞价型实例按照分配策略（`priceCapacityOptimized`、`capacityOptimized`、`diversified` 或 `lowestPrice`）执行分配。

平衡最低价格和可用容量

为了获得价格最低价格 Spot 容量池与具有最高可用容量的 Spot 容量池之间的平衡，我们建议您使用 `priceCapacityOptimized` 分配策略。该策略根据池的价格以及这些池中竞价型实例的可用容量来决定向哪些池请求竞价型实例。这意味着将从我们认为短期内中断概率最低的池中请求竞价型实例，同时还要考虑价格。

如果您的实例集运行弹性和无状态的工作负载（包括容器化应用程序、微服务、Web 应用程序、数据和分析作业以及批量处理），则使用 `priceCapacityOptimized` 分配策略以实现最大的成本节约和可用容量。

如果实例集运行的工作负载可能会因重启工作而导致更高的中断成本，则应设置检查点，以便应用程序中断时可从该点重启。通过使用检查点，可以使 `priceCapacityOptimized` 分配策略变得非常适合这些工作负载，因其会从价格最低的池中分配容量，这些池同时还具有较低的竞价型实例中断率。

有关使用 `priceCapacityOptimized` 分配策略的示例配置，请参阅 示例 10：在具有优先级的容量优化队列中启动竞价型实例 (p. 956)。

当工作负载拥有较高中断成本时

如果您运行的工作负载使用价格相似的实例类型，或中断成本非常高，以至于任何成本节约都不足以负担一个轻微中断，则可以选择使用 `capacityOptimized` 策略。此策略从可用容量最多的 Spot 容量池分配容量，这些容量池中断的可能性更低，从而可降低您工作负载的整体成本。有关使用 `capacityOptimized` 分配策略的示例配置，请参阅 示例 8：配置容量再平衡以启动替换竞价型实例 (p. 954)。

如果必须将中断的可能性降至最低，但某些实例类型的首选项又很紧要时，则您可以通过使用 capacityOptimizedPrioritized 分配策略来表达您的池优先级，然后将要使用的实例类型的顺序设置为从最高到最低优先级。有关示例配置，请参阅 示例 9：在容量优化的队列中启动竞价型实例 (p. 955)。

请注意，仅当您的实例集使用启动模板时，才支持使用优先级。还需注意，为 capacityOptimizedPrioritized 设置优先级时，如果按需 AllocationStrategy 设置为 prioritized，那么相同的优先级也会应用于您的按需型实例。

当您的工作负载时间灵活且可用容量不是一个因素时

如果您的实例集较小或运行时间较短，则可以使用 priceCapacityOptimized 来最大限度地节省成本，同时还要考虑可用容量。

如果您的工作负载时间灵活且可用容量不是一个因素，则可以选择使用 lowestPrice 分配策略来最大限度地节省成本。然而请注意，由于 lowestPrice 分配策略仅考虑实例价格而不考虑可用容量，因此可能会导致较高的竞价型实例中断率。

当您的实例集较大或运行时间较长时

如果队列较大或长时间运行，则可以通过使用 diversified 策略在多个池间分配 Spot 实例 来提高队列的可用性。例如，如果竞价型实例集指定 10 个池，目标容量为 100 个实例，则实例集会在每个池中启动 10 个竞价型实例。如果某个池的 Spot 价格超过您在该池中的最高价，您的队列仅 10% 受到影响。使用此策略还可降低您的队列对单个池的 Spot 价格随时间上涨的敏感度。使用 diversified 策略时，Spot 队列不在 Spot 价格等于或高于按需价格的任何池中启动 Spot 实例。

若要创建低成本且多元化的实例集，请将 lowestPrice 策略与 InstancePoolsToUseCount 结合使用。例如，如果您的目标容量是 10 个竞价型实例，并且您（为 InstancePoolsToUseCount）指定了 2 个 Spot 容量池，则竞价型实例集将从两个价格最低的池提取实例，以满足您的 Spot 容量。

您可以使用少量或大量的 Spot 容量池以在其中分配您的竞价型实例。例如，如果您运行批处理，我们建议指定少量的 Spot 容量池（例如，InstancePoolsToUseCount=2）以确保队列始终具有计算容量，同时尽可能节省成本。如果您运行 Web 服务，我们建议您指定大量 Spot 容量池（例如，InstancePoolsToUseCount=10）以尽可能减少某个 Spot 容量池临时不可用造成的影响。

请注意，竞价型实例集会尽力尝试根据您指定的池数量提取竞价型实例。如果某个池在满足您所需的容量之前耗尽 Spot 容量，则竞价型实例集将继续从价格次低的池中提取实例，以满足您的请求。为确保达到目标容量，您可能会从超过指定数量的池接收竞价型实例。同样，如果大多数池没有 Spot 容量，则您可能会从少于指定数量的池接收完整目标容量。

维持目标容量

在竞价型实例因 Spot 价格或 Spot 容量池的可用容量发生变化而终止之后，maintain 类型的竞价型实例集会启动替换竞价型实例。分配策略确定从哪个池启动替换实例，如下所示：

- 如果分配策略是 priceCapacityOptimized，则实例集在具有最多竞价型实例容量的池中启动替换实例，同时还要考虑价格并确定价格最低且具有高可用容量的池。
- 如果分配策略是 capacityOptimized，则实例集在当前具有最多竞价型实例可用容量的池中启动替换实例。
- 如果分配策略是 diversified，则队列在其余池间分配替换 Spot 实例。
- 如果分配策略是 lowestPrice，则 队列在当前具有最低 Spot 价格的池中启动替换实例。
- 如果分配策略是 lowestPrice 与 InstancePoolsToUseCount 的组合，则队列选择具有最低价格的 Spot 容量池并跨您指定数量的 Spot 容量池启动 Spot 实例。

竞价型实例集的基于属性的实例类型选择

创建竞价型实例集时，必须指定一种或多种实例类型以配置机群中的按需型实例和竞价型实例。除了手动指定实例类型外，还可以指定实例必须具有的属性，Amazon EC2 将使用这些属性标识所有实例类型。这称

为基于属性的实例类型选择。例如，您可以指定实例所需的最小和最大 vCPU 数量，竞价型实例集将使用满足这些 vCPU 要求的任何可用实例类型启动实例。

基于属性的实例类型选择是工作负载和框架的理想选择，这些工作负载和框架可以灵活地确定所用的实例类型，例如在运行容器或 Web 机群、处理大数据以及实施持续集成和部署 (CI/CD) 工具等情况下。

优点

基于属性的实例类型选择具有以下优势：

- 有如此多的实例类型可供使用，因此找到适用于您的工作负载的实例类型可能非常耗时。当您指定实例属性时，实例类型将自动具有工作负载所需的属性。
- 要为竞价型实例集手动指定多种实例类型，您必须为每种实例类型创建单独的启动模板覆盖。但是，借助基于属性的实例类型选择，要提供多种实例类型，您只需在启动模板或启动模板覆盖中指定实例属性即可。
- 当您指定实例属性而不是实例类型时，您的机群可以在新一代实例类型发布时使用这些实例类型，“满足未来”机群配置的需求。
- 当您指定实例属性而不是实例类型时，竞价型实例集可以从各种实例类型中进行选择以启动竞价型实例，从而遵循灵活选择实例类型 Spot 最佳实践 (p. 451)。

主题

- 基于属性的实例类型选择的工作原理 (p. 875)
- 注意事项 (p. 877)
- 通过基于属性的实例类型选择创建竞价型实例集 (p. 877)
- 有效配置示例和无效配置示例 (p. 879)
- 预览具有指定属性的实例类型 (p. 885)

基于属性的实例类型选择的工作原理

要在机群配置中使用基于属性的实例类型选择，请将实例类型列表替换为实例所需的实例属性列表。竞价型实例集将在具有指定实例属性的任何可用实例类型上启动实例。

主题

- 实例属性的类型 (p. 875)
- 在何处配置基于属性的实例类型选择 (p. 875)
- 预置机群时，竞价型实例集如何使用基于属性的实例类型选择 (p. 876)
- 价格保护 (p. 876)

实例属性的类型

您可以指定几个实例属性来表示计算需求。有关每个属性和默认值的描述，请参阅 Amazon EC2 API 参考中的 InstanceRequirements。

在何处配置基于属性的实例类型选择

根据您使用的是控制台还是 Amazon CLI，可以按如下方式为基于属性的实例类型选择指定实例属性：

在控制台中，您可以在以下一个或两个机群配置组件中指定实例属性：

- 在启动模板中，并在实例集请求中引用启动模板
- 在机群请求中

在 Amazon CLI 中，您可以在以下一个或全部机群配置组件中指定实例属性：

- 在启动模板中，并在机群请求中引用启动模板
- 在启动模板覆盖中

  如果您想混合应用使用不同 AMI 的实例，则可以在多个启动模板覆盖中指定实例属性。例如，不同的实例类型可以使用 x86 和基于 ARM 的处理器。
- 在启动规范中

预置机群时，竞价型实例集如何使用基于属性的实例类型选择

竞价型实例集通过以下方式预置机群：

- 竞价型实例集标识具有指定属性的实例类型。
- 竞价型实例集使用价格保护确定要排除的实例类型。
- 竞价型实例集根据具有匹配实例类型的Amazon区域或可用区确定将从中启动实例的容量池。
- 竞价型实例集应用指定的分配策略确定从中启动实例的容量池。

  请注意，基于属性的实例类型选择不会选择从中预置机群的容量池；这是分配策略的任务。可能有大量具有指定属性的实例类型，其中一些类型可能成本高昂。竞价型和按需型的 `lowestPrice` 默认分配策略可保证竞价型实例集将从成本最低的容量池启动实例。

  如果您指定分配策略，竞价型实例集将根据指定的分配策略启动实例。
  - 对于竞价型实例，基于属性的实例类型选择支持 `capacityOptimizedPrioritized`、`capacityOptimized` 和 `lowestPrice` 分配策略。
  - 对于按需型实例，基于属性的实例类型选择支持 `lowestPrice` 分配策略。
- 如果没有适用于具有指定实例属性的实例类型的容量，则无法启动任何实例，并且机群返回错误。

价格保护

价格保护是一项功能，可以防止竞价型实例集使用您认为成本过高的实例类型，即使它们恰好适合您指定的属性。当您使用基于属性的实例类型选择创建机群时，默认情况下会启用价格保护，并为按需型实例和竞价型实例设置了单独的阈值。当 Amazon EC2 选择具有您的属性的实例类型时，会排除定价高于阈值的实例类型。阈值表示您将支付的最大值，以高于具有指定属性的成本最低的最新一代 M、C 或 R 实例类型的百分比表示。

如果不指定阈值，默认情况下将使用以下阈值：

- 对于按需型实例，价格保护阈值设置为 20%。
- 对于竞价型实例，价格保护阈值设置为 100%。

指定价格保护阈值

创建竞价型实例集时，配置机群以使用基于属性的实例类型选择，然后执行以下操作：

- 控制台

  若要指定按需型实例价格保护阈值，请在 Additional instance attribute（其他实例属性）项下，选择 On-demand price protection（按需价格保护），然后选择 Add Attribute（添加属性）。在 On-Demand price protection percentage（按需价格保护百分比）项中，输入以百分比表示的价格保护阈值。

  若要指定竞价型实例价格保护阈值，请在 Additional instance attribute（其他实例属性）项下，选择 Spot price protection（Spot 价格保护），然后选择 Add Attribute（添加属性）。在 Spot price protection percentage（Spot 价格保护百分比）项中，输入以百分比表示的价格保护阈值。

- Amazon CLI

  若要指定按需型实例价格保护阈值，请在 JSON 配置文件的 `InstanceRequirements` 结构中，为 `OnDemandMaxPricePercentageOverLowestPrice` 输入以百分比表示的价格保护阈值。

  若要指定竞价型实例价格保护阈值，请在 JSON 配置文件的 `InstanceRequirements` 结构中，为 `SpotMaxPricePercentageOverLowestPrice` 输入以百分比表示的价格保护阈值。

有关创建机群的更多信息，请参阅 通过基于属性的实例类型选择创建竞价型实例集 (p. 877)。

> **Note**
>
> 创建竞价型实例集时，如果将 Total target capacity（总目标容量）类型设置为 vCPUs (vCPU) 或 Memory (MiB) [内存（MiB）]（控制台），或将 `TargetCapacityUnitType` 设置为 `vcpu` 或 `memory-mib`（Amazon CLI），则价格保护阈值将基于每个 vCPU 或每个内存的价格应用，而不是基于每个实例的价格应用。

注意事项

- 您可以在竞价型实例集中指定实例类型或实例属性，但不能同时指定两者。

  使用 CLI 时，启动模板覆盖将覆盖启动模板。例如，如果启动模板包含实例类型，而启动模板覆盖包含实例属性，则由实例属性标识的实例将覆盖启动模板中的实例类型。
- 使用 CLI 时，如果将实例属性指定为覆盖，也无法指定权重或优先级。
- 在一个请求配置中，最多可以指定四个 `InstanceRequirements` 结构。

通过基于属性的实例类型选择创建竞价型实例集

您可以通过 Amazon EC2 控制台或 Amazon CLI 将机群配置为使用基于属性的实例类型选择。

主题

- 使用控制台创建竞价型实例集 (p. 877)
- 使用 Amazon CLI 创建竞价型实例集 (p. 878)

使用控制台创建竞价型实例集

配置竞价型实例集以使用基于属性的实例类型选择（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Spot Requests（竞价型请求），然后选择 Request Spot Instances（请求竞价型实例）。
3. 按照步骤创建竞价型实例集。有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)。

   创建竞价型实例集时，按如下方式配置机群以使用基于属性的实例类型选择：

   a. 对于 Instance type requirements（实例类型要求），选择 Specify instance attributes that match your compute requirements（指定符合计算要求的实例属性）。
   b. 对于 vCPU，输入所需的最小和最大 vCPU 数。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。
   c. 对于 Memory (GiB)（内存 (GiB)），输入所需的最小和最大内存量。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。
   d. （可选）对于 Additional instance attributes（其它实例属性），您可以选择指定一个或多个属性以更详细地表达计算要求。每个额外属性都会进一步增加对您的请求的限制。

e. （可选）展开 Preview matching instance types（预览匹配的实例类型），查看具有指定属性的实例类型。

使用 Amazon CLI 创建竞价型实例集

配置竞价型实例集以使用基于属性的实例类型选择（Amazon CLI）

使用 request-spot-fleet (Amazon CLI) 命令可创建竞价型实例集。请在 JSON 文件中指定机群配置。

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

示例 *file_name*.json 文件

以下示例包含配置竞价型实例集的参数，以便使用基于属性的实例类型选择，后附文本说明。

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

基于属性的实例类型选择的属性在 InstanceRequirements 结构中指定。在此示例中，指定了两个属性：

- VCpuCount – 至少指定了 2 个 vCPU。由于未指定最大值，因此没有最大限制。
- MemoryMiB – 至少指定了 4 MiB 的内存。由于未指定最大值，因此没有最大限制。

将识别具有 2 个或更多 vCPU 和 4 MiB 或更大内存的任何实例类型。然而，当竞价型实例集预置实例集 (p. 876)时，价格保护和分配策略可能会排除某些实例类型。

有关您可以指定的所有可能属性的列表和描述，请参阅 Amazon EC2 API Reference（《Amazon EC2 API 参考》）中的 InstanceRequirements。

> **Note**
>
> 当 InstanceRequirements 包含在机群配置中时，必须排除 InstanceType 和 WeightedCapacity；它们无法与实例属性同时确定机群配置。

JSON 还包含以下实例集配置：

- "AllocationStrategy": "*priceCapacityOptimized*" – 实例集中竞价型实例的分配策略。

- "LaunchTemplateName": "*my-launch-template*", "Version": "*1*" – 启动模板包含一些实例配置信息，但如果指定了任何实例类型，则这些配置信息将被 InstanceRequirements 中指定的属性覆盖。
- "TargetCapacity": *20* – 目标容量为 20 个竞价型实例。
- "Type": "*request*" – 实例集的请求类型是 request。

有效配置示例和无效配置示例

如果您使用 Amazon CLI 创建竞价型实例集，必须确保机群配置有效。以下示例展示了有效配置和无效配置。

如果配置包含以下项，则视为无效：

- 单个 Overrides 结构，但同时包含 InstanceRequirements 和 InstanceType
- 两个 Overrides 结构，其中一个包含 InstanceRequirements，而另一个包含 InstanceType
- 两个 InstanceRequirements 结构，但在同一 LaunchTemplateSpecification 中具有重叠的属性值

示例配置

- 有效配置：具有覆盖的单个启动模板 (p. 879)
- 有效配置：具有多个 InstanceRequirements 的单个启动模板 (p. 880)
- 有效配置：两个启动模板，每个都具有覆盖 (p. 881)
- 有效配置：仅指定 InstanceRequirements，且属性值不重叠 (p. 882)
- 配置无效：Overrides 包含 InstanceRequirements 和 InstanceType (p. 883)
- 配置无效：两个 Overrides 包含 InstanceRequirements 和 InstanceType (p. 883)
- 配置无效：属性值重叠 (p. 884)

有效配置：具有覆盖的单个启动模板

以下配置有效。包含一个启动模板和一个 Overrides 结构（包含一个 InstanceRequirements 结构）。下面是示例配置的文本说明。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
```

```
                        "Max": 10000
                    },
                    "RequireHibernateSupport": true
                }
            }
        ]
    }
],
    "TargetCapacity": 5000,
        "OnDemandTargetCapacity": 0,
        "TargetCapacityUnitType": "vcpu"
}
}
```

InstanceRequirements

要使用基于属性的实例选择，您必须在机群配置中包含 InstanceRequirements 结构，并为机群中的实例指定所需的属性。

在上述示例中，指定了以下实例属性：

- VCpuCount – 实例类型的 vCPU 数量必须最少为 2 个，最多为 8 个。
- MemoryMiB – 实例类型的最大内存必须为 10240MiB。最小值 0 表示没有最低限制。
- MemoryGiBPerVCpu – 实例类型的每个 vCPU 内存最大值必须为 10000GiB。Min 参数是可选的。省略此属性表示没有最低限制。

TargetCapacityUnitType

TargetCapacityUnitType 参数为目标容量指定单位。在该示例中，目标容量是 5000，目标容量单位类型是 vcpu，它们共同指定了所需的 5000 个 vCPU 目标容量。竞价型实例集将启动足够多的实例，以便机群中的 vCPU 总数为 5000 个 vCPU。

有效配置：具有多个 InstanceRequirements 的单个启动模板

以下配置有效。包含一个启动模板和一个 Overrides 结构（包含两个 InstanceRequirements 结构）。InstanceRequirements 中指定的属性有效，因为值不重叠，第一个 InstanceRequirements 结构指定 VCpuCount 为 0-2 个 vCPU，而第二个 InstanceRequirements 结构指定 4-8 个 vCPU。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

有效配置：两个启动模板，每个都具有覆盖

以下配置有效。包含两个启动模板，每个模板都有一个 Overrides 结构（包含一个 InstanceRequirements 结构）。此配置适用于在同一机群中支持 arm 和 x86 架构。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
```

```
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

有效配置：仅指定 InstanceRequirements，且属性值不重叠

以下配置有效。包含两个 LaunchTemplateSpecification 结构，每个结构都有一个启动模板和一个 Overrides 结构（包含一个 InstanceRequirements 结构）。InstanceRequirements 中指定的属性有效，因为值不重叠，第一个 InstanceRequirements 结构指定 VCpuCount 为 0-2 个 vCPU，而第二个 InstanceRequirements 结构指定 4-8 个 vCPU。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
```

```
        "Type": "maintain"
    }
}
```

配置无效：Overrides 包含 InstanceRequirements 和 InstanceType

以下配置无效。Overrides 结构同时包含 InstanceRequirements 和 InstanceType。对于 Overrides，可以指定 InstanceRequirements 或 InstanceType，但不能同时指定两者。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

配置无效：两个 Overrides 包含 InstanceRequirements 和 InstanceType

以下配置无效。Overrides 结构同时包含 InstanceRequirements 和 InstanceType。您可以指定 InstanceRequirements 或 InstanceType，但不能同时指定两者，即使采用不同的 Overrides 结构也是如此。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
```

```
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

配置无效：属性值重叠

以下配置无效。两个 InstanceRequirements 结构，每个结构都包含 "VCpuCount": {"Min": 0, "Max": 2}。这些属性的值重叠，这将导致容量池重复。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
            }
        ]
    }
    ],
    "TargetCapacity": 1,
    "OnDemandTargetCapacity": 0,
    "Type": "maintain"
}
}
```

预览具有指定属性的实例类型

您可以使用 get-instance-types-from-instance-requirements Amazon CLI 命令预览与您指定的属性匹配的实例类型。这对于在不启动任何实例的情况下确定要在请求配置中指定的属性尤其有用。请注意，该命令不考虑可用容量。

通过使用 Amazon CLI 指定属性来预览实例类型列表

1. （可选）要生成所有可以指定的可能属性，请使用 get-instance-types-from-instance-requirements 命令和 `--generate-cli-skeleton` 参数。您可以选择使用 `input > attributes.json` 将输出定向到某个文件以将其保存。

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

预期输出

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
```

```
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. 使用上一步的输出创建 JSON 配置文件，然后按如下方式进行配置：

   Note

   您必须提供 `ArchitectureTypes`、`VirtualizationTypes`、`VCpuCount` 和 `MemoryMiB` 的值。您可以省略其它属性；如果省略，则使用默认值。
   有关每个属性及其默认值的描述，请参阅 Amazon EC2 命令行参考中的 get-instance-types-from-instance-requirements。

   a. 对于 `ArchitectureTypes`，请指定一个或多个处理器架构类型。

   b. 对于 `VirtualizationTypes`，请指定一个或多个虚拟化类型。

   c. 对于 `VCpuCount`，请指定最小和最大 vCPU 数量。要指定没有最低限制，对于 `Min`，请指定 `0`。要指定没有最大限制，请省略 `Max` 参数。

d. 对于 MemoryMiB，请指定最小和最大内存量（以 MiB 为单位）。要指定没有最低限制，对于 Min，请指定 0。要指定没有最大限制，请省略 Max 参数。

e. 您可以选择指定一个或多个其他属性来进一步限制返回的实例类型列表。

3. 要预览具有您在 JSON 文件中所指定属性的实例类型，请使用 get-instance-types-from-instance-requirements 命令，然后使用 --cli-input-json 参数指定 JSON 文件的名称和路径。您可以选择将输出格式设置为以表格格式显示。

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

示例 *attributes.json* 文件

在此示例中，JSON 文件包含所需属性。它们是 ArchitectureTypes、VirtualizationTypes、VCpuCount 和 MemoryMiB。此外，还包含可选属性 InstanceGenerations。请注意，对于 MemoryMiB，可以省略 Max 值，指示没有限制。

```
{
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

输出示例

```
----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+--------------------------------------+
||            InstanceTypes           ||
|+--------------------------------------+|
||            InstanceType            ||
|+--------------------------------------+|
||  c4.xlarge                         ||
||  c5.xlarge                         ||
||  c5a.xlarge                        ||
||  c5ad.xlarge                       ||
||  c5d.xlarge                        ||
||  c5n.xlarge                        ||
||  c6a.xlarge                         ||
...
```

4. 在确定满足您的需求的实例类型后，请记下您使用的实例属性，以便在配置机群请求时可以使用。

Spot 队列中的按需实例

为确保始终拥有实例容量，您可以在 Spot 队列请求中包含按需容量请求。在 Spot 队列请求中，您需要指定所需的目标容量以及该容量中有多少必须是按需容量。余量由 Spot 容量组成，后者在有可用的 Amazon EC2 容量并且可用时启动。例如，如果您在竞价型实例集请求中指定目标容量为 10，按需容量为 8，则 Amazon EC2 会将 8 个容量单位作为按需型实例启动，2 个容量单位（10-8=2）作为竞价型实例启动。

针对按需容量优化实例类型

竞价型实例集尝试满足您的按需容量时，它会默认首先启动价格最低的实例类型。如果 `OnDemandAllocationStrategy` 设置为 `prioritized`，竞价型实例集将使用优先级来确定首先使用什么实例类型来满足按需容量。

优先级分配给启动模板覆盖，优先级最高的最先启动。

示例：确定实例类型的优先级

在本例中，您可以配置三个启动模板覆盖，每个覆盖具有不同的实例类型。

实例类型的按需价格在价格范围内。以下是本例中使用的实例类型，按价格顺序列出，从最便宜的实例类型开始：

- `m4.large` – 最便宜
- `m5.large`
- `m5a.large`

如果您不使用优先级来确定顺序，实例集将从最便宜的实例类型开始满足按需容量。

但是，假设您有想要先使用的未用 `m5.large` 预留实例。您可以设置启动模板覆盖优先级，以便按优先级顺序使用实例类型，如下所示：

- `m5.large` – 优先级 1
- `m4.large` – 优先级 2
- `m5a.large` – 优先级 3

容量再平衡

您可以配置竞价型实例集以在 Amazon EC2 发出再平衡建议以通知您竞价型实例处于较高的中断风险时启动替换竞价型实例。容量再平衡功能可在运行中的实例被 Amazon EC2 中断之前，主动使用新竞价型实例扩展您的队列，从而帮助您维护工作负载的可用性。有关更多信息，请参阅EC2 实例再平衡建议 (p. 480)。

要配置竞价型实例集以启动替换竞价型实例，您可以使用 Amazon EC2 控制台或 Amazon CLI。

- Amazon EC2 控制台：您必须在创建 Spot 队列时选中 Capacity rebalance (容量再平衡) 复选框。有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台） (p. 901)中的步骤 6.d.。
- Amazon CLI：使用 request-spot-fleet 命令和 `SpotMaintenanceStrategies` 结构中的相关参数。有关更多信息，请参阅示例启动配置 (p. 966)。

限制

- 容量再平衡仅适用于类型为 `maintain` 的机群。
- 队列运行时，您无法修改容量再平衡设置。要更改容量再平衡设置，您必须删除此队列并创建新队列。

配置选项

竞价型实例集的 `ReplacementStrategy` 支持以下两个值：

`launch-before-terminate`

Amazon EC2 可以在新的替换竞价型实例启动后终止接收再平衡通知的竞价型实例。如果指定 `launch-before-terminate`，还必须为 `termination-delay` 指定值。启动新的替换实例后，Amazon EC2 将等待 `termination-delay` 的持续时间，然后终止旧实例。对于 `termination-delay`，最短为 120 秒（2 分钟），最长为 7200 秒（2 小时）。

建议仅当您可以预测实例关闭过程完成所需的时长时才使用 `launch-before-terminate`。这将确保只有在关闭过程完成后才终止旧实例。请注意，Amazon EC2 可能会在 `termination-delay` 之前中断旧实例，并发出两分钟警告。

我们强烈建议不要将 `lowestPrice` 分配策略与 `launch-before-terminate` 结合使用，以避免替换竞价型实例也处于中断风险升高的状态。

`launch`

针对现有竞价型实例发出再平衡通知时，Amazon EC2 将启动替换竞价型实例。Amazon EC2 不会终止接收再平衡通知的实例。您可以终止旧实例，也可以使其保持运行状态。在实例运行期间，您需要为它们付费。

注意事项

如果为容量再平衡配置 Spot 队列，请考虑以下事项：

在请求中提供尽可能多的 Spot 容量池

将您的 Spot 队列配置为使用多种实例类型和多个可用区。这提供了在各种 Spot 容量池中启动竞价型实例的灵活性。有关更多信息，请参阅灵活地选择实例类型和可用区 (p. 451)。

避免替换竞价型实例中断的风险升高

如果您使用 `lowestPrice` 分配策略，替换竞价型实例可能会面临中断升高的风险。这是因为，即使替换竞价型实例可能在启动后不久中断，Amazon EC2 始终会在当时具有可用容量的价格最低池中启动实例。为避免中断风险升高，我们强烈建议不要使用 `lowestPrice` 分配策略，而建议使用 `capacityOptimized` 或 `capacityOptimizedPrioritized` 分配策略。这些策略确保替换竞价型实例在最佳的竞价型容量池中启动，因此在不久的将来不太可能被中断。有关更多信息，请参阅使用价格和容量优化分配策略 (p. 451)。

只有可用性相同或更好时，Amazon EC2 才会启动新实例

容量再平衡的目标之一是提高竞价型实例的可用性。如果现有竞价型实例收到再平衡建议，Amazon EC2 只有在新实例提供与现有实例相同或更好的可用性时才会启动新实例。如果新实例的中断风险比现有实例更高，那么 Amazon EC2 将不会启动新实例。但是，Amazon EC2 将继续评测 Spot 容量池，并在可用性改善时启动新实例。

如果 Amazon EC2 没有主动启动新实例，则您的现有实例可能会中断。发生这种情况时，无论新实例的中断风险是否较高，Amazon EC2 都会尝试启动新实例。

容量再平衡不会提高您的竞价型实例中断率

当您启用容量再平衡时，它不会提高您的竞价型实例中断率 (p. 484)（在 Amazon EC2 需要收回容量时回收的竞价型实例的数量）。然而，如果容量再平衡检测到实例存在中断风险，Amazon EC2 将立即尝试启动新实例。结果是，与存在风险的实例中断后等待 Amazon EC2 启动新实例相比，可能会替换更多实例。

虽然在启用了容量再平衡的情况下您可以更换更多实例，但在中断您的实例之前，您会有更多时间采取行动，从而因为处于主动而非被动地位而受益。使用 Spot Instance interruption notice (p. 490)（竞价型实例中断通知），您通常最多只有两分钟的时间来正常关闭您的实例。借助容量再平衡提前启动新实例，您可以使现有流程更有可能在存在风险的实例上完成，您可以启动实例关闭程序，并防止在存在风

险的实例上安排新工作。您还可以开始准备新启动的实例，以接管应用程序。借助容量再平衡的主动替换，您可以因绝佳的连续性而受益。

作为演示使用容量再平衡的风险和优点的理论示例，请考虑以下场景：

- 下午 2:00 – 收到针对实例 A 的再平衡建议，Amazon EC2 立即开始尝试启动替换实例 B，让您有时间启动关闭程序。*
- 下午 2:30 - 收到针对实例 B 的再平衡建议，该实例将被替换为实例 C，让您有时间启动关闭程序。*
- 下午 2:32 - 如果未启用容量再平衡，并且如果在下午 2:32 收到针对实例 A 的竞价型实例中断通知，则您最多只有两分钟时间采取行动，但实例 A 将一直运行到此时。

* 如果指定了 `launch-before-terminate`，Amazon EC2 将在替换实例上线后终止存在风险的实例。

Amazon EC2 可以启动新替换竞价型实例，直到已执行容量达到目标容量的两倍

为容量再平衡配置竞价型实例集时，EC2 会尝试为接收再平衡建议的每个竞价型实例启动新的替换竞价型实例。在竞价型实例收到再平衡建议后，它不再统计为已执行容量的一部分。根据替换策略，Amazon EC2 将在预配置的终止延迟后终止实例，或使其保持运行状态。这使您有机会对实例执行再平衡操作 (p. 481)。

如果您的队列达到目标容量的两倍，即使替换实例本身收到再平衡建议，它也会停止启动新的替换实例。

例如，您创建的竞价型实例集目标容量为 100 个竞价型实例。所有竞价型实例都会收到再平衡建议，这将导致 Amazon EC2 启动 100 个替换竞价型实例。这使已执行的竞价型实例的数量增加到 200 个，是目标容量的两倍。一些替换实例会收到再平衡建议，但由于队列不能超过目标容量的两倍，因此不会再启动更多替换实例。

请注意，在实例运行期间，您需要为所有实例付费。

我们建议您将竞价型实例集配置为终止接收再平衡建议的竞价型实例

如果您将竞价型实例集配置为实现容量再平衡，我们建议仅当您可以预测实例关闭过程完成所需的时长时才选择 `launch-before-terminate` 和适当的终止延迟。这将确保只有在关闭过程完成后才终止旧实例。

如果您选择自行终止建议再平衡的实例，我们建议您监控机群中的竞价型实例接收的再平衡建议信号。通过监控信号，您可以在 Amazon EC2 中断受影响的实例之前快速对其执行再平衡操作 (p. 481)，然后您可以手动终止它们。如果您不终止实例，则需要在实例运行期间继续为其付费。Amazon EC2 不会自动终止接收再平衡建议的实例。

您可以使用 Amazon EventBridge 或实例元数据设置通知。有关更多信息，请参阅监控再平衡建议信号 (p. 481)。

在计算横向缩减或扩展期间的已执行容量时，竞价型实例集不计入收到再平衡建议的实例

如果您的 Spot 队列针对容量再平衡进行了配置，并且您将目标容量更改为向内或向外扩展，则队列不会将标记为再平衡的实例计算为已执行容量的一部分，如下所示：

- 横向缩减 – 如果您降低所需的目标容量，Amazon EC2 将终止未标记为再平衡的实例，直到达到所需容量。标记为再平衡的实例不计入已执行容量。

  例如，您创建的竞价型实例集目标容量为 100 个竞价型实例。10 个实例会收到再平衡建议，因此 Amazon EC2 会启动 10 个新的替换实例，从而获得 110 个实例的执行容量。然后，您将目标容量减少到 50 个（横向缩减），但已执行的容量实际上为 60 个实例，因为 Amazon EC2 不会终止标记为再平衡的 10 个实例。您需要手动终止这些实例，也可以让它们保持运行状态。
- 横向扩展 – 如果您增加所需的目标容量，Amazon EC2 将启动新实例，直到达到所需容量。标记为再平衡的实例不计入已执行容量。

  例如，您创建的竞价型实例集目标容量为 100 个竞价型实例。10 个实例会收到再平衡建议，因此 Amazon EC2 会启动 10 个新的替换实例，从而获得 110 个实例的执行容量。然后，您将目标容量增加到 200（扩展），但已执行的容量实际上为 210 个实例，因为标记为再平衡的 10 个实例不被队列计入目标容量的一部分。您需要手动终止这些实例，也可以让它们保持运行状态。

Spot 价格覆盖

每个 Spot 队列请求可以包含全局最高价格，或使用默认值（按需价格）。Spot 队列将该价格作为每个启动规范的默认最高价。

您可以选择在一个或多个启动规范中指定最高价。该价格是启动规范特有的。如果启动规范包含特定的价格，则 Spot 队列使用该最高价以覆盖全局最高价。不包含特定最高价的任何其他启动规范仍使用全局最高价。

控制支出

在达到目标容量或您愿意支付的最大金额时，Spot 队列停止启动实例。要控制您每小时为队列支付的金额，您可以为 Spot 实例指定 `SpotMaxTotalPrice` 并为按需实例指定 `OnDemandMaxTotalPrice`。在达到最高总价时，即使未达到目标容量，Spot 队列也会停止启动实例。

以下示例显示了两个不同的方案。在第一个方案中，在达到目标容量时，Spot 队列停止启动实例。在第二个方案中，在达到您愿意支付的最大金额时，Spot 队列停止启动实例。

示例：在达到目标容量时，停止启动实例

假设发出 `m4.large` 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`：1.50 美元

竞价型实例集启动 10 个按需型实例，因为总价 1.00 美元（10 个实例 x 0.10 美元）不超过 `OnDemandMaxTotalPrice`（1.50 美元）。

示例：在达到最高总价时，停止启动实例

假设发出 `m4.large` 按需实例请求，其中：

- 按需价格：每小时 0.10 美元
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`：0.80 美元

如果竞价型实例集启动按需目标容量（10 个按需型实例），则每小时的总成本为 1.00 USD。该值超过了为 `OnDemandMaxTotalPrice` 指定的金额（0.80 美元）。为了防止支出超过您愿意支付的金额，竞价型实例集仅启动 8 个按需型实例（低于按需目标容量），因为启动更多实例将超过 `OnDemandMaxTotalPrice`。

Spot 队列实例权重

在请求 Spot 实例 队列时，可以使用实例权重定义每种实例类型为应用程序性能贡献的容量单位，并相应地为每个 Spot 容量池调整最高价。

默认情况下，您指定的价格是每实例小时 价格。在使用实例权重功能时，您指定的价格是每单位小时 价格。您可以将某种实例类型的价格除以它表示的单位数来计算每单位小时价格。竞价型实例集通过将目标容量除以实例权重，计算出要启动的竞价型实例数。如果结果不是整数，则 Spot 队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。Spot 队列可以选择您在启动规范中指定的任意池，即使所启动实例的容量超过请求的目标容量也是如此。

下表提供了确定目标容量为 10 的 Spot 队列请求的每单位价格的计算示例。

实例类型	实例权重	每实例小时价格	每单位小时价格	启动的实例数
`r3.xlarge`	2	0.05 美元	0.025	5

实例类型	实例权重	每实例小时价格	每单位小时价格	启动的实例数
			(0.05 除以 2)	(10 除以 2)

实例类型	实例权重	每实例小时价格	每单位小时价格	启动的实例数
r3.8xlarge	8	0.10 美元	0.0125 (0.10 除以 8)	2 (10 除以 8，结果向上舍入)

按如下所示使用 Spot 队列实例权重，在执行时具有每单位最低价格的池中预置所需的目标容量：

1. 采用实例（默认设置）或采用所选单位（如虚拟 CPU、内存、存储或吞吐量）为 Spot 队列设置目标容量。
2. 设置每单位价格。
3. 对于每个启动配置，请指定权重，这是实例类型向目标容量提供的单位数。

实例权重示例

考虑一个具有以下配置的 Spot 队列请求：

- 目标容量为 24
- 一个实例类型为 r3.2xlarge 且权重为 6 的启动规范
- 一个实例类型为 c3.xlarge 且权重为 5 的启动规范

每个权重表示相应实例类型向目标容量提供的单位数。如果第一个启动规范提供了最低的每单位价格 (r3.2xlarge 每实例小时价格除以 6)，Spot 队列将启动其中的四个实例 (24 除以 6)。

如果第二个启动规范提供了最低的每单位价格（c3.xlarge 每实例小时价格除以 5），则竞价型实例集会启动 5 个这样的实例（24 除以 5，结果向上舍入）。

实例权重和分配策略

考虑一个具有以下配置的 Spot 队列请求：

- 目标容量为 30
- 一个实例类型为 c3.2xlarge 且权重为 8 的启动规范
- 一个实例类型为 m3.xlarge 且权重为 8 的启动规范
- 一个实例类型为 r3.xlarge 且权重为 8 的启动规范

Spot 队列会启动四个实例 (30 除以 8，结果向上舍入)。在使用 lowestPrice 策略时，所有四个实例均来自提供最低每单位价格的池。使用 diversified 策略时，竞价型实例集会在所有三个池中各启动一个实例，并在三个池中提供最低每单位价格的那个池中启动第四个实例。

使用 Spot 队列

要开始使用 Spot 队列，请创建一个 Spot 队列请求，其中包括目标容量、可选的按需部分、实例的一个或多个启动规范以及您愿意支付的最高价。队列请求必须包括定义队列启动实例所需信息（例如 AMI、实例类型、子网或可用区、一个或多个安全组）的启动规范。

如果队列包括竞价型实例，Amazon EC2 将尝试在 Spot 价格变化时保持队列的目标容量。

提交一次性请求后，其目标容量则无法修改。要更改目标容量，请取消请求并重新提交新请求。

Spot 队列请求在过期或您取消它之前保持有效。当您取消实例集请求时，您可以指定取消该请求是否终止该队列中的 Spot 实例。

目录

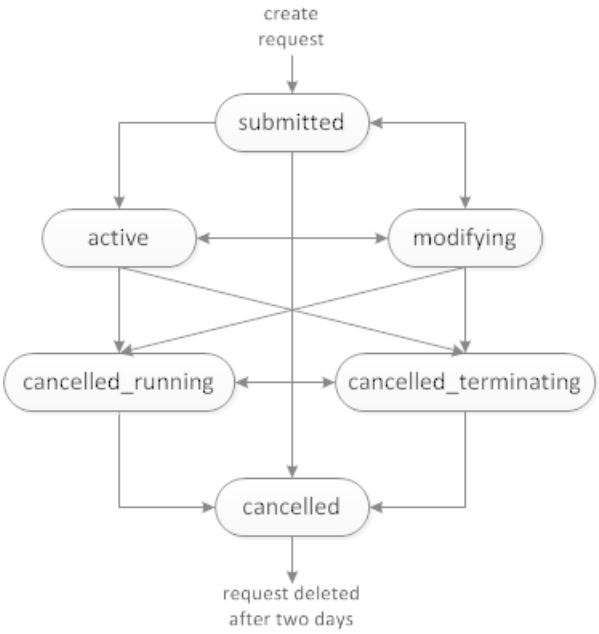
- Spot 队列请求状态 (p. 893)
- Spot 队列运行状况检查 (p. 894)
- Spot 队列权限 (p. 894)
- 创建 Spot 队列请求 (p. 900)
- 标记 Spot 队列 (p. 904)
- 描述竞价型实例集 (p. 910)
- 修改 Spot 队列请求 (p. 910)
- 取消 Spot 队列请求 (p. 911)

Spot 队列请求状态

Spot 队列请求可以处于以下某种状态：

- `submitted` – 正在评估竞价型实例集请求，并且 Amazon EC2 正准备启动目标数量的实例。
- `active` – 已验证竞价型实例集，并且 Amazon EC2 正在尝试维护目标数量的正在运行的竞价型实例。请求会保持此状态，直到修改或取消它。
- `modifying` – 竞价型实例集请求正在修改中。请求将保持该状态，直到完全处理修改或取消了 Spot 队列。无法修改一次性 `request`，并且这一状态不适用于此类 Spot 请求。
- `cancelled_running` – 竞价型实例集已取消且不启动其他竞价型实例。其现有竞价型实例继续运行，直至被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。
- `cancelled_terminating` – 竞价型实例集已取消且其竞价型实例正在终止。请求会保持此状态，直到所有实例都已终止。
- `cancelled` – 竞价型实例集已取消且没有正在运行的竞价型实例。Spot 队列请求将在其实例终止两天后被删除。

以下显示了请求状态之间的转换。如果超出 Spot 队列限制，将会立即取消请求。



Spot 队列运行状况检查

竞价型实例集每 2 分钟检查一次队列中竞价型实例的运行状况。实例的运行状况为 `healthy` 或 `unhealthy`。

Spot 队列将使用 Amazon EC2 提供的状态检查来确定实例的运行状况。如果在连续三次运行状况检查中，实例状态检查或系统状态检查的状态有任一项为 `unhealthy`，则可确定该实例的运行状况为 `impaired`。有关更多信息，请参阅实例的状态检查 (p. 975)。

您可以配置您的队列以替换运行状况不佳的竞价型实例。启用运行状况检查替换后，如果竞价型实例被报告为 `unhealthy`，则会被替换。在替换运行状况不佳的竞价型实例时，队列的容量可能在几分钟内降至其目标容量之下。

要求

- 只有在保持目标容量（类型 `maintain` 的队列）的情况下 Spot 队列 才支持运行状况检查替换，而不支持一次性 Spot 队列（类型 `request` 的队列）。
- 仅对竞价型实例支持运行状况检查替换。对于 按需型实例 不支持此功能。
- 您可以将 Spot 队列配置为仅在您创建它时替换运行状况不佳的实例。
- 用户仅在其有权调用 `ec2:DescribeInstanceStatus` 操作时才能使用运行状况检查替换。

Console

使用控制台配置竞价型实例集以替换运行状况不佳的竞价型实例

1. 按创建 Spot 队列的步骤操作。有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)。
2. 要配置队列以替换运行状况不佳的 Spot 实例，请为 Health check（运行状况检查）选择 Replace unhealthy instances（替换运行状况不佳的实例）。要启用此选项，您必须先选择 Maintain target capacity (保持目标容量)。

Amazon CLI

使用 Amazon CLI 配置竞价型实例集以替换运行状况不佳的竞价型实例

1. 按创建 Spot 队列的步骤操作。有关更多信息，请参阅使用 Amazon CLI 创建竞价型实例集 (p. 903)。
2. 要配置队列以替换运行状况不佳的 Spot 实例，对于 `ReplaceUnhealthyInstances`，请输入 `true`。

Spot 队列权限

如果用户打算创建或管理竞价型实例集，您需要为其授予所需权限。

如果您使用 Amazon EC2 控制台创建竞价型实例集，将创建两个名为 `AWSServiceRoleForEC2SpotFleet` 和 `AWSServiceRoleForEC2Spot` 的服务相关角色和一个名为 `aws-ec2-spot-fleet-tagging-role` 的角色，这些角色为竞价型实例集授予代表您请求、启动、终止和标记资源的权限。如果您使用 Amazon CLI 或 API，您必须确保这些角色存在。

按照以下说明授予所需的权限并创建角色。

权限和角色

- 向用户授予竞价型实例集权限 (p. 895)

- Spot 队列的服务相关角色 (p. 896)
- 竞价型实例的服务相关角色 (p. 898)
- 用于标记 Spot 队列的 IAM 角色 (p. 898)

向用户授予竞价型实例集权限

如果用户打算创建或管理竞价型实例集，请确保为其授予所需的权限。

为竞价型实例集创建策略

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Policies、Create policy。
3. 在 Create policy (创建策略) 页面上，选择 JSON，然后将文本替换为以下内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

上述示例策略为用户授予多数竞价型实例集使用案例所需的权限。要将用户限制为特定的 API 操作，请仅指定这些 API 操作。

所需的 EC2 和 IAM API

必须在策略中包含以下 API：

- `ec2:RunInstances` – 需要其启动竞价型实例集中的实例
- `ec2:CreateTags` – 需要其标记竞价型实例集请求、实例或卷
- `iam:PassRole` – 需要其指定竞价型实例集角色
- `iam:CreateServiceLinkedRole` – 需要其创建服务相关角色

- `iam:ListRoles` – 需要其枚举现有的 IAM 角色
- `iam:ListInstanceProfiles` – 需要其枚举现有的实例配置文件

  Important

  如果您在启动规范或启动模板中为 IAM 实例配置文件指定角色，则必须授予用户将该角色传递给服务的权限。为此，在 IAM policy 中，包括 "`arn:aws:iam::*:role/IamInstanceProfile-role`" 作为 `iam:PassRole` 操作的资源。有关更多信息，请参阅 IAM 用户指南中的向用户授予将角色传递给 Amazon 服务的权限。

竞价型实例集 API

根据需要，将以下 Spot 队列 API 操作添加到策略中：

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

可选的 IAM API

（可选）要允许用户使用 IAM 控制台创建角色或实例配置文件，您必须在策略中添加以下操作：

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. 选择Review policy（查看策略）。
5. 在查看策略页面上，输入策略名称和描述，然后选择创建策略。
6. 要提供访问权限，请为您的用户、组或角色添加权限：

   - 通过身份提供商在 IAM 中托管的用户：

     创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
   - IAM 用户：
     - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
     - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

Spot 队列的服务相关角色

Amazon EC2 使用服务相关角色获取代表您调用其他Amazon服务所需的权限。服务相关角色是一种独特类型的 IAM 角色，它与Amazon服务直接相关。服务相关角色提供了一种将权限委托给 Amazon 服务的安全方式，因为只有相关服务才能担任服务相关角色。有关更多信息，请参阅 IAM 用户指南 中的使用服务相关角色。

Amazon EC2 使用名为 AWSServiceRoleForEC2SpotFleet 的服务相关角色代表您启动和管理实例。

Important

如果在 Spot 队列中指定加密的 AMI (p. 196) 或加密的 Amazon EBS 快照 (p. 1504)，则必须为 AWSServiceRoleForEC2SpotFleet 角色授予使用该 CMK 的权限，以便 Amazon EC2 可以代表您启动实例。有关更多信息，请参阅授予对用于加密的 AMI 和 EBS 快照的 CMK 的访问权限 (p. 898)。

AWSServiceRoleForEC2SpotFleet 授予的权限

Amazon EC2 使用 AWSServiceRoleForEC2SpotFleet 完成以下操作：

- `ec2:RequestSpotInstances` - 请求 Spot 实例
- `ec2:RunInstances` - 启动实例
- `ec2:TerminateInstances` - 终止实例
- `ec2:DescribeImages` - 描述实例的 Amazon 系统映像 (AMI)
- `ec2:DescribeInstanceStatus` - 监控实例的状态。
- `ec2:DescribeSubnets` - 描述实例的子网
- `ec2:CreateTags` – 在竞价型实例集请求、实例和卷中添加标签
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - 将指定的实例添加到指定的负载均衡器
- `elasticloadbalancing:RegisterTargets` - 向指定目标组注册指定目标

创建服务相关角色

在大多数情况下，无需手动创建服务相关角色。Amazon EC2 在您首次使用控制台创建 Spot 队列时创建 AWSServiceRoleForEC2SpotFleet 服务相关角色。

如果在 2017 年 10 月之前具有活动 Spot 队列请求（此时 Amazon EC2 开始支持该服务相关角色），则 Amazon EC2 在您的Amazon账户中创建 AWSServiceRoleForEC2SpotFleet 角色。有关更多信息，请参阅 IAM 用户指南中的我的Amazon账户中出现新角色。

如果您使用 Amazon CLI 或 API 来创建竞价型实例集，则必须确保此角色存在。

要使用控制台创建 AWSServiceRoleForEC2SpotFleet

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色）。
3. 选择 Create role（创建角色）。
4. 对于Select type of trusted entity（选择受信任实体的类型），选择 Amazon service（服务）。
5. 在 Choose a use case (选择使用案例)、Or select a service to view its use cases (或选择服务以查看其使用案例) 下，选择 EC2。
6. 在 Select your use case (选择您的使用案例) 下，选择 EC2 - Spot Fleet (EC2 – Spot 队列)。
7. 选择Next: Permissions（下一步: 权限）。
8. 在下一页上，选择 Next: Tags (下一步: 标记)。
9. 在下一页上，选择 Next:Review（下一步: 审核）。
10. 在 Review (审核) 页面上，选择 Create role (创建角色)。

要使用 Amazon CLI 创建 AWSServiceRoleForEC2SpotFleet

如下所示使用 create-service-linked-role 命令。

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

如果您不再需要使用 Spot 队列，我们建议您删除 AWSServiceRoleForEC2SpotFleet 角色。从您的账户中删除该角色后，如果您使用控制台请求 Spot 队列，Amazon EC2 将再次创建该角色。有关更多信息，请参阅 IAM 用户指南 中的删除服务相关角色。

授予对用于加密的 AMI 和 EBS 快照的 CMK 的访问权限

如果在 Spot 队列请求中指定加密的 AMI (p. 196) 或加密的 Amazon EBS 快照 (p. 1504)，并且您使用客户托管的客户主密钥 (CMK) 进行加密，则必须为 AWSServiceRoleForEC2SpotFleet 角色授予使用该 CMK 的权限，以便 Amazon EC2 可以代表您启动实例。为此，您必须在 CMK 中添加授权，如以下过程中所示。

在提供权限时，授权是密钥策略的替代方法。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用授权和在 Amazon KMS 中使用密钥策略。

为 AWSServiceRoleForEC2SpotFleet 角色授予使用 CMK 的权限

- 使用 create-grant 命令在 CMK 中添加授权，并指定授予权限的委托人（AWSServiceRoleForEC2SpotFleet 服务相关角色）以执行授权允许的操作。CMK 是由 `key-id` 参数和 CMK 的 ARN 指定的。委托人是由 `grantee-principal` 参数和 AWSServiceRoleForEC2SpotFleet 服务相关角色的 ARN 指定的。

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

竞价型实例的服务相关角色

Amazon EC2 使用名为 AWSServiceRoleForEC2Spot 的服务相关角色代表您启动和管理 Spot 实例。有关更多信息，请参阅竞价型实例请求的服务相关角色 (p. 458)。

用于标记 Spot 队列的 IAM 角色

`aws-ec2-spot-fleet-tagging-role` IAM 角色授予竞价型实例集标记竞价型实例集请求、实例和卷的权限。有关更多信息，请参阅标记 Spot 队列 (p. 904)。

> **Important**
>
> 如果您选择在实例集中标记实例并选择保持目标容量（竞价型实例集请求属于类型 `maintain`），用户与 `IamFleetRole` 的权限差异可能会导致实例集中实例的标记行为不一致。如果 `IamFleetRole` 不包含 `CreateTags` 权限，则可能不会标记由队列启动的某些实例。虽然我们正在努力修复这种不一致性，但为了确保队列启动的所有实例都被标记，我们建议您为 `aws-ec2-spot-fleet-tagging-role` 使用 `IamFleetRole` 角色。或者，要使用现有角色，请将 `AmazonEC2SpotFleetTaggingRole` Amazon 托管策略附加到现有角色。否则，您需要手动将 `CreateTags` 权限添加到现有策略。

创建用于标记 Spot 队列的 IAM 角色

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色）。
3. 选择 Create role（创建角色）。
4. 在 Select trusted entity（选择可信实体）页面中，在 Trusted entity type（可信实体类型）下选择 service（Amazon 服务）。
5. 在使用案例下，从其他 Amazon 服务的使用案例中选择 EC2，然后选择 EC2 – 竞价型实例集标记。
6. 选择 Next（下一步）。

7. 在 Add permissions（添加权限）页面上，选择 Next（下一步）。
8. 在 Name, review, and create（命名、检查和创建）页面上，对于 Role name（角色名称），输入角色的名称（例如 **aws-ec2-spot-fleet-tagging-role**）。
9. 检查此页面上的信息，然后选择 Create role（创建角色）。

跨服务混淆代理问题防范

混淆代理问题是一个安全问题，即没有执行操作权限的实体可能会迫使更具权限的实体执行该操作。我们建议在 aws-ec2-spot-fleet-tagging-role 信任策略中使用 aws:SourceArn 和 aws:SourceAccount 全局条件上下文键，以限制竞价型实例集为其他服务提供的资源访问权限。

将 aws:SourceArn 和 aws:SourceAccount 条件键添加到 **aws-ec2-spot-fleet-tagging-role** 信任策略

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles（角色）。
3. 查找您之前创建的 aws-ec2-spot-fleet-tagging-role，然后选择该链接（不是复选框）。
4. 在 Summary（摘要）下，选择 Trust relationships（信任关系）选项卡，然后选择 Edit trust policy（编辑信任策略）。
5. 在 JSON 语句中，添加一个包含您的 aws:SourceAccount 和 aws:SourceArn 全局条件上下文键的 Condition 元素，以防止混淆代理人问题，如下所示：

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
```

> **Note**
>
> 如果 aws:SourceArn 值包含账户 ID，并且您同时使用了这两个全局条件上下文键，则 aws:SourceAccount 值和 aws:SourceArn 值中的账户在同一策略语句中使用时，必须使用相同的账户 ID。

最终的信任策略将如下所示：

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. 选择 Update policy（更新策略）。

下表提供了 aws:SourceArn 的潜在值，以根据不同的明确程度限制 aws-ec2-spot-fleet-tagging-role 的范围。

API 操作	调用的服务	范围	**aws:SourceArn**
RequestSpotFleet	Amazon STS (AssumeRole)	将 aws-ec2-spot-fleet-tagging-role 上的 AssumeRole 功能限定为指定账户中的竞价型实例集请求。	arn:aws:ec2:*:*123456789012*:sp fleet-request/sfr-*
RequestSpotFleet	Amazon STS (AssumeRole)	将 aws-ec2-spot-fleet-tagging-role 上的 AssumeRole 功能限定为指定账户和指定区域中的竞价型实例集请求。请注意，此角色将不能在其他区域使用。	arn:aws:ec2:*us-east-1*:*123456789012*:spot-fleet-request/sfr-*
RequestSpotFleet	Amazon STS (AssumeRole)	将 aws-ec2-spot-fleet-tagging-role 上的 AssumeRole 功能限定为仅影响实例集 sfr-11111111-1111-1111-1111-1111111111111 的操作。请注意，此角色可能无法用于其他竞价型实例集。此外，此角色不能用于通过请求竞价型实例集来启动任何新的竞价型实例集。	arn:aws:ec2:*us-east-1*:*123456789012*:spot-fleet-request/sfr-11111111-1111-1111-1111-11111111111

创建 Spot 队列请求

使用 Amazon Web Services Management Console 快速创建竞价型实例集请求，只需选择您的应用程序或任务需要及最低计算规格即可。Amazon EC2 会配置一个最符合您需求并遵循 Spot 最佳实践的队列。有关更多信息，请参阅快速创建 Spot 队列请求（控制台）(p. 900)。否则，您可以修改任意默认设置。有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)和使用 Amazon CLI 创建竞价型实例集 (p. 903)。

创建 Spot 队列的选项

- 快速创建 Spot 队列请求（控制台）(p. 900)
- 使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)
- 使用 Amazon CLI 创建竞价型实例集 (p. 903)

快速创建 Spot 队列请求（控制台）

按照以下步骤快速创建 Spot 队列请求。

使用推荐设置创建 Spot 队列请求（控制台）

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。

2. 如果您是首次接触 Spot，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot 实例 (请求 Spot 实例)。
3. 在 Launch parameters（启动参数）下，选择 Manually configure launch parameters（手动配置启动参数）。
4. 对于 AMI，选择一个 AMI。
5. 在 Target capacity（目标容量）下，对于 Total target capacity（总目标容量），请指定要请求的单位数。对于单位类型，您可以选择 Instances（实例）、vCPU 或 Memory (MiB)（内存 (MiB)）。
6. 对于 Your fleet request at a glance（您的机群请求概览），查看您的机群配置，然后选择 Launch（启动）。

使用已定义的参数创建 Spot 队列请求（控制台）

您可以使用自己定义的参数创建竞价型实例集。

使用已定义的参数创建 Spot 队列请求（控制台）

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 如果您是首次接触 Spot，则会看到一个欢迎页面；请选择 Get started。否则，请选择 Request Spot 实例 (请求 Spot 实例)。
3. 对于 Launch parameters（启动参数），请执行以下操作：

   a. 要在 Spot 控制台中定义启动参数，请选择 Manually configure launch parameters（手动配置启动参数）。

   b. 对于 AMI，选择 Amazon 提供的基本 AMI，或者选择 Search for AMI（搜索 AMI）以使用来自我们用户社群、Amazon Web Services Marketplace 或您自己的 AMI。

   c. （可选）对于 Key pair name (密钥对名称)，选择现有密钥对或新建一个密钥对。

      [现有密钥对] 选择所需的密钥对。

      [新密钥对] 选择 Create new key pair（创建新密钥对）以前往 Key Pairs（密钥对）页面。完成之后，返回 Spot Requests（竞价型请求）页面并刷新列表。

   d. （可选）展开 Additional launch parameters（其它启动参数），然后执行以下操作：

      i. （可选）要启用 Amazon EBS 优化，对于 EBS-optimized（EBS 优化），请选择 Launch EBS-optimized instances（启动 EBS 优化实例）。

      ii. （可选）要为实例添加临时性块级存储，请对 Instance store (实例存储) 选择 Attach at launch (启动时附加)。

      iii. （可选）要添加存储，请选择 Add new volume（添加新卷），然后根据实例类型指定其它实例存储卷或 Amazon EBS 卷。

      iv. (可选) 默认情况下，已为您的实例启用基本监控。要启用详细监控，对于 Monitoring（监控），请选择 Enable CloudWatch detailed monitoring（启用 CloudWatch 详细监控）。

      v. （可选）要运行专用 Spot 实例，请为 Tenancy (租期) 选择 Dedicated - run a dedicated instance (专用 – 运行专用实例)。

      vi. （可选）对于 Security groups (安全组)，选择一个或多个安全组，或者新建一个。

      [现有安全组] 选择一个或多个所需的安全组。

      [新安全组] 选择 Create new security group（新建安全组）以前往 Security Groups（安全组）页面。完成之后，返回 Spot Requests（Spot 请求）并刷新列表。

      vii. （可选）要能够通过 Internet 访问实例，请对 Auto-assign IPv4 Public IP (自动分配 IPv4 公有 IP) 选择 Enable (启用)。

      viii. （可选）要使用 IAM 角色启动 Spot 实例，请对 IAM 实例配置文件选择角色。

      ix. (可选) 要运行启动脚本，请将其复制到 User data。

x. （可选）要添加标签，请选择 Create tag（创建标签），输入标签的键和值，然后选择 Create（创建）。对每个标签重复此操作。

对于每个标签，要使用相同标签标记实例和竞价型实例集请求，请确保同时选择了 Instance（实例）和 Fleet（机群）。要仅标记由队列启动的实例，清除 Fleet（队列）。要仅标记竞价型实例集请求，请清除 Instance（实例）。

4. 对于 Additional request details (其他请求详细信息)，执行以下操作：

   a. 查看其他请求详细信息。要进行更改，请清除 Apply defaults (应用默认设置)。

   b. （可选）对于 IAM fleet role (IAM 队列角色)，您可以使用默认角色或选择其他角色。要在更改角色后使用默认角色，请选择 Use default role (使用默认角色)。

   c. （可选）对于 Maximum price (最高价)，您可以使用默认最高价（按需价格），也可以指定您愿意支付的最高价。如果您的最高价低于选定的实例类型的 Spot 价格，则不会启动您的竞价型实例。

   d. (可选) 要创建仅在特定时间段内有效的请求，请编辑请求有效起始时间和请求有效截止时间。

   e. （可选）默认情况下，我们会在竞价型实例集请求过期时终止竞价型实例。要保持这些实例在请求过期后继续运行，请清除 Terminate the instances when the request expires (请求到期时终止实例)。

   f. （可选）要向负载均衡器注册 Spot 实例，请选择 Receive traffic from one or more load balancers (从一个或多个负载均衡器接收流量)，然后选择一个或多个经典负载均衡器或目标组。

5. 对于 Minimum compute unit (最小计算单位)，选择您的应用程序或任务所需的最低硬件规格（vCPU、内存和存储），即 as specs (按规格) 或 as an instance type (按实例类型)。

   - 对于 as specs (按规格)，请指定所需的 vCPUs 数和内存量。
   - 对于 as an instance type (按实例类型)，接受默认实例类型，或者选择 Change instance type (更改实例类型) 以选择其他实例类型。

6. 对于 Target capacity（目标容量），执行以下操作：

   a. 对于 Total target capacity（总目标容量），请指定要请求的单位数。对于单位类型，您可以选择 Instances（实例）、vCPU 或 Memory (MiB)（内存 (MiB)）。要将目标容量指定为 0 以便以后可增加容量，请选择 Maintain target capacity (保持目标容量)。

   b. （可选）对于 Include On-Demand base capacity（包括按需基本容量），请指定要请求的按需单位数。该数字必须小于 Total target capacity (总目标容量)。Amazon EC2 会计算差值，并将差值分配给要请求的 Spot 单位。

      Important

      要指定可选的按需容量，您必须先选择一个启动模板。

   c. (可选) 预设情况下，在竞价型实例中断时，Spot 服务将终止这些实例。要保持目标容量，请选择保持目标容量。这样，您就可以指定 Spot 服务在竞价型实例中断时终止、停止或休眠这些实例。为此，请从中断行为中选择相应的选项。

   d. （可选）要允许竞价型实例集在系统针对实例集中的现有竞价型实例发出实例再平衡通知时启动替换竞价型实例，请选择 Capacity rebalance（容量再平衡），然后选择实例替换策略。如果选择 Launch before terminate（终止前启动），请指定竞价型实例集终止旧实例之前的延迟（以秒为单位）。有关更多信息，请参阅容量再平衡 (p. 888)。

   e. （可选）要控制每小时为队列中所有的 Spot 实例支付的金额，请选择 Set maximum cost for Spot Instances（设置 Spot 实例的最大成本），然后输入您每小时愿意支付的最大总额。当达到最大总额后，即使未达到目标容量，竞价型实例集也会停止启动竞价型实例。有关更多信息，请参阅控制支出 (p. 891)。

7. 对于 Network（网络），执行以下操作：

   a. 对于 Network (网络)，选择现有 VPC 或新建一个。

      [现有 VPC] 选择所需的 VPC。

[新 VPC] 选择 Create new VPC (新建 VPC) 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。

b. （可选）对于 Availability Zone (可用区)，让 Amazon 为 Spot 实例选择可用区，或者指定一个或多个可用区。

如果您在一个可用区中有多个子网，则请从 Subnet (子网) 中选择合适的子网。要添加子网，请选择 Create new subnet (新建子网) 以前往 Amazon VPC 控制台。完成之后，请返回向导并刷新列表。

8. 对于 Instance type requirements（实例类型要求），可以指定实例属性，然后让 Amazon EC2 使用这些属性识别最佳实例类型，也可以指定实例列表。有关更多信息，请参阅竞价型实例集的基于属性的实例类型选择 (p. 874)。

a. 如果选择 Specify instance attributes that match your compute requirements（指定符合计算要求的实例属性），请按如下方式指定实例属性：

i. 对于 vCPU，请输入所需的最小和最大 vCPU 数。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。

ii. 对于 Memory (GiB)（内存 (GiB)），输入所需的最小和最大内存量。要指定没有限制，请选择 No minimum（没有最小值）和/或 No maximum（没有最大值）。

iii. （可选）对于 Additional instance attributes（其它实例属性），您可以选择指定一个或多个属性以更详细地表达计算要求。每个额外属性都会进一步增加对您的请求的限制。您可以省略其它属性；如果省略，则使用默认值。有关每个属性及其默认值的描述，请参阅 Amazon EC2 命令行参考中的 get-spot-placement-scores。

iv. （可选）要查看具有指定属性的实例类型，请展开 Preview matching instance types（预览匹配的实例类型）。要排除在请求中使用的实例类型，请选择实例，然后选择 Exclude selected instance types（排除选定的实例类型）。

b. 如果选择 Manually select instance types（手动选择实例类型），竞价型实例集将提供实例类型默认列表。要选择更多实例类型，请选择 Add instance types（添加实例类型），选择要在请求中使用的实例类型，然后选择 Select（选择）。要删除实例类型，请选择实例类型，然后选择 Delete（删除）。

9. 对于 Allocation strategy（分配策略），选择满足您的需求的策略。有关更多信息，请参阅竞价型实例的分配策略 (p. 872)。

10. 对于 Your fleet request at a glance（您的机群请求概览），查看您的机群配置，并在必要时进行任何调整。

11. （可选）要下载一个启动配置副本以用于 Amazon CLI，请选择 JSON config (JSON 配置)。

12. 选择 Launch。

竞价型实例集请求类型为 `fleet`。执行请求后，系统会添加请求类型 `instance`，此时其状态为 `active` 和 `fulfilled`。

使用 Amazon CLI 创建竞价型实例集

使用 Amazon CLI 创建竞价型实例集请求

- 使用 request-spot-fleet 命令可创建 Spot 队列请求。

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关示例配置文件，请参阅Spot 队列示例配置 (p. 958)。

下面是示例输出：

```
{
```

```
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

标记 Spot 队列

要对您的 Spot 队列请求进行分类和管理，您可使用自定义元数据标记它们。您可以在创建 Spot 队列请求时或之后为其分配标签。您可以使用 Amazon EC2 控制台或命令行工具分配标签。

在标记 Spot 队列请求时，不会自动标记 Spot 队列启动的实例和卷。您需要明确标记 Spot 队列启动的实例和卷。您可以选择仅将标签分配给 Spot 队列请求，仅分配给队列启动的实例，仅分配给附加到队列启动的实例的卷，或者分配给所有这三种内容。

> **Note**
>
> 仅附加到按需型实例的卷支持卷标签。您无法标记附加到竞价型实例的卷。

有关标签的工作原理的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

目录

- 先决条件 (p. 904)
- 标记新的 Spot 队列 (p. 905)
- 标记新的 Spot 队列及其启动的实例和卷 (p. 906)
- 标记现有的 Spot 队列 (p. 908)
- 查看 Spot 队列请求标签 (p. 908)

先决条件

授予用户标记资源的权限。有关更多信息，请参阅示例：标记资源 (p. 1261)。

授予用户标记资源的权限

创建包含以下内容的 IAM policy：

- `ec2:CreateTags` 操作。这将授予用户创建标签的权限。
- `ec2:RequestSpotFleet` 操作。这将授予用户创建竞价型实例集请求的权限。
- 对于 `Resource`，您必须指定 `"*"`。这允许用户标记所有资源类型。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Important**
>
> 对于 `spot-fleet-request` 资源，我们目前不支持资源级权限。如果您指定 `spot-fleet-request` 以作为资源，在您尝试标记队列时，将会发生未经授权异常。以下示例说明如何不 设置策略。

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

标记新的 Spot 队列

使用控制台标记新的 Spot 队列请求

1. 按照使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)过程操作。
2. （可选）要添加标签，请展开 Additional configurations (其他配置)，选择 Add new tag (添加新标签)，然后输入标签的键和值。对每个标签重复此操作。

   对于每个标签，您可以使用相同标签标记 Spot 队列请求和实例。要对两者进行标记，请确保同时选择 Instance tags (实例标签) 和 Fleet tags (队列标签)。要仅标记 Spot 队列请求，请清除 Instance tags (实例标签)。要仅标记由队列启动的实例，请清除 Fleet tags (队列标签)。
3. 填写必填字段以创建 Spot 队列请求，然后选择 Launch (启动)。有关更多信息，请参阅使用已定义的参数创建 Spot 队列请求（控制台）(p. 901)。

使用 Amazon CLI 标记新的竞价型实例集请求

要在创建 Spot 队列请求时标记该请求，请按以下方式配置 Spot 队列请求配置：

- 在 `SpotFleetRequestConfig` 中指定竞价型实例集请求的标签。
- 对于 `ResourceType`，请指定 `spot-fleet-request`。如果指定其他值，队列请求将失败。
- 对于 `Tags`，请指定键值对。您可以指定多个键值对。

在以下示例中，使用两个标签来标记 Spot 队列请求：键=环境，值=生产；键=成本中心，值=123。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large"
            }
        ],
```

```
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

标记新的 Spot 队列及其启动的实例和卷

标记新的竞价型实例集请求及其使用 Amazon CLI 启动的实例和卷

要在创建 Spot 队列请求时标记该请求，并在队列启动实例和卷时标记它们，请按以下方式配置 Spot 队列请求配置：

Spot 队列请求标签：

- 在 SpotFleetRequestConfig 中指定竞价型实例集请求的标签。
- 对于 ResourceType，请指定 spot-fleet-request。如果指定其他值，队列请求将失败。
- 对于 Tags，请指定键值对。您可以指定多个键值对。

实例标签：

- 为 LaunchSpecifications 中的实例指定标签。
- 对于 ResourceType，请指定 instance。如果指定其他值，队列请求将失败。
- 对于 Tags，请指定键值对。您可以指定多个键值对。

  或者，您可以在 Spot 队列请求中引用的启动模板 (p. 590)中为实例指定标签。

卷标签：

- 在 Spot 队列请求中引用的启动模板 (p. 590)中为卷指定标签。不支持 LaunchSpecifications 中的卷标记。

在以下示例中，使用两个标签来标记 Spot 队列请求：键=环境，值=生产；键=成本中心，值=123。由队列启动的实例使用一个标签（与 Spot 队列请求的其中一个标签相同）进行标记：键=成本中心，值=123。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
```

```
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

使用 Amazon CLI 标记由竞价型实例集启动的实例

要在队列启动实例时标记实例，您可以在 Spot 队列请求中引用的启动模板 (p. 590)中指定标记，也可以在 Spot 队列请求配置中指定标记，如下所示：

- 为 LaunchSpecifications 中的实例指定标签。
- 对于 ResourceType，请指定 instance。如果指定其他值，队列请求将失败。
- 对于 Tags，请指定键值对。您可以指定多个键值对。

在以下示例中，由队列启动的实例使用一个标签进行标记：键=成本中心，值=123。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchSpecifications": [
            {
```

```
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

使用 Amazon CLI 标记挂载至由竞价型实例集启动的按需型实例的卷

要在队列创建卷时标记这些卷，您必须在 Spot 队列请求中引用的启动模板 (p. 590)中指定标签。

Note

仅附加到按需型实例的卷支持卷标签。您无法标记附加到竞价型实例的卷。
不支持 LaunchSpecifications 中的卷标记。

标记现有的 Spot 队列

使用控制台标记现有 Spot 队列请求

创建 Spot 队列请求后，您可以使用控制台向队列请求添加标签。

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 选择 Spot 队列请求。
3. 选择 Tags (标签) 选项卡，然后选择 Create Tag (创建标签)。

使用 Amazon CLI 标记现有竞价型实例集请求

可以使用 create-tags 命令标记现有的资源。在以下示例中，使用以下标签标记现有 Spot 队列请求：键=目的，值=测试。

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

查看 Spot 队列请求标签

使用控制台查看 Spot 队列请求标签

1. 在 https://console.aws.amazon.com/ec2spot 处打开 Spot 控制台。
2. 选择您的 Spot 队列请求并选择 Tags (标签) 选项卡。

描述 Spot 队列请求标记

使用 describe-tags 命令可查看指定资源的标签。在以下示例中，您将描述指定 Spot 队列请求的标签。

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

您还可以通过描述 Spot 队列请求来查看 Spot 队列请求的标签。

使用 describe-spot-fleet-requests 命令可查看指定的 Spot 队列请求的配置，其中包括为队列请求指定的任何标签。

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
```

```
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

描述竞价型实例集

在最高价超过 Spot 价格并具有可用的容量时，竞价型实例集会启动竞价型实例。竞价型实例 将一直运行，直到这些实例中断，或者您终止这些实例。

描述竞价型实例集（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择 Spot 队列请求。要查看配置详细信息，请选择 Description (描述)。
4. 要列出 Spot 队列的 Spot 实例，请选择 Instances (实例)。
5. 要查看 Spot 队列的历史记录，请选择 History (历史记录)。

描述竞价型实例集 (Amazon CLI)

使用 describe-spot-fleet-requests 命令可描述 Spot 队列请求。

```
aws ec2 describe-spot-fleet-requests
```

使用 describe-spot-fleet-instances 命令可描述指定 Spot 队列的 Spot 实例。

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

使用 describe-spot-fleet-request-history 命令可描述指定 Spot 队列请求的历史记录。

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

修改 Spot 队列请求

您可以修改活动的 Spot 队列请求以完成以下任务：

- 提高目标容量和按需部分
- 降低目标容量和按需部分

> **Note**
>
> 您无法修改一次性 Spot 队列请求。您只能在创建 Spot 队列请求时选择了 Maintain target capacity (保持目标容量) 的情况下修改 Spot 队列请求。

当您增加目标容量时，竞价型实例集会启动其他竞价型实例。当您提高按需部分时，竞价型实例集会启动其他按需型实例。

当您增加目标容量时，竞价型实例集会根据其竞价型实例集请求的分配策略启动其他竞价型实例。如果分配策略为 `lowestPrice`，竞价型实例集将从竞价型实例集请求中价格最低的 Spot 容量池启动实例。如果分配策略为 `diversified`，竞价型实例集将在竞价型实例集请求中的池间分配实例。

在减少目标容量时，Spot 队列将取消超过新目标容量的任何打开的请求。您可以请求竞价型实例集终止竞价型实例，直到队列的大小达到新目标容量。如果分配策略为 `lowestPrice`，则竞价型实例集将终止每单位价格最高的实例。如果分配策略为 `diversified`，则竞价型实例集将在池间终止实例。或者，您可以请求竞价型实例集保持队列当前的队列大小，而不替换已中断的任何竞价型实例或者您手动终止的任何竞价型实例。

当竞价型实例集因目标容量下降而终止某个实例时，该实例将收到一条竞价型实例中断通知。

修改 Spot 队列请求（控制台）

1. 在 https://console.aws.amazon.com/ec2spot/home/fleet 处打开 Spot 控制台。
2. 选择 Spot 队列请求。
3. 依次选择 Actions (操作) 和 Modify target capacity (修改目标容量)。
4. 在 Modify target capacity 中，执行以下操作：
   a. 输入新的目标容量和按需部分。
   b. （可选）如果您要减少目标容量，但是要使队列保持其当前大小，请清除 Terminate instances (终止实例)。
   c. 选择 Submit（提交）。

使用 Amazon CLI 修改竞价型实例集请求

使用 modify-spot-fleet-request 命令可更新指定 Spot 队列请求的目标容量。

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

可以按如下所示修改前面的命令，以减少指定竞价型实例集的目标容量而不因此终止任何竞价型实例。

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

取消 Spot 队列请求

如果您不再需要竞价型实例集，可以取消竞价型实例集请求。取消实例集请求后，与实例集关联的所有竞价型实例请求也将取消，从而不会启动任何新的竞价型实例。

取消竞价型实例集请求后，您还必须指定是否要终止其所有实例。包括按需型实例和竞价型实例。

如果您指定必须在取消实例集请求后终止实例，实例集请求会进入 `cancelled_terminating` 状态。否则，实例集请求将进入 `cancelled_running` 状态，并且实例将继续运行直至遇到中断或您手动将其终止。

取消 Spot 队列请求（控制台）

1. 在 https://console.aws.amazon.com/ec2spot/home/fleet 处打开 Spot 控制台。
2. 选择 Spot 队列请求。
3. 依次选择操作和取消请求。
4. 在取消竞价型实例请求对话框中，执行以下操作：

a. 要取消竞价型实例集请求同时终止关联实例，请将终止实例复选框保持为选中状态。要取消竞价型实例集请求而不终止关联实例，请清除终止实例复选框。
b. 选择 Confirm（确认）。

使用 Amazon CLI 取消竞价型实例集请求并终止其实例

使用 cancel-spot-fleet-requests 命令可以取消指定的竞价型实例集请求并终止其按需型实例和竞价型实例。

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

输出示例

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

使用 Amazon CLI 取消竞价型实例集请求而不终止其实例

您可以使用 `--no-terminate-instances` 参数修改上一个命令，以取消指定的竞价型实例集而不终止其按需型实例和竞价型实例。

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

输出示例

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

Spot 队列的 CloudWatch 指标

Amazon EC2 提供可用于监控 Spot 队列的 Amazon CloudWatch 指标。

> **Important**
>
> 为确保准确性，我们建议您在使用这些指标时启用详细监控。有关更多信息，请参阅对实例启用或禁用详细监控 (p. 1001)。

有关 Amazon EC2 提供的 CloudWatch 指标的更多信息，请参阅 使用 CloudWatch 监控您的实例 (p. 1000)。

Spot 队列指标

AWS/EC2Spot 命名空间包含以下指标以及针对队列中的 Spot 实例 的 CloudWatch 指标。有关更多信息，请参阅实例指标 (p. 1003)。

指标	描述
AvailableInstancePoolsCount	Spot 队列请求中指定的 Spot 容量池。 单位：计数
BidsSubmittedForCapacity	Amazon EC2 已提交 Spot 队列请求的容量。 单位：计数
EligibleInstancePoolCount	在 Amazon EC2 可以完成请求的 Spot 队列请求中指定的 Spot 容量池。在您愿意为竞价型实例支付的最高价格低于 Spot 价格或 Spot 价格高于按需型实例价格的池中，Amazon EC2 不会完成请求。 单位：计数
FulfilledCapacity	Amazon EC2 已执行的容量。 单位：计数
MaxPercentCapacityAllocation	竞价型实例集请求中指定的所有竞价型实例集池间的 PercentCapacityAllocation 最大值。 单位：百分比
PendingCapacity	TargetCapacity 与 FulfilledCapacity 之间的区别。 单位：计数
PercentCapacityAllocation	针对所指定维度的 Spot 容量池分配的容量。要获取所有 Spot 容量池中记录的最大值，请使用 MaxPercentCapacityAllocation。 单位：百分比
TargetCapacity	Spot 队列请求的目标容量。 单位：计数
TerminatingCapacity	因预置容量大于目标容量而终止的容量。 单位：计数

如果指标的度量单位是 Count，则最有用的统计信息是 Average。

Spot 队列维度

要筛选您的 Spot 队列的数据，请使用以下维度。

Dimensions	描述
AvailabilityZone	按照可用区筛选数据。

Dimensions	描述
FleetRequestId	按照 Spot 队列请求筛选数据。
InstanceType	按实例类型筛选数据。

查看 Spot 队列的 CloudWatch 指标

您可以使用 Amazon CloudWatch 控制台查看 Spot 队列的 CloudWatch 指标。这些指标显示为监控图表。如果 Spot 队列处于活动状态，这些图表会显示数据点。

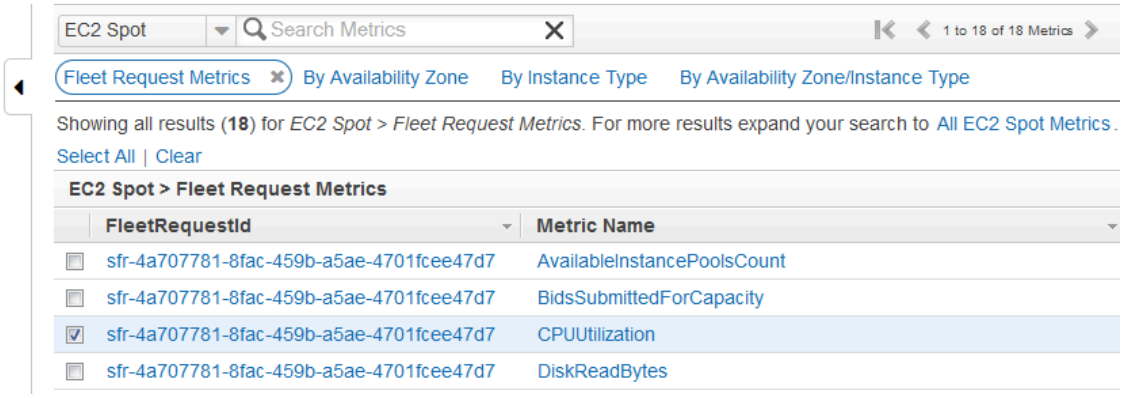
指标首先按命名空间进行分组，然后按各命名空间内的各种维度组合进行分组。例如，您可以按 Spot 队列请求 ID、实例类型或可用区查看所有 Spot 队列指标或 Spot 队列指标组。

查看 Spot 队列指标

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 Spot 命名空间。

   Note

   如果未显示 EC2 Spot 命名空间，这种情况有两个原因。您尚未使用的竞价型实例集 – 只有正在使用的 Amazon 服务才会将指标发送到 Amazon CloudWatch。或者，如果过去两周没有使用过 Spot 队列，则不会显示命名空间。
4. (可选) 要按维度筛选指标，请选择下列选项之一：
   - Fleet Request Metrics (队列请求指标) – 按 Spot 队列请求分组
   - By Availability Zone (按可用区) – 按 Spot 队列请求和可用区分组
   - By Instance Type (按实例类型) – 按 Spot 队列请求和实例类型分组
   - By Availability Zone/Instance Type (按可用区/实例类型) – 按 Spot 队列请求、可用区和实例类型分组
5. 要查看指标的数据，请选中指标旁边的复选框。



Spot 队列的自动扩展

自动扩展是根据需求自动增加或减少 Spot 队列目标容量的能力。Spot 队列能够根据一个或多个扩展策略，在您选择的范围内启动实例 (扩展) 或终止实例 (缩减)。

Spot 队列支持以下类型的自动扩展：

- 目标跟踪扩展 (p. 916) – 根据特定指标的目标值，增加或减少队列的当前容量。这与恒温器保持家里温度的方式类似—您选择一个温度，恒温器将完成所有其他工作。
- 步进扩展 (p. 917) – 根据一组扩展调整，增加或减小队列的当前容量，这些调整称为步进调整，将根据警报严重程度发生变化。
- 计划扩展 (p. 918) – 根据日期和时间增加或减少队列的当前容量。

如果使用实例权重 (p. 891)，请记住，Spot 队列可以根据需要超出目标容量。执行容量可以是浮点数，但目标容量必须是整数，因此 Spot 队列向上舍入到下一个整数。在您查看触发警报时扩展策略的结果时，必须考虑这些行为。例如，假设目标容量为 30，执行容量为 30.1，扩展策略减 1。当触发报警时，自动扩展过程将 30.1 减 1 得到 29.1，然后将其向上取整为 30，因此不执行扩展操作。再如，假设您选择的实例权重为 2、4 和 8，目标容量为 10，但没有权重 2 实例可用，因此为执行容量为 12 的 Spot 队列预置权重为 4 和 8 的实例。如果扩展策略将目标容量减少 20% 并触发警报，则自动扩展过程将 12 减 12*0.2 得到 9.6，然后将其向上取整为 10，因此不执行扩展操作。

您为 Spot 队列创建的扩展策略支持冷却时间。这是扩展活动完成后上一个与触发相关的扩展活动可影响将来扩展事件的秒数。对于扩大策略，虽然冷却时间有效，但启动冷却的上一个扩大事件所添加的容量将计算为下一次扩大所需容量的一部分。旨在持续 (但不过度) 扩大。对于缩小策略，冷却时间用于阻止后续缩小请求，直至到期。旨在谨慎地缩小以保护您的应用程序的可用性。但是，如果在缩小后，另一个警报在冷却时间内触发了扩大策略，自动扩展将立即扩大您的可扩展目标。

建议将随实例指标扩展的频率设置为 1 分钟，这可确保更快地响应使用率变化。如果将随指标扩展的频率设置为 5 分钟，可能会导致响应时间变慢，并且可能导致系统依据陈旧的指标数据进行扩展。要每隔 1 分钟向 CloudWatch 发送一次实例的指标数据，您必须专门启用详细监控。有关更多信息，请参阅对实例启用或禁用详细监控 (p. 1001)和使用已定义的参数创建 Spot 队列请求（控制台） (p. 901)。

有关为 Spot 队列配置扩展的更多信息，请参阅以下资源：

- Amazon CLI Command Reference 的 application-autoscaling 部分
- Application Auto Scaling API 参考
- Application Auto Scaling 用户指南

Spot 队列自动扩展所需的 IAM 权限

通过结合使用 Amazon EC2、Amazon CloudWatch 和 Application Auto Scaling API 可实现 Spot 队列的自动扩展。通过 Amazon EC2 可创建 Spot 队列请求，通过 CloudWatch 可创建警报，通过 Application Auto Scaling 可创建扩展策略。

除竞价型实例集的 IAM 权限 (p. 895)和 Amazon EC2 外，访问实例集扩展设置的用户必须具有使用支持动态扩缩的服务的适当权限。用户必须具有使用以下示例策略中的操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
```

```
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

您还可以创建自己的 IAM 策略，从而使 Application Auto Scaling API 调用获得更精细的权限。有关更多信息，请参阅 Application Auto Scaling 用户指南中的身份验证和访问控制。

Application Auto Scaling 服务还需要描述 Spot 队列和 CloudWatch 警报的权限，以及代表您修改 Spot 队列目标容量的权限。如果您为竞价型实例集启用自动扩展功能，它将创建一个名为 `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest` 的服务相关角色。此服务相关角色授予 Application Auto Scaling 权限，以描述策略警报、监控队列的当前容量以及修改队列的容量。Application Auto Scaling 的原托管竞价型实例集角色为 `aws-ec2-spot-fleet-autoscale-role`，但今后已不再需要。此服务相关角色是 Application Auto Scaling 的默认角色。有关更多信息，请参阅 Application Auto Scaling 用户指南 中的服务相关角色权限。

使用目标跟踪策略扩展 Spot 队列

在使用目标跟踪扩展策略时，您可以选择一个指标并设置一个目标值。Spot 队列将创建和管理触发扩展策略的 CloudWatch 警报，并根据指标和目标值计算扩展调整。扩展策略根据需要增加或减少容量，将指标保持在指定的目标值或接近指定的目标值。除了将指标保持在目标值附近以外，目标跟踪扩展策略还会根据由于负载模式波动而造成的指标波动进行调节，并最大限度减少队列容量发生快速波动的情况。

您可以为 Spot 队列创建多个目标跟踪扩展策略，但前提是它们分别使用不同的指标。队列根据提供最大队列容量的策略进行扩展。这样，您就可以涵盖多种方案，并确保始终具有足够的容量以处理您的应用程序工作负载。

为了确保应用程序可用性，队列针对指标尽快按比例向外扩展，但会逐渐向内扩展。

当竞价型实例集因目标容量下降而终止某个实例时，该实例将收到一条竞价型实例中断通知。

请勿编辑或删除 Spot 队列为目标跟踪扩展策略管理的 CloudWatch 警报。在删除目标跟踪扩展策略时，Spot 队列将自动删除警报。

限制

竞价型实例集请求必须使用 `maintain` 作为请求类型。`request` 类型的请求不支持自动扩缩。

配置目标跟踪策略（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求，然后选择 Auto Scaling。
4. 如果未配置自动扩展，请选择 Configure。
5. 使用 Scale capacity between 设置队列的最小和最大容量。队列的自动扩展操作不会超出最小或最大容量范围。
6. 对于 Policy name（策略名称），输入此策略的名称。
7. 选择一个目标指标。
8. 为该指标键入一个目标值。
9. (可选) 设置冷却时间以修改默认冷却时间。

10. (可选) 选择禁用向内扩展以禁止根据当前配置创建向内扩展策略。您可以使用不同的配置创建一个向内扩展策略。
11. 选择 Save。

使用 Amazon CLI 配置目标跟踪策略

1. 使用 register-scalable-target 命令将 Spot 队列请求注册为可扩展目标。
2. 使用 put-scaling-policy 命令创建扩展策略。

使用步进扩展策略扩展 Spot 队列

在使用步进扩展策略时，您可以指定 CloudWatch 警报以触发扩展过程。例如，如果您希望在 CPU 利用率达到特定水平时扩展，可以使用 Amazon EC2 提供的 `CPUUtilization` 指标创建警报。

在创建步进扩展策略时，您必须指定以下扩展调整类型之一：

- Add (增加) – 按指定的容量单位数量或当前容量的指定百分比来增加队列的目标容量。
- Remove (移走) – 按指定的容量单位数量或当前容量的指定百分比来缩减队列的目标容量。
- Set to (设定为) – 将队列的目标容量设为指定的容量单位数量。

当触发警报时，自动扩展过程使用执行容量和扩展策略计算新的目标容量，然后相应地更新目标容量。例如，假设目标容量和执行容量为 10，扩展策略加 1。触发警报时，自动扩展过程为 10 增加 1 得到 11，因此 Spot 队列将启动 1 个实例。

当竞价型实例集因目标容量下降而终止某个实例时，该实例将收到一条竞价型实例中断通知。

限制

竞价型实例集请求必须使用 `maintain` 作为请求类型。`request` 类型的请求或 Spot 型限制不支持自动扩展。

先决条件

- 考虑哪些 CloudWatch 指标对您的应用程序比较重要。您可以根据 Amazon 提供的指标或您自己的自定义指标来创建 CloudWatch 告警。
- 如果您打算在扩展策略中使用 Amazon 指标，请为其启用 CloudWatch 指标集合（如果提供这些指标的服务默认未启用它的话）。

创建 CloudWatch 警报

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Alarms (警报)。
3. 选择 Create Alarm (创建警报)。
4. 在 Specify metric and conditions (指定指标和条件) 页面上，选择 Select metric (选择指标)。
5. 选择 EC2 Spot、Fleet Request Metrics（队列请求指标），选择一个指标（例如 TargetCapacity），然后选择 Select metric（选择指标）。

   这将显示 Specify metric and conditions (指定指标和条件) 页面，其中显示一个图表以及有关所选指标的其他信息。
6. 在 Period (周期) 下，选择警报的评估周期，例如 1 分钟。评估警报时，每个周期都聚合到一个数据点。

   Note

   周期越短，创建的警报越敏感。

7. 在 Conditions (条件) 下，通过定义阈值条件来定义警报。例如，您可以定义一个阈值，在指标值大于或等于 80% 时触发警报。
8. 在 Additional configuration (附加配置) 下，对于 Datapoints to alarm (触发警报的数据点数)，请指定必须有多少个数据点（评估期）处于 ALARM 状态才会触发警报，例如，1 个或 2 个（共 3 个）评估期。这将创建一个警报，如果多个连续周期超出阈值，该警报将进入 ALARM（警报）状态。有关更多信息，请参阅Amazon CloudWatch 用户指南中的评估警报。
9. 对于 Missing data treatment (缺失数据处理)，选择某个选项（或保留 Treat missing data as missing (将缺失的数据视为缺失) 的默认值）。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的配置 CloudWatch 警报处理缺少数据的方式。
10. 选择 Next（下一步）。
11. （可选）要接收扩展事件的通知，在 Notification (通知) 中，您可以选择或创建要用于接收通知的 Amazon SNS 主题。当然，您也可以立即删除通知，之后按需添加通知。
12. 选择 Next（下一步）。
13. 在 Add a description (添加描述) 下，输入警报的名称和描述，然后选择 Next (下一步)。
14. 选择 Create Alarm (创建警报)。

为您的 Spot 队列配置分步扩展策略（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求，然后选择 Auto Scaling。
4. 如果未配置自动扩展，请选择 Configure。
5. 使用 Scale capacity between 设置队列的最小和最大容量。队列的自动扩展操作不会超出最小或最大容量范围。
6. 最初，Scaling policies 包含名为 ScaleUp 和 ScaleDown 的策略。您可以完善这些策略，或选择 Remove policy 来删除它们。您也可以选择 Add policy (添加策略)。
7. 要定义策略，请执行以下操作：
   a. 对于 Policy name（策略名称），输入此策略的名称。
   b. 对于 Policy trigger (策略触发器)，可以选择现有的警报，或选择 Create new alarm (新建警报) 来打开 Amazon CloudWatch 控制台并创建警报。
   c. 对于 Modify capacity，请选择扩展调整类型、数字及单位。
   d. （可选）要执行步进扩展，请选择 Define steps。默认情况下，添加策略的下限为负无穷，上限为警报阈值。默认情况下，删除策略的下限为警报阈值，上限为正无穷。要添加其他步骤，请选择 Add step。
   e. （可选）要修改冷却时间的默认值，请从 Cooldown period (冷却时间) 中选择一个数字。
8. 选择 Save。

使用 Amazon CLI 为竞价型实例集配置分步扩展策略

1. 使用 register-scalable-target 命令将 Spot 队列请求注册为可扩展目标。
2. 使用 put-scaling-policy 命令创建扩展策略。
3. 使用 put-metric-alarm 命令创建触发扩展策略的警报。

使用计划扩展功能扩展 Spot 队列

按计划扩展使您可以按照可预测的需求变化来扩展应用程序。要使用计划扩展，请创建指示 Spot 队列在特定时间执行扩展活动的计划操作。创建计划操作时，您可以指定现有的 Spot 扩展、执行扩展活动的时间、最小容量和最大容量。您可以创建仅扩展一次或按重复计划扩展的计划操作。

您只能为已存在的 Spot 队列 创建计划操作。您不能在创建 Spot 队列的同时创建计划操作。

限制

竞价型实例集请求必须使用 `maintain` 作为请求类型。`request` 类型的请求或 Spot 型限制不支持自动扩展。

创建一次性计划操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求并选择屏幕底部附近的 Scheduled Scaling (计划扩展) 选项卡。
4. 选择 Create Scheduled Action (创建计划扩展)。
5. 对于 Name (名称)，请指定计划操作的名称。
6. 对于 Minimum capacity (最小容量) 和/或 Maximum capacity (最大容量)，输入所需的值。
7. 对于 Recurrence (重复次数)，选择 Once (一次)。
8. （可选）对于 Start time (开始时间) 和/或 End time (结束时间)，选择所需的日期和时间。
9. 选择 Submit（提交）。

按照重复计划扩展

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求并选择屏幕底部附近的 Scheduled Scaling (计划扩展) 选项卡。
4. 对于 Recurrence（重复次数），选择预定义计划之一（例如 Every day（每天）），或者选择 Custom（自定义）并输入 cron 表达式。有关计划扩展所支持的 cron 表达式的更多信息，请参阅 Amazon CloudWatch Events 用户指南 中的 cron 表达式。
5. （可选）对于 Start time (开始时间) 和/或 End time (结束时间)，选择所需的日期和时间。
6. 选择 Submit（提交）。

编辑计划操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求并选择屏幕底部附近的 Scheduled Scaling (计划扩展) 选项卡。
4. 选择所需的计划操作，然后依次选择 Actions (操作) 和 Edit (编辑)。
5. 进行所需的更改，然后选择 Submit (提交)。

删除计划操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Spot Requests。
3. 选择您的 Spot 队列请求并选择屏幕底部附近的 Scheduled Scaling (计划扩展) 选项卡。
4. 选择所需的计划操作，然后依次选择 Actions (操作) 和 Delete (删除)。
5. 当系统提示进行确认时，选择 Delete (删除)。

使用 Amazon CLI 管理计划扩展

使用以下命令：

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

使用 Amazon EventBridge 监控队列事件

当 EC2 或 Spot 队列的状态发生变化时，队列将发出通知。该通知作为发送到 Amazon EventBridge（以前称为 Amazon CloudWatch Events）的事件提供。尽最大努力发出事件。

使用 Amazon EventBridge，您可以创建触发编程操作以响应事件的规则。例如，您可以创建两个 EventBridge 规则，一个在队列状态变化时触发，另一个在队列中的实例终止时触发。您可以配置第一条规则，这样如果队列状态发生变化，该规则将调用 SNS 主题以向您发送电子邮件通知。您可以配置第二条规则，这样如果实例被终止，该规则将调用 Lambda 函数以启动新实例。

主题

- EC2 队列 事件类型 (p. 920)
- Spot 队列事件类型 (p. 924)
- 创建 Amazon EventBridge 规则 (p. 929)

EC2 队列 事件类型

> Note
>
> 只有类型 `maintain` 和 `request` 的队列才能触发事件。类型 `instant` 的队列不会触发事件，因为它们提交同步一次性请求，并且队列的状态立即可在响应中获知。

EC2 队列 事件类型有五种。对于每种事件类型，都有几个子类型。

事件以 JSON 格式发送到 EventBridge。事件中的下列字段构成规则中定义并触发操作的事件模式：

`"source": "aws.ec2fleet"`

识别来自 EC2 队列 的事件。

`"detail-type": "EC2 Fleet State Change"`

识别事件类型。

`"detail": { "sub-type": "submitted" }`

识别事件子类型。

事件类型

- EC2 队列状态变化 (p. 920)
- EC2 实例集竞价型实例请求更改 (p. 921)
- EC2 队列实例更改 (p. 922)
- EC2 队列信息 (p. 923)
- EC2 队列错误 (p. 924)

EC2 队列状态变化

当 EC2 队列 状态变化时，EC2 队列 会将 `EC2 Fleet State Change` 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

`sub-type` 可使用的值为：

`active`

EC2 队列 请求已验证，并且 Amazon EC2 正在尝试使正在运行的实例保持目标数量。

`deleted`

EC2 队列 请求已删除，没有正在运行的实例。EC2 队列 将在其实例终止两天后被删除。

`deleted_running`

EC2 队列 请求已删除，且不启动其他实例。现有实例将继续运行，直至被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。

`deleted_terminating`

EC2 队列 请求已删除，正在终止其实例。请求会保持此状态，直到所有实例都已终止。

`expired`

EC2 队列 请求已过期。如果请求使用 `TerminateInstancesWithExpiration` 集创建，则随后的 `terminated` 事件指示实例已终止。

`modify_in_progress`

正在修改 EC2 队列 请求。请求将保持该状态，直到完全处理修改。

`modify_succeeded`

EC2 队列 请求已修改。

`submitted`

EC2 队列 正在接受评估，并且 Amazon EC2 正准备启动目标数量的实例。

`progress`

该 EC2 队列 请求正在执行过程中。

EC2 实例集竞价型实例请求更改

当队列中的 Spot 实例请求状态变化时，EC2 队列 会将 `EC2 Fleet Spot Instance Request Change` 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

sub-type 可使用的值为：

active

竞价型实例请求已执行并有关联的竞价型实例。

cancelled

您取消了竞价型实例请求，或竞价型实例请求已过期。

disabled

您停止了竞价型实例。

submitted

已提交竞价型实例请求。

EC2 队列实例更改

当队列中的实例状态变化时，EC2 队列 会将 EC2 Fleet Instance Change 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
```

```
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

sub-type 可使用的值为：

launched

启动了一个新实例。

terminated

实例已终止。

termination_notified

当 Amazon EC2 在缩减期间终止竞价型实例时，机群的目标容量被缩减，例如，从目标容量 4 减至目标容量 3 时，会发送实例终止通知。

EC2 队列信息

在履行过程中出错时，EC2 队列 会将 EC2 Fleet Information 事件发送到 Amazon EventBridge。信息事件不会阻止队列尝试实现其目标容量。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

sub-type 可使用的值为：

fleetProgressHalted

每个启动规范中的价格无效，因为它低于 Spot 价格（所有启动规范都已生成 launchSpecUnusable 事件）。如果 Spot 价格发生变化，启动规范可能会变为有效。

launchSpecTemporarilyBlacklisted

配置无效，多次启动实例的尝试都已失败。有关更多信息，请参阅事件的描述。

launchSpecUnusable

启动规范中的价格无效，因为它低于 Spot 价格。

`registerWithLoadBalancersFailed`

尝试向负载均衡器注册实例失败。有关更多信息，请参阅事件的描述。

EC2 队列错误

在履行过程中出错时，EC2 队列 会将 `EC2 Fleet Error` 事件发送到 Amazon EventBridge。错误事件阻止了队列尝试实现其目标容量。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not supported
 for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

`sub-type` 可使用的值为：

`iamFleetRoleInvalid`

EC2 机群没有启动或终止实例所需的权限。

`allLaunchSpecsTemporarilyBlacklisted`

所有配置均无效，多次启动实例的尝试已失败。有关更多信息，请参阅事件的描述。

`spotInstanceCountLimitExceeded`

您已达到可启动的竞价型实例的数量限制。

`spotFleetRequestConfigurationInvalid`

该配置无效。有关更多信息，请参阅事件的描述。

Spot 队列事件类型

Spot 队列事件类型有五种。对于每种事件类型，都有几个子类型。

事件以 JSON 格式发送到 EventBridge。事件中的下列字段构成规则中定义并触发操作的事件模式：

`"source": "aws.ec2spotfleet"`

识别来自 Spot 队列的事件。

`"detail-type": "EC2 Spot Fleet State Change"`

识别事件类型。

`"detail": { "sub-type": "submitted" }`

识别事件子类型。

事件类型

- EC2 Spot 队列状态变化 (p. 925)
- EC2竞价型实例集竞价型实例请求更改 (p. 926)
- EC2 Spot 队列实例更改 (p. 926)
- EC2 Spot 队列信息 (p. 927)
- EC2 Spot 队列错误 (p. 928)

EC2 Spot 队列状态变化

当 Spot 队列状态变化时，Spot 队列会将 `EC2 Spot Fleet State Change` 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
    "detail": {
        "sub-type": "submitted"
    }
}
```

`sub-type` 可使用的值为：

`active`

已验证竞价型实例集请求，并且 Amazon EC2 正在尝试维护目标数量的正在运行的实例。

`cancelled`

竞价型实例集请求已取消，没有正在运行的实例。Spot 队列将在其实例终止两天后被删除。

`cancelled_running`

竞价型实例集请求已取消，且不启动其他实例。现有实例将继续运行，直至被中断或终止。请求会保持此状态，直到所有实例都已中断或终止。

`cancelled_terminating`

竞价型实例集请求已取消，正在终止其实例。请求会保持此状态，直到所有实例都已终止。

`expired`

Spot 队列请求已过期。如果请求使用 `TerminateInstancesWithExpiration` 集创建，则随后的 `terminated` 事件指示实例已终止。

`modify_in_progress`

Spot 队列请求正在修改中。请求将保持该状态，直到完全处理修改。

`modify_succeeded`

Spot 队列请求已修改。

`submitted`

正在评估 Spot 队列请求，并且 Amazon EC2 正准备启动目标数量的实例。

`progress`

Spot 队列请求正在执行过程中。

EC2竞价型实例集竞价型实例请求更改

当队列中的 Spot 实例请求状态变化时，Spot 队列会将 `EC2 Spot Fleet Spot Instance Request Change` 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

`sub-type` 可使用的值为：

`active`

竞价型实例请求已执行并有关联的竞价型实例。

`cancelled`

您取消了竞价型实例请求，或竞价型实例请求已过期。

`disabled`

您停止了竞价型实例。

`submitted`

已提交竞价型实例请求。

EC2 Spot 队列实例更改

当队列中的实例状态变化时，Spot 队列会将 `EC2 Spot Fleet Instance Change` 事件发送到 Amazon EventBridge。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":\"ami-032930428bf1abbff
\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

sub-type 可使用的值为：

launched

启动了一个新实例。

terminated

实例已终止。

termination_notified

当 Amazon EC2 在缩减期间终止竞价型实例时，机群的目标容量被缩减，例如，从目标容量 4 减至目标容量 3 时，会发送实例终止通知。

EC2 Spot 队列信息

在履行过程中出错时，Spot 队列会将 EC2 Spot Fleet Information 事件发送到 Amazon EventBridge。信息事件不会阻止队列尝试实现其目标容量。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot bid
 price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
```

```
}
```

sub-type 可使用的值为：

fleetProgressHalted

每个启动规范中的价格无效，因为它低于 Spot 价格（所有启动规范都已生成 launchSpecUnusable 事件）。如果 Spot 价格发生变化，启动规范可能会变为有效。

launchSpecTemporarilyBlacklisted

配置无效，多次启动实例的尝试都已失败。有关更多信息，请参阅事件的描述。

launchSpecUnusable

启动规范中的价格无效，因为它低于 Spot 价格。

registerWithLoadBalancersFailed

尝试向负载均衡器注册实例失败。有关更多信息，请参阅事件的描述。

EC2 Spot 队列错误

在履行过程中出错时，Spot 队列会将 EC2 Spot Fleet Error 事件发送到 Amazon EventBridge。错误事件阻止了队列尝试实现其目标容量。

以下是此事件的示例数据。

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface with
 DeviceIndex 0. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

sub-type 可使用的值为：

iamFleetRoleInvalid

竞价型实例集不具有启动或终止实例所需的权限。

allLaunchSpecsTemporarilyBlacklisted

所有配置均无效，多次启动实例的尝试已失败。有关更多信息，请参阅事件的描述。

spotInstanceCountLimitExceeded

您已达到可启动的竞价型实例的数量限制。

`spotFleetRequestConfigurationInvalid`

该配置无效。有关更多信息，请参阅事件的描述。

创建 Amazon EventBridge 规则

当 EC2 或 Spot 队列发出状态变更通知时，该通知的事件将发送到 Amazon EventBridge。如果 EventBridge 检测到与规则中定义的模式匹配的事件模式，则 EventBridge 调用规则中指定的一个或多个目标。

当事件模式与规则匹配时，您可以编写 EventBridge 规则并自动执行要采取的操作。

主题

- 使用 Amazon EventBridge 规则监控 EC2 队列事件 (p. 929)
- 创建 Amazon EventBridge 规则以监控 Spot 队列事件 (p. 932)

使用 Amazon EventBridge 规则监控 EC2 队列事件

为 EC2 队列发出状态变更通知时，该通知的事件将以 JSON 文件的形式发送到 Amazon EventBridge。当事件模式与规则匹配时，您可以编写 EventBridge 规则并自动执行要采取的操作。如果 EventBridge 检测到与规则中定义的模式匹配的事件模式，则 EventBridge 调用规则中指定的一个或多个目标。

下列字段构成规则中定义的事件模式：

`"source": "aws.ec2fleet"`

识别来自 EC2 队列 的事件。

`"detail-type": "EC2 Fleet State Change"`

识别事件类型。

`"detail": { "sub-type": "submitted" }`

识别事件子类型。

有关 EC2 队列事件和示例事件数据的列表，请参阅the section called “EC2 队列 事件类型” (p. 920)。

示例

- 创建 EventBridge 规则以发送通知 (p. 929)
- 创建 EventBridge 规则以触发 Lambda 函数 (p. 931)

创建 EventBridge 规则以发送通知

下面的示例可创建 EventBridge 规则，以便在 Amazon EC2 每次发出 EC2 队列状态变化通知时发送电子邮件、短信或移动推送通知。本示例中的信号作为 `EC2 Fleet State Change` 事件发出，这将触发规则定义的操作。

创建 EventBridge 规则之前，您必须为电子邮件、短信或移动推送通知创建 Amazon SNS 主题。

创建 EventBridge 规则以在 EC2 队列 状态变化时发送通知

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。

3. 对于定义规则详细信息，请执行以下操作：

   a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

      规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

   b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。

   c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。

   d. 选择 Next（下一步）。

4. 对于 Build event pattern（构建事件模式），执行以下操作：

   a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。

   b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 `EC2 Fleet Instance Change` 事件。

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"]
      }
      ```

      要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

      i. 要使用模板创建事件模式，请执行以下操作：

         A. 选择 Event pattern form（事件模式表）。

         B. 对于 Event source（事件源），选择 Amazon services（服务）。

         C. 对于 Amazon 服务，选择 EC2 实例集。

         D. 对于 Event type（事件类型），选择 EC2 Fleet Instance Change（EC2 实例集实例更改）。

         E. 要自定义模板，请选择 Edit pattern（编辑模式），然后进行更改以匹配示例事件模式。

      ii. （可选）要指定自定义事件模式，请执行以下操作：

         A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。

         B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。

   c. 选择 Next（下一步）。

5. 对于 Select target(s)（选择目标），请执行以下操作：

   a. 对于 Target types（目标类型），选择 Amazon service（服务）。

   b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。

   c. 对于 Topic（主题），选择现有主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

   d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。

   e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。

7. 对于 Review and create（查看与创建），执行以下操作：

   a. 查看规则的详细信息并根据需要对其进行修改。

   b. 选择 Create rule（创建规则）。

有关更多信息，请参阅 Amazon EventBridge 用户指南中的 Amazon EventBridge 规则和 Amazon EventBridge 事件模式。

创建 EventBridge 规则以触发 Lambda 函数

下面的示例可创建 EventBridge 规则，以便在 Amazon EC2 每次在实例启动时发出 EC2 队列实例变更通知时触发 Lambda 函数。本示例中的信号作为 `EC2 Fleet Instance Change` 事件子类型 `launched` 发出，这将触发规则定义的操作。

在创建 EventBridge 规则之前，您必须创建 Lambda 函数。

创建要在 EventBridge 规则中使用的 Lambda 函数

1. 打开 Amazon Lambda 控制台，地址：https://console.aws.amazon.com/lambda/。
2. 选择创建函数。
3. 输入函数的名称，配置代码，然后选择 Create function（创建函数）。

   有关使用 Lambda 的更多信息，请参阅 Amazon Lambda 开发人员指南中的使用控制台创建 Lambda 函数。

创建 EventBridge 规则以在 EC2 队列 中的实例改变状态时触发 Lambda 函数

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于定义规则详细信息，请执行以下操作：

   a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

      规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

   b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。

   c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。

   d. 选择 Next（下一步）。

4. 对于 Build event pattern（构建事件模式），执行以下操作：

   a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。

   b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 `EC2 Fleet Instance Change` 事件和 `launched` 子类型。

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

      要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

      i. 要使用模板创建事件模式，请执行以下操作：

         A. 选择 Event pattern form（事件模式表）。

         B. 对于 Event source（事件源），选择 Amazon services（服务）。

         C. 对于 Amazon 服务，选择 EC2 实例集。

D. 对于 Event type（事件类型），选择 EC2 Fleet Instance Change（EC2 实例集实例更改）。

E. 选择 Edit pattern（编辑模式），然后添加 `"detail": {"sub-type": ["launched"]` 以匹配示例事件模式。对于正确的 JSON 格式，在前面的方括号（`,`）之后插入一个逗号（`]`）。

ii. （可选）要指定自定义事件模式，请执行以下操作：

A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。

B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。

c. 选择 Next（下一步）。

5. 对于 Select target(s)（选择目标），请执行以下操作：

a. 对于 Target types（目标类型），选择 Amazon service（服务）。

b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。

c. 对于 Topic（主题），选择 Lambda function（Lambda 函数），对于 Function（函数），选择您创建的用于在事件发生时响应的函数。

d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。

e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。

7. 对于 Review and create（查看与创建），执行以下操作：

a. 查看规则的详细信息并根据需要对其进行修改。

b. 选择 Create rule（创建规则）。

有关如何创建 Lambda 函数和运行 Lambda 函数的 EventBridge 规则的教程，请参阅 Amazon Lambda 开发人员指南中的教程：使用 EventBridge 记录 Amazon EC2 实例的状态。

创建 Amazon EventBridge 规则以监控 Spot 队列事件

为 Spot 队列发出状态变更通知时，该通知的事件将以 JSON 文件的形式发送到 Amazon EventBridge。当事件模式与规则匹配时，您可以编写 EventBridge 规则并自动执行要采取的操作。如果 EventBridge 检测到与规则中定义的模式匹配的事件模式，则 EventBridge 调用规则中指定的一个或多个目标。

下列字段构成规则中定义的事件模式：

```
"source": "aws.ec2spotfleet"
```

识别来自 Spot 队列的事件。

```
"detail-type": "EC2 Spot Fleet State Change"
```

识别事件类型。

```
"detail": { "sub-type": "submitted" }
```

识别事件子类型。

有关 Spot 队列事件和示例事件数据的列表，请参阅the section called “Spot 队列事件类型” (p. 924)。

示例

- 创建 EventBridge 规则以发送通知 (p. 929)

- 创建 EventBridge 规则以触发 Lambda 函数 (p. 931)

创建 EventBridge 规则以发送通知

下面的示例可创建 EventBridge 规则，以便在 Amazon EC2 每次发出 Spot 队列状态变更通知时发送电子邮件、短信或移动推送通知。本示例中的信号作为 `EC2 Spot Fleet State Change` 事件发出，这将触发规则定义的操作。创建 EventBridge 规则之前，您必须为电子邮件、短信或移动推送通知创建 Amazon SNS 主题。

要创建 EventBridge 以在 Spot 队列状态发生变化时发送通知

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于定义规则详细信息，请执行以下操作：
   a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

      规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
   b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。
   c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。
   d. 选择 Next（下一步）。
4. 对于 Build event pattern（构建事件模式），执行以下操作：
   a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。
   b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 `EC2 Spot Fleet Instance Change` 事件。

      ```
      {
       "source": ["aws.ec2spotfleet"],
       "detail-type": ["EC2 Spot Fleet Instance Change"]
      }
      ```

      要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

      i. 要使用模板创建事件模式，请执行以下操作：

         A. 选择 Event pattern form（事件模式表）。
         B. 对于 Event source（事件源），选择 Amazon services（服务）。
         C. 对于 Amazon 服务，选择 EC2 竞价型实例集。
         D. 对于 Event type（事件类型），选择 EC2 Spot Fleet Instance Change（EC2 竞价型实例集实例更改）。
         E. 要自定义模板，请选择 Edit pattern（编辑模式），然后进行更改以匹配示例事件模式。

      ii. （可选）要指定自定义事件模式，请执行以下操作：

         A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。
         B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。
   c. 选择 Next（下一步）。
5. 对于 Select target(s)（选择目标），请执行以下操作：
   a. 对于 Target types（目标类型），选择 Amazon service（服务）。
   b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。

c. 对于 Topic（主题），选择现有主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。

e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。
7. 对于 Review and create（查看与创建），执行以下操作：

a. 查看规则的详细信息并根据需要对其进行修改。

b. 选择 Create rule（创建规则）。

有关更多信息，请参阅 Amazon EventBridge 用户指南中的 Amazon EventBridge 规则和 Amazon EventBridge 事件模式。

创建 EventBridge 规则以触发 Lambda 函数

下面的示例可创建 EventBridge 规则，以便在 Amazon EC2 每次在实例启动时发出 Spot 队列实例变更通知时触发 Lambda 函数。本示例中的信号作为 `EC2 Spot Fleet Instance Change` 事件子类型 `launched` 发出，这将触发规则定义的操作。

在创建 EventBridge 规则之前，您必须创建 Lambda 函数。

创建要在 EventBridge 规则中使用的 Lambda 函数

1. 打开 Amazon Lambda 控制台，地址：https://console.aws.amazon.com/lambda/。
2. 选择创建函数。
3. 输入函数的名称，配置代码，然后选择 Create function（创建函数）。

   有关使用 Lambda 的更多信息，请参阅 Amazon Lambda 开发人员指南中的使用控制台创建 Lambda 函数。

创建 EventBridge 规则以在 Spot 队列中的实例改变状态时触发 Lambda 函数

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于定义规则详细信息，请执行以下操作：

a. 输入规则的 Name (名称) 和“Description (描述)”（可选）。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

b. 对于 Event bus（事件总线），选择 default（默认）。当您账户中的某个 Amazon 服务生成一个事件时，它始终会发送到您账户的默认事件总线。

c. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。

d. 选择 Next（下一步）。

4. 对于 Build event pattern（构建事件模式），执行以下操作：

a. 对于 Event source（事件源），选择 Amazon 事件或 EventBridge 合作伙伴事件。

b. 对于 Event pattern（事件模式），在此示例中，您将指定以下事件模式以匹配 `EC2 Spot Fleet Instance Change` 事件和 `launched` 子类型。

```
{
```

```
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

要添加事件模式，您可以通过选择 Event pattern form（事件模式表）使用模板，或者通过选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））指定您自己的模式，如下所示：

i. 要使用模板创建事件模式，请执行以下操作：

A. 选择 Event pattern form（事件模式表）。
B. 对于 Event source（事件源），选择 Amazon services（服务）。
C. 对于 Amazon 服务，选择 EC2 竞价型实例集。
D. 对于 Event type（事件类型），选择 EC2 Spot Fleet Instance Change（EC2 竞价型实例集实例更改）。
E. 选择 Edit pattern（编辑模式），然后添加 `"detail": {"sub-type": ["launched"]` 以匹配示例事件模式。对于正确的 JSON 格式，在前面的方括号（`,`）之后插入一个逗号（`]`）。

ii. （可选）要指定自定义事件模式，请执行以下操作：

A. 选择 Custom pattern (JSON editor)（自定义模式（JSON 编辑器））。
B. 在 Event pattern（事件模式）框中，为此示例添加事件模式。

c. 选择 Next（下一步）。

5. 对于 Select target(s)（选择目标），请执行以下操作：

a. 对于 Target types（目标类型），选择 Amazon service（服务）。
b. 对于 Select a target（选择目标），选择 SNS topic（SNS 主题）以在事件发生时发送电子邮件、短信或移动推送通知。
c. 对于 Topic（主题），选择 Lambda function（Lambda 函数），对于 Function（函数），选择您创建的用于在事件发生时响应的函数。
d. （可选）在 Additional settings（其他设置）下，您可以选择配置其他设置。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的创建对事件作出反应的 Amazon EventBridge 规则（步骤 16）。
e. 选择 Next（下一步）。

6. （可选）对于 Tags（标签），您可以选择向规则分配一个或多个标签，然后选择 Next（下一步）。
7. 对于 Review and create（查看与创建），执行以下操作：

a. 查看规则的详细信息并根据需要对其进行修改。
b. 选择 Create rule（创建规则）。

有关如何创建 Lambda 函数和运行 Lambda 函数的 EventBridge 规则的教程，请参阅 Amazon Lambda 开发人员指南中的教程：使用 EventBridge 记录 Amazon EC2 实例的状态。

EC2 队列和 Spot 队列教程

以下教程将引导您完成创建 EC2 队列和 Spot 队列的常用流程。

教程

- 教程：将 EC2 队列 与实例权重一起使用 (p. 936)
- 教程：使用 EC2 队列 并将按需作为主容量 (p. 938)

- 教程：使用目标容量预留启动按需实例 (p. 939)
- 教程：将 Spot 实例集与实例权重一起使用 (p. 943)

教程：将 EC2 队列 与实例权重一起使用

该教程使用名为 Example Corp 的虚构公司说明使用实例权重请求 EC2 队列的过程。

目标

Example Corp 是一家医药公司，该公司想要使用 Amazon EC2 的计算功能来筛查可能用于对抗癌症的化学成分。

计划

Example Corp 首先查看Spot 最佳实践。然后，Example Corp 确定了他们的 EC2 队列的要求。

实例类型

Example Corp 有一个计算和内存密集型应用程序，该应用程序在至少 60 GB 内存和八个虚拟 CPU (vCPU) 的情况下性能最佳。他们希望以尽可能低的价格为该应用程序提供尽可能多的这些资源。Example Corp 认定以下任意 EC2 实例类型都能满足其需求：

实例类型	内存 (GiB)	vCPU
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

以单位数表示的目标容量

采用实例权重，目标容量可以等于几个实例 (默认) 或一些因素 (如内核 (vCPU)、内存 (GiB) 和存储 (GB)) 的组合。将其应用程序的基本要求 (60 GB RAM 和八个 vCPU) 作为一个单位，Example Corp 确定，此数量的 20 倍应可满足其需求。因此该公司将其EC2 队列请求的目标容量设置为 20。

实例权重

确定目标容量后，Example Corp 计算了实例权重。为了计算每个实例类型的实例权重，他们按如下所示确定每个实例类型需要多少单位才能达到目标容量：

- r3.2xlarge (61.0 GB, 8 vCPUs) = 1 个 20 单位
- r3.4xlarge (122.0 GB, 16 vCPUs) = 2 个 20 单位
- r3.8xlarge (244.0 GB, 32 vCPUs) = 4 个 20 单位

因此，Example Corp 在其EC2 队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时价格

Example Corp 将每实例小时按需价格作为其价格的起点。他们也可以使用最近的 Spot 价格或两者的组合。为了计算每单位小时价格，他们将每实例小时起始价格除以权重。例如：

实例类型	按需价格	实例权重	每单位小时价格
r3.2xLarge	0.7 美元	1	0.7 美元

实例类型	按需价格	实例权重	每单位小时价格
r3.4xLarge	1.4 美元	2	0.7 美元
r3.8xLarge	2.8 美元	4	0.7 美元

Example Corp 可能会使用每单位小时全局价格 0.7 美元，这对于所有三种实例类型来说是非常有竞争力的。他们可能还会使用每单位小时全局价格 0.7 USD，并在 `r3.8xlarge` 启动规范中使用特定的每单位小时价格 0.9 USD。

验证权限

在创建 EC2 队列请求之前，Example Corp 验证它是否拥有具备所需权限的 IAM 角色。有关更多信息，请参阅EC2 队列先决条件 (p. 854)。

创建启动模板

接下来，Example Corp 会创建启动模板。启动模板 ID 将在下一个步骤中使用。有关更多信息，请参阅创建启动模板 (p. 590)。

创建 EC2 队列

Example Corp 为其 EC2 队列创建一个具有以下配置的文件 (`config.json`)。在以下示例中，将资源标识符替换为您自己的资源标识符。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp 使用以下 create-fleet 命令创建 EC2 队列。

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

有关更多信息，请参阅创建 EC2 队列 (p. 860)。

执行

分配策略确定竞价型实例所来自的 Spot 容量池。

使用 `lowest-price` 策略（这是默认策略）时，Spot 实例来自在执行时具有最低每单位价格的池。为了提供 20 个单位的容量，EC2 队列有三种做法：启动 20 个 `r3.2xlarge` 实例（20 除以 1）、10 个 `r3.4xlarge` 实例（20 除以 2）或 5 个 `r3.8xlarge` 实例（20 除以 4）。

如果 Example Corp 使用 `diversified` 策略，则 Spot 实例来自所有三个池。EC2 队列会启动 6 个 `r3.2xlarge` 实例（提供 6 个单位）、3 个 `r3.4xlarge` 实例（提供 6 个单位）和 2 个 `r3.8xlarge` 实例（提供 8 个单位），总共 20 个单位。

教程：使用 EC2 队列 并将按需作为主容量

该教程使用名为 ABC Online 的虚构公司说明请求 EC2 队列并将按需作为主容量和 Spot 容量（如果可用）的过程。

目标

ABC Online 是一家餐饮送货公司，想要能够跨 EC2 实例类型和购买选项预配置 Amazon EC2 容量，以实现其预期的扩展、性能和成本。

计划

ABC Online 需要在高峰期内有固定容量运行，但也想要以较低价格增加容量，从而获益。ABC Online 确定了其 EC2 队列的以下要求：

- 按需型实例容量 – ABC Online 需要使用 15 个按需型实例，以确保它们可以处理高峰期的流量。
- 竞价型实例容量 – ABC Online 希望能够以较低的价格预置 5 个竞价型实例来提高性能。

验证权限

在创建 EC2 队列之前，ABC Online 验证它是否拥有具备所需权限的 IAM 角色。有关更多信息，请参阅EC2 队列先决条件 (p. 854)。

创建启动模板

接下来，ABC Online 会创建启动模板。启动模板 ID 将在下一个步骤中使用。有关更多信息，请参阅创建启动模板 (p. 590)。

创建 EC2 队列

ABC Online 为其 EC2 队列创建一个具有以下配置的文件 (`config.json`)。在以下示例中，将资源标识符替换为您自己的资源标识符。

```
{
    "LaunchTemplateConfigs": [
        {
```

```
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online 使用以下 create-fleet 命令创建 EC2 队列。

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

有关更多信息，请参阅创建 EC2 队列 (p. 860)。

执行

分配策略确定按需容量始终得到满足，而目标容量的余额将在具有容量且可用的情况下作为 Spot 容量执行。

教程：使用目标容量预留启动按需实例

本教程将指导您完成必须执行的所有步骤，以便 EC2 队列将按需实例启动到 `targeted` 容量预留。

您将学习如何将队列配置为使用 `targeted` 启动按需实例时，首先使用按需容量预留。您还将了解如何配置队列，以便当按需目标总容量超过可用未使用容量预留的数量时，队列使用指定的分配策略来选择启动剩余目标容量的实例池。

EC2 队列配置

在本教程中，队列配置如下所示：

- 目标容量：10 个按需实例
- 未使用总数 `targeted` 容量预留：6（少于队列的 10 个按需实例的按需目标容量）
- 容量预留池数量：2 (`us-east-1a` 和 `us-east-1b`)
- 每个池的容量预留数量：3
- 按需分配策略：`lowest-price`（如果未使用的容量预留数少于按需目标容量，队列将根据按需分配策略确定启动剩余的按需容量的池。）

  请注意，您也可以使用 `prioritized` 分配策略而不是 `lowest-price` 分配策略。

要将按需实例启动到 targeted 能力预留，您必须执行以下几个步骤：

- 步骤 1：创建容量预留 (p. 940)
- 步骤 2：创建容量预留资源组 (p. 940)
- 步骤 3：将容量预留添加到容量预留资源组 (p. 940)
- （可选）步骤 4：查看资源组中的容量预留 (p. 941)
- 步骤 5：创建启动模板，该模板指定容量预留的目标是特定资源组 (p. 941)
- （可选）步骤 6：描述启动模板 (p. 941)

- 步骤 7：创建 EC2 队列 (p. 942)
- （可选）步骤 8：查看剩余未使用的容量预留数 (p. 943)

步骤 1：创建容量预留

使用创建容量预留命令创建容量预留，三个 us-east-1a，另外三个 us-east-1b。除了可用区之外，容量预留的其他属性是相同的。

us-east-1a 中的 3 个容量预留

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

生成的容量预留 ID 示例

```
cr-1234567890abcdef1
```

us-east-1b 中的 3 个容量预留

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

生成的容量预留 ID 示例

```
cr-54321abcdef567890
```

步骤 2：创建容量预留资源组

使用 resource-groups 服务和 create-group 命令可创建容量预留资源组。在此示例中，资源组名为 my-cr-group。有关必须创建资源组原因的信息，请参阅 将 容量预留 用于 按需型实例 (p. 849)。

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-types",
 "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

步骤 3：将容量预留添加到容量预留资源组

使用 resource-groups 服务和 group-resources 命令将您在步骤 1 中创建的容量预留添加到容量预留资源组。请注意，您必须通过其 ARN 引用按需容量预留。

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
```

```
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

输出示例

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

（可选）步骤 4：查看资源组中的容量预留

使用 `resource-groups` 服务和 list-group-resources 命令可根据需要描述资源组以查看其容量预留。

```
aws resource-groups list-group-resources --group my-cr-group
```

输出示例

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

步骤 5：创建启动模板，该模板指定容量预留的目标是特定资源组

使用 create-launch-template 命令可创建启动模板，在此启动模板中指定要使用的容量预留。在此示例中，队列将使用已添加到资源组的 `targeted` 容量预留。因此，启动模板数据指定容量预留以特定资源组为目标。在此示例中，启动模板名为 `my-launch-template`。

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

（可选）步骤 6：描述启动模板

使用 describe-launch-template 命令可根据需要描述启动模板以查看其配置。

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

输出示例

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

步骤 7：创建 EC2 队列

创建一个 EC2 队列，指定将启动的实例配置信息。以下 EC2 队列配置仅显示该示例的相关配置。启动模板 `my-launch-template` 是您在步骤 5 中创建的启动模板。有两个实例池，每个实例池具有相同的实例类型 (`c5.xlarge`)，但具有不同的可用区域（`us-east-1a` 和 `us-east-1b`）。实例池的价格是相同的，因为定价是针对区域定义的，而不是按可用区定义的。总目标容量为 10，而原定设置目标容量类型为 `on-demand`。按需分配策略为 `lowest-price`。容量预留的使用策略是 `use-capacity-reservations-first`。

Note

队列类型必须为 `instant`。其他队列类型不支持 `use-capacity-reservations-first`。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
```

```
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

在使用上述配置创建 `instant` 队列后，将启动下面的 10 个实例来满足目标容量：

- 容量预留首先用于启动 6 个按需实例，如下所示：
  - 3 个按需实例启动到 `us-east-1a` 中的 3 个`c5.xlarge` `targeted`容量预留
  - 3 个按需实例启动到 `us-east-1b` 中的 3 个`c5.xlarge` `targeted`容量预留
- 为了满足目标容量，根据按需分配策略，将 4 个额外的按需实例启动到常规按需容量中（在本示例中为 `lowest-price`）。但是，由于池的价格相同（因为价格是每个区域而不是每个可用区），因此队列将在其中一个池中启动剩余的 4 个按需实例。

（可选）步骤 8：查看剩余未使用的容量预留数

在启动队列后，您可以运行 describe-capacity-reservations 来查看保留的未使用的容量预留的数目。在此示例中，您应看到以下响应，该响应指示所有池中的所有 容量预留 均已使用。

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

教程：将 Spot 实例集与实例权重一起使用

该教程使用名为 Example Corp 的虚构公司说明使用实例权重请求 Spot 队列的过程。

目标

Example Corp 是一家医药公司，该公司想要利用 Amazon EC2 的计算功能来筛查可能用于对抗癌症的化学成分。

计划

Example Corp 首先查看Spot 最佳实践。然后，Example Corp 确定了他们的 Spot 队列的以下要求。

实例类型

Example Corp 有一个计算和内存密集型应用程序，该应用程序在至少 60 GB 内存和八个虚拟 CPU (vCPU) 的情况下性能最佳。他们希望以尽可能低的价格为该应用程序提供尽可能多的这些资源。Example Corp 认定以下任意 EC2 实例类型都能满足其需求：

实例类型	内存 (GiB)	vCPU
r3.2xlarge	61	8

实例类型	内存 (GiB)	vCPU
r3.4xlarge	122	16
r3.8xlarge	244	32

以单位数表示的目标容量

采用实例权重，目标容量可以等于几个实例 (默认) 或一些因素 (如内核 (vCPU)、内存 (GiB) 和存储 (GB)) 的组合。将其应用程序的基本要求 (60 GB RAM 和八个 vCPU) 作为 1 个单位，Example Corp 决定 20 倍此数量可满足其需求。因此该公司将其 Spot 队列请求的目标容量设置为 20。

实例权重

确定目标容量后，Example Corp 计算了实例权重。为了计算每个实例类型的实例权重，他们按如下所示确定每个实例类型需要多少单位才能达到目标容量：

- r3.2xlarge (61.0 GB, 8 vCPUs) = 1 个 20 单位
- r3.4xlarge (122.0 GB, 16 vCPUs) = 2 个 20 单位
- r3.8xlarge (244.0 GB, 32 vCPUs) = 4 个 20 单位

因此，Example Corp 在其 Spot 队列请求中将实例权重 1、2 和 4 分配给相应的启动配置。

每单位小时价格

Example Corp 将每实例小时按需价格作为其价格的起点。他们也可以使用最近的 Spot 价格或两者的组合。为了计算每单位小时价格，他们将每实例小时起始价格除以权重。例如：

实例类型	按需价格	实例权重	每单位小时价格
r3.2xLarge	0.7 美元	1	0.7 美元
r3.4xLarge	1.4 美元	2	0.7 美元
r3.8xLarge	2.8 美元	4	0.7 美元

Example Corp 可能会使用每单位小时全局价格 0.7 美元，这对于所有三种实例类型来说是非常有竞争力的。他们可能还会使用每单位小时全局价格 0.7 USD，并在 `r3.8xlarge` 启动规范中使用特定的每单位小时价格 0.9 USD。

验证权限

在创建 Spot 队列请求之前，Example Corp 会验证它是否拥有具备所需权限的 IAM 角色。有关更多信息，请参阅Spot 队列权限 (p. 894)。

创建请求

Example Corp 为其竞价型实例集请求创建一个具有以下配置的文件（`config.json`）：

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
```

```
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 2
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.8xlarge",
      "SubnetId": "subnet-482e4972",
      "SpotPrice": "0.90",
      "WeightedCapacity": 4
    }
  ]
}
```

Example Corp 使用 request-spot-fleet 命令创建 Spot 队列请求。

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

有关更多信息，请参阅Spot 队列请求类型 (p. 871)。

执行

分配策略确定竞价型实例所来自的 Spot 容量池。

使用 `lowestPrice` 策略（这是默认策略）时，Spot 实例来自在执行时具有最低每单位价格的池。为了提供 20 个单位的容量，竞价型实例集有三种做法：启动 20 个 `r3.2xlarge` 实例（20 除以 1）、10 个 `r3.4xlarge` 实例（20 除以 2）或 5 个 `r3.8xlarge` 实例（20 除以 4）。

如果 Example Corp 使用 `diversified` 策略，则 Spot 实例来自所有三个池。竞价型实例集会启动 6 个 `r3.2xlarge` 实例（提供 6 个单位）、3 个 `r3.4xlarge` 实例（提供 6 个单位）和 2 个 `r3.8xlarge` 实例（提供 8 个单位），总共 20 个单位。

EC2 队列和 Spot 队列配置示例

下列示例显示了可用来创建 EC2 队列和 Spot 队列的启动配置。

主题

- EC2 队列 示例配置 (p. 945)
- Spot 队列示例配置 (p. 958)

EC2 队列 示例配置

下列示例显示了可与 create-fleet 命令结合使用以创建 EC2 队列的启动配置。有关参数的更多信息，请参阅 Amazon CLI 命令参考中的 create-fleet。

示例

- 示例 1：启动竞价型实例作为默认购买选项 (p. 946)
- 示例 2：启动按需型实例作为默认购买选项 (p. 946)
- 示例 3：启动按需型实例作为主容量 (p. 947)
- 示例 4：使用 lowest-price 分配策略启动 Spot 实例 (p. 947)
- 示例 5：使用多个容量保留按需启动实例 (p. 948)
- 示例 6：当总目标容量大于未使用的容量预留数量时，使用容量预留启动按需实例 (p. 950)
- 示例 7：使用容量预留启动按需实例 (p. 952)
- 示例 8：配置容量再平衡以启动替换竞价型实例 (p. 954)
- 示例 9：在容量优化的队列中启动竞价型实例 (p. 955)
- 示例 10：在具有优先级的容量优化队列中启动竞价型实例 (p. 956)
- 示例 11：在价格容量优化的实例集中启动竞价型实例 (p. 957)
- 示例 12：配置基于属性的实例类型选择 (p. 958)

示例 1：启动竞价型实例作为默认购买选项

下面的示例指定了 EC2 队列中所需的最少参数：启动模板、目标容量和默认购买选项。启动模板由其启动模板 ID 和版本号标识。队列的目标容量为 2 个实例，默认购买选项为 `spot`，因此队列启动两个 Spot 实例。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

示例 2：启动按需型实例作为默认购买选项

下面的示例指定了 EC2 队列中所需的最少参数：启动模板、目标容量和默认购买选项。启动模板由其启动模板 ID 和版本号标识。队列的目标容量为 2 个实例，默认购买选项为 `on-demand`，因此队列启动两个 按需实例。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
```

```
}
```

示例 3：启动按需型实例作为主容量

下面的示例为队列指定 2 个实例的总目标容量和 1 个按需实例的目标容量。默认购买选项为 spot。队列按照指定的方式启动 1 个按需型实例，但需要再启动一个实例以满足总目标容量要求。差值的购买选项是通过 TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType 计算得出，因而实例集会启动 1 个竞价型实例。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

示例 4：使用 lowest-price 分配策略启动 Spot 实例

如果未指定 Spot 实例的分配策略，则使用默认分配策略 lowest-price。以下示例使用 lowest-price 分配策略。覆盖启动模板的三个启动规范有不同的实例类型，但有相同的权重容量和子网。总目标容量为两个实例，默认购买选项为 spot。EC2 实例集按启动规范的最低价格实例类型启动两个竞价型实例。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
  "Overrides": [
        {
          "InstanceType": "c4.large",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-a4f6c5d3"
        },
        {
          "InstanceType": "c3.large",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-a4f6c5d3"
        },
        {
          "InstanceType": "c5.large",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-a4f6c5d3"
        }
      ]

        }
    ],
    "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

示例 5：使用多个容量保留按需启动实例

可以通过将 容量预留 的使用策略配置为 use-capacity-reservations-first 来将队列配置为在启动按需实例 时首先使用 按需容量预留。此示例演示了当容量预留数量超过满足目标容量所需的容量预留数量时，队列如何选择要使用的容量预留。

队列配置如下所示：

- 目标容量：12 个按需实例
- 未使用的容量预留总数：15（超过了队列的 12 个按需实例的目标容量）
- 容量预留池数量：3 (m5.large、m4.xlarge 和 m4.2xlarge)
- 每个池的容量预留数量：5
- 按需分配策略：lowest-price（当多个实例池中存在多个未使用的容量预留时，队列将根据按需分配策略确定启动按需实例的池。）

  请注意，您也可以使用 prioritized 分配策略而不是 lowest-price 分配策略。

容量预留

账户在 3 个不同的池中有以下 15 个未使用的 容量预留。每个池中的 容量预留 数由 AvailableInstanceCount 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

队列配置

以下队列配置仅显示该示例的相关配置。总目标容量为 12，而默认目标容量类型为 on-demand。按需分配策略为 lowest-price。容量预留的使用策略是 use-capacity-reservations-first。

在此示例中，个按需型实例 价格为：

- m5.large – 每小时 0.096 美元
- m4.xlarge – 每小时 0.20 美元
- m4.2xlarge – 每小时 0.40 美元

> **Note**
>
> 队列类型必须为类型 instant。其他队列类型不支持 use-capacity-reservations-first。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

在使用上述配置创建 instant 队列后，将启动下面的 12 个实例来满足目标容量：

- us-east-1a 中的 5 个 m5.large 按需实例–us-east-1a 中的 m5.large 是最低的价格,并且有 5 个可用的未使用 m5.large 容量预留
- us-east-1a 中的 5 个 m4.xlarge 按需实例 – us-east-1a 中的 m4.xlarge 是第二低的价格，并且有 5 个可用的未使用 m4.xlarge 容量预留
- us-east-1a 中的 2 个 m4.2xlarge 按需实例 – us-east-1a 中的 m4.2xlarge 是第三低的价格，并且有 5 个可用的未使用 m4.2xlarge 容量预留，只需其中的 2 个即可满足目标容量

在启动队列后，您可以运行 describe-capacity-reservations 来查看保留的未使用的 容量预留 的数目。在此示例中，您该看到以下响应，该响应指示已使用所有 m5.large 和 m4.xlarge 容量预留，有 3 个 m4.2xlarge 容量预留未使用。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

示例 6：当总目标容量大于未使用的容量预留数量时，使用容量预留启动按需实例

可以通过将 容量预留 的使用策略配置为 use-capacity-reservations-first 来将队列配置为在启动 按需实例 时首先使用 按需容量预留。此示例演示了当总目标容量超过可用未使用容量预留数时，队列如何选择要在其中启动按需实例的实例池。

在此示例中，队列配置如下所示：

- 目标容量：16 个按需实例
- 未使用的容量预留总数：15（少于队列的 16 个按需实例的目标容量）
- 容量预留池数量：3 (m5.large、m4.xlarge 和 m4.2xlarge)
- 每个池的容量预留数量：5
- 按需分配策略：lowest-price（如果未使用的容量预留数少于按需目标容量，队列将根据按需分配策略确定启动剩余的按需容量的池。）

  请注意，您也可以使用 prioritized 分配策略而不是 lowest-price 分配策略。

容量预留

账户在 3 个不同的池中有以下 15 个未使用的 容量预留。每个池中的 容量预留 数由 AvailableInstanceCount 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
```

```
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

队列配置

以下队列配置仅显示该示例的相关配置。总目标容量为 16，而默认目标容量类型为 on-demand。按需分配策略为 lowest-price。容量预留的使用策略是 use-capacity-reservations-first。

在此示例中，个按需型实例 价格为：

- m5.large – 每小时 0.096 美元
- m4.xlarge – 每小时 0.20 美元
- m4.2xlarge – 每小时 0.40 美元

> **Note**
>
> 队列类型必须为 instant。其他队列类型不支持 use-capacity-reservations-first。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
```

```
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

在使用上述配置创建 instant 队列后，将启动下面的 16 个实例来满足目标容量：

- us-east-1a 中的 6个 m5.large 按需实例–us-east-1a 中的 m5.large 是最低的价格，并且有 5 个可用的未使用 m5.large 容量预留。容量预留首先用于启动 5 个按需实例。使用了剩余 m4.xlarge 和 m4.2xlarge 容量保留后，为了满足目标容量，将额外的按需实例启动到常规按需容量中（在本示例中为 lowest-price）。
- us-east-1a 中的 5个 m4.xlarge 按需实例–us-east-1a 中的 m4.xlarge 是第二低的价格，并且有 5 个可用的未使用 m4.xlarge 容量预留。
- us-east-1a 中的 5个 m4.2xlarge 按需实例–us-east-1a 中的 m4.2xlarge 是第三低的价格，并且有 5 个可用的未使用 m4.2xlarge 容量预留。

在启动队列后，您可以运行 describe-capacity-reservations 来查看保留的未使用的 容量预留 的数目。在此示例中，您应看到以下响应，该响应指示所有池中的所有 容量预留 均已使用。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

示例 7：使用容量预留启动按需实例

通过将容量保留的使用策略设置为 use-capacity-reservations-first，您可以将震源组配置为在启动按需实例时首先使用 targeted 按需容量保留。此示例演示如何将按需实例启动到 targeted 容量预留，其中容量预留的属性相同，但其可用区域除外 (us-east-1a 和 us-east-1b)。它还演示了当总目标容量超过可用未使用容量预留数时，队列如何选择要在其中启动按需实例的实例池。

在此示例中，队列配置如下所示：

- 目标容量：10 个按需实例
- 未使用总数 targeted 容量预留：6（少于队列的 10 个按需实例的按需目标容量）
- 容量预留池数量：2 (us-east-1a 和 us-east-1b)
- 每个池的容量预留数量：3
- 按需分配策略：lowest-price（如果未使用的容量预留数少于按需目标容量，队列将根据按需分配策略确定启动剩余的按需容量的池。）

请注意，您也可以使用 prioritized 分配策略而不是 lowest-price 分配策略。

有关完成此示例所必须执行的过程的演练，请参阅 教程：使用目标容量预留启动按需实例 (p. 939)。

容量预留

账户在 2 个不同的池中有以下 6 个未使用的容量预留。在此示例中，池因其可用区而异。每个池中的 容量预留 数由 AvailableInstanceCount 指示。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

队列配置

以下队列配置仅显示该示例的相关配置。总目标容量为 10，而默认目标容量类型为 on-demand。按需分配策略为 lowest-price。容量预留的使用策略是 use-capacity-reservations-first。

在此示例中，us-east-1 中 c5.xlarge 的按需实例价格为：每小时 0.17 美元

Note

队列类型必须为 instant。其他队列类型不支持 use-capacity-reservations-first。

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
```

```
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

在使用上述配置创建 instant 队列后，将启动下面的 10 个实例来满足目标容量：

- 容量预留首先用于启动 6 个按需实例，如下所示：
  - 3 个按需实例启动到 us-east-1a 中的 3 个c5.xlarge targeted容量预留
  - 3 个按需实例启动到 us-east-1b 中的 3 个c5.xlarge targeted容量预留
- 为了满足目标容量，根据按需分配策略，将 4 个额外的按需实例启动到常规按需容量中（在本示例中为 lowest-price）。但是，由于池的价格相同（因为价格是每个区域而不是每个可用区），因此队列将在一个池中启动剩余的 4 个按需实例。

在启动队列后，您可以运行 describe-capacity-reservations 来查看保留的未使用的 容量预留 的数目。在此示例中，您应看到以下响应，该响应指示所有池中的所有 容量预留 均已使用。

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

示例 8：配置容量再平衡以启动替换竞价型实例

下面的示例将 EC2 实例集配置为在 Amazon EC2 为队列中的竞价型实例发出再平衡建议时启动替换竞价型实例。要配置 Spot 实例 的自动替换，对于 ReplacementStrategy，请指定 launch-before-terminate。要配置从启动新替换竞价型实例到自动删除旧竞价型实例的时间延迟，请对于 termination-delay，请指定值（以秒为单位）。有关更多信息，请参阅配置选项 (p. 849)。

> **Note**
>
> 我们建议仅当您可以预测实例关闭过程完成所需的时长时才使用 launch-before-terminate，这样只有在这些过程完成后才会终止旧实例。在实例运行期间，您需要为它们付费。

容量再平衡策略的有效性取决于 EC2 队列 请求中指定的 Spot 容量池的数量。我们建议您使用一组多样化的实例类型和可用区配置队列，对于 AllocationStrategy，请指定 capacity-optimized。有关为容量再平衡配置 EC2 队列 时应考虑的内容的更多信息，请参阅容量再平衡 (p. 849)。

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
```

```
                        {
                            "InstanceType": "c3.large",
                            "WeightedCapacity": 1,
                             "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        },
                        {
                            "InstanceType": "c4.large",
                            "WeightedCapacity": 1,
                             "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        },
                        {
                            "InstanceType": "c5.large",
                            "WeightedCapacity": 1,
                             "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

示例 9：在容量优化的队列中启动竞价型实例

以下示例演示如何使用针对容量进行优化的 Spot 分配策略配置 EC2 队列。要优化容量，您必须将 `AllocationStrategy` 设置为 `capacity-optimized`。

在以下示例中，三个启动规范指定了三个 Spot 容量池。目标容量为 50 个竞价型实例。EC2 实例集尝试在 Spot 容量池中启动 50 个竞价型实例，并为启动的实例数量提供最佳容量。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
```

```
                    },
                     {
                         "InstanceType": "m4.2xlarge",
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         },
                     },
                     {
                         "InstanceType": "c5.2xlarge",
                         "Placement": {
                             "AvailabilityZone": "us-west-2b"
                         }
                     }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

示例 10：在具有优先级的容量优化队列中启动竞价型实例

以下示例演示如何通过 Spot 分配策略配置 EC2 队列，该策略针对容量进行优化，同时尽最大努力使用优先级。

使用 `capacity-optimized-prioritized` 分配策略时，您可以使用 `Priority` 参数指定 Spot 容量池的优先级，数字越小优先级越高。如果您平等地支持多个 Spot 容量池，您还可以为它们设置相同的优先级。如果您没有为某个池设置优先级，则该池将在优先级方面被视为最后一个。

要设置 Spot 容量池的优先级，您必须将 `AllocationStrategy` 设置为 `capacity-optimized-prioritized`。EC2 队列首先会针对容量进行优化，但会尽最大努力遵循优先级。（例如，如果遵循优先级不会显著影响 EC2 队列预置最佳容量的能力）。对于必须最大限度地减少中断可能性，同时对某些实例类型的偏好也很重要的工作负载来说，这是一个不错的选择。

在以下示例中，三个启动规范指定了三个 Spot 容量池。对每个池进行优先级排序，数字越小优先级越高。目标容量为 50 个竞价型实例。EC2 实例集尝试以最高优先级在 Spot 容量池中启动 50 个竞价型实例，但首先针对容量进行优化。

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                         {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "Placement": {
```

```
                            "AvailabilityZone": "us-west-2b"
                        },
                    },
                    {
                        "InstanceType": "c5.2xlarge",
                        "Priority": 3,
                        "Placement": {
                            "AvailabilityZone": "us-west-2b"
                        }
                    }
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

示例 11：在价格容量优化的实例集中启动竞价型实例

以下示例演示了如何通过 Spot 分配策略配置 EC2 实例集，该策略针对容量和最低价格进行了优化。若要在考虑价格的同时优化容量，必须将 Spot `AllocationStrategy` 设置为 `price-capacity-optimized`。

在以下示例中，三个启动规范指定了三个 Spot 容量池。目标容量为 50 个竞价型实例。EC2 实例集尝试在 Spot 容量池中启动 50 个竞价型实例，并为启动的实例数量提供最佳容量，同时选择最低价格的池。

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            },
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            }
                        }
                    ]
            }
    ],
    "TargetCapacitySpecification": {
```

```
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

示例 12：配置基于属性的实例类型选择

以下示例演示了如何配置 EC2 实例集，以使用基于属性的实例类型选择来识别实例类型。若要指定所需的实例属性，请在 `InstanceRequirements` 结构中指定属性。

在以下示例中，指定了 2 个实例属性：

- `VCpuCount` – 至少指定了 2 个 vCPU。由于未指定最大值，因此没有最大限制。
- `MemoryMiB` – 至少指定了 4 MiB 的内存。由于未指定最大值，因此没有最大限制。

将识别具有 2 个或更多 vCPU 和 4 MiB 或更大内存的任何实例类型。然而，当 EC2 实例集预置实例集 (p. 837)时，价格保护和分配策略可能会排除某些实例类型。

有关您可以指定的所有可能属性的列表和描述，请参阅 Amazon EC2 API Reference（《Amazon EC2 API 参考》）中的 InstanceRequirements。

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Spot 队列示例配置

以下各示例显示了可与 request-spot-fleet 命令结合使用以创建 Spot 队列请求的启动配置。有关更多信息，请参阅创建 Spot 队列请求 (p. 900)。

> **Note**
>
> 对于 Spot 队列，您无法在启动规范中指定网络接口 ID。请确保在启动规范中省略 `NetworkInterfaceID` 参数。

示例

- 示例 1：使用区域中价格最低的可用区或子网启动竞价型实例 (p. 959)
- 示例 2：使用指定列表中价格最低的可用区或子网启动竞价型实例 (p. 959)
- 示例 3：使用指定列表中价格最低的实例类型启动竞价型实例 (p. 961)
- 示例 4。覆盖请求的价格 (p. 962)
- 示例 5：使用多样化分配策略启动 Spot 队列 (p. 963)
- 示例 6：使用实例权重启动 Spot 队列 (p. 965)
- 示例 7：启动具有按需容量的 Spot 队列 (p. 966)
- 示例 8：配置容量再平衡以启动替换竞价型实例 (p. 966)
- 示例 9：在容量优化的队列中启动竞价型实例 (p. 967)
- 示例 10：在具有优先级的容量优化队列中启动竞价型实例 (p. 968)
- 示例 11：在 priceCapacityOptimized 实例集中启动竞价型实例 (p. 969)
- 示例 12：配置基于属性的实例类型选择 (p. 969)

示例 1：使用区域中价格最低的可用区或子网启动竞价型实例

以下示例指定一个没有可用区或子网的启动规范。Spot 队列会在具有默认子网且价格最低的可用区中启动实例。您支付的价格不得超过按需价格。

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

示例 2：使用指定列表中价格最低的可用区或子网启动竞价型实例

以下示例指定具有的可用区或子网不同但实例类型和 AMI 相同的两种启动规范。

Availability Zones (可用区)

Spot 队列会在价格最低的指定可用区的默认子网中启动实例。

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
```

```
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "m3.medium",
        "Placement": {
            "AvailabilityZone": "us-west-2a, us-west-2b"
        },
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ]
}
```

Subnets (子网)

您可以指定默认子网或非默认子网，并且非默认子网可来自默认 VPC 或非默认 VPC。Spot 服务会在位于价格最低的可用区的子网中启动实例。

您无法在 Spot 队列请求中指定来自相同可用区的不同子网。

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "m3.medium",
        "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
        }
    }
  ]
}
```

如果在默认 VPC 中启动实例，则实例在默认情况下会收到一个公有 IPv4 地址。如果在非默认 VPC 中启动实例，则实例在默认情况下不会收到一个公有 IPv4 地址。在启动规范中使用网络接口来将一个公有 IPv4 地址分配给在非默认 VPC 中启动的实例。指定网络接口时，您必须包括使用网络接口的子网 ID 和安全组 ID。

```
  ...
    {
        "ImageId": "ami-1a2b3c4d",
        "KeyName": "my-key-pair",
        "InstanceType": "m3.medium",
        "NetworkInterfaces": [
            {
                "DeviceIndex": 0,
                "SubnetId": "subnet-1a2b3c4d",
                "Groups": [ "sg-1a2b3c4d" ],
                "AssociatePublicIpAddress": true
            }
        ],
        "IamInstanceProfile": {
            "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
        }
    }
```

```
  ...
```

示例 3：使用指定列表中价格最低的实例类型启动竞价型实例

以下示例指定实例类型不同、但 AMI 和可用区或子网相同的两种启动配置。Spot 队列使用价格最低的指定实例类型启动实例。

可用区：

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "cc2.8xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

子网

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "cc2.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
```

```
            "InstanceType": "r3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

示例 4。覆盖请求的价格

我们建议您使用默认最高价 (这是按需价格)。如果愿意，您可以为队列请求以及各个启动规范指定最高价。

以下示例为队列请求以及两个启动规范 (共三个) 指定最高价。队列请求的最高价用于未指定最高价的任何启动规范。Spot 队列使用价格最低的实例类型启动实例。

可用区：

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
}
```

子网

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "SubnetId": "subnet-1a2b3c4d",
```

```
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

示例 5：使用多样化分配策略启动 Spot 队列

以下示例使用 diversified 分配策略。启动规范具有不同的实例类型，但具有相同的 AMI 和可用区或子网。Spot 队列在 3 个启动规范间分配 30 个实例，以便每种类型有 10 个实例。有关更多信息，请参阅竞价型实例的分配策略 (p. 872)。

可用区：

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

子网

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
```

```
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

在其中一个可用区中断的情况下，增加 EC2 容量可以满足 Spot 请求的几率的最佳实践是跨区域实现多样化。对于这种情况，请在启动规范中包含每个对您可用的可用区。并且，不是每次使用同一个子网，而是使用三个唯一的子网（每个子网映射到不同的区域）。

可用区：

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

子网

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
```

```
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

示例 6：使用实例权重启动 Spot 队列

以下示例使用实例权重，这意味着价格是每单位小时价格，而不是每实例小时价格。每个启动配置列出不同的实例类型和不同的权重。Spot 队列选择每单位小时价格最低的实例类型。竞价型实例集通过将目标容量除以实例权重，计算出要启动的竞价型实例数。如果结果不是整数，则 Spot 队列会将其向上舍入到下一个整数，以便队列的大小不低于其目标容量。

如果 `r3.2xlarge` 请求成功，Spot 将预置其中的 4 个实例。将 20 除以 6 可得到总共 3.33 个实例，然后向上舍入为 4 个实例。

如果 `c3.xlarge` 请求成功，Spot 将预置其中的 7 个实例。将 20 除以 3 可得到总共 6.66 个实例，然后向上舍入为 7 个实例。

有关更多信息，请参阅Spot 队列实例权重 (p. 891)。

可用区：

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "WeightedCapacity": 3
      }
    ]
}
```

子网

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 6
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 3
        }
    ]
}
```

示例 7：启动具有按需容量的 Spot 队列

为确保始终拥有实例容量，您可以在 Spot 队列请求中包含按需容量请求。如果具有容量，则将始终执行按需请求。目标容量的余量将在具有容量且可用的情况下作为 Spot 容量执行。

以下示例将所需的目标容量指定为 10，其中 5 个必须为按需容量。未指定 Spot 容量；它由目标容量减去按需容量的余量隐含指定。Amazon EC2 启动 5 个容量单位作为按需容量，并在有可用的 Amazon EC2 容量并且可用时，启动 5 个容量单位 (10-5=5) 作为 Spot 容量。

有关更多信息，请参阅Spot 队列中的按需实例 (p. 888)。

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

示例 8：配置容量再平衡以启动替换竞价型实例

下面的示例将竞价型实例集配置为在 Amazon EC2 为队列中的竞价型实例发出再平衡建议时启动替换竞价型实例。要配置 Spot 实例 的自动替换，对于 `ReplacementStrategy`，请指定 `launch-before-terminate`。要配置从启动新替换竞价型实例到自动删除旧竞价型实例的时间延迟，请对于 `termination-delay`，请指定值（以秒为单位）。有关更多信息，请参阅配置选项 (p. 889)。

> **Note**
>
> 我们建议仅当您可以预测实例关闭过程完成所需的时长时才使用 `launch-before-terminate`。这将确保只有在关闭过程完成后才终止旧实例。在实例运行期间，您需要为它们付费。

容量再平衡策略的有效性取决于 Spot 队列请求中指定的 Spot 容量池的数量。我们建议您使用一组多样化的实例类型和可用区配置队列，对于 `AllocationStrategy`，请指定 `capacityOptimized`。有关为容量再平衡配置竞价型实例集时应考虑的内容的更多信息，请参阅 容量再平衡 (p. 888)。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                           "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

示例 9：在容量优化的队列中启动竞价型实例

以下示例演示如何使用针对容量进行优化的 Spot 分配策略配置 Spot 队列。要优化容量，您必须将 `AllocationStrategy` 设置为 `capacityOptimized`。

在以下示例中，三个启动规范指定了三个 Spot 容量池。目标容量为 50 个竞价型实例。竞价型实例集尝试在 Spot 容量池中启动 50 个竞价型实例，并为启动的实例数量提供最佳容量。

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
```

```
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       }
                ]
           }
      ]
}
```

示例 10：在具有优先级的容量优化队列中启动竞价型实例

以下示例演示如何通过 Spot 分配策略配置 Spot 队列，该策略针对容量进行优化，同时尽最大努力使用优先级。

使用 `capacityOptimizedPrioritized` 分配策略时，您可以使用 `Priority` 参数指定 Spot 容量池的优先级，数字越小优先级越高。如果您平等地支持多个 Spot 容量池，您还可以为它们设置相同的优先级。如果您没有为某个池设置优先级，则该池将在优先级方面被视为最后一个。

要设置 Spot 容量池的优先级，您必须将 `AllocationStrategy` 设置为 `capacityOptimizedPrioritized`。Spot 队列首先会针对容量进行优化，但会尽最大努力遵循优先级。（例如，如果遵循优先级不会显著影响 Spot 队列预置最佳容量的能力）。对于必须最大限度地减少中断可能性，同时对某些实例类型的偏好也很重要的工作负载来说，这是一个不错的选择。

在以下示例中，三个启动规范指定了三个 Spot 容量池。对每个池进行优先级排序，数字越小优先级越高。目标容量为 50 个竞价型实例。竞价型实例集尝试以最高优先级在 Spot 容量池中启动 50 个竞价型实例，但首先针对容量进行优化。

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                           "InstanceType": "r4.2xlarge",
                           "Priority": 1,
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Priority": 2,
```

```
                        "AvailabilityZone": "us-west-2b"
                    },
                    {
                        "InstanceType": "c5.2xlarge",
                        "Priority": 3,
                        "AvailabilityZone": "us-west-2b"
                    }
                ]
            }
        ]
}
```

示例 11：在 priceCapacityOptimized 实例集中启动竞价型实例

以下示例演示了如何通过 Spot 分配策略配置竞价型实例集，该策略针对容量和最低价格进行了优化。若要在考虑价格的同时优化容量，必须将 Spot `AllocationStrategy` 设置为 `priceCapacityOptimized`。

在以下示例中，三个启动规范指定了三个 Spot 容量池。目标容量为 50 个竞价型实例。竞价型实例集尝试在 Spot 容量池中启动 50 个竞价型实例，并为启动的实例数量提供最佳容量，同时选择最低价格的池。

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                          "InstanceType": "r4.2xlarge",
                          "AvailabilityZone": "us-west-2a"
                      },
                      {
                          "InstanceType": "m4.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                      },
                      {
                          "InstanceType": "c5.2xlarge",
                          "AvailabilityZone": "us-west-2b"
                      }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

示例 12：配置基于属性的实例类型选择

以下示例演示了如何配置竞价型实例集，以使用基于属性的实例类型选择来识别实例类型。若要指定所需的实例属性，请在 `InstanceRequirements` 结构中指定属性。

在以下示例中，指定了 2 个实例属性：

- `VCpuCount` – 至少指定了 2 个 vCPU。由于未指定最大值，因此没有最大限制。

- MemoryMiB – 至少指定了 4 MiB 的内存。由于未指定最大值，因此没有最大限制。

将识别具有 2 个或更多 vCPU 和 4 MiB 或更大内存的任何实例类型。然而，当竞价型实例集预置实例集 (p. 876)时，价格保护和分配策略可能会排除某些实例类型。

有关您可以指定的所有可能属性的列表和描述，请参阅 Amazon EC2 API Reference（《Amazon EC2 API 参考》）中的 InstanceRequirements。

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

队列配额

常用的 Amazon EC2 配额（以前称为限额）适用于由 EC2 实例集或竞价型实例集启动的实例，例如竞价型实例限制 (p. 502)和卷限制 (p. 1607)。

此外，以下配额将适用：

配额描述	配额
每个区域中状态为 active、deleted_running 和 cancelled_running 的 EC2 实例集和竞价型实例集的数量	1,000 [1] [2] [3] [4]
Spot 容量池数量（实例类型和子网的唯一组合）	300 [1] [4]
启动规范中的用户数据大小	16 KB [2]
每个 EC2 实例集或竞价型实例集的目标容量	10000
区域中所有 EC2 实例集和竞价型实例集的目标容量	100,000 [1]
EC2 队列请求或 Spot 队列请求不能跨区域。	
EC2 队列请求或 Spot 队列请求不能跨同一可用区内的不同子网。	

[1] 这些限制同时适用于您的 EC2 实例集和竞价型实例集。

[2] 这些是硬配额。您无法请求增加这些配额。

[3] 删除 EC2 实例集或取消竞价型实例集请求之后，如果您指定在您删除或取消请求时该实例集不应终止其竞价型实例，实例集请求将输入 `deleted_running`（EC2 实例集）或 `cancelled_running`（竞价型实例集）状态，并且实例将继续运行直至它们中断或您手动将其终止。如果终止这些实例，实例集请求将输入 `deleted_terminating`（EC2 实例集）或 `cancelled_terminating`（竞价型实例集）状态，并且不计入此配额。有关更多信息，请参阅 删除 EC2 队列 (p. 867) 和 取消 Spot 队列请求 (p. 911)：

[4] 此配额仅适用于 `request` 或 `maintain` 类型的实例集。此配额不适用于 `instant` 实例集。

请求增加目标容量配额

如果您需要的容量超出目标容量的默认配额，您可以在此请求增加配额。

请求增加目标容量配额

1. 打开 Amazon Web Services Support Center 的 Create case（创建案例）表。
2. 选择 Service Limit increase (提高服务限制)。
3. 对于 Limit type（限制类型），选择 EC2 Fleet（EC2 实例集）。
4. 对于 Region（区域），选择请求增加配额的 Amazon 区域。
5. 对于 Limit（限制），选择 Target Fleet Capacity per Fleet (in units)（每个实例集的目标实例集容量（单位））或 Target Fleet Capacity per Region (in units)（每个区域的目标实例集容量（单位）），具体取决于您要增加的配额。
6. 对于 New limit value（新增限制值），输入新的配额值。
7. 要请求增加其他配额，选择 Add another request（添加另一个请求），然后重复步骤 4-6。
8. 对于 Use case description（使用案例描述），输入请求增加配额的原因。
9. 在 Contact options（联系选项）下，指定您首选的联系语言和联系方式。
10. 选择 Submit（提交）。

监控 Amazon EC2

监控是保持 Amazon Elastic Compute Cloud (Amazon EC2) 实例和Amazon解决方案的可靠性、可用性和性能的重要部分。您的 Amazon 解决方案的所有组成部分都应收集监控数据，以便更轻松地调试出现的多点故障。但是，在开始监控 Amazon EC2 前，您应创建包括以下内容的监控计划：

- 您的监控目标是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

在定义监控目标并创建监控计划后，下一步是在您的环境中建立正常 Amazon EC2 性能的基准。您应该在不同时间和不同负载条件下测量 Amazon EC2 的性能。监控 Amazon EC2 时，您应存储所收集的监控数据的历史记录。您可将当前 Amazon EC2 性能与这些历史数据进行比较，这样可帮助您确定性能的正常模式和异常模式，找出解决问题的方法。例如，您可以监控 EC2 实例的 CPU 使用率、磁盘 I/O 和网络使用率。如果性能低于您所建立的基准，则您可能需要重新配置或优化实例以降低 CPU 使用率、改进磁盘 I/O 或减少网络流量。

要建立基准，您至少应监控以下各项：

要监控的项目	Amazon EC2 指标	监控代理/CloudWatch Logs
CPU 使用率	CPU 利用率 (p. 1002)	
网络使用率	NetworkIn (p. 1002) 网络输出 (p. 1002)	
磁盘性能	磁盘读取操作 (p. 1002) 磁盘写入操作 (p. 1002)	
磁盘读取/写入	磁盘读取字节数 (p. 1002) 磁盘写入字节数 (p. 1002)	
内存利用率、磁盘交换利用率、磁盘空间利用率、页面文件利用率、日志收集		[Linux 和 Windows Server 实例] 使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器收集指标和日志 [在 Windows Server 实例上从以前的 CloudWatch Logs 代理迁移] 将 Windows Server 实例日志收集迁移到 CloudWatch 代理

自动和手动监控

Amazon提供各种可以用来监控 Amazon EC2 的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。

监控工具

- 自动监控工具 (p. 973)
- 手动监控工具 (p. 974)

自动监控工具

您可以使用以下自动化监控工具来查看 Amazon EC2 并在出现错误时向您报告：

- 系统状态检查 – 监控使用您的实例所需的Amazon系统，以确保这些系统正常工作。这些检查会检测出需要 Amazon 参与修复的实例问题。当一个系统状态检查故障时，您可以等待 Amazon 修复故障，或者您也可以亲自解决该故障（例如，通过停止和重启或终止和替换实例）。导致系统状态检查出现故障的问题示例包括：
  - 网络连接丢失
  - 系统电源损耗
  - 物理主机上的软件问题
  - 物理主机上影响到网络连接状态的硬件问题

  有关更多信息，请参阅实例的状态检查 (p. 975)。
- 实例状态检查 – 监控各个实例的软件和网络配置。这些检查检测需要您参与修复的问题。一旦发生实例状态检查故障，一般需要都您亲自解决这些问题（例如，通过重启实例或者在您的操作系统中进行修改）。可能导致实例状态检查出现故障的问题示例包括：
  - 系统状态检查故障
  - 网络或启动配置错误
  - 内存耗尽
  - 文件系统损坏
  - 内核不兼容

  有关更多信息，请参阅实例的状态检查 (p. 975)。
- Amazon CloudWatch 警报 – 在您指定的时间段内监控单个指标，并根据指标值在一些时间段内与给定阈值的对比情况执行一个或多个操作。操作是一个发送到 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略的通知。警报只会调用操作进行持续的状态变更。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态，该状态必须改变并在指定数量的时间段内一直保持。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。
- Amazon EventBridge – 自动执行Amazon服务并自动响应系统事件。Amazon服务中的事件将近实时传输到 EventBridge，并且您可以指定要在事件匹配您编写的规则时执行的自动操作。有关更多信息，请参阅什么是 Amazon EventBridge？。
- Amazon CloudWatch Logs – 监控、存储和访问来自 Amazon EC2 实例、Amazon CloudTrail 或其他来源的日志文件。有关更多信息，请参阅 Amazon CloudWatch Logs 用户指南。
- CloudWatch 代理 – 从 EC2 实例和本地服务器上的主机和访客中收集日志和系统级指标。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器中收集指标和日志。
- 适用于 Microsoft System Center Operations Manager 的 Amazon Management Pack – 将 Amazon EC2 实例与在其中运行的 Windows 或 Linux 操作系统相关联。Amazon 管理包是 Microsoft System Center Operations Manager 的一种扩展程序。它使用数据中心内的指定计算机（称为观察程序节点）和 Amazon Web Services API 远程发现并收集 Amazon 资源的相关信息。有关更多信息，请参阅适用于 Microsoft System Center 的 Amazon 管理包。

手动监控工具

监控 Amazon EC2 的另一重要部分需要手动监控一些项目，监控脚本、状态检查和 CloudWatch 警报并不考察这些项目的指标。Amazon EC2 和 CloudWatch 控制台控制面板提供您的 Amazon EC2 环境状态的概览视图。

- Amazon EC2 控制面板显示：
  - 按区域显示服务运行状况和计划的事件
  - 实例状态
  - 状态检查
  - 警报状态
  - 实例指标详细信息（在导航窗格中，选择 Instances (实例) 以选择一个实例，然后选择 Monitoring (监控) 选项卡）
  - 卷指标详细信息（在导航窗格中，选择 Volumes (卷) 以选择一个卷，然后选择 Monitoring (监控) 选项卡）
- Amazon CloudWatch 控制面板显示：
  - 当前警报和状态
  - 告警和资源图表
  - 服务运行状况

  此外，您还可以使用 CloudWatch 执行以下操作：
  - 将 Amazon EC2 监控数据绘制成图表以排除问题和发现趋势
  - 搜索并浏览您所有的 Amazon 资源指标
  - 创建和编辑警报以接收有关问题的通知
  - 一目了然地查看您的警报和 Amazon 资源的概览信息

监控最佳实践

使用以下监控最佳实践，帮助您执行 Amazon EC2 监控任务。

- 让监控成为优先事务，阻止小问题演变为大问题。
- 创建并实施从 Amazon 解决方案各个部分收集监控数据的监控计划，以便更轻松地调试发生的多点故障。您的监控计划至少应该解决以下问题：
  - 您的监控目标是什么？
  - 您将监控哪些资源？
  - 监控这些资源的频率如何？
  - 您将使用哪些监控工具？
  - 谁负责执行监控任务？
  - 出现错误时应通知谁？
- 尽可能自动监控任务。
- 检查 EC2 实例的日志文件。

监控实例状态

您可以通过查看实例的状态检查和计划事件来监控您的实例状态。

状态检查反映 Amazon EC2 自动检查的结果信息。这些自动检查会检测出指定的问题是否影响您的实例。该状态检查信息与 Amazon CloudWatch 提供的数据一起为您的每一个实例提供详细的操作可视性。

您也可以查看为实例计划的特定事件的状态。事件状态提供了有关为实例计划的未来各项活动的信息，例如重启或停用。它们还提供了各个事件的计划开始时间和结束时间。

目录

- 实例的状态检查 (p. 975)
- 实例的状态更改事件 (p. 979)
- 实例的计划事件 (p. 981)

实例的状态检查

使用实例状态监控，您可以快速确定 Amazon EC2 是否已经检测到可能阻止您的实例运行应用程序的任何问题。Amazon EC2 会对每个运行的 EC2 实例执行自动检查以识别硬件和软件问题。您可以通过查看这些状态检查的结果来识别特定的和可检测的问题。事件状态数据扩充了 Amazon EC2 已提供的有关每个实例状态（如 `pending`、`running`、`stopping`）的信息以及 Amazon CloudWatch 监控的利用率指标（CPU 利用率、网络流量和磁盘活动）。

状态检查每分钟进行一次，会返回一个通过或失败状态。如果所有的检查都通过，则实例的整体状态是OK。如果有一个或多个检查故障，则整体状态为受损。状态检查是内置到 Amazon EC2 中的，所以不能禁用或删除。

当状态检查失败时，状态检查的相应 CloudWatch 指标将增加。有关更多信息，请参阅状态检查指标 (p. 1007)。您可以使用这些指标创建基于状态检查结果触发的 CloudWatch 警报。例如，您可以创建一个警报来提醒您在一个指定实例上的状态检查中返回了故障状态。有关更多信息，请参阅创建和编辑状态检查警报 (p. 978)。

您也可以创建 Amazon CloudWatch 警报，用于监控 Amazon EC2 实例并在实例由于潜在问题而受损时自动恢复实例。有关更多信息，请参阅恢复实例 (p. 640)。

目录

- 状态检查类型 (p. 975)
- 查看状态检查 (p. 976)
- 报告实例状态 (p. 977)
- 创建和编辑状态检查警报 (p. 978)

状态检查类型

状态检查可分为两种类型：系统状态检查和实例状态检查。

系统状态检查

系统状态检查监控您的实例在其上运行的 Amazon 系统。这些检查会检测出需要 Amazon 参与修复的深层实例问题。如果系统状态检查失败，您可以选择等待 Amazon 修复问题，也可以自行解决问题。对于由 Amazon EBS 支持的实例，您也可自行停止和启动实例，在大多数情况下，这会导致实例被迁移至新的主机。对于由实例存储支持的 Linux 实例，您可以终止并替换实例。对于 Windows 实例，根卷必须是 Amazon EBS 卷；根卷不支持实例存储。请注意，实例存储卷是临时的，实例停止后所有数据都会丢失。

以下是可能导致系统状态检查失败的问题的示例：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上影响到网络连接状态的硬件问题

Note

如果在裸机实例上从操作系统重新启动，系统状态检查可能会暂时返回失败状态。当实例变为可用时，系统状态检查应返回通过状态。

实例状态检查

实例状态检查 监控各个实例的软件和网络配置。Amazon EC2 通过向网络接口 (NIC) 发送地址解析协议 (ARP) 请求，检查实例的运行状况。这些检查检测需要您参与修复的问题。如果实例状态检查失败，通常必须由您自行解决问题（例如，重启实例或更改实例配置）。

以下是可能导致实例状态检查失败的问题的示例：

- 系统状态检查故障
- 网络或启动配置不正确
- 内存耗尽
- 文件系统损坏
- 内核不兼容

Note

如果在裸机实例上从操作系统重新启动，实例状态检查可能会暂时返回失败状态。当实例变为可用时，实例状态检查应返回通过状态。

查看状态检查

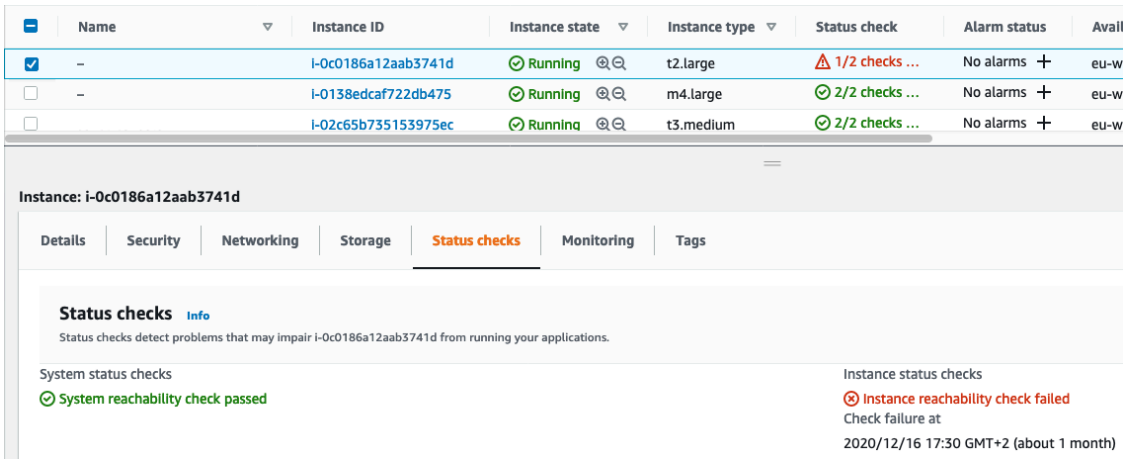
您可以使用 Amazon EC2 控制台或 Amazon CLI 来查看和使用状态检查。

使用控制台查看状态

要使用 Amazon EC2 控制台查看状态检查，请执行以下步骤。

查看状态检查（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 实例页面上的状态检查列中会列出每个实例的运行状态。
4. 要查看特定实例的状态，请选择该实例，然后选择 Status Checks（状态检查）选项卡。



如果实例状态检查失败，通常必须由您自行解决问题（例如，通过重启实例或更改实例配置）。要自行解决系统或实例状态检查失败问题，请参阅 通过故障状态检查来排查实例问题 (p. 1704)。

5. 要查看状态检查的 CloudWatch 指标，选择实例，然后选择 Monitoring (监控) 选项卡。滚动，直到您看到以下指标的图表：

   - 状态检查失败（任意）
   - 状态检查失败（实例）
   - 状态检查失败（系统）

使用命令行查看状态

您可以使用 describe-instance-status (Amazon CLI) 命令查看正在运行的实例的状态检查。

要查看所有实例的状态，请使用以下命令。

```
aws ec2 describe-instance-status
```

要获取实例状态为 `impaired` 的所有实例的状态，请使用以下命令。

```
aws ec2 describe-instance-status \
    --filters Name=instance-status.status,Values=impaired
```

要获取单一实例的状态，请使用以下命令。

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

或者，使用以下 命令：

- Get-EC2InstanceStatus (Amazon Tools for Windows PowerShell)
- DescribeInstanceStatus（Amazon EC2 查询 API）

如果您的实例发生了状态检查故障，请参阅 通过故障状态检查来排查实例问题 (p. 1704)。

报告实例状态

如果您的实例出现了问题但其状态并未显示为受损，或者如果您想要向 Amazon 发送有关您遇到的受损实例问题的更多详细信息，您可提供反馈。

我们利用报告的反馈来识别影响到多数客户的问题，但不会对单独的账户问题做出回应。提供反馈并不会改变您当前看到的实例状态检查结果。

使用控制台报告状态反馈

报告实例状态（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例，选择状态检查选项卡，选择操作（页面下半部分中的第二个操作菜单），然后选择报告实例状态。
4. 填写报告实例状态表单，然后选择提交。

使用命令行报告状态反馈

可以使用 report-instance-status (Amazon CLI) 命令发送有关受损实例状态的反馈。

```
aws ec2 report-instance-status \
    --instances i-1234567890abcdef0 \
    --status impaired \
    --reason-codes code
```

或者，使用以下 命令：

- Send-EC2InstanceStatus (Amazon Tools for Windows PowerShell)
- ReportInstanceStatus（Amazon EC2 查询 API）

创建和编辑状态检查警报

您可以使用状态检查指标 (p. 1007)创建 CloudWatch 警报，以在实例的状态检查失败时向您发送通知。

使用控制台创建状态检查警报

使用以下过程配置一个警报，当实例的状态检查失败时，该警报将通过电子邮件向您发送通知，或者停止、终止或恢复实例。

创建状态检查警报（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例，选择状态检查选项卡，然后依次选择操作、创建状态检查警报。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面的 Add or edit alarm（添加或编辑警报）下，选择 Create an alarm（创建警报）。
5. 对于警报通知，打开开关以配置 Amazon Simple Notification Service (Amazon SNS) 通知。选择现有 Amazon SNS 主题或输入名称来创建新主题。

   如果您向收件人列表添加了电子邮件地址或创建了新的主题，则 Amazon SNS 将向每个新地址发送一封订阅确认电子邮件。每个收件人必须通过选择该邮件中包含的链接来确认订阅。警报通知仅发送至经过确认的地址。
6. 对于警报操作，打开开关以指定触发警报时要执行的操作。选择操作。
7. 对于警报阈值，请指定警报的指标和条件。

   您可以保留 Group samples by（样本分组方式）和 Type of data to sample（要采样的数据类型）的原定设置 [Average（平均值）和 Status check failed:either（状态检查失败：任一）]，也可以根据自己的需求进行更改。

   在 Consecutive period（连续周期）中，设置要评估的周期数，然后在 Period（时间段）中输入评估时间段的持续时间，此评估时间段结束后才会触发警报并发送电子邮件。
8. （可选）对于样本指标数据，选择添加到控制面板。
9. 选择 Create（创建）。

在您需要更改实例状态警报时，您可以对其进行编辑。

使用控制台编辑状态检查警报

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。

3. 选择所需实例，然后依次选择操作、监控、管理 CloudWatch 警报。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面的 Add or edit alarm（添加或编辑警报）下，选择 Edit an alarm（编辑警报）。
5. 对于 Search for alarm（搜索警报），选择警报。
6. 完成更改后，选择 Update（更新）。

使用 Amazon CLI 创建状态检查警报

在以下示例中，当实例的实例检查或系统状态检查在至少两个期间连续失败后，警报将向 SNS 主题 `arn:aws:sns:us-west-2:111122223333:my-sns-topic` 发送通知。使用的 CloudWatch 指标为 `StatusCheckFailed`。

使用 Amazon CLI 创建状态检查警报

1. 选择一个现有 SNS 主题或创建一个新的主题。有关更多信息，请参阅 Amazon Command Line Interface 用户指南中的在您的 Amazon SNS 中使用 Amazon CLI。
2. 使用以下 list-metrics 命令查看 Amazon EC2 的可用 Amazon CloudWatch 指标。

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. 使用以下 put-metric-alarm 命令创建警报。

```
aws cloudwatch put-metric-alarm --alarm-name StatusCheckFailed-Alarm-for-
i-1234567890abcdef0 --metric-name StatusCheckFailed --namespace AWS/EC2 --
statistic Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --unit
 Count --period 300 --evaluation-periods 2 --threshold 1 --comparison-operator
 GreaterThanOrEqualToThreshold --alarm-actions arn:aws:sns:us-west-2:111122223333:my-
sns-topic
```

周期为收集 Amazon CloudWatch 指标所需的时间范围（以秒为单位）。此示例使用 300，这是 60 秒乘以 5 分钟得到的结果。评估期是必须将指标数值与阈值相比较的连续周期数。此示例使用 2。警报操作是要在此警报触发时执行的操作。此示例将此警报配置为使用 Amazon SNS 发送电子邮件。

实例的状态更改事件

当实例状态发生更改时，Amazon EC2 会向 Amazon EventBridge 发送 `EC2 Instance State-change Notification` 事件。

以下是此事件的示例数据。在此示例中，实例进入了 `pending` 状态。

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

state 可使用的值为：

- pending
- running
- stopping
- stopped
- shutting-down
- terminated

当您启用或启动实例时，它会进入 pending 状态，然后进入 running 状态。当您停止实例时，它会进入 stopping 状态，然后进入 stopped 状态。当您终止实例时，它会进入 shutting-down 状态，然后进入 terminated 状态。

在实例状态更改时接收电子邮件通知

若要在实例状态更改时接收电子邮件通知，请创建一个 Amazon SNS 主题，然后为 EC2 Instance State-change Notification 事件创建一条 EventBridge 规则。

创建 SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择 Create topic（创建主题）。
4. 对于 Type（类型），选择 Standard（标准）。
5. 对于 Name（名称），请为主题输入一个名称。
6. 选择 Create topic（创建主题）。
7. 选择 Create subscription（创建订阅）。
8. 对于协议，选择电子邮件。
9. 对于 Endpoint（端点），请输入接收通知的电子邮件地址。
10. 选择 Create subscription（创建订阅）。
11. 您将收到电子邮件消息，其主题行为：Amazon Notification - Subscription Confirmation。请按照说明确认订阅。

创建 EventBridge 规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于 Name（名称），请为规则输入一个名称。
4. 对于 Rule type（规则类型），选择 Rule with an event pattern（具有事件模式的规则）。
5. 选择 Next（下一步）。
6. 对于 Event pattern（事件模式），执行以下操作：
   a. 对于事件源，选择 Amazon Web Services。
   b. 对于 Amazon Web Service，请选择 EC2。
   c. 对于事件类型，请选择 EC2 实例状态更改通知。
   d. 默认情况下，我们会就任何实例的任何状态更改发送通知。如果愿意，您可以选择特定状态或特定实例。
7. 选择 Next（下一步）。
8. 按以下操作指定目标：

a. 对于 Target types（目标类型），选择 Amazon Web Service。
b. 对于 Select a target（选择一个目标），选择 SNS topic（SNS 主题）。
c. 对于 Topic（主题），请选择您在上一步中创建的 SNS 主题。

9. 选择 Next（下一步）。
10. （可选）向规则添加标签。
11. 选择 Next（下一步）。
12. 选择 Create rule（创建规则）。
13. 为测试规则，请发起状态更改。例如，开始已停止的实例、停止正在运行的实例或启动实例。您将收到电子邮件消息，其主题行为：Amazon Notification Message。电子邮件正文包含事件数据。

实例的计划事件

Amazon 可为您的实例计划事件，例如重启、停止/启动或停用。这些事件不会频繁发生。如果您的一个实例将受某计划事件影响，则 Amazon 将在该计划事件发生之前向与您的 Amazon 账户关联的电子邮件地址发送电子邮件。该电子邮件将提供有关该事件的详细信息，包括开始和结束日期。根据事件的不同，您也许能够采取操作来控制事件的发生时间。Amazon 还会发送 Amazon Health 事件，您可以使用 Amazon CloudWatch Events 对该事件进行监控和管理。有关使用 CloudWatch 监控 Amazon Health 事件的详细信息，请参阅使用 CloudWatch Events 监控 Amazon Health 事件。

计划的事件由 Amazon 管理；您无法为实例计划事件。您可以查看由 Amazon，在计划重新启动、停用或停止实例时执行操作。

要更新账户的联系人信息以确保获得有关计划事件的通知，请转至 Account Settings 页。

> **Note**
>
> 当实例受计划事件的影响并且它属于自动扩缩组的一部分时，Amazon EC2 Auto Scaling 最终将其替换为其运行状况检查的一部分，您无需采取进一步措施。有关由 Amazon EC2 Auto Scaling 执行的运行状况检查的更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的 Auto Scaling 实例的运行状况检查。

目录

- 计划的事件类型 (p. 981)
- 查看计划的事件 (p. 982)
- 使用计划停止或停用的实例 (p. 985)
- 使用计划重启的实例 (p. 985)
- 使用计划维护的实例 (p. 987)
- 重新安排计划的事件 (p. 987)
- 定义计划事件的事件窗口 (p. 989)

计划的事件类型

Amazon EC2 可以创建以下类型的实例事件，其中事件在计划的时间发生：

- 实例停止：实例在计划的时间停止。再次启动实例时，实例会迁移至新主机。仅适用于 Amazon EBS 支持的实例。
- 实例停用：在计划的时间，由 Amazon EBS 支持的实例将停止；由实例存储支持的实例将终止。
- 实例重启：在计划的时间实例重启。
- 系统重启：在计划的时间实例的主机重启。
- 系统维护：在计划的时间，实例可能会因网络维护或电源维护受到暂时的影响。

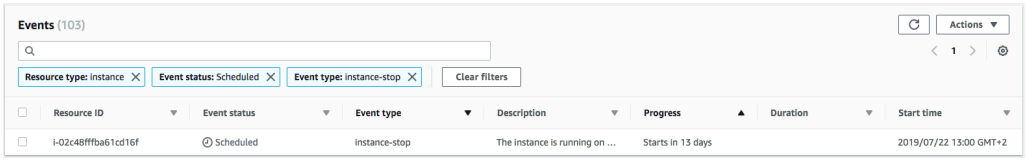
查看计划的事件

除了通过电子邮件接收计划事件的通知外，您还可使用以下方法之一查看计划的事件。

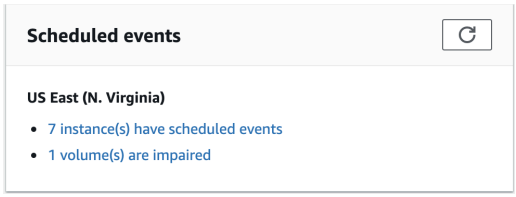
New console

使用控制台查看实例的计划事件

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 您可以在以下屏幕中查看计划的事件：
   - 在导航窗格中，选择 Events。将显示与事件关联的所有资源。您可以按 Resource ID (资源 ID)、Resource type (资源类型)、Availability zone (可用区)、Event status (事件状态) 或 Event type (事件类型) 进行筛选。



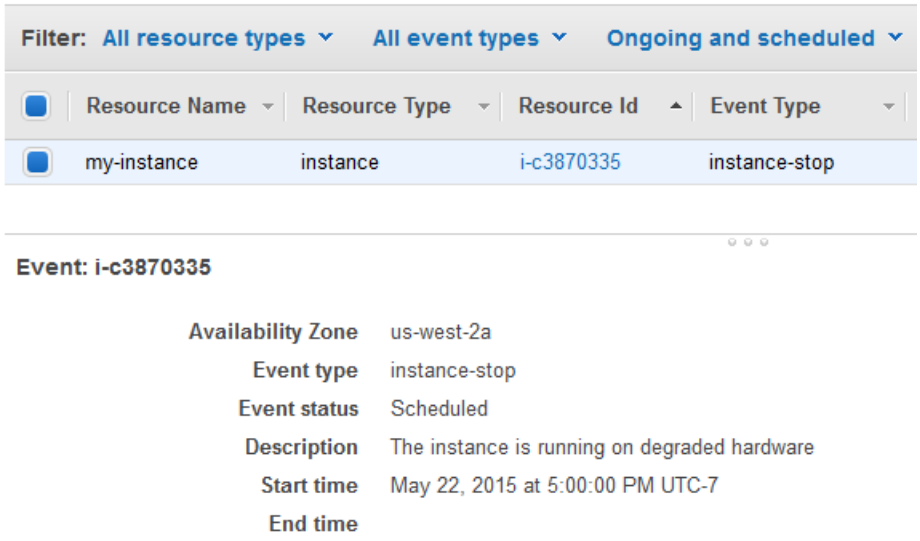
   - 或者，在导航窗格中，选择 EC2 Dashboard。计划的事件下将显示与事件关联的所有资源。



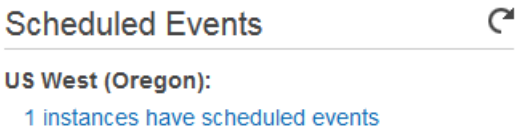
Old console

使用控制台查看实例的计划事件

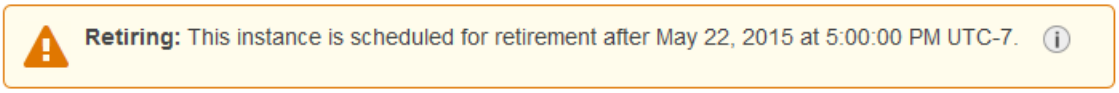
1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 您可以在以下屏幕中查看计划的事件：
   - 在导航窗格中，选择 Events。将显示与事件关联的所有资源。您可按资源类型或按特定事件类型进行筛选。您可选择资源来查看详细信息。



- 或者，在导航窗格中，选择 EC2 Dashboard。Scheduled Events 下将显示与事件关联的所有资源。



- 还将显示受影响资源的一些事件。例如，在导航窗格中，选择 Instances (实例)，然后选择一个实例。如果所选实例具有关联的实例停止或实例停用事件，则该事件将显示在底部窗格中。



Amazon CLI

使用 Amazon CLI 查看实例的计划事件

使用 describe-instance-status 命令。

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

以下示例输出显示重启事件：

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

以下示例输出显示实例停用事件。

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

使用 Amazon Tools for Windows PowerShell 查看实例的计划事件

使用以下 Get-EC2InstanceStatus 命令。

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

以下示例输出显示实例停用事件。

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

使用实例元数据查看实例的计划事件

您可以使用实例元数据服务版本 2 或实例元数据服务版本 1 从实例元数据 (p. 754)中检索有关实例的活动维护事件的信息。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

以下是 JSON 格式的计划系统重启事件信息的示例输出。

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

使用实例元数据查看有关实例的已完成或已取消事件的事件历史记录

您可以使用实例元数据服务版本 2 或实例元数据服务版本 1 从实例元数据 (p. 754)中检索有关已完成或已取消的事件的信息。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

以下是 JSON 格式的已取消和已完成系统重启事件相关信息的示例输出。

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

Amazon Health

您可以使用 Amazon Health Dashboard 了解可能影响您的实例的事件。Amazon Health Dashboard 会分三组管理问题：未处理问题、已计划更改和其他通知。已计划更改组包含正在进行或即将进行的项目。

有关更多信息，请参阅 Amazon Health 用户指南中的 Amazon Health Dashboard 入门。

使用计划停止或停用的实例

当 Amazon 检测到您的实例的基础主机存在无法修复的故障时，它将计划实例停止或终止，这取决于实例根设备的类型。如果根设备为 EBS 卷，则将计划实例停止。如果根设备为实例存储卷，则将计划实例终止。有关更多信息，请参阅实例指令引退 (p. 632)。

Important

实例停止、休眠或终止后，实例存储卷上存储的所有数据都会丢失。这包括附加到使用 EBS 卷作为根设备的实例的实例存储卷。在实例停止、休眠或终止之前，请务必保存实例存储卷中以后可能需要的数据。

Amazon EBS 支持的实例操作

您可等待实例按计划停止。您也可自行停止并启动实例，这会将实例迁移至新的主机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 停止和启动您的实例 (p. 610)。

您可以自动化立即停止并启动以响应计划的实例停止事件。有关更多信息，请参阅 Amazon Health 用户指南中的自动化 EC2 实例的操作。

实例存储支持的实例的操作

建议您在实例按计划终止之前，从最新的 AMI 启动替代实例并将所有必需数据迁移至替代实例。然后，您可终止原始实例，或等待其按计划终止。

使用计划重启的实例

当 Amazon 必须执行安装更新或维护基础主机等任务时，它可计划实例或基础主机进行重启。您可以重新计划大部分重启事件 (p. 987)，以便您的实例在适合您的特定日期和时间重启。

如果您停止链接的 EC2-Classic 实例 (p. 1203)，它会自动取消与 VPC 的链接，并且 VPC 安全组不再与实例关联。您可以在重新启动之后，再次将实例链接到 VPC。

查看重启事件类型

您可以使用以下方法之一来查看某个重启事件是实例重启还是系统重启。

New console

使用控制台查看计划重启事件的类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Resource type: instance (资源类型：实例)。
4. 对于每个实例，查看 Event Type (事件类型) 列中的值。该值为 system-reboot 或 instance-reboot。

Old console

使用控制台查看计划重启事件的类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Instance resources (实例资源)。
4. 对于每个实例，查看 Event Type (事件类型) 列中的值。该值为 system-reboot 或 instance-reboot。

Amazon CLI

使用 Amazon CLI 查看计划重启事件的类型

使用 describe-instance-status 命令。

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

对于计划的重启事件，Code 的值是 system-reboot 或 instance-reboot。以下示例输出显示 system-reboot 事件。

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

实例重启操作

您可以等待实例重启在计划的维护时段进行，或者重新计划 (p. 987)实例重启在适合您的日期和时间进行，或者在您方便的时间自行重新启动 (p. 631)实例。

在实例重启之后，将清除计划的事件并更新事件说明。底层主机上的所有挂起维护都会完成，并且在实例完全启动后，即可再次开始使用您的实例。

系统重启操作

您无法自行重启系统。您可以等待系统重启在计划的维护时段进行，或者您可以重新计划 (p. 987)系统重启在适合您的日期和时间进行。系统重启通常在几分钟内完成。在系统重启之后，实例将保留其 IP 地址和 DNS 名称，并且本地实例存储卷上的任何数据将会得到保留。在系统重启完成之后，将清除实例的计划事件，并且您可验证实例上的软件是否按预期运行。

或者，如果有必要在其他时间维护实例，并且您无法重新计划系统重启，则您可以停止并启动 Amazon EBS 支持的实例，这会将它迁移到新主机。但是，本地实例存储卷上的数据将不会保留。您也可以自动化立即停止并启动实例以响应计划的系统重启事件。有关更多信息，请参阅 Amazon Health 用户指南中的自动化 EC2 实例的操作。对于由实例存储支持的实例，如果您无法重新计划系统重启，可在计划的维护时段之前从最新的 AMI 启动替代实例，并将所有必需数据迁移至替代实例，然后终止原始实例。

使用计划维护的实例

当 Amazon 必须维护实例的基础主机时，它将计划实例的维护。维护事件有两种：网络维护和电源维护。

在网络维护期间，计划的实例会在短时间内失去网络连接。在维护完成后，将恢复与实例的正常网络连接。

在电源维护期间，计划的实例将短时间脱机，然后重启。执行重启后，将保留您的所有实例的配置设置。

在实例重启后 (这通常需要几分钟)，验证您的应用程序是否按预期运行。此时，您的实例应该不再具有与之关联的计划事件，或者如果有，该计划事件的描述应该以 [Completed] 开头。实例状态说明的刷新有时需要长达 1 个小时。已完成的维护事件将在 Amazon EC2 控制台面板上显示长达一周时间。

Amazon EBS 支持的实例操作

您可等待维护按计划进行。您也可停止并启动实例，这会将实例迁移至新的主机。有关停止实例的更多信息，以及有关实例停止时的实例配置更改的信息，请参阅 停止和启动您的实例 (p. 610)。

您可以自动化立即停止并启动以响应计划维护事件。有关更多信息，请参阅 Amazon Health 用户指南中的自动化 EC2 实例的操作。

实例存储支持的实例的操作

您可等待维护按计划进行。或者，如果您想在计划的维护时间段内保持正常操作，可在计划的维护时间段之前从最新的 AMI 启动替代实例，并将所有必需数据迁移至替代实例，然后终止原始实例。

重新安排计划的事件

您可以重新安排一个事件，以便它在适合您的特定日期和时间发生。只有具有截止期限的事件才可以重新计划。重新计划事件还有其他限制 (p. 989)。

您可以使用以下方法之一重新计划事件。

New console

使用控制台重新安排事件

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Resource type: instance (资源类型：实例)。
4. 选择一个或多个实例，然后依次选择 Actions (操作)、Schedule Event (计划事件)。

只有具有事件截止期限（由 Deadline (截止期限) 值指示）的事件才可以重新计划。如果某个选定的事件没有截止期限，则会禁用 Actions (操作) 下的 Schedule Event (计划事件)。

5. 对于 New start time (新的开始时间)，为事件输入新的日期和时间。新的日期和时间必须早于 Event deadline (事件截止期限)。
6. 选择 Save（保存）。

   更新的事件开始时间可能需要一两分钟才会反映在控制台中。

Old console

使用控制台重新安排事件

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 从筛选器列表中选择 Instance resources (实例资源)。
4. 选择一个或多个实例，然后选择 Actions (操作) 和 Schedule Event (计划事件)。

   只有具有事件截止日期（由 Event Deadline (事件截止期限) 的值指示）的事件才可以重新计划。
5. 对于 Event start time (事件开始时间)，为事件输入新的日期和时间。新的日期和时间必须早于 Event Deadline (事件截止期限)。
6. 选择 Schedule Event (计划事件)。

   更新的事件开始时间可能需要一两分钟才会反映在控制台中。

Amazon CLI

使用 Amazon CLI 重新安排事件

1. 只有具有事件截止日期（由 `NotBeforeDeadline` 的值指示）才可以重新计划。使用 describe-instance-status 命令查看 `NotBeforeDeadline` 参数值。

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

   以下示例输出显示因 `system-reboot` 包含值而可以重新计划的 `NotBeforeDeadline` 事件。

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

2. 若要重新计划事件，应使用 modify-instance-event-start-time 命令。使用 `not-before` 参数指定新的事件开始时间。新的事件开始时间必须早于 `NotBeforeDeadline`。

```
aws ec2 modify-instance-event-start-time --instance-id i-1234567890abcdef0
 --instance-event-id instance-event-0d59937288b749b32 --not-
before 2019-03-25T10:00:00.000
```

在 describe-instance-status 命令返回更新的 `not-before` 参数值之前可能需要一两分钟。

限制

- 只有具有事件截止日期的事件才可以重新计划。可以将事件重新计划到事件截止日期之前的日期。控制台中的 Deadline (截止期限) 列和 `NotBeforeDeadline` 中的 Amazon CLI 字段指示了事件是否具有截止期限。
- 只有尚未开始的事件才可以重新计划。控制台中的 Start time (开始时间) 列和 `NotBefore` 中的 Amazon CLI 字段指示了事件的开始时间。还有 5 分钟便要按计划开始的事件无法重新计划。
- 新的事件开始时间离当前时间必须至少有 60 分钟。
- 如果您使用控制台重新计划多个事件，则事件截止期限由具有最早的事件截止期限的事件决定。

定义计划事件的事件窗口

您可以为重新启动、停止或终止 Amazon EC2 实例的计划事件定义自定义事件窗口。您可以将一个或多个实例与事件窗口关联。如果计划了这些实例的计划事件，Amazon 将在关联事件窗口中调度事件。

通过指定工作负载在非高峰期间发生的事件窗口，可以使用事件窗口最大化工作负载可用性。您还可以将事件窗口与内部维护计划保持一致。

您可以通过指定一组时间范围来定义事件窗口。最短持续时间为 2 小时。总计组合时间范围必须至少为 4 小时。

您可以使用实例 ID 或实例标签将一个或多个实例与事件窗口相关联。您还可以使用主机 ID 将专属主机与事件窗口相关联。

> Warning
>
> 事件窗口仅适用于停止、重新启动或终止实例的计划事件。
> 事件窗口不适用于：
>
> - 加速计划事件和网络维护事件。
> - 未计划维护，如 AutoRecovery 和未计划重新启动。

使用事件窗口

- 注意事项 (p. 989)
- 查看事件窗口 (p. 990)
- 创建事件窗口 (p. 991)
- 修改事件窗口 (p. 995)
- 删除事件窗口 (p. 999)
- 标记事件窗口 (p. 1000)

注意事项

- 所有事件窗口均采用 UTC 时间。
- 每周活动窗口的最短持续时间为 4 小时。
- 事件窗口内的时间范围必须至少为 2 小时。
- 一个事件窗口只能关联一个目标类型（实例 ID、专属主机 ID 或实例标签）。
- 一个目标（实例 ID、专属主机 ID 或实例标签）只能关联一个事件窗口。
- 一个事件窗口最多可以关联 100 个实例 ID 或 50 个专属主机 ID 或 50 个实例标签。实例标签可以关联任意数量的实例。

- 每个 Amazon 区域最多可以创建 200 个事件窗口。
- 与事件窗口关联的多个实例可能会同时发生计划的事件。
- 如果 Amazon 已计划事件，修改事件窗口不会更改计划事件的时间。如果事件有截止日期，您可以重新计划事件 (p. 987)。
- 您可以在计划事件发生之前停止和启动实例，将实例迁移到新主机，且计划事件不再发生。

查看事件窗口

您可以使用以下方法之一查看事件窗口。

Console

使用控制台查看事件窗口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 选择 Actions (操作)，然后选择 Manage event windows (管理事件窗口)。
4. 选择事件窗口以查看其详细信息。

Amazon CLI

使用 Amazon CLI 描述所有事件窗口

使用 describe-instance-event-windows 命令。

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

预期输出

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

使用 Amazon CLI 描述特定事件窗口

使用 describe-instance-event-windows 命令与 `--instance-event-window-id` 参数来描述特定事件窗口。

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

使用 Amazon CLI 描述符合一个或多个筛选条件的事件窗口

使用 describe-instance-event-windows 命令与 `--filters` 参数。在下面的示例中，`instance-id` 筛选条件用于描述与指定实例关联的所有事件窗口。

使用筛选器时，它会进行直接匹配。但是，`instance-id` 筛选器不同。如果没有与实例 ID 直接匹配，它会回退到与事件窗口的间接关联，例如实例标签或专属主机 ID（如果实例位于专属主机）。

有关支持的筛选器的列表，请参阅 Amazon CLI 参考中的 describe-instance-event-windows。

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

预期输出

在以下示例中，实例位于与事件窗口关联的专属主机上。

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

创建事件窗口

您可以创建一个或多个事件窗口。对于每个事件窗口，您可以指定一个或多个时间块。例如，您可以创建一个带有时间块的事件窗口，发生于每天凌晨 4 点，持续 2 个小时。或者，您可以创建一个带有时间块的事件窗口，发生于星期日凌晨 2 点至凌晨 4 点以及星期三凌晨 3 点至凌晨 5 点。

有关事件窗口约束，请参阅本主题之前所述的 注意事项 (p. 989)。

事件窗口每周重复出现，直至将其删除。

使用以下方法之一创建事件窗口：

Console

使用控制台创建事件窗口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 选择 Create instance event window (创建实例事件窗口)。
4. 对于 Event window name (事件窗口名称)，输入事件窗口的描述性名称。
5. 对于 Event window schedule (事件窗口时间表)，选择通过使用 Cron schedule builder（Cron 计划生成器）或指定时间范围来指定事件窗口中的时间块。
   - 如果选择 Cron schedule builder (Cron 计划生成器)，请指定以下内容：
     1. 对于 Days (UTC) (天数(UTC))，请指定发生事件窗口的具体日期。
     2. 对于 Start time (UTC) (开始时间(UTC))，请指定事件窗口开始的时间。
     3. 对于 Duration (持续时间)，请指定事件窗口中时间块的持续时间。每个时间块的最短持续时间为 2 小时。事件窗口的最短持续时间总计必须等于或超过 4 小时。所有时间均采用 UTC。
   - 如果选择 Time ranges (时间范围)，选择 Add new time range (添加新时间范围)，并指定开始以及结束日期和时间。每个时间范围重复此操作。每个时间范围的最短持续时间为 2 小时。所有时间范围总计最小持续时间必须等于或超过 4 小时。
6. （可选）对于 Target details (目标详细信息)，将一个或多个实例与事件窗口相关联，这样如果计划维护实例，计划事件将在关联的事件窗口期间发生。您可以使用实例 ID 或实例标签将一个或多个实例与事件窗口相关联。您可以使用主机 ID 将专属主机与事件窗口相关联。

   请注意，您可以在不将目标与窗口关联的情况下创建事件窗口。稍后，您可以修改窗口以关联一个或多个目标。
7. （可选）对于 Event window tags (事件窗口标签)，选择 Add tag (添加标签)，然后输入标签键和值。对每个标签重复此操作。
8. 选择 Create event window (创建事件窗口)。

Amazon CLI

要使用 Amazon CLI 创建事件窗口，首先要创建事件窗口，然后您将一个或多个目标与事件窗口相关联。

创建事件窗口

您可以在创建事件窗口时定义一组时间范围或 Cron 表达式，但不能同时定义两者。

使用 Amazon CLI 创建有时间范围的事件窗口

使用 create-instance-event-window 命令并指定 `--time-range` 参数。您不能同时指定 `--cron-expression` 参数。

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-window,Tags=[{Key=K1,Value=V1}]"
 \
    --name myEventWindowName
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
```

```
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

使用 Amazon CLI 使用创建一个有 Cron 表达式的事件窗口

使用 create-instance-event-window 命令并指定 `--cron-expression` 参数。您不能同时指定 `--time-range` 参数。

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-window,Tags=[{Key=K1,Value=V1}]"
 \
    --name myEventWindowName
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

将目标与事件窗口关联

一个事件窗口只能关联一个目标类型（实例 ID、专属主机 ID 或实例标签）。

使用 Amazon CLI 将实例标签与事件窗口相关联

使用 associate-instance-event-window 命令并指定 `instance-event-window-id` 参数以指定事件窗口。要关联实例标签，请指定 `--association-target` 参数，并为参数值指定一个或多个标签。

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

使用 Amazon CLI 将一个或多个实例与事件窗口相关联

使用 associate-instance-event-window 命令并指定 `instance-event-window-id` 参数以指定事件窗口。要关联实例，请指定 `--association-target` 参数，并为参数值指定一个或多个实例 ID。

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

使用 Amazon CLI 将专属主机与事件窗口相关联

使用 associate-instance-event-window 命令并指定 `instance-event-window-id` 参数以指定事件窗口。要关联专属主机，请指定 `--association-target` 参数，并为参数值指定一个或多个专属主机 ID。

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
```

```
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

修改事件窗口

您可以修改事件窗口中除 ID 之外的所有字段。例如，夏令时开始时，您可能需要修改事件窗口计划。对于现有事件窗口，您可能需要添加或移除目标。

使用以下方法之一修改事件窗口：

Console

使用控制台修改事件窗口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 选择 Actions (操作)，然后选择 Manage event windows (管理事件窗口)。
4. 选择要修改的事件窗口，然后选择 Actions (操作)、Modify instance event window (修改实例事件窗口)。
5. 在事件窗口中修改字段，然后选择 Modify event window (修改事件窗口)。

Amazon CLI

要使用 Amazon CLI 修改事件窗口，您可以修改时间范围或 Cron 表达式，并将一个或多个目标与事件窗口关联或取消关联。

修改事件窗口时间

您可以在修改事件窗口时修改时间范围或 Cron 表达式，但不能同时修改两者。

使用 Amazon CLI 修改事件窗口的时间范围

使用 modify-instance-event-window 命令并指定要修改的事件窗口。指定 `--time-range` 参数以修改时间范围。您不能同时指定 `--cron-expression` 参数。

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

使用 Amazon CLI 修改事件窗口的一组时间范围

使用 modify-instance-event-window 命令并指定要修改的事件窗口。指定 `--time-range` 参数以修改时间范围。您不能在相同调用中同时指定 `--cron-expression` 参数。

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday", "EndHour": 8}]'
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
```

```
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

使用 Amazon CLI 修改事件窗口的 Cron 表达式

使用 modify-instance-event-window 命令并指定要修改的事件窗口。指定 `--cron-expression` 参数以修改 Cron 表达式。您不能同时指定 `--time-range` 参数。

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

修改与事件窗口关联的目标

您可以将其他目标与事件窗口相关联。您还可以取消现有目标与事件窗口的关联。但是，一个事件窗口只能关联一个目标类型（实例 ID、专属主机 ID 或实例标签）。

将其他目标与事件窗口相关联

有关如何将目标与事件窗口相关联的说明，请参阅 Associate a target with an event window。

使用 Amazon CLI 取消实例标签与事件窗口的关联

使用 disassociate-instance-event-window 命令并指定 instance-event-window-id 参数以指定事件窗口。要取消关联实例标签，请指定 --association-target 参数，并为参数值指定一个或多个标签。

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

使用 Amazon CLI 取消一个或多个实例与事件窗口的关联

使用 disassociate-instance-event-window 命令并指定 instance-event-window-id 参数以指定事件窗口。要取消关联实例，请指定 --association-target 参数，并为参数值指定一个或多个实例 ID。

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

使用 Amazon CLI 取消专属主机与事件窗口的关联

使用 disassociate-instance-event-window 命令并指定 instance-event-window-id 参数以指定事件窗口。要取消关联专属主机，请指定 --association-target 参数，并为参数值指定一个或多个专属主机 ID。

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

预期输出

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

删除事件窗口

您可以使用以下方法之一，一次删除一个事件窗口。

Console

使用控制台删除事件窗口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 选择 Actions (操作)，然后选择 Manage event windows (管理事件窗口)。
4. 选择要删除的事件窗口，然后选择 Actions (操作)、Delete instance event window (删除实例事件窗口)。
5. 当系统提示时，输入 **delete**，然后选择删除。

Amazon CLI

使用 Amazon CLI 删除事件窗口

使用 delete-instance-event-window 命令并指定要删除的事件窗口。

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

使用 Amazon CLI 强制删除事件窗口

使用 `--force-delete` 参数（如果事件窗口当前与目标相关联）。

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

预期输出

```
{
    "InstanceEventWindowState": {
```

```
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

标记事件窗口

您可以在创建事件窗口时或之后对其进行标记。

要在创建事件窗口时对其进行标记，请参阅 创建事件窗口 (p. 991)。

使用以下方法之一标记事件窗口。

Console

使用控制台标记现有事件窗口：

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。
3. 选择 Actions (操作)，然后选择 Manage event windows (管理事件窗口)。
4. 选择要标记的事件窗口，然后选择 Actions (操作)、Manage instance event window (管理实例事件窗口)。
5. 选择 Add tag (添加标签) 标记该窗口。对每个标签重复此操作。
6. 选择 Save（保存）。

Amazon CLI

使用 Amazon CLI 标记现有事件窗口

使用 create-tags 命令标记现有的资源。在以下示例中，使用以下标签标记现有事件窗口：键=目的，值=测试。

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

使用 CloudWatch 监控您的实例

您可以使用 Amazon CloudWatch 监控您的实例，此工具可从 Amazon EC2 收集原始数据，并将数据处理为易读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。

默认情况下，Amazon EC2 每隔 5 分钟向 CloudWatch 发送一次指标数据。要每隔 1 分钟向 CloudWatch 发送一次实例的指标数据，可以对实例启用详细监控。有关更多信息，请参阅对实例启用或禁用详细监控 (p. 1001)。

Amazon EC2 控制台将根据来自 Amazon CloudWatch 的原始数据显示一系列图表。根据您的需求，您可能更愿意从 Amazon CloudWatch 而非控制台中的图表中获取实例数据。

有关 Amazon CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南。

目录

- 对实例启用或禁用详细监控 (p. 1001)
- 列出实例的可用 CloudWatch 指标 (p. 1002)

- 获取实例的指标统计数据 (p. 1012)
- 绘制实例的指标图形 (p. 1019)
- 为实例创建 CloudWatch 警报 (p. 1020)
- 创建停止、终止、重启或恢复实例的警报 (p. 1021)

对实例启用或禁用详细监控

默认情况下，已对您的实例启用基本监控。您可以选择启用详细监控。当您启用详细监控后，Amazon EC2 控制台将以 1 分钟为间隔显示实例的监控图表。

下面介绍了实例的基本和详细监控的数据间隔和费用。

监控类型	描述	收费
基本监控	数据在 5 分钟期间内自动可用。	免费。
详细监控	数据在 1 分钟期间内可用。要获得此级别的数据，您必须为实例专门启用此监控。对于您已启用详细监控的实例，您还可以跨组 (相似实例所在组) 获得聚合数据。	您需要按发送到 CloudWatch 的每个指标付费。您无需为数据存储付费。有关更多信息，请参阅 Amazon CloudWatch 定价页面上的付费套餐和示例 1 – EC2 详细监控。

主题

- 所需的 IAM 权限 (p. 1001)
- 启用详细监控 (p. 1001)
- 禁用详细监控 (p. 1002)

所需的 IAM 权限

要启用对实例的详细监控，用户必须具有使用 MonitorInstances API 操作的权限。要关闭对实例的详细监控，用户必须具有使用 UnmonitorInstances API 操作的权限。

启用详细监控

在实例启动时或在实例运行或停止后，可对实例启用详细监控。在实例上启用详细监控不会影响对附加到实例的 EBS 卷的监控。有关更多信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)。

Console

启用对现有实例的详细监控

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择操作、监控、管理详细监控。
4. 在详细监控详细信息页面上，对于详细监控，选中启用复选框。
5. 选择 Save（保存）。

要在启动实例时启用详细监视

在使用 Amazon Web Services Management Console启动实例时，请在 Configure Instance Details 页面上选中 Monitoring 复选框。

Amazon CLI

启用对现有实例的详细监控

使用以下 monitor-instances 命令对指定实例启用详细监控。

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

要在启动实例时启用详细监视

结合使用 run-instances 命令和 --monitoring 标志来启用详细监控。

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

禁用详细监控

可以在实例启动时或在实例运行或停止后，对实例禁用详细监控。

Console

禁用详细监控

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择操作、监控、管理详细监控。
4. 在详细监控详细信息页面上，对于详细监控，清除启用复选框。
5. 选择 Save（保存）。

Amazon CLI

禁用详细监控

使用以下 unmonitor-instances 命令对指定实例禁用详细监控。

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

列出实例的可用 CloudWatch 指标

Amazon EC2 将指标发送到 Amazon CloudWatch。可使用 Amazon Web Services Management Console、Amazon CLI 或 API 列出 Amazon EC2 发送到 CloudWatch 的指标。默认情况下，每个数据点中包含的是实例自启动后的 5 分钟内的活动。如果您启用了详细监控，则每个数据点包含自启动后的 1 分钟内的活动。请注意，对于统计数据 Minimum、Maximum 和 Average，EC2 提供的指标的最小粒度为 1 分钟。

有关获取这些指标的统计数据的信息，请参阅 获取实例的指标统计数据 (p. 1012)。

目录

- 实例指标 (p. 1003)
- CPU 积分指标 (p. 1004)
- 专属主机指标 (p. 1006)
- 基于 Nitro 的实例的 Amazon EBS 指标 (p. 1006)
- 状态检查指标 (p. 1007)
- 流量镜像指标 (p. 1008)

- Auto Scaling 组指标 (p. 1008)
- Amazon EC2 指标维度 (p. 1008)
- Amazon EC2 使用情况指标 (p. 1008)
- 使用控制台列出指标 (p. 1009)
- 使用 Amazon CLI 列出指标 (p. 1011)

实例指标

AWS/EC2 命名空间包括以下实例指标。

指标	描述
CPUUtilization	当前正在实例上使用的已分配 EC2 计算单位的百分率。此指标确定在选定实例上运行应用程序所需的处理能力。 根据实例类型，如果未向实例分配整个处理器核心，则操作系统中的工具显示的百分率可能与 CloudWatch 不同。 单位：百分比
DiskReadOps	在指定时间段内从可供实例使用的所有实例存储卷完成的读取操作数。 要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。 如果没有实例存储卷，则值为 0 或不报告指标。 单位：计数
DiskWriteOps	在指定时间段内向可供实例使用的所有实例存储卷完成的写入操作数。 要计算该周期的每秒平均 I/O 操作数 (IOPS)，请将该周期的总操作数除以总秒数。 如果没有实例存储卷，则值为 0 或不报告指标。 单位：计数
DiskReadBytes	从可供实例使用的所有实例存储卷读取的字节数。 该指标用来确定应用程序从实例的硬盘读取的数据量。它可以用来确定应用程序的速度。 报告的数量是该期间内接收的字节数。如果您使用的是基本（5 分钟）监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细（1 分钟）监控，请将其除以 60。 如果没有实例存储卷，则值为 0 或不报告指标。 单位：字节
DiskWriteBytes	向可供实例使用的所有实例存储卷写入的字节数。 该指标用来确定应用程序向实例的硬盘写入的数据量。它可以用来确定应用程序的速度。

指标	描述
	报告的数量是该期间内接收的字节数。如果您使用的是基本（5 分钟）监控，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细（1 分钟）监控，请将其除以 60。 如果没有实例存储卷，则值为 0 或不报告指标。 单位：字节
MetadataNoToken	在没有令牌的情况下成功访问实例元数据服务的次数。 该指标用于确定是否有任何进程正在使用 实例元数据服务版本 1 访问实例元数据，但未使用令牌。如果所有请求都使用支持令牌的会话（即 实例元数据服务版本 2），则该值为 0。有关更多信息，请参阅转换为使用 实例元数据服务版本 2 (p. 757)。 单位：计数
NetworkIn	实例在所有网络接口上收到的字节数。此指标用于确定流向单个实例的传入网络流量。 报告的数量是该期间内接收的字节数。如果您使用的是基本（5 分钟）监控且统计数据为 Sum，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细（1 分钟）监控且统计数据为 Sum，请将其除以 60。 单位：字节
NetworkOut	实例在所有网络接口上发送的字节数。此指标用于确定来自单个实例的传出网络流量。 报告的数字是该时间段内发送的字节数。如果您使用的是基本（5 分钟）监控且统计数据为 Sum，则可以将此数字除以 300 以获得字节/秒。如果您使用的是详细（1 分钟）监控且统计数据为 Sum，请将其除以 60。 单位：字节
NetworkPacketsIn	实例在所有网络接口上收到的数据包数。此指标依据单个实例上的数据包数量来标识传入流量的量。 此指标仅可用于基本监控（5 分钟期间）。要计算实例 5 分钟内每秒收到的数据包数 (PPS)，请将 Sum 统计数据除以 300。 单位：计数
NetworkPacketsOut	实例在所有网络接口上发送的数据包数。此指标依据单个实例上的数据包数量标识传出流量的量。 此指标仅可用于基本监控（5 分钟期间）。要计算实例 5 分钟内每秒发送的数据包数（PPS），请将 Sum 统计数据除以 300。 单位：计数

CPU 积分指标

AWS/EC2 命名空间包括 可突增性能实例 (p. 274)的以下 CPU 积分指标。

指标	描述
CPUCreditUsage	实例为保持 CPU 使用率而花费的 CPU 积分数。一个 CPU 积分等于一个 vCPU 按 100% 利用率运行一分钟，或者 vCPU、利用率和时间的等效组合（例如， 一个 vCPU 按 50% 利用率运行两分钟，或者两个 vCPU 按 25% 利用率运行两分钟）。 CPU 信用指标仅每 5 分钟提供一次。如果您指定一个大于五分钟的时间段，请使用Sum 统计数据，而非 Average 统计数据。 单位：积分 (vCPU 分钟)
CPUCreditBalance	实例自启动后已累积获得的 CPU 积分数。对于 T2 标准，CPUCreditBalance 还包含已累积的启动积分数。 在获得积分后，积分将在积分余额中累积；在花费积分后，将从积分余额中扣除积分。积分余额具有最大值限制，这是由实例大小决定的。在达到限制后，将丢弃获得的任何新积分。对于 T2 标准，启动积分不计入限制。 实例可以花费 CPUCreditBalance 中的积分，以便突增到基准 CPU 使用率以上。 在实例运行过程中，CPUCreditBalance 中的积分不会过期。在 T3 或 T3a 实例停止时，CPUCreditBalance 值将保留七天。之后，所有累积的积分都将丢失。在 T2 实例停止时，CPUCreditBalance 值不会保留，并且所有累积的积分都将丢失。 CPU 信用指标仅每 5 分钟提供一次。 单位：积分 (vCPU 分钟)
CPUSurplusCreditBalance	在 unlimited 值为零时，CPUCreditBalance 实例花费的超额积分数。 CPUSurplusCreditBalance 值由获得的 CPU 积分支付。如果超额积分数超出实例可在 24 小时周期内获得的最大积分数，则超出最大积分数的已花费超额积分将产生额外费用。 CPU 信用指标仅每 5 分钟提供一次。 单位：积分 (vCPU 分钟)
CPUSurplusCreditsCharged	未由获得的 CPU 积分支付并且会产生额外费用的已花费超额积分数。 在出现以下任一情况时，将对花费的超额积分收费： • 花费的超额积分超出实例可在 24 小时周期内获得的最大积分数。对于超出最大积分数的所花费超额积分，将在该小时结束时向您收费。 • 实例已停止或终止。 • 实例从 unlimited 切换为 standard。 CPU 信用指标仅每 5 分钟提供一次。 单位：积分 (vCPU 分钟)

专属主机指标

AWS/EC2 命名空间包括 T3 专属主机的下列指标。

指标	描述
DedicatedHostCPUUtilization	在专属主机上运行的实例当前正在使用的已分配计算容量的百分比。 单位：百分比

基于 Nitro 的实例的 Amazon EBS 指标

AWS/EC2 命名空间包括基于 Nitro 的实例的以下 Amazon EBS 指标。有关基于 Nitro 的实例类型的列表，请参阅基于 Nitro 系统构建的实例 (p. 246)。

指标	描述
EBSReadOps	在指定时间段内在挂载到实例的所有 Amazon EBS 卷中完成的读取操作数。 要计算该时间段的平均每秒读取 I/O 操作数 (读取 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算读取 IOPS。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。 单位：计数
EBSWriteOps	在指定时间段内在附加到实例的所有 EBS 卷中完成的写入操作数。 要计算该时间段的平均每秒写入 I/O 操作数 (写入 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算写入 IOPS。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。 单位：计数
EBSReadBytes	在指定时间段内从附加到实例的所有 EBS 卷中读取的字节数。 报告的数字是在该时间段内读取的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒读取的字节数。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。 单位：字节
EBSWriteBytes	在指定时间段内写入附加到实例的所有 EBS 卷的字节数。 报告的数字是在该时间段内写入的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒写入的字节数。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。 单位：字节

指标	描述
EBSIOBalance%	提供有关突增存储桶中剩余的 I/O 积分百分比的信息。此指标仅对基本监控可用。 此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关支持此指标的实例大小的完整列表，请参阅 默认为 EBS 优化 (p. 1523) 表 Instance size（实例大小）栏中带星号（*）的实例类型。 Sum 统计数据不适用于该指标。 单位：百分比
EBSByteBalance%	提供有关突增存储桶中剩余的吞吐量积分百分比的信息。此指标仅对基本监控可用。 此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关支持此指标的实例大小的完整列表，请参阅 默认为 EBS 优化 (p. 1523) 表 Instance size（实例大小）栏中带星号（*）的实例类型。 Sum 统计数据不适用于该指标。 单位：百分比

有关为 EBS 卷提供的指标的信息，请参阅 Amazon EBS 指标 (p. 1564)。有关为 Spot 队列提供的指标的信息，请参阅 Spot 队列的 CloudWatch 指标 (p. 912)。

状态检查指标

AWS/EC2 命名空间包括以下状态检查指标。默认情况下，状态检查指标可在 1 分钟的频率下免费提供。对于新启动的实例，状态检查指标数据仅在实例完成初始化状态之后 (实例进入运行状态的几分钟之内) 提供。有关 EC2 状态检查的更多信息，请参阅实例的状态检查 (p. 975)。

指标	描述
StatusCheckFailed	报告实例在上一分钟是否通过了实例状态检查和系统状态检查。 此指标可以是 0 (通过) 或 1 (失败)。 默认情况下，此指标可在 1 分钟的频率下免费提供。 单位：计数
StatusCheckFailed_Instance	报告实例在上个 1 分钟内是否通过了 实例状况检查。 此指标可以是 0 (通过) 或 1 (失败)。 默认情况下，此指标可在 1 分钟的频率下免费提供。 单位：计数
StatusCheckFailed_System	报告实例在上一分钟内是否通过了 系统状况检查。 此指标可以是 0 (通过) 或 1 (失败)。

指标	描述
	默认情况下，此指标可在 1 分钟的频率下免费提供。 单位：计数

流量镜像指标

AWS/EC2 命名空间包含镜像流量的指标。有关更多信息，请参阅《Amazon VPC Traffic Mirroring 指南》中的使用 Amazon CloudWatch 监控镜像的流量。

Auto Scaling 组指标

AWS/AutoScaling 命名空间包括 Auto Scaling 组的指标。有关更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的监控 Auto Scaling 组和实例的 CloudWatch 指标。

Amazon EC2 指标维度

您可以使用以下维度来优化上表中列出的指标。

维度	描述
AutoScalingGroupName	该维度筛选您为指定容量组中的所有实例请求的数据。如果您使用 Auto Scaling，Auto Scaling 组就是您定义的实例集合。当实例在上述 Auto Scaling 组中时，该维度仅供 Amazon EC2 指标使用。可供启用了详细或基本监控的实例使用。
ImageId	该维度筛选您为运行此 Amazon EC2 Amazon Machine Image (AMI) 的所有实例而请求的数据。可供启用了详细监控功能的实例使用。
InstanceId	该维度筛选您仅为已识别实例请求的数据。这样有助于您精确定位要对其监控数据的确切实例。
InstanceType	该维度筛选您为以这一指定实例类型运行的所有实例请求的数据。这样有助于您按运行的实例类型给数据分类。例如，您可以比较 m1.small 实例和 m1.large 实例的数据，以确定哪一个对您的应用程序具有更好的商业价值。可供启用了详细监控功能的实例使用。

Amazon EC2 使用情况指标

您可以使用 CloudWatch 用量指标来提供账户资源使用情况的可见性。使用这些指标在 CloudWatch 图表和控制面板上可视化当前服务用量。

Amazon EC2 用量指标与 Amazon 服务配额对应。您可以配置警报，以在用量接近服务配额时向您发出警报。有关 CloudWatch 与 Service Quotas 集成的更多信息，请参阅《Amazon CloudWatch 用户指南》中的 Amazon 使用情况指标。

Amazon EC2 在 AWS/Usage 命名空间中发布以下指标。

指标	描述
ResourceCount	您账户中运行的指定资源的数量。资源由与指标关联的维度定义。

指标	描述
	此指标最有用的统计数据是 MAXIMUM，这表示 1 分钟期间内使用的最大资源数。

以下维度用于优化由 Amazon EC2 发布的用量指标。

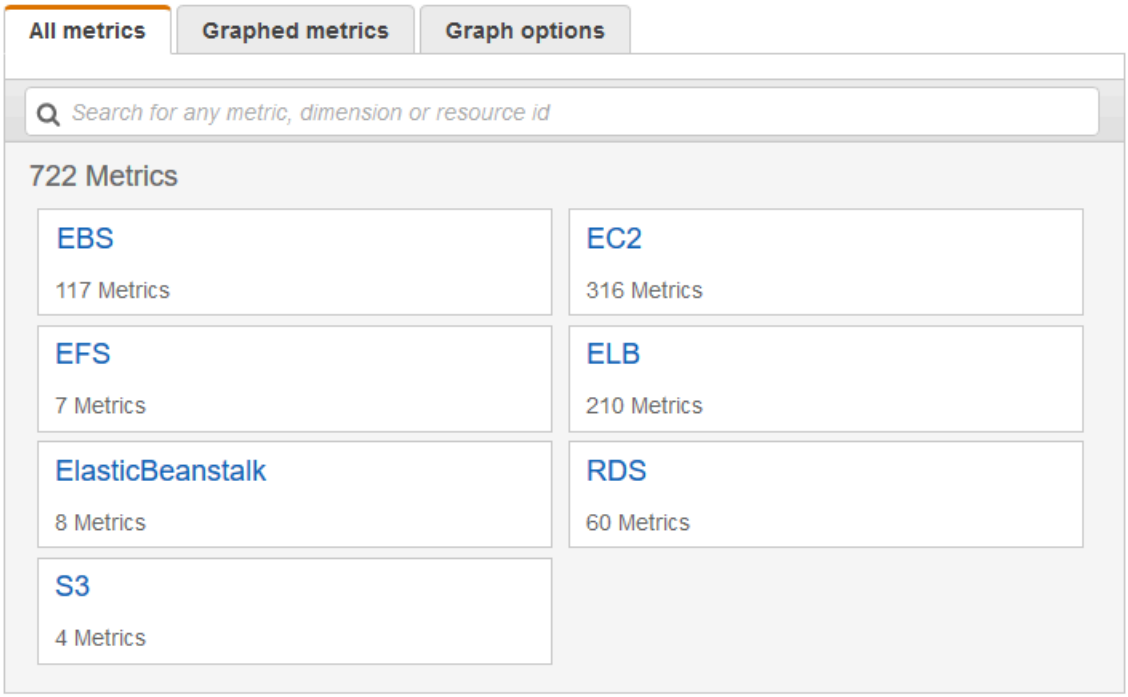
维度	描述
Service	包含该资源的 Amazon 服务的名称。对于 Amazon EC2 用量指标，此维度的值为 EC2。
Type	正在报告的实体的类型。目前，Amazon EC2 用量指标的唯一有效值为 Resource。
Resource	正在运行的资源的类型。目前，Amazon EC2 用量指标的唯一有效值是 vCPU，它返回有关正在运行的实例的信息。
Class	所跟踪的资源的类。对于以 vCPU 作为 Resource 维度的值的 Amazon EC2 用量指标，有效值为 Standard/OnDemand、F/OnDemand、G/OnDemand、Inf/OnDemand、P/OnDemand 和 X/OnDemand。 此维度的值定义由该指标报告的实例类型的第一个字母。例如，Standard/OnDemand 返回有关类型以 A、C、D、H、I、M、R、T 和 Z 开头的所有正在运行的实例的信息，并且 G/OnDemand 返回有关类型以 G 开头的所有正在运行的实例的信息。

使用控制台列出指标

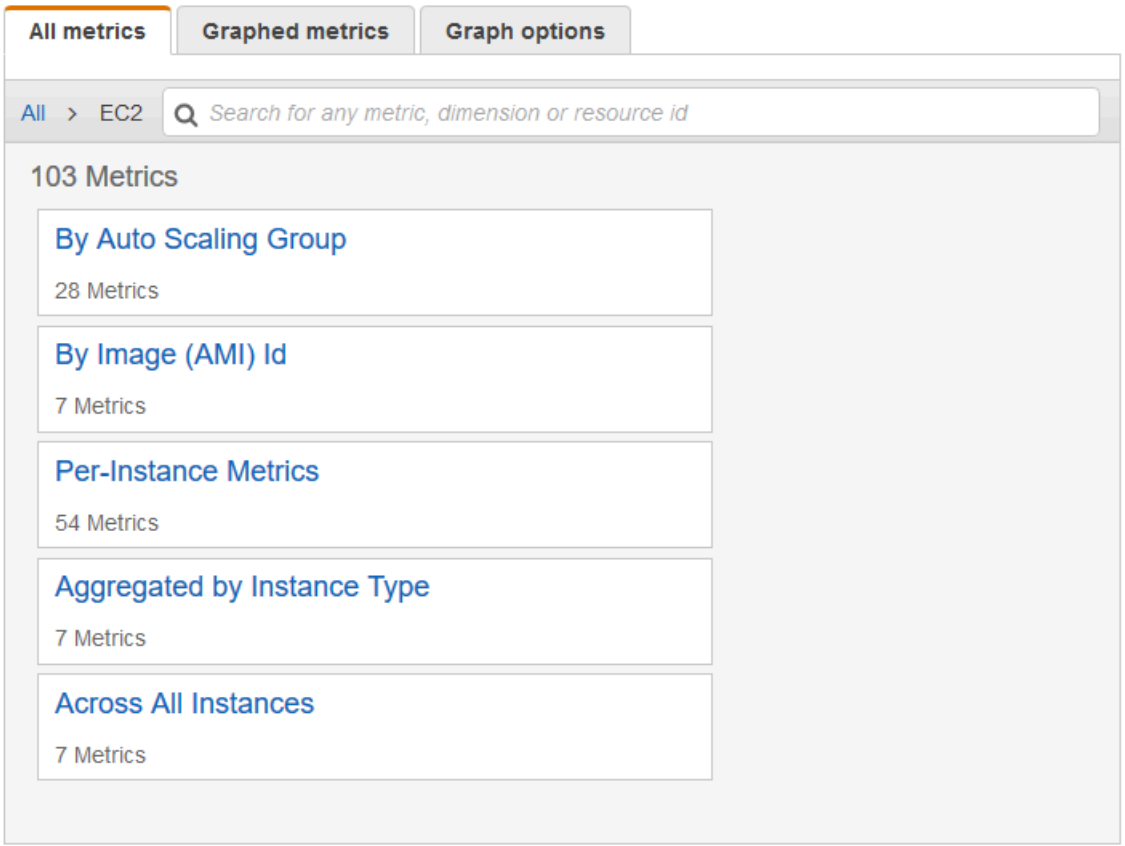
指标首先按命名空间进行分组，然后按各命名空间内的各种维度组合进行分组。例如，您可以查看由 Amazon EC2 提供的所有指标或按实例 ID、实例类型、映像 (AMI) ID 或 Auto Scaling 组分组的指标。

按类别查看可用指标（控制台）

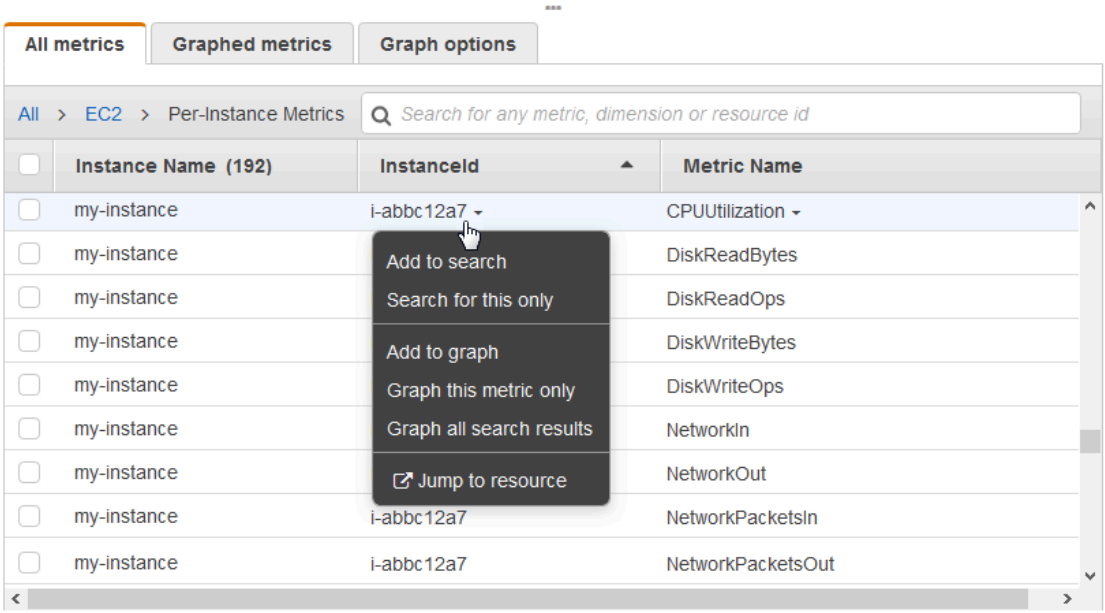
1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 指标命名空间。



4. 选择指标维度（例如 Per-Instance Metrics (每个实例的指标)）。



5. 要对指标进行排序，请使用列标题。要为指标绘制图表，请选中该指标旁的复选框。要按资源进行筛选，请选择资源 ID，然后选择 Add to search。要按指标进行筛选，请选择指标名称，然后选择 Add to search。



使用 Amazon CLI 列出指标

使用 list-metrics 命令列出实例的 CloudWatch 指标。

列出 Amazon EC2 的所有可用指标（Amazon CLI）

以下示例指定 AWS/EC2 命名空间以查看 Amazon EC2 的所有指标。

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

下面是示例输出：

```
{
  "Metrics": [
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkOut"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "CPUUtilization"
```

```
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

列出实例的所有可用指标 (Amazon CLI)

以下示例指定 AWS/EC2 命名空间和 InstanceId 维度以仅查看指定实例的结果。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
 Name=InstanceId,Value=i-1234567890abcdef0
```

列出所有实例的指标 (Amazon CLI)

以下示例指定 AWS/EC2 命名空间和指标名称以仅查看指定指标的结果。

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

获取实例的指标统计数据

您可以获取有关实例的 CloudWatch 指标的统计信息。

目录

- 统计数据概述 (p. 1012)
- 获取特定实例的统计数据 (p. 1013)
- 聚合不同实例的统计数据 (p. 1016)
- 按 Auto Scaling 组聚合统计数据 (p. 1018)
- 按 AMI 聚合统计数据 (p. 1019)

统计数据概述

统计数据是指定时间段内的指标数据汇总。CloudWatch 提供统计数据的依据是您的自定义数据所提供的指标数据点，或其他 Amazon 服务向 CloudWatch 提供的指标数据点。聚合通过使用命名空间、指标名称、维度以及数据点度量单位在您指定的时间段内完成。下表介绍了可用的统计信息。

统计数据	描述
Minimum	指定时间段内的最低观察值。可以使用此值来决定应用程序的活动量是否较低。
Maximum	指定时间段内的最高观察值。可以使用此值来决定应用程序的活动量是否较高。
Sum	为匹配指标所提交的所有的值添加在一起。此统计信息的作用是决定指标的总量。

统计数据	描述
Average	指定时间段内 Sum / SampleCount 的值。通过将此统计信息与 Minimum 和 Maximum 进行比较，可以决定指标的完整范围以及平均使用率与 Minimum 和 Maximum 的接近程度。这样的比较可以帮助了解何时应该根据需要增加或减少资源。
SampleCount	数据点计数 (数量) 用于统计信息的计算。
pNN.NN	指定的百分位数的值。您可以指定任何百分位数，最多使用两位小数 (例如 p95.45)。

获取特定实例的统计数据

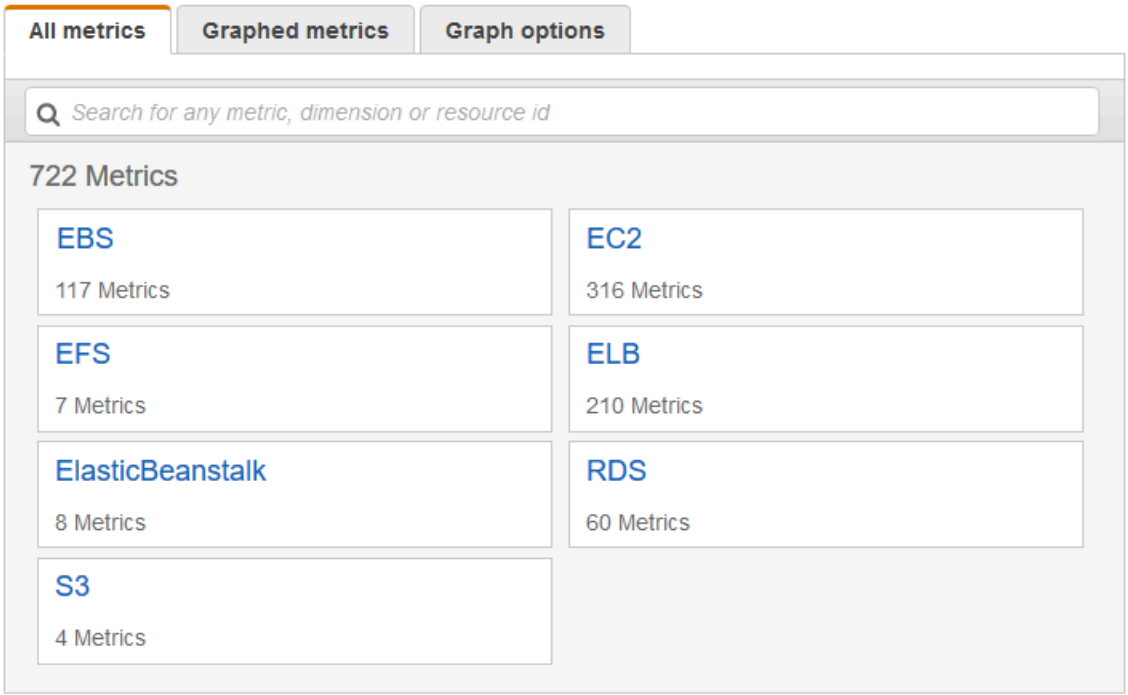
以下示例显示了如何使用 Amazon Web Services Management Console 或 Amazon CLI 来确定特定 EC2 实例的最大 CPU 利用率。

要求

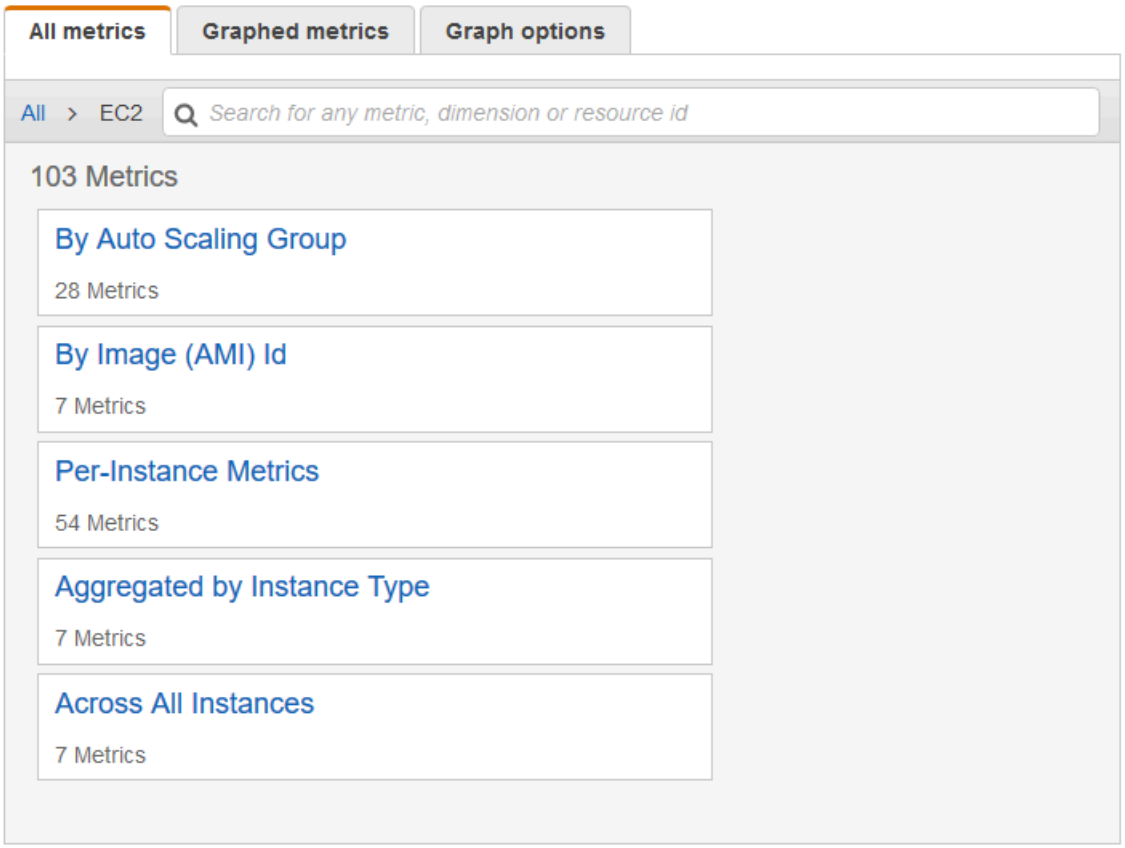
- 您必须拥有实例的 ID。可使用 Amazon Web Services Management Console 或 describe-instances 命令获取实例 ID。
- 默认情况下，基本监控已启用，但您可以启用详细监控。有关更多信息，请参阅对实例启用或禁用详细监控 (p. 1001)。

显示指定实例的 CPU 利用率（控制台）

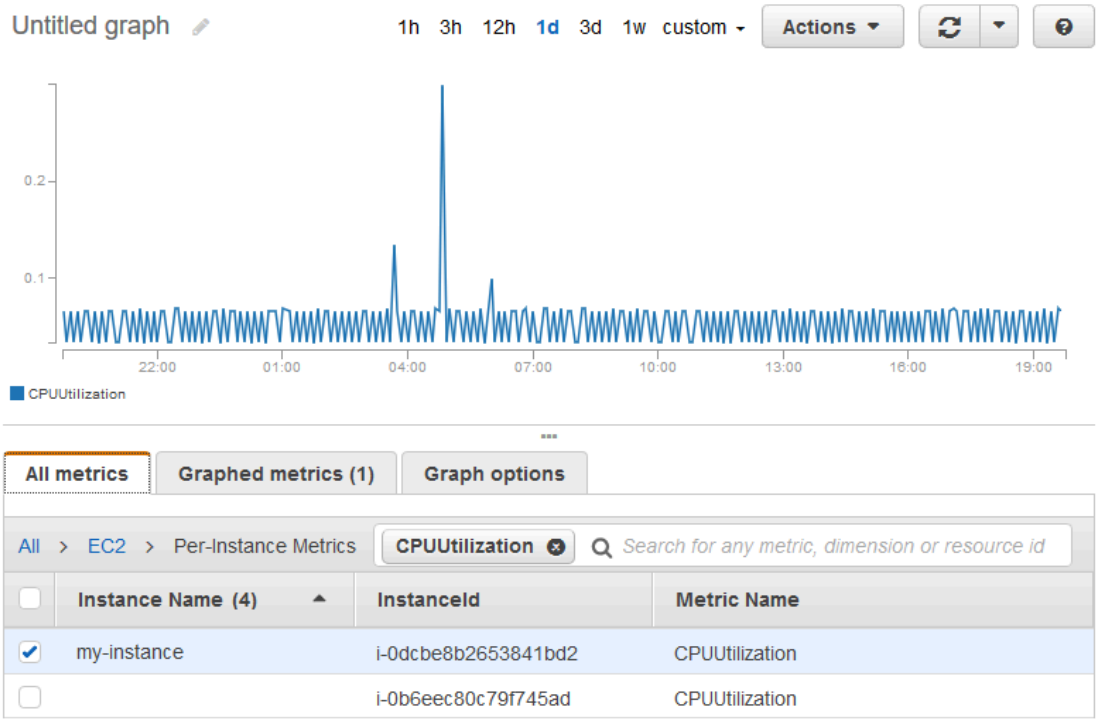
1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 指标命名空间。



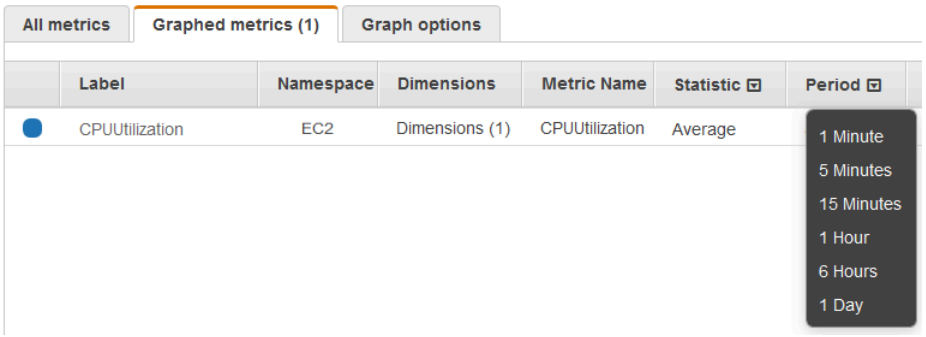
4. 选择 Per-Instance Metrics (每个实例的指标) 维度。



5. 在搜索框中，输入 **`CPUUtilization`** 并按 Enter。选择特定实例所在的行，这将显示该实例的 CPUUtilization 指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。



6. 要更改指标的统计数据或时间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。



获取特定实例的 CPU 利用率 (Amazon CLI)

使用以下 get-metric-statistics 命令获取指定实例的 CPUUtilization 指标（使用指定周期和时间间隔）：

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization  --
period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

下面是示例输出。每个数值代表一个 EC2 实例的最大 CPU 使用率百分比。

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

聚合不同实例的统计数据

聚合统计信息适用于已经启用详细监控的实例。聚合中不包含使用基本监控的实例。在获取多实例聚合统计数据前，必须启用详细监控 (p. 1001)（另外收费），以提供以 1 分钟为间隔的数据。

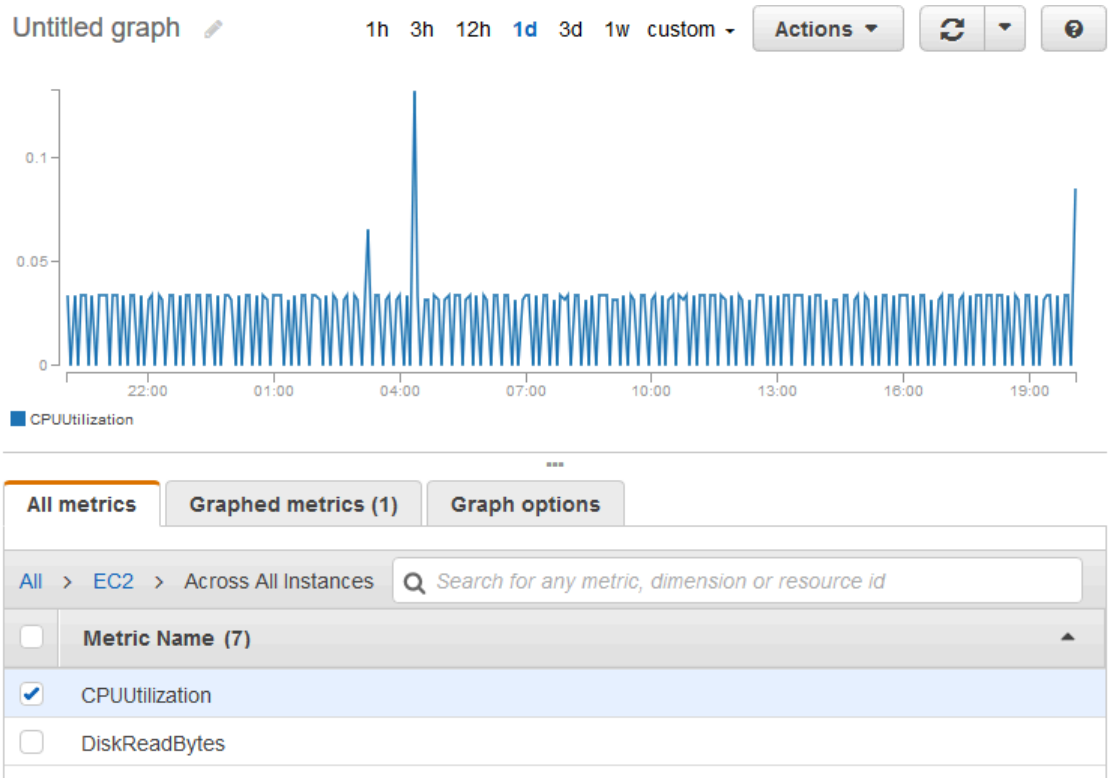
请注意，Amazon CloudWatch 不能跨各个 Amazon 区域聚合数据。指标在各区域间彼此独立。

此示例显示了如何使用详细监控来获取 EC2 实例的平均 CPU 使用率。因为未指定任何维度，所以 CloudWatch 会返回 AWS/EC2 命名空间中所有维度的统计数据。

> **Important**
>
> 此方法可以在 Amazon 命名空间中检索所有维度，但不适用于发布到 Amazon CloudWatch 的自定义命名空间。对于自定义命名空间，必须指定与任意给定数据关联的完整的维度组，以检索包含数据点的统计数据。

显示实例的平均 CPU 利用率（控制台）

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 命名空间，然后选择 Across All Instances (跨所有实例)。
4. 选择包含 CPUUtilization 的行，这将显示所有 EC2 实例的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。



5. 要更改指标的统计数据或时间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

获取实例的平均 CPU 利用率 (Amazon CLI)

使用 get-metric-statistics 命令 (如下所示) 获取实例的平均 CPUUtilization 指标。

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

下面是示例输出：

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
```

```
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

按 Auto Scaling 组聚合统计数据

您可以聚合 Auto Scaling 组中 EC2 实例的统计数据。请注意，Amazon CloudWatch 不能跨各个 Amazon 区域聚合数据。指标在各区域间彼此独立。

此示例说明如何检索为一个 Auto Scaling 组写入磁盘的字节总数。总数以 1 分钟为周期 24 小时为间隔针对指定 Auto Scaling 组中的所有 EC2 实例计算得出。

显示一个 Auto Scaling 组中的实例的 DiskWriteBytes（控制台）

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 命名空间，然后选择 By Auto Scaling Group。
4. 选择 DiskWriteBytes 指标和特定 Auto Scaling 组所在的行，这将显示 Auto Scaling 组中实例的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
5. 要更改指标的统计数据或时间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

显示一个 Auto Scaling 组中的实例的 DiskWriteBytes（Amazon CLI）

使用 get-metric-statistics 命令，如下所示。

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes --
period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

下面是示例输出：

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "DiskWriteBytes"
}
```

按 AMI 聚合统计数据

您可以聚合已启用详细监控的实例的统计数据。聚合中不包含使用基本监控的实例。在获取多实例聚合统计数据前，必须启用详细监控 (p. 1001)（另外收费），以提供以 1 分钟为间隔的数据。

请注意，Amazon CloudWatch 不能跨各个 Amazon 区域聚合数据。指标在各区域间彼此独立。

此示例显示了如何确定使用特定 Amazon Machine Image (AMI) 的所有实例的平均 CPU 使用率。平均值以 60 秒为时间间隔 1 天为周期。

按 AMI 显示平均 CPU 利用率（控制台）

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EC2 命名空间，然后选择 By Image (AMI) Id。
4. 选择 CPUUtilization 指标和特定 AMI 所在的行，这将显示指定 AMI 的指标的图表。要为该图标命名，请选择铅笔图标。要更改时间范围，请选择某个预定义的值或选择 custom。
5. 要更改指标的统计数据或时间段，请选择 Graphed metrics 选项卡。选择列标题或单个值，然后选择其他值。

获取某个映像 ID 的平均 CPU 利用率 (Amazon CLI)

使用 get-metric-statistics 命令，如下所示。

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization  --
period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

下面是示例输出。每个数值代表运行指定 AMI 的 EC2 实例的平均 CPU 使用率百分比。

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

绘制实例的指标图形

在您启动实例后，可以打开 Amazon EC2 控制台并在 Monitoring（监控）选项卡上查看实例的监控图表。每个图表以一个可用的 Amazon EC2 指标为基础。

可供使用图形如下：

- CPU 平均使用率 (%)
- 平均读磁盘数 (字节)
- 平均写磁盘数 (字节)
- 最大网络输入 (字节)
- 最大网络输出 (字节)
- 读磁盘操作概括 (计数)
- 写磁盘操作概括 (计数)
- 状态概括 (任意)
- 实例状态概括 (计数)
- 系统状态概括 (计数)

有关指标及其向图表提供的数据的更多信息，请参阅 列出实例的可用 CloudWatch 指标 (p. 1002)。

使用 CloudWatch 控制台绘制指标图标

您还可以使用 CloudWatch 控制台将 Amazon EC2 和其他 Amazon 服务生成的指标数据绘制成图表。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的绘制指标图表。

为实例创建 CloudWatch 警报

您可以创建 CloudWatch 警报来监控您的任一实例的 CloudWatch 指标。当该指标达到指定阈值时，CloudWatch 自动向您发送通知。您可以使用 Amazon EC2 控制台创建 CloudWatch 警报，或者使用 CloudWatch 控制台提供的更多高级选项。

使用 CloudWatch 控制台创建警报

有关示例，请参阅Amazon CloudWatch 用户指南中的创建 Amazon CloudWatch 警报。

使用 Amazon EC2 控制台创建警报

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、Manage CloudWatch alarms（管理 CloudWatch 警报）。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）详细信息页面中的 Add or edit alarm（添加或编辑警报）下，选择 Create an alarm（创建警报）。
5. 对于警报通知，选择打开或关闭开关来配置 Amazon Simple Notification Service (Amazon SNS) 通知。输入现有 Amazon SNS 主题或输入名称来创建新主题。
6. 对于警报操作，选择打开或关闭开关来指定触发警报时要执行的操作。从下拉列表中选择一个操作。
7. 对于警报阈值，选择警报的指标和条件。例如，您可以为样本分组依据（平均）和要采样的数据类型（CPU 利用率）保留默认设置。对于警报触发条件，选择 >= 并输入 **0.80**。对于连续周期，输入 **1**。对于时段，选择 5 分钟。
8. （可选）对于样本指标数据，选择添加到控制面板。
9. 选择 Create（创建）。

您可以从 Amazon EC2 控制台或 CloudWatch 控制台编辑 CloudWatch 警报设置。如果要删除警报，可以从 CloudWatch 控制台执行此操作。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的编辑或删除 CloudWatch 告警。

创建停止、终止、重启或恢复实例的警报

利用 Amazon CloudWatch 警报操作，您可创建自动停止、终止、重启或恢复实例的警报。当不再需要某个实例运行时，您可使用停止或终止操作来帮助您节省资金。如果发生了系统损害，您可使用重启和恢复操作自动重启这些实例或将它们恢复到新硬件上。

`AWSServiceRoleForCloudWatchEvents` 服务相关角色使 Amazon 能够代表您执行警报操作。当您首次在 Amazon Web Services Management Console、Amazon CLI 或 IAM API 中创建告警时，CloudWatch 会为您创建服务相关角色。

在许多情况下，您可能需要自动终止或停止实例。例如，您可能拥有专用于批工资单处理作业或科学计算任务的实例，这些实例在运行一段时间后就完成了其工作。与其让这些实例空闲 (并产生费用)，不如将其停止或终止以节省开支。使用停止警报操作和使用终止警报操作的主要区别在于，停止的实例在以后需要再次运行时，可以轻松地启动，并且可以保留相同的实例 ID 和根卷，而终止的实例则无法再启动。如此就必须启动一个新的实例。停止或终止实例后，实例存储卷上的数据将丢失。

您可以向为 Amazon EC2 每个实例指标设置的任何警报添加停止、终止、重启或恢复操作，这些指标包括 Amazon CloudWatch 提供的基本和详细监控指标（在 `AWS/EC2` 命名空间中），以及包含 `InstanceId` 维度的任何自定义指标，只要其值引用有效运行的 Amazon EC2 实例。

控制台支持

可使用 Amazon EC2 控制台或 CloudWatch 控制台创建警报。本文档中的过程使用 Amazon EC2 控制台。有关使用 CloudWatch 控制台的过程，请参阅《Amazon CloudWatch 用户指南》中的创建停止、终止、重新启动或恢复实例的告警。

权限

您必须拥有 `iam:CreateServiceLinkedRole` 才能创建或修改执行 EC2 告警操作的告警。服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向 Amazon Web Service 委派权限的角色。

目录

- 在 Amazon CloudWatch 警报中添加停止操作 (p. 1021)
- 在 Amazon CloudWatch 警报中添加终止操作 (p. 1022)
- 在 Amazon CloudWatch 警报中添加重启操作 (p. 1023)
- 在 Amazon CloudWatch 警报中添加恢复操作 (p. 1024)
- 使用 Amazon CloudWatch 控制台查看警报和操作历史记录 (p. 1025)
- Amazon CloudWatch 警报操作场景 (p. 1025)

在 Amazon CloudWatch 警报中添加停止操作

可以创建当达到一定阈值后停止 Amazon EC2 实例的警报。例如，您可能运行了开发或测试实例而偶尔忘记将其关闭。可以创建当平均 CPU 使用率低于 10% 达 24 小时时触发的警报，同时告知其为空闲并不再使用。可以根据需要调整阈值、持续时间和周期，还可以添加 Amazon Simple Notification Service (Amazon SNS) 通知，以便在触发警报后，您能够收到电子邮件。

可以停止或终止将 Amazon EBS 卷用作根设备的实例，但只能终止将实例存储用作根设备的实例。停止或终止实例后，实例存储卷上的数据将丢失。

创建停止空闲实例的警报（Amazon EC2 控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。

3. 选择所需实例，然后依次选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、Manage CloudWatch alarms（管理 CloudWatch 警报）。

   或者，您可以在 Alarm status（警报状态）列中选择加号（  ）。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面上，执行以下操作：

   a. 选择 Create an alarm（创建警报）。

   b. 要在警报触发时接收电子邮件，对于 Alarm notification（警报通知），选择现有的 Amazon SNS 主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

   c. 开启 Alarm action（警报操作），然后选择 Stop（停止）。

   d. 对于 Group samples by（样本分组方式）和 Type of data to sample（要采样的数据类型），选择统计数据和指标。在此示例中，选择 Average（平均值）和 CPU utilization（CPU 利用率）。

   e. 对于 Alarm When（警报时间）和 Percent（百分比），请指定指标阈值。在此示例中，请指定 <= 和 10%。

   f. 对于 Consecutive period（连续周期）和 Period（周期），请指定警报的评估周期。在此示例中，将 1 个连续周期指定为 5 分钟。

   g. Amazon CloudWatch 自动为您创建警报名称。要更改名称，请在 Alarm name（警报名称）中输入新名称。警报名称必须仅包含 ASCII 字符。

      Note

      可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

   h. 选择 Create（创建）。

在 Amazon CloudWatch 警报中添加终止操作

可以创建当达到一定阈值时自动终止 EC2 实例的警报 (只要该实例未启用终止保护)。例如，某个实例已经完成工作，您不再需要此实例而想将其终止。如果可能在之后使用该实例，则应该选择停止而不是终止。终止实例后，实例存储卷上的数据将丢失。有关为实例启用和禁用终止保护的信息，请参阅 启用终止保护 (p. 637)。

创建终止空闲实例的警报（Amazon EC2 控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、Manage CloudWatch alarms（管理 CloudWatch 警报）。

   或者，您可以在 Alarm status（警报状态）列中选择加号（  ）。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面上，执行以下操作：

   a. 选择 Create an alarm（创建警报）。

   b. 要在警报触发时接收电子邮件，对于 Alarm notification（警报通知），选择现有的 Amazon SNS 主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

   c. 开启 Alarm action（警报操作），然后选择 Terminate（终止）。

   d. 对于 Group samples by（样本分组方式）和 Type of data to sample（要采样的数据类型），选择统计数据和指标。在此示例中，选择 Average（平均值）和 CPU utilization（CPU 利用率）。

e. 对于 Alarm When（警报时间）和 Percent（百分比），请指定指标阈值。在此示例中，请指定 => 和 10%。

f. 对于 Consecutive period（连续周期）和 Period（周期），请指定警报的评估周期。在此示例中，将 24 个连续周期指定为 1 小时。

g. Amazon CloudWatch 自动为您创建警报名称。要更改名称，请在 Alarm name（警报名称）中输入新名称。警报名称必须仅包含 ASCII 字符。

Note

可以在创建警报前根据自己的要求调整警报配置，也可以在之后编辑配置。这包括指标、阈值、时长、操作和通知等设置。但是，警报创建后其名称无法再次编辑。

h. 选择 Create（创建）。

在 Amazon CloudWatch 警报中添加重启操作

您可创建监控 Amazon EC2 实例并自动重启此实例的 Amazon CloudWatch 警报。在实例运行状况检查失败时，推荐重启警报操作（与恢复警报操作相反，该操作适合系统运行状况检查失败的情况）。实例重启相当于操作系统重启。在许多情况下，只需要几分钟时间即可重启您的实例。重启实例时，其仍驻留在相同的物理主机上，因此您的实例将保留其公有 DNS 名称、私有 IP 地址及其实例存储卷上的任何数据。

与停止并重新启动您的实例不同，重启实例不会启动新的实例计费周期（最低收取一分钟的费用）。重启实例后，实例存储卷上的数据会保留。重启后，必须将实例存储卷重新挂载到文件系统中。有关更多信息，请参阅重启实例 (p. 631)。

Important

为了避免重启操作与恢复操作之间的竞争情况，请避免为重启警报和恢复警报设置相同的评估周期数。我们建议您将重启警报设置为 3 个 1 分钟的评估期。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的评估警报。

创建重启实例的警报（Amazon EC2 控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、Manage CloudWatch alarms（管理 CloudWatch 警报）。

   或者，您可以在 Alarm status（警报状态）列中选择加号（  ）。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面上，执行以下操作：

   a. 选择 Create an alarm（创建警报）。

   b. 要在警报触发时接收电子邮件，对于 Alarm notification（警报通知），选择现有的 Amazon SNS 主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

   c. 开启 Alarm action（警报操作），然后选择 Reboot（重启）。

   d. 对于 Group samples by（样本分组方式）和 Type of data to sample（要采样的数据类型），选择统计数据和指标。在此示例中，选择 Average（平均值）和 Status check failed: instance（状态检查失败：实例）。

   e. 对于 Consecutive period（连续周期）和 Period（周期），请指定警报的评估周期。在此示例中，输入 3 个 5 分钟的连续周期。

   f. Amazon CloudWatch 自动为您创建警报名称。要更改名称，请在 Alarm name（警报名称）中输入新名称。警报名称必须仅包含 ASCII 字符。

g. 选择 Create（创建）。

在 Amazon CloudWatch 警报中添加恢复操作

您可以创建 Amazon CloudWatch 警报来监控 Amazon EC2 实例。如果实例因需要 Amazon 参与才能修复的基础硬件故障或问题而受损，您可自动恢复实例。无法恢复终止的实例。恢复的实例与原始实例相同，包括实例 ID、私有 IP 地址、弹性 IP 地址以及所有实例元数据。

CloudWatch 会阻止您将恢复操作添加到位于不支持恢复操作的实例上的警报。

当 `StatusCheckFailed_System` 警报触发且恢复操作启动时，您在创建警报及相关恢复操作时所选择的 Amazon SNS 主题将向您发出通知。在实例恢复过程中，实例将在重启时迁移，并且内存中的所有数据都将丢失。当该过程完成后，会向您已配置警报的 SNS 主题发布信息。任何订阅此 SNS 主题的用户都将收到一封电子邮件通知，其中包括恢复尝试的状态以及任何进一步的指示。您将注意到，实例会在已恢复的实例上重启。

> **Note**
>
> 恢复操作仅适用于 `StatusCheckFailed_System`，而不能用于 `StatusCheckFailed_Instance`。

下列问题可能导致系统状态检查失败：

- 网络连接丢失
- 系统电源损耗
- 物理主机上的软件问题
- 物理主机上影响到网络连接状态的硬件问题

仅具有以下特性的实例支持恢复操作。有关更多信息，请参阅恢复您的实例。

如果您的实例具有公有 IP 地址，它会在恢复后保留公有 IP 地址。

> **Important**
>
> 为了避免重启操作与恢复操作之间的竞争情况，请避免为重启警报和恢复警报设置相同的评估周期数。我们建议您将恢复警报设置为 2 个 1 分钟的评估期。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的评估警报。

创建恢复实例的警报（Amazon EC2 控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择所需实例，然后依次选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、Manage CloudWatch alarms（管理 CloudWatch 警报）。

   或者，您可以在 Alarm status（警报状态）列中选择加号（  ）。
4. 在 Manage CloudWatch alarms（管理 CloudWatch 警报）页面上，执行以下操作：
   a. 选择 Create an alarm（创建警报）。
   b. 要在警报触发时接收电子邮件，对于 Alarm notification（警报通知），选择现有的 Amazon SNS 主题。您首先需要使用 Amazon SNS 控制台创建 Amazon SNS 主题。有关更多信息，请参阅Amazon Simple Notification Service 开发人员指南中的使用 Amazon SNS 进行应用程序对人 (A2P) 消息传送。

Note

用户必须订阅指定的 SNS 主题才能在触发警报时收到电子邮件通知。执行实例自动恢复操作时，Amazon Web Services 账户根用户 始终会收到电子邮件通知，即使未指定 SNS 主题或者根用户未订阅指定 SNS 主题也是如此。

c. 开启 Alarm action（警报操作），然后选择 Recover（恢复）。

d. 对于 Group samples by（样本分组方式）和 Type of data to sample（要采样的数据类型），选择统计数据和指标。在此示例中，选择 Average（平均值）和 Status check failed: system（状态检查失败：系统）。

e. 对于 Consecutive period（连续周期）和 Period（周期），请指定警报的评估周期。在此示例中，输入 2 个 5 分钟的连续周期。

f. Amazon CloudWatch 自动为您创建警报名称。要更改名称，请在 Alarm name（警报名称）中输入新名称。警报名称必须仅包含 ASCII 字符。

g. 选择 Create（创建）。

使用 Amazon CloudWatch 控制台查看警报和操作历史记录

您可以在 Amazon CloudWatch 控制台中查看警报和操作历史记录。Amazon CloudWatch 会保留最近两周的警报和操作历史记录。

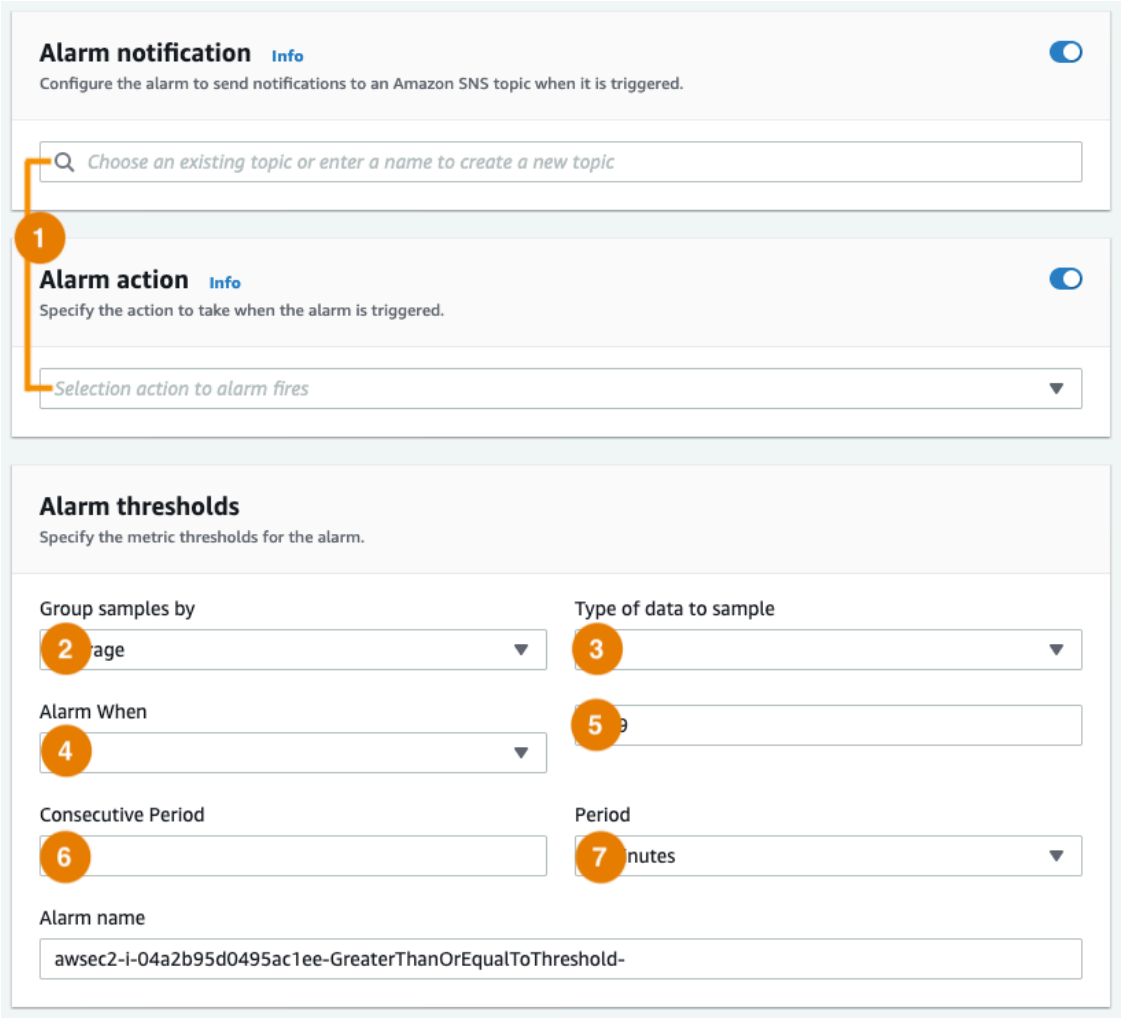
查看已触发的警报和操作的历史记录（CloudWatch 控制台）

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Alarms (警报)。
3. 选择一个警报。
4. Details 选项卡显示最近的状态转换以及时间和指标值。
5. 选择 History 选项卡可以查看最近的历史记录条目。

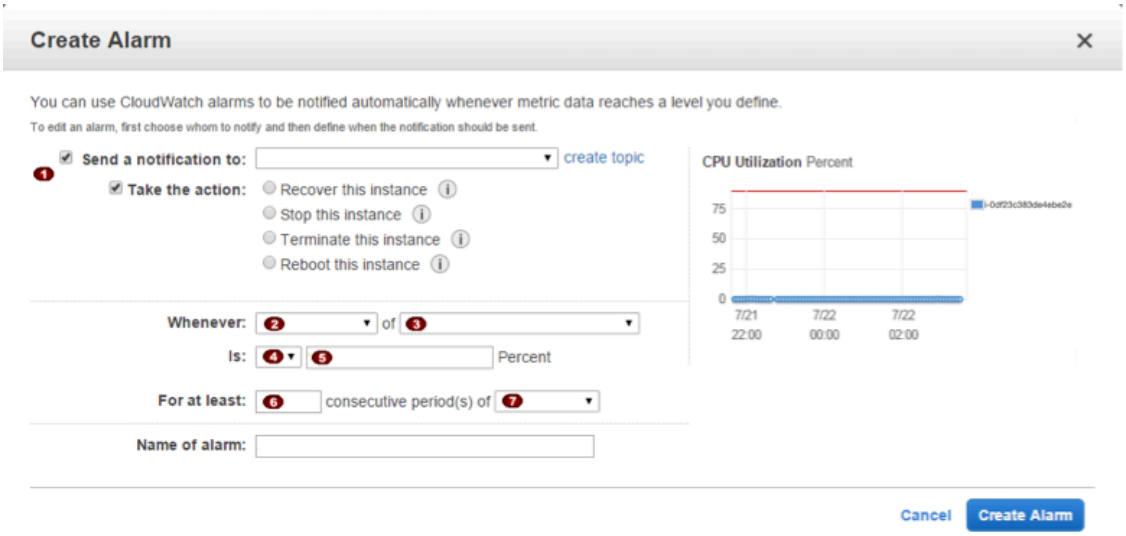
Amazon CloudWatch 警报操作场景

可以使用 Amazon EC2 控制台创建当满足一定条件时停止或终止 Amazon EC2 实例的警报操作。在下方的控制台页面屏幕截图中，您设置了警报操作，我们对设置进行了编号。我们还对后续场景中的设置进行了编号，帮助您创建合适的操作。

New console



Old console



场景 1：停止空闲开发和测试实例

创建当用于软件开发或测试的实例空闲达到至少 1 小时时停止该实例的警报。

设置	值
1	停止
2	最高
3	CPU 利用率
4	<=
5	10%
6	1
7	1 小时

场景 2：停止空闲实例

创建一个当实例空闲达到 24 小时时停止该实例并发送电子邮件的警报。

设置	值
1	停止并发送电子邮件
2	平均值
3	CPU 利用率
4	<=
5	5%
6	24
7	1 小时

场景 3：发送有关出现异常高流量的 Web 服务器的电子邮件

创建一个当实例的出站网络流量每天超过 10 GB 时发送电子邮件的警报。

设置	值
1	电子邮件
2	总计
3	网络输出
4	>
5	10GB
6	24

设置	值
7	1 小时

场景 4：停止出现异常高流量的 Web 服务器

创建当出站流量超过每小时 1 GB 时停止实例并发送短消息 (SMS) 的警报。

设置	值
1	停止并发送短消息
2	总计
3	网络输出
4	>
5	1GB
6	1
7	1 小时

场景 5：停止受损的实例

创建当实例连续 3 次状态检查 (每隔 5 分钟执行一次) 皆为故障时将其停止的警报。

设置	值
1	停止
2	平均值
3	状态检查失败：系统
4	-
5	-
6	1
7	15 分钟

场景 6：在批处理作业完成时终止实例

创建当实例不再发送结果数据时终止运行批处理作业的实例的警报。

设置	值
1	终止
2	最高
3	网络输出

设置	值
4	<=
5	100000 字节
6	1
7	5 分钟

使用 EventBridge 自动执行 Amazon EC2

您可以使用 Amazon EventBridge 自动执行您的 Amazon Web Services 和自动响应系统事件，例如应用程序可用性问题或资源更改。Amazon 服务中的事件将近乎实时传输到 EventBridge。您可以创建规则来指示要关注的事件，以及在事件匹配规则时要执行的操作。可自动触发的操作包括：

- 调用 Amazon Lambda 函数
- 调用 Amazon EC2 Run Command
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 Amazon Step Functions 状态机
- 通知 Amazon SNS 主题
- 通知 Amazon SQS 队列

以下示例说明如何将 EventBridge 与 Amazon EC2 结合使用：

- 每当实例进入运行状态时激活 Lambda 函数。
- 在创建或修改 Amazon EBS 卷时通知 Amazon SNS 主题。
- 当另一个 Amazon 服务中发生特定事件时，使用 Amazon EC2 Run Command 向一个或多个 Amazon EC2 实例发送命令。

有关更多信息，请参阅 Amazon EventBridge 用户指南。

Amazon EC2 事件类型

Amazon EC2 支持以下事件类型：

- EC2 AMI 状态变化 (p. 201)
- EC2 实例集错误 (p. 924)
- EC2 实例集信息 (p. 923)
- EC2 实例集实例更改 (p. 922)
- EC2 实例集竞价型实例请求更改 (p. 921)
- EC2 实例集状态更改 (p. 920)
- EC2 实例再平衡建议 (p. 481)
- EC2 实例状态更改通知 (p. 979)
- EC2 竞价型实例集错误 (p. 928)
- EC2 竞价型实例集信息 (p. 927)
- EC2 竞价型实例集实例更改 (p. 926)
- EC2 竞价型实例集竞价型实例请求更改 (p. 926)
- EC2 竞价型实例集状态更改 (p. 925)

- EC2 竞价型实例中断警告 (p. 491)
- EC2 竞价型实例请求履行 (p. 480)

有关 Amazon EBS 支持的事件类型的信息，请参阅 the section called “EBS EventBridge 事件” (p. 1569)。

监控 Amazon EC2 Linux 实例的内存和磁盘指标

您可以使用 Amazon CloudWatch 从操作系统中收集 EC2 实例的指标和日志。

> Important
>
> CloudWatch 监控脚本已弃用。建议您使用 CloudWatch 代理收集指标和日志。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器中收集指标。
> 如果您仍在从弃用的监控脚本迁移到代理，并且需要有关监控脚本的信息，请参阅 已弃用：使用 CloudWatch 监控脚本收集指标 (p. 1030)。

使用 CloudWatch 代理收集指标

您可以使用 CloudWatch 代理收集来自 Amazon EC2 实例和本地服务器的系统指标与日志文件。代理支持 Windows Server 和 Linux，并使您能够选择要收集的指标，包括子资源指标（如每 CPU 内核）。建议您使用代理（而不是已启用的监控脚本）收集指标和日志。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器中收集指标和日志。

已弃用：使用 CloudWatch 监控脚本收集指标

> Important
>
> CloudWatch 监控脚本已弃用。我们为尚未从已弃用的监控脚本迁移到 CloudWatch 代理的客户提供有关监控脚本的信息。
> 建议您使用 CloudWatch 代理收集指标和日志。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 CloudWatch 代理从 Amazon EC2 实例和本地服务器中收集指标和日志。

监控脚本演示如何为 Amazon CloudWatch 生成和使用自定义指标。这些示例 Perl 脚本包含一个功能完备的示例，用于报告 Linux 实例的内存、交换文件和磁盘空间使用率指标。

在使用这些脚本时，将对自定义指标收取相应的标准 Amazon CloudWatch 使用费。有关更多信息，请参阅 Amazon CloudWatch 定价页。

目录

- 支持的系统 (p. 1030)
- 所需权限 (p. 1031)
- 安装所需的程序包 (p. 1031)
- 安装监控脚本 (p. 1032)
- mon-put-instance-data.pl (p. 1033)
- mon-get-instance-stats.pl (p. 1035)
- 在控制台中查看自定义指标 (p. 1036)
- 问题排查 (p. 1036)

支持的系统

已使用以下系统在实例上测试监控脚本。不支持在任何其他操作系统上使用监控脚本。

- Amazon Linux 2
- Amazon Linux AMI 2014.09.2 和更高版本
- Red Hat Enterprise Linux 6.9 和 7.4
- SUSE Linux Enterprise Server 12
- Ubuntu Server 14.04 和 16.04

所需权限

确保脚本具有通过将 IAM 角色与您的实例关联来调用以下操作的权限：

- `cloudwatch:PutMetricData`
- `cloudwatch:GetMetricStatistics`
- `cloudwatch:ListMetrics`
- `ec2:DescribeTags`

有关更多信息，请参阅使用 IAM 角色 (p. 1280)。

安装所需的程序包

对于 Linux 的某些版本，您必须先安装额外的 Perl 模块，然后才能使用监控脚本。

在 Amazon Linux 2 和 Amazon Linux AMI 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install -y perl-Switch perl-DateTime perl-Sys-Syslog perl-LWP-Protocol-https
 perl-Digest-SHA.x86_64
```

在 Ubuntu 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo apt-get update
sudo apt-get install unzip
sudo apt-get install libwww-perl libdatetime-perl
```

在 Red Hat Enterprise Linux 7 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install perl-Switch perl-DateTime perl-Sys-Syslog perl-LWP-Protocol-https
 perl-Digest-SHA --enablerepo="rhui-REGION-rhel-server-optional" -y
sudo yum install zip unzip
```

在 Red Hat Enterprise Linux 6.9 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

2. 在命令提示符下，按如下方式安装程序包：

```
sudo yum install perl-DateTime perl-CPAN perl-Net-SSLeay perl-IO-Socket-SSL perl-
Digest-SHA gcc -y
sudo yum install zip unzip
```

3. 以权限经过提升的用户身份运行 CPAN：

```
sudo cpan
```

出现提示时始终按 Enter，直到您看到以下提示：

```
cpan[1]>
```

4. 在 CPAN 提示下，运行以下的每个命令：运行一个命令，该命令将进行安装，然后在您返回到 CPAN 提示时运行下一个命令。在系统提示继续完成该过程时像之前一样按 Enter：

```
cpan[1]> install YAML
cpan[2]> install LWP::Protocol::https
cpan[3]> install Sys::Syslog
cpan[4]> install Switch
```

在 SUSE 上安装所需的程序包

1. 登录您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 在运行 SUSE Linux Enterprise Server 12 的服务器上，您可能需要下载 `perl-Switch` 程序包。您可以使用以下命令来下载并安装此程序包：

```
wget http://download.opensuse.org/repositories/devel:/languages:/perl/SLE_12_SP3/
noarch/perl-Switch-2.17-32.1.noarch.rpm
sudo rpm -i perl-Switch-2.17-32.1.noarch.rpm
```

3. 安装所需的程序包，如下所示：

```
sudo zypper install perl-Switch perl-DateTime
sudo zypper install -y "perl(LWP::Protocol::https)"
```

安装监控脚本

下列步骤介绍如何在 EC2 Linux 实例上下载、解压缩和配置 CloudWatch 监控脚本。

要下载、安装和配置监控脚本

1. 在命令提示符下，移至希望存储监控脚本的文件夹，并运行以下命令下载监控脚本：

```
curl https://aws-cloudwatch.s3.amazonaws.com/downloads/
CloudWatchMonitoringScripts-1.2.2.zip -O
```

2. 运行以下命令安装您下载的监控脚本：

```
unzip CloudWatchMonitoringScripts-1.2.2.zip && \
rm CloudWatchMonitoringScripts-1.2.2.zip && \
cd aws-scripts-mon
```

监控脚本的程序包中包含以下文件：

- CloudWatchClient.pm – 共享 Perl 模块，以简化从其他脚本调用 Amazon CloudWatch 的过程。
- mon-put-instance-data.pl – 收集 Amazon EC2 实例中的系统指标（内存、交换、磁盘空间利用率）并将其发送到 Amazon CloudWatch。
- mon-get-instance-stats.pl – 查询 Amazon CloudWatch 并显示在其上运行此脚本的 EC2 实例的最近利用率统计数据。
- awscreds.template – Amazon 凭证的文件模板，储存您的访问密钥 ID 和秘密访问密钥。
- LICENSE.txt – 包含 Apache 2.0 许可证的文本文件。
- NOTICE.txt – 版权声明。

mon-put-instance-data.pl

此脚本会收集当前系统的内存、交换和磁盘空间使用率数据。然后远程调用 Amazon CloudWatch，以自定义指标的形式报告收集到的数据。

选项

名称	说明
`--mem-util`	以百分比收集和发送 MemoryUtilization 指标。此指标计算应用程序分配和操作系统使用的内存，如果您指定 `--mem-used-incl-cache-buff` 选项，则还将缓存和缓冲区内存包括在已用内存中。
`--mem-used`	收集和发送 MemoryUsed 指标 (以兆字节报告)。此指标计算应用程序分配和操作系统使用的内存，如果您指定 `--mem-used-incl-cache-buff` 选项，则还将缓存和缓冲区内存包括在已用内存中。
`--mem-used-incl-cache-buff`	如果包括此选项，则在报告 `--mem-util`、`--mem-used` 和 `--mem-avail` 的指标时，当前用于缓存和缓冲区的内存将计为“已用”。
`--mem-avail`	收集和发送 MemoryAvailable 指标 (以兆字节报告)。此指标计算应用程序分配和操作系统使用的内存，如果您指定 `--mem-used-incl-cache-buff` 选项，则还将缓存和缓冲区内存包括在已用内存中。
`--swap-util`	收集和发送 SwapUtilization 指标 (以百分比报告)。
`--swap-used`	收集和发送 SwapUsed 指标 (以兆字节报告)。
`--disk-path=PATH`	选择要报告的磁盘。 PATH 可以为需要报告的文件系统指定装入点或装入点上的任何文件。如需选择多个磁盘，请为每个磁盘分别指定 `--disk-path=PATH`。 要为装载于 / 和 /home 位置的文件系统选择磁盘，请使用下列参数： `--disk-path=/ --disk-path=/home`
`--disk-space-util`	收集和发送选定磁盘的 DiskSpaceUtilization 指标。指标以百分比报告。 请注意，此脚本计算的磁盘使用率指标与 df -k -l 命令计算的值不同。如果您认为 df -k -l 计算的值更有用，则可以在脚本中更改计算结果。
`--disk-space-used`	收集和发送选定磁盘的 DiskSpaceUsed 指标。指标默认以千兆字节报告。

名称	说明
	受限于 Linux 操作系统中的保留磁盘空间，已用磁盘空间和可用磁盘空间可能无法准确相加得到磁盘空间总量。
--disk-space-avail	收集和发送选定磁盘的 DiskSpaceAvailable 指标。指标以千兆字节报告。 受限于 Linux 操作系统中的保留磁盘空间，已用磁盘空间和可用磁盘空间可能无法准确相加得到磁盘空间总量。
--memory-units=UNITS	指定报告内存使用率所采用的单位。如果不指定，则内存以兆字节报告。单位可以是以下一种：字节、千字节、兆字节、千兆字节。
--disk-space-units=UNITS	指定报告磁盘空间使用率所采用的单位。如果不指定，则磁盘空间以千兆字节报告。单位可以是以下一种：字节、千字节、兆字节、千兆字节。
--aws-credential-file=PATH	提供包含 Amazon 凭证的文件的位置。 此参数不能与 --aws-access-key-id 和 --aws-secret-key 参数一起使用。
--aws-access-key-id=VALUE	指定用于识别发起人的 Amazon 访问密钥 ID。必须与 --aws-secret-key 选项一起使用。不要将该选项与 --aws-credential-file 参数一起使用。
--aws-secret-key=VALUE	指定用于签署 CloudWatch 请求的 Amazon 秘密访问密钥。必须与 --aws-access-key-id 选项一起使用。不要将该选项与 --aws-credential-file 参数一起使用。
--aws-iam-role=VALUE	指定用于提供 Amazon 凭证的 IAM 角色。必须提供 =VALUE 值。如果不指定凭证，则会应用与 EC2 实例关联的默认 IAM 角色。只能使用一个 IAM 角色。如果未找到任何 IAM 角色，或者找到多个 IAM 角色，则脚本会返回一条错误信息。 请勿将该选项与 --aws-credential-file、--aws-access-key-id 或 --aws-secret-key 参数一起使用。
--aggregated[=only]	为实例类型、AMI ID 及区域整体情况添加聚合指标。=only 值是可选的，如果指定，则脚本只报告聚合指标。
--auto-scaling[=only]	为 Auto Scaling 组添加聚合指标。=only 值为可选，如果指定，则脚本只会报告 Auto Scaling 指标。与使用脚本的 IAM 用户或角色关联的 IAM policy 需要具有调用 EC2 操作 DescribeTags 的权限。
--verify	会对收集指标的脚本执行一次试运行，准备完整 HTTP 请求，但是不会调用 CloudWatch 以报告数据。该选项还会检查是否已提供凭证。在详细模式中运行时，该选项输出的指标会发送到 CloudWatch。
--from-cron	从 cron 调用脚本时，请使用该选项。使用该选项时，会阻止所有诊断输出，但会将错误消息发送到用户的本地系统日志。
--verbose	显示脚本正在处理的内容的详细信息。
--help	显示使用率信息。
--version	显示脚本的版本号。

示例

以下示例假设您提供了一个 IAM 角色或 awscreds.conf 文件。否则，您必须使用 --aws-access-key-id 和 --aws-secret-key 参数为这些命令提供凭证。

以下示例执行简单的测试运行而不将数据发布到 CloudWatch。

```
./mon-put-instance-data.pl --mem-util --verify --verbose
```

以下示例收集所有可用内存指标并将其发送到 CloudWatch，将缓存和缓冲区内存计为“已用”

```
./mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --mem-used --mem-avail
```

以下示例收集 Auto Scaling 组的聚合指标并将其发送到 Amazon CloudWatch，但不报告单独的实例指标。

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --auto-scaling=only
```

以下示例收集实例类型、AMI ID 和区域的聚合指标并将其发送到 Amazon CloudWatch，但不报告单独的实例指标

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --aggregated=only
```

要为向 CloudWatch 报告的指标制定 cron 计划，请使用 crontab -e 命令开始编辑 crontab。添加下列命令，每五分钟将内存和磁盘空间使用率报告到 CloudWatch：

```
*/5 * * * * ~/aws-scripts-mon/mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --disk-space-util --disk-path=/ --from-cron
```

如果脚本遇到错误，它会在系统日志中写下错误消息。

mon-get-instance-stats.pl

此脚本可在使用最近小时数提供的时间间隔内查询 CloudWatch 中有关内存、交换和磁盘空间指标的统计数据。将为对其运行此脚本的 Amazon EC2 实例提供该数据。

选项

名称	说明
--recent-hours=N	指定报告依据的最近小时数，由 N 表示，其中 N 是一个整数。
--aws-credential-file=PATH	提供包含 Amazon 凭证的文件的位置。
--aws-access-key-id=VALUE	指定用于识别发起人的 Amazon 访问密钥 ID。必须与 --aws-secret-key 选项一起使用。不要将该选项与 --aws-credential-file 选项一起使用。
--aws-secret-key=VALUE	指定用于签署 CloudWatch 请求的 Amazon 秘密访问密钥。必须与 --aws-access-key-id 选项一起使用。不要将该选项与 --aws-credential-file 选项一起使用。
--aws-iam-role=VALUE	指定用于提供 Amazon 凭证的 IAM 角色。必须提供 =VALUE 值。如果不指定凭证，则会应用与 EC2 实例关联的默认 IAM 角色。只能使用一个 IAM 角色。如果未找到任何 IAM 角色，或者找到多个 IAM 角色，则脚本会返回一条错误信息。

名称	说明
	请勿将该选项与 `--aws-credential-file`、`--aws-access-key-id` 或 `--aws-secret-key` 参数一起使用。
`--verify`	执行脚本的测试运行。该选项还会检查是否已提供凭证。
`--verbose`	显示脚本正在处理的内容的详细信息。
`--help`	显示使用率信息。
`--version`	显示脚本的版本号。

示例

要获得最近 12 小时的使用率统计数据，请运行以下命令：

```
./mon-get-instance-stats.pl --recent-hours=12
```

以下为响应示例：

```
Instance metric statistics for the last 12 hours.

CPU Utilization
    Average: 1.06%, Minimum: 0.00%, Maximum: 15.22%

Memory Utilization
    Average: 6.84%, Minimum: 6.82%, Maximum: 6.89%

Swap Utilization
    Average: N/A, Minimum: N/A, Maximum: N/A

Disk Space Utilization on /dev/xvda1 mounted as /
    Average: 9.69%, Minimum: 9.69%, Maximum: 9.69%
```

在控制台中查看自定义指标

在成功运行 `mon-put-instance-data.pl` 脚本后，您可以在 Amazon CloudWatch 控制台中查看自定义指标。

要查看自定义指标

1. 如前所述运行 `mon-put-instance-data.pl`。
2. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
3. 选择 View Metrics。
4. 对于 Viewing，由脚本发布的自定义指标带有前缀 `System/Linux`。

问题排查

CloudWatchClient.pm 模块在本地缓存实例元数据。如果您从运行监控脚本的实例中创建 AMI，在缓存 TTL (默认值：6 小时；对于 Auto Scaling 组为 24 小时) 内从此 AMI 启动的任何实例都将使用原始实例的实例 ID 发送指标。缓存 TTL 时间段过后，脚本会检索新数据，监控脚本将使用当前实例的实例 ID。要立即更正此问题，请使用以下命令删除缓存数据：

```
rm /var/tmp/aws-mon/instance-id
```

使用 Amazon CloudTrail 记录 Amazon EC2 和 Amazon EBS API 调用

Amazon EC2 和 Amazon EBS 与 Amazon CloudTrail 集成，该服务在 Amazon EC2 和 Amazon EBS 中提供用户、角色或 Amazon 服务所采取的操作的记录。CloudTrail 将对 Amazon EC2 和 Amazon EBS 的所有 API 调用作为事件捕获，包括来自控制台的调用和对API 的代码调用。如果您创建了跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 Amazon EC2 和 Amazon EBS 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。通过使用 CloudTrail 收集的信息，您可以确定向 Amazon EC2 和 Amazon EBS发出的请求、从中发出请求的 IP 地址、发出请求的用户、发出请求的时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 Amazon CloudTrail 用户指南。

CloudTrail 中的 Amazon EC2 和 Amazon EBS 信息

在您创建 Amazon Web Services 账户 时，将在该账户上启用 CloudTrail。当 Amazon EC2 和 Amazon EBS 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon Web Service 事件一同保存在事件历史记录中。您可以在 Amazon Web Services 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon Web Services 账户 中的事件（包括 Amazon EC2 和 Amazon EBS 的事件），请创建跟踪。通过跟踪，CloudTrail 可将日志文件传送至 Amazon S3 桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有Amazon Web Services 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 Amazon服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅：

- 为您的 Amazon Web Services 账户 创建跟踪
- Amazon Web Service与 CloudTrail 日志的集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon EC2 操作和 Amazon EBS 管理操作都由 CloudTrail 记录，并记录在 Amazon EC2 API Reference 钟。例如，调用 RunInstances、DescribeInstances 或 CreateImage 操作会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 Amazon Web Service 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon EC2 和 Amazon EBS 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的日志文件记录显示，用户终止了一个实例。

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```


使用 Amazon CloudTrail 审计通过 EC2 Instance Connect 连接的用户

使用 Amazon CloudTrail 审计通过 EC2 Instance Connect 连接到实例的用户。

使用 Amazon CloudTrail 控制台审计通过 EC2 Instance Connect 的 SSH 活动

1. 从 Amazon CloudTrail 打开 https://console.amazonaws.cn/cloudtrail/ 控制台。
2. 验证您是否位于正确的区域中。
3. 在导航窗格中，选择事件历史记录。
4. 对于筛选条件，请选择事件源，然后选择 ec2-instance-connect.amazonaws.com。
5. （可选）对于时间范围，请选择一个时间范围。

6. 选择刷新事件图标。
7. 该页面显示与 SendSSHPublicKey API 调用对应的事件。使用箭头展开一个事件以查看其他详细信息，例如，用于建立 SSH 连接的用户名和 Amazon 访问密钥以及源 IP 地址。
8. 要以 JSON 格式显示完整事件信息，请选择查看事件。requestParameters 字段包含用于建立 SSH 连接的目标实例 ID、操作系统用户名和公有密钥。


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


如果已将 Amazon 账户配置为在 S3 存储桶中收集 CloudTrail 事件，您可以按编程方式下载和审计该信息。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的获取和查看 CloudTrail 日志文件。

Amazon EC2 中的联网功能

通过 Amazon VPC，您可以在专供您的Amazon账户使用的虚拟网络（称为 Virtual Private Cloud (VPC)）中启动Amazon资源，如 Amazon EC2 实例。启动实例时，您可以从 VPC 中选择子网。该实例配置了主网络接口，即逻辑虚拟网卡。该实例从子网的 IPv4 地址接收主要私有 IP 地址，并将其分配到主网络接口。

您可以控制实例是否从 Amazon 的公有 IP 地址池接收公有 IP 地址。实例的公有 IP 地址会与您的实例关联，直至实例停止或终止。如果您需要持久性公有 IP 地址，可以为 Amazon 账户分配弹性 IP 地址，并将其与实例或网络接口关联。在您释放弹性 IP 地址之前，该地址仍然与您的 Amazon 账户关联，您可以根据需要将其从一个实例移动到另一个实例。您可以在 Amazon 账户中使用您自己的 IP 地址，它会显示为地址池，然后从地址池中分配弹性 IP 地址。

要提高网络性能并减少延迟，您可以在置放群组中启动实例。您可以使用增强型联网功能显著地提高每秒数据包数 (PPS) 性能。您可以使用 Elastic Fabric Adapter (EFA) 加速高性能计算和机器学习应用程序，这是一种可以附加到支持的实例类型的网络设备。

功能

- 区域和可用区 (p. 1040)
- Amazon EC2 实例 IP 寻址 (p. 1053)
- Amazon EC2 实例主机名类型 (p. 1067)
- 在 Amazon EC2 中使用您自己的 IP 地址 (BYOIP) (p. 1070)
- 为 Amazon EC2 网络接口分配前缀 (p. 1083)
- 弹性 IP 地址 (p. 1094)
- 弹性网络接口 (p. 1104)
- Amazon EC2 实例网络带宽 (p. 1141)
- Linux 上的增强联网 (p. 1142)
- 置放群组 (p. 1177)
- EC2 实例的网络最大传输单位 (MTU) (p. 1192)
- Virtual Private Cloud (p. 1194)
- EC2-Classic (p. 1196)

区域和可用区

Amazon EC2 托管在全球多个位置。这些位置由 Amazon Web Services 区域、可用区、Local Zones、Amazon Outposts 和 Wavelength Zones 组成。

- 每个区域都是一个单独的地理区域。
- 可用区是每个区域内的多个相互隔离的位置。
- Local Zones 让您可以在多个离最终用户较近的位置放置资源（如计算和存储）。
- Amazon Outposts 可将本机 Amazon 服务、基础设施和运营模式引入几乎任何数据中心、主机托管空间或本地设施。
- 利用 Wavelength 区域，开发人员可以为 5G 设备和最终用户打造具有超低延迟的应用程序。Wavelength 可以将标准 Amazon 计算和存储服务部署到电信运营商的 5G 网络边缘。

Amazon运行着具有高可用性的先进数据中心。数据中心有时会发生影响托管于同一位置的所有实例的可用性的故障，虽然这种故障极少发生。如果您将所有实例都托管在受故障影响的同一个位置，则您的所有实例都将不可用。

要帮助您确定哪种部署最适合您，请参阅 Amazon Wavelength 常见问题解答。

目录

- 区域 (p. 1041)
- 可用区 (p. 1045)
- Local Zones (p. 1048)
- Wavelength 区域 (p. 1050)
- Amazon Outposts (p. 1052)

区域

从设计而言，每个 区域都与其他 区域隔离。这可实现最大程度的容错能力和稳定性。

当您查看资源时，只会看到与您指定的 区域关联的资源。这是因为 区域间彼此隔离，而且我们不会自动跨区域复制资源。

当您启动某个实例时，必须选择位于同一区域的 AMI。如果 AMI 在其他区域，您可将该 AMI 复制到您使用的区域。有关更多信息，请参阅复制 AMI (p. 172)。

请注意，在区域之间传输数据需要收费。有关更多信息，请参阅 Amazon EC2 定价 - 数据传输。

目录

- 可用区 (p. 1041)
- 区域和终端节点 (p. 1042)
- 描述您的区域 (p. 1043)
- 获取区域名称 (p. 1043)
- 指定资源的区域 (p. 1044)

可用区

您的账户确定了适用于您的区域。

- Amazon Web Services 账户 提供多个区域，因此您可在符合您要求的位置启动 Amazon EC2 实例。例如，您可能希望在欧洲区域启动实例以更多符合欧洲客户的要求或满足法律要求。
- Amazon GovCloud（美国西部）账户提供对 Amazon GovCloud（美国西部）区域和 Amazon GovCloud（美国东部）区域的访问。有关更多信息，请参阅Amazon GovCloud (US)。
- 您只能通过 Amazon（Amazon中国）账户访问北京和宁夏区域。有关更多信息，请参阅 中国的 Amazon Web Services。

下表列出的是 Amazon Web Services 账户 提供的区域。您不能通过 Amazon Web Services 账户 描述或访问其他区域，例如 Amazon GovCloud (US) Regions 或中国区域。要使用 2019 年 3 月 20 日之后推出的区域，您必须启用区域。有关更多信息，请参阅 Amazon 一般参考中的管理 Amazon 区域。

代码	名称	选择加入状态
us-east-2	US East (Ohio)	可选
us-east-1	美国东部（弗吉尼亚北部）	可选

代码	名称	选择加入状态
us-west-1	美国西部（加利福尼亚北部）	可选
us-west-2	美国西部（俄勒冈）	可选
af-south-1	Africa (Cape Town)	必需
ap-east-1	Asia Pacific (Hong Kong)	必填
ap-south-2	亚太地区（海得拉巴）	必填
ap-southeast-3	亚太地区（雅加达）	必填
ap-southeast-4	亚太地区（墨尔本）	必填
ap-south-1	Asia Pacific (Mumbai)	可选
ap-northeast-3	Asia Pacific (Osaka)	可选
ap-northeast-2	Asia Pacific (Seoul)	可选
ap-southeast-1	亚太地区（新加坡）	可选
ap-southeast-2	亚太地区（悉尼）	可选
ap-northeast-1	亚太区域（东京）	可选
ca-central-1	Canada (Central)	可选
eu-central-1	Europe (Frankfurt)	可选
eu-west-1	欧洲（爱尔兰）	可选
eu-west-2	Europe (London)	可选
eu-south-1	Europe (Milan)	必需
eu-west-3	Europe (Paris)	可选
eu-south-2	欧洲（西班牙）	必填
eu-north-1	欧洲（斯德哥尔摩）	可选
eu-central-2	欧洲（苏黎世）	必填
me-south-1	中东（巴林）	必填
me-central-1	中东（阿联酋）	必填
sa-east-1	南美洲（圣保罗）	可选

如需更多信息，请参阅 Amazon 全球基础设施。

每个区域可用区的数量和映射可能因 Amazon Web Services 账户 而异。要获取可用于您账户的可用区列表，可使用 Amazon EC2 控制台或命令行界面。有关更多信息，请参阅描述您的区域 (p. 1043)。

区域和终端节点

当您通过命令行界面或 API 操作使用实例时，必须指定其区域终端节点。有关 Amazon EC2 的区域和终端节点的更多信息，请参阅 Amazon Web Services General Reference 中的 Amazon EC2 终端节点和配额。

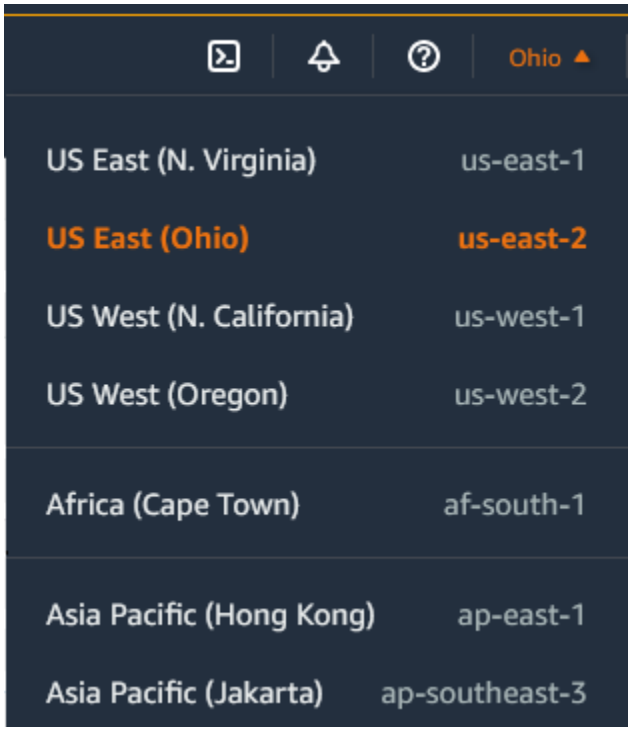
有关 Amazon GovCloud（美国西部）中的端点和协议的更多信息，请参阅《Amazon GovCloud (US) 用户指南》中的服务端点。

描述您的区域

您可使用 Amazon EC2 控制台或命令行界面来确定适用于您的账户的区域。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

使用控制台查找您的区域

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选中 Regions（区域）选择器。



3. 此区域的 EC2 资源显示在资源部分中的 EC2 控制面板上。

使用 Amazon CLI 查找您的区域

使用如下 describe-regions 命令描述为您的账户启用的区域。

```
aws ec2 describe-regions
```

要描述所有区域（包括为账户禁用的任何区域），请添加 `--all-regions` 选项，如下所示。

```
aws ec2 describe-regions --all-regions
```

获取区域名称

您可以使用 Amazon Lightsail API 查看区域的名称。

使用 Amazon CLI 查看区域名称

如下所示使用 get-regions 命令，描述指定区域的名称。

```
aws lightsail get-regions --query "regions[?name=='region-name'].displayName" --output text
```

以下示例返回 us-east-2 区域的名称。

```
aws lightsail get-regions --query "regions[?name=='us-east-2'].displayName" --output text
```

下面是输出：

```
Ohio
```

指定资源的区域

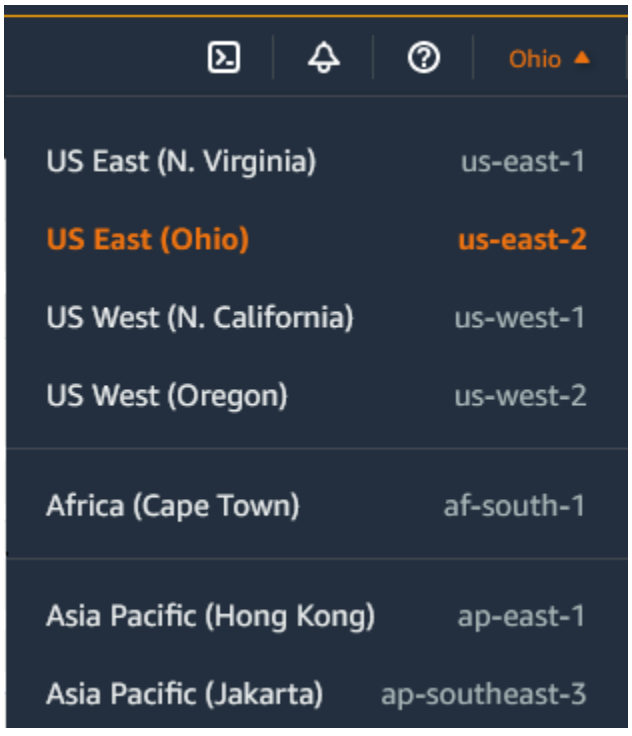
每次创建 Amazon EC2 资源时，您都可为该资源指定区域。您可以使用 Amazon Web Services Management Console或命令行为资源指定区域。

注意事项

某些 Amazon 资源可能并非在所有区域都可用。在启动实例之前，确保您可以在所需区域中创建所需的资源。

使用控制台为资源指定区域

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选中 Regions（区域）选择器，然后选择区域。



使用命令行指定默认区域

可以将环境变量的值设置为所需的区域终端节点（例如，https://ec2.us-east-2.amazonaws.com）：

- `AWS_DEFAULT_REGION` (Amazon CLI)
- `Set-AWSDefaultRegion` (Amazon Tools for Windows PowerShell)

或者，您可针对各个单独的命令使用 `--region` (Amazon CLI) 或 `-Region` (Amazon Tools for Windows PowerShell) 命令行选项。例如：`--region us-east-2`。

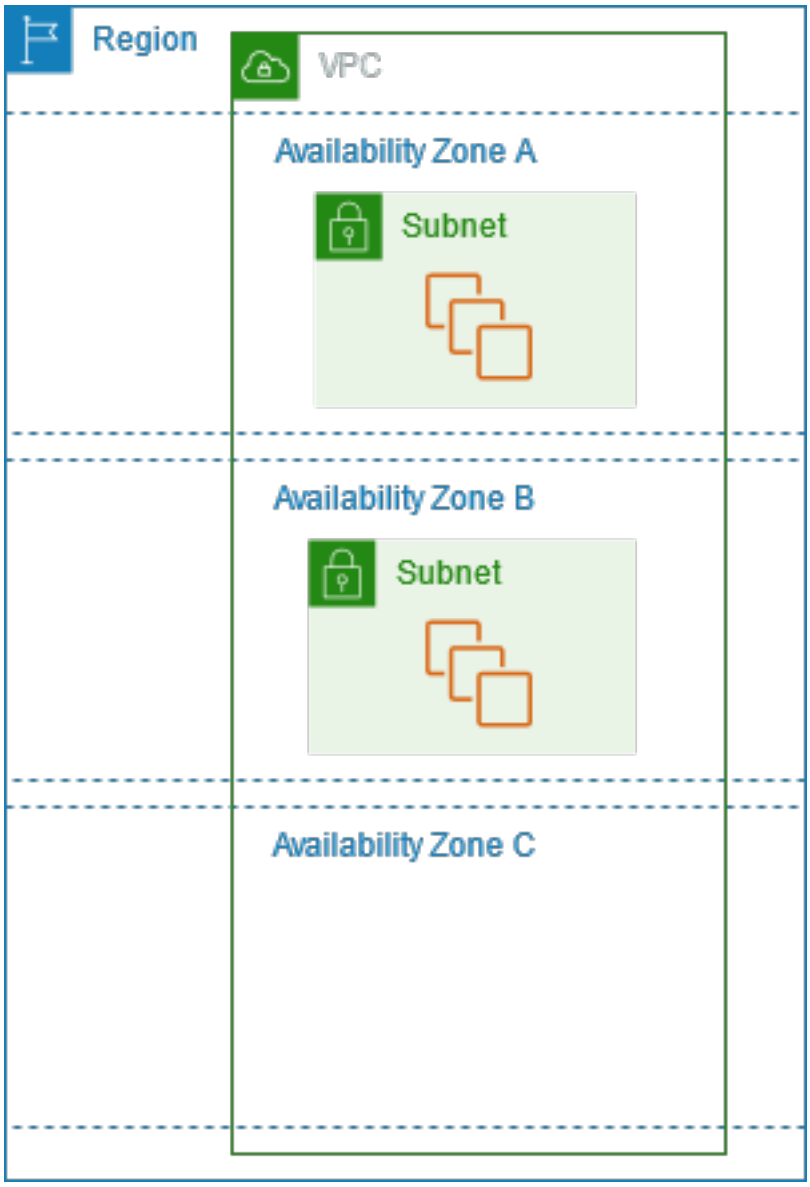
有关适用于 Amazon EC2 的端点的更多信息，请参阅《Amazon 一般参考》中的服务端点。

可用区

每个区域都有多个相互隔离的位置，称为可用区。可用区的代码由其区域代码后跟一个字母标识符组成。例如，`us-east-1a`。

启动实例时，您可以选择区域和 Virtual Private Cloud (VPC)，然后可以从可用区中选择子网，也可以让我们为您选择子网。如果您的实例分布在多个可用区且其中的某个实例发生故障，则您可对您的应用程序进行相应设计，以使另一可用区中的实例可代为处理相关请求。您也可使用弹性 IP 地址来掩蔽某个可用区中的实例所发生的故障，方法是快速将该地址重新映射到另一可用区中的实例。

下图说明 Amazon 区域中的多个可用区。可用区 A 和可用区 B 各有一个子网，每个子网均有实例。可用区 C 没有子网，因此您无法在此可用区内启动实例。



随着可用区域中内容的增加，我们对其进行扩展的能力会逐渐受限。如果发生此情况，我们可能会阻止您在扩展能力受限的可用区内启动实例，除非您在此可用区中已拥有实例。最终，我们还可能将扩展能力受限的可用区从新账户的可用区列表中删除。因此，您的不同账户在一个区域中可用的可用区数量可能不同。

目录

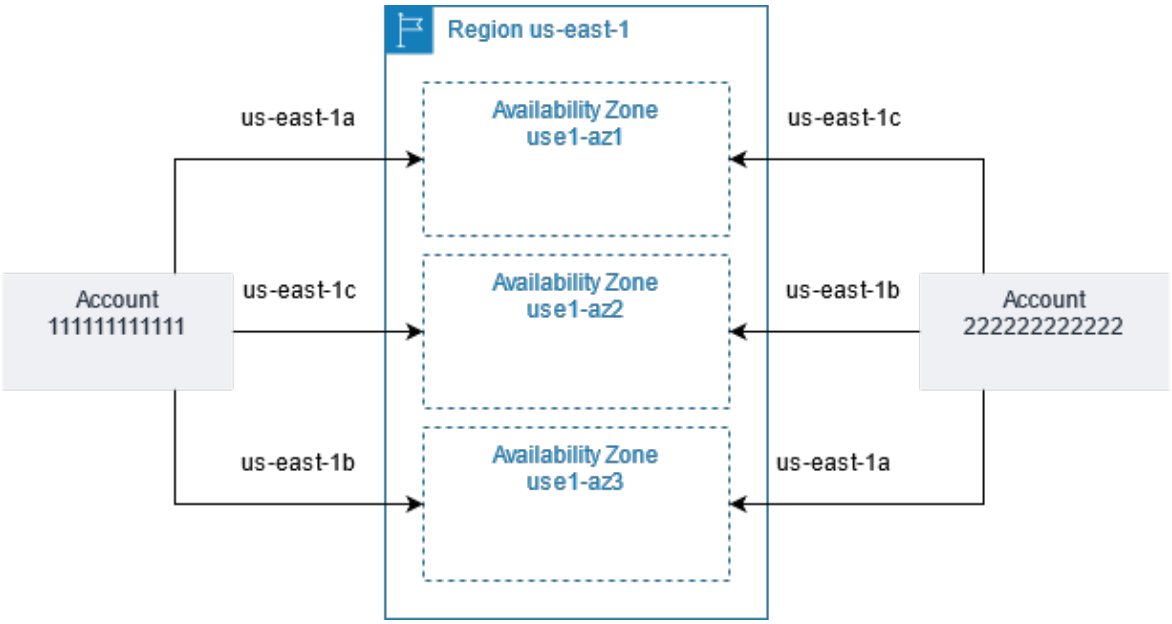
- AZ ID (p. 1047)
- 描述您的可用区 (p. 1047)
- 在可用区中启动实例 (p. 1048)
- 将实例迁移到其他可用区 (p. 1048)

AZ ID

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个 Amazon Web Services 账户 的代码。例如，您 Amazon Web Services 账户 的可用区 `us-east-1a` 可能与另一 Amazon Web Services 账户 的 `us-east-1a` 不在同一实际位置。

要跨账户协调可用区，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，`use1-az1` 是 `us-east-1` 区域的可用区 ID，它在每个 Amazon Web Services 账户 中的实际位置均相同。您可以查看您账户的可用区 ID，以确定您的资源相对于另一个账户中的资源所在的实际位置。例如，如果您在 AZ ID 为 `use1-az2` 的可用区中与另一个账户共享一个子网，则在 AZ ID 也为 `use1-az2` 的可用区中该账户便可使用这一子网。

下图展示了可用区代码到可用区 ID 有着不同映射的两个账户。



描述您的可用区

您可使用 Amazon EC2 控制台或命令行界面来确定适用于您的账户的可用区。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

使用控制台查找可用区

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选中 Regions（区域）选择器，然后选择区域。
3. 在导航窗格上，选择 EC2 Dashboard。
4. 可用区在 Service health（服务运行状况）窗格中列出。

使用 Amazon CLI 查找您的可用区

- 使用如下的 describe-availability-zones 命令描述在指定区域内已为您的账户启用的可用区。

```
aws ec2 describe-availability-zones --region region-name
```

- 使用如下 describe-availability-zones 命令描述可用区，而不管选择加入状态如何。

```
aws ec2 describe-availability-zones --all-availability-zones
```

在可用区中启动实例

当您启动实例时，请选择能让您的实例更接近特定客户的区域，或选择能够满足法律或您的其他要求的区域。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。

当您启动实例时，可以选择指定您所用区域中的可用区。如果您未指定可用区，我们将为您选择一个可用区。启动初始实例时，我们建议您接受默认可用区，因为这允许我们根据系统运行状况和可用容量为您选择最佳可用区。如果您要启动其他实例，则除非您的新实例必须接近正在运行的实例或必须与正在运行的实例相隔离，否则请不要为新实例指定可用区。

将实例迁移到其他可用区

如有必要，您可以将实例从一个可用区迁移到另一个可用区。例如，如果您尝试修改实例的实例类型，而我们无法在当前可用区中启动新实例类型的实例，您可以将实例迁移到具有新实例类型容量的可用区。

迁移过程包括：

- 从原始实例创建 AMI
- 在新可用区中启动实例
- 更新新实例的配置，如以下过程所示

将实例迁移到其他可用区

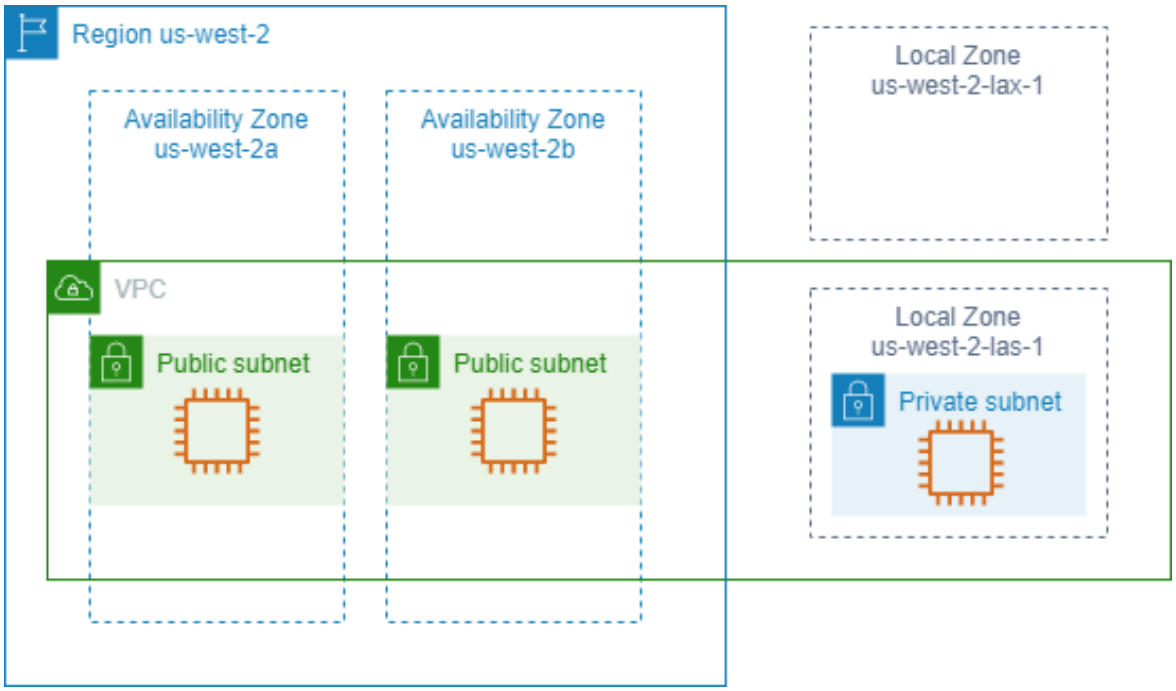
1. 从该实例创建 AMI。迁移过程取决于操作系统和实例的根设备卷的类型。有关更多信息，请参阅对应于您的操作系统和根设备卷的文档：
   - 创建由 Amazon EBS 支持的 Linux AMI
   - 创建由实例存储支持的 Linux AMI
   - 创建自定义 Windows AMI
2. 如果需要保留实例的私有 IPv4 地址，必须删除当前可用区中的子网，然后在新可用区中用与原始子网相同的 IPv4 地址范围创建子网。请注意，在删除子网前，您必须终止该子网中的所有实例。因此，您应从子网中的所有实例创建 AMI，这样您就可以将当前子网中的所有实例迁移到新子网。
3. 指定新的可用区或子网，从您刚创建的 AMI 启动一个实例。您可以使用与初始实例相同的实例类型，也可以选择新实例类型。有关更多信息，请参阅在可用区中启动实例 (p. 1048)。
4. 如果原始实例有关联的弹性 IP 地址，则请将其与新实例相关联。有关更多信息，请参阅解除弹性 IP 地址的关联 (p. 1098)。
5. 如果原始实例是 Reserved Instance，请更改预留的可用区。（如果您还更改了实例类型，则可以更改预留的实例类型。）有关更多信息，请参阅提交修改请求 (p. 439)。
6. （可选）终止原始实例。有关更多信息，请参阅终止实例 (p. 636)。

Local Zones

本地区域是在地理上靠近您的用户的 Amazon 区域的扩展。Local Zones 有自己的互联网连接并支持 Amazon Direct Connect，以便在本地区域中创建的资源可以通过低延迟通信为本地用户提供服务。有关更多信息，请参阅 Amazon Local Zones。

本地区域的代码由其区域代码后跟一个指示其实际位置的标识符组成。例如，在洛杉矶的 `us-west-2-lax-1`。

下图说明了 Amazon 区域 us-west-2、其两个可用区及其两个本地区域。VPC 跨多个可用区和其中一个本地区域。VPC 中的每个区域都有一个子网，每个子网都有一个实例。



要使用 Local Zones，您必须先启用它。有关更多信息，请参阅the section called “选择加入 Local Zones” (p. 1049)。接下来，在本地扩展区中创建子网。最后，在 Local Zone 子网中启动实例等资源，以确保您的应用程序靠近用户。

目录

- 选择加入 Local Zones (p. 1049)
- 在 Local Zones 中启动实例 (p. 1050)

选择加入 Local Zones

您必须选择加入 Local Zones，然后才能为资源或服务指定本地区域。

考虑因素

某些 Amazon 资源可能并非在所有区域都可用。在特定的 Local Zones内启动实例之前，请确保您可以在所需的区域或本地区域内创建您需要的资源。有关每个 Local Zone 中支持的服务列表，请参阅 Amazon Local Zones 功能。

要使用控制台选择加入 Local Zones

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在页面左上角，选择新的 EC2 体验。您无法使用旧的控制台体验完成此任务。
3. 在导航栏中，选中 Regions（区域）选择器，然后选择父级区域。
4. 在导航窗格上，选择 EC2 Dashboard。
5. 在页面的右上角，选择账户属性，然后选择区域。
6. 要启用 Local Zone，请选择 Manage（管理）。
7. 对于 区域组，选择已启用。

8. 选择更新区域组。

要使用 Amazon CLI 选择加入 Local Zones

使用 modify-availability-zone-group 命令。

在 Local Zones 中启动实例

启动实例时，您可以指定位于 Local Zone 中的子网。您可以从网络边界组分配 IP 地址。网络边界组是一组唯一的可用区、Local Zones 或 Wavelength 区域（Amazon 可从中通告 IP 地址，例如 `us-west-2-lax-1a`）。

您可以从网络边界组分配以下 IP 地址：

- Amazon 提供的弹性 IPv4 地址
- Amazon 提供的 IPv6 VPC 地址（仅在洛杉矶区域可用）

有关如何在 Local Zone 中启动实例的更多信息，请参阅《Amazon Local Zone 用户指南》中的 Amazon Local Zone 入门。

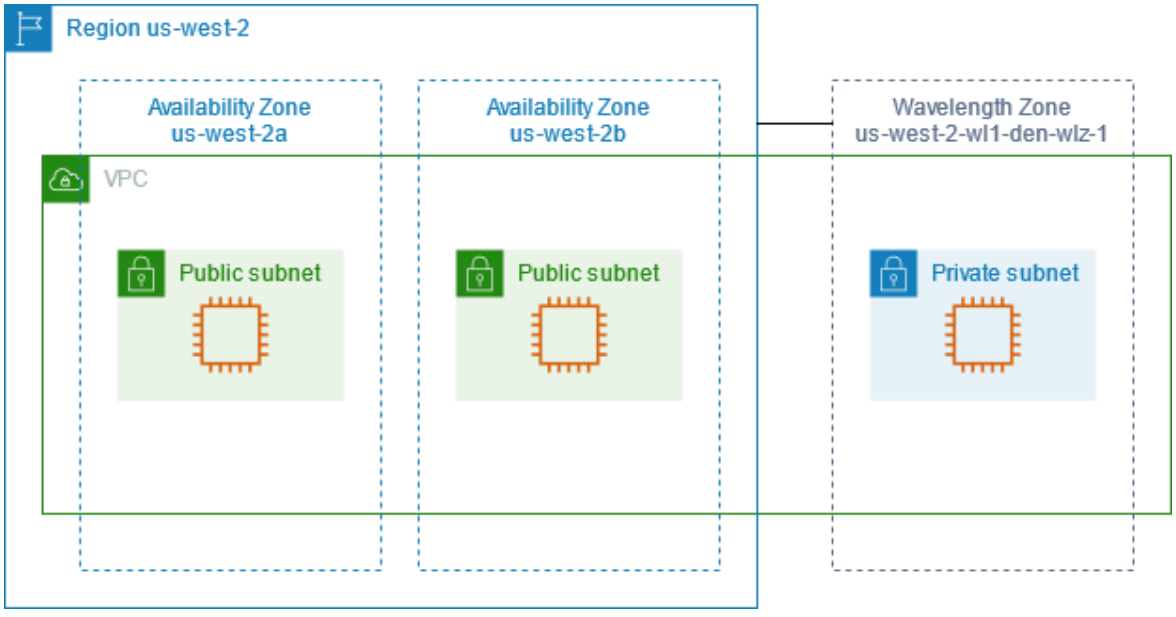
Wavelength 区域

利用 Amazon Wavelength，开发人员可以为移动设备和最终用户打造具有超低延迟的应用程序。Wavelength 可以将标准 Amazon 计算和存储服务部署到电信运营商的 5G 网络边缘。开发人员可以将 Virtual Private Cloud（VPC）扩展到一个或多个 Wavelength 区域，然后使用 Amazon EC2 实例等 Amazon 资源来运行需要超低延迟并连接到区域中的 Amazon 服务的应用程序。

Wavelength 区域是在其中部署 Wavelength 基础设施的运营商位置中的隔离区域。Wavelength 区域与一个区域相关联。Wavelength 区域是区域的逻辑扩展，由区域中的控制平面管理。

Wavelength 区域的代码由其区域代码后跟一个指示实际位置的标识符组成。例如，在波士顿的 `us-east-1-wl1-bos-wlz-1`。

下图说明了 Amazon 区域 `us-west-2`、其两个可用区及 Wavelength 区域。VPC 跨多个可用区和 Wavelength 区域。VPC 中的每个区域都有一个子网，每个子网都有一个实例。



要使用 Wavelength 区域，您必须首先选择加入此区域。有关更多信息，请参阅the section called “启用 Wavelength 区域” (p. 1051)。接下来，在 Wavelength 区域中创建子网。最后，在 Wavelength 区域子网中启动资源，以便您的应用程序更接近最终用户。

Wavelength 区域并非在每个区域中都可用。有关支持 Wavelength 区域的区域的信息，请参阅 Amazon Wavelength 开发人员指南中的可用 Wavelength 区域。

目录

- 描述您的 Wavelength 区域 (p. 1051)
- 启用 Wavelength 区域 (p. 1051)
- 在 Wavelength 区域中启动实例 (p. 1052)

描述您的 Wavelength 区域

您可使用 Amazon EC2 控制台或命令行界面来确定适用于您的账户的 Wavelength 区域。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

使用控制台查找 Wavelength 区域

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选中 Regions（区域）选择器，然后选择区域。
3. 在导航窗格上，选择 EC2 Dashboard。
4. 在页面的右上角，选择账户属性，然后选择区域。

使用 Amazon CLI 查找 Wavelength 区域

- 使用如下的 describe-availability-zones 命令描述在指定区域内已为您的账户启用的 Wavelength Zone。

```
aws ec2 describe-availability-zones --region region-name
```

- 使用如下 describe-availability-zones 命令描述 Wavelength 区域，而不管选择加入状态如何。

```
aws ec2 describe-availability-zones --all-availability-zones
```

启用 Wavelength 区域

在为资源或服务指定 Wavelength 区域之前，必须启用 Wavelength 区域。

注意事项

- 某些 Amazon 资源并非在所有区域中都可用。在特定的 Wavelength 区域中启动实例之前，请确保您可以在所需的区域或 Wavelength 区域中创建您需要的资源。

使用控制台选择加入 Wavelength 区域

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在页面左上角，选择新的 EC2 体验。您无法使用旧的控制台体验完成此任务。
3. 在导航栏中，选中 Regions（区域）选择器，然后选择区域。
4. 在导航窗格上，选择 EC2 Dashboard。
5. 在页面的右上角，选择账户属性，然后选择区域。

6. 在 Wavelength Zones（Wavelength 区域）下，为 Wavelength 区域选择 Manage（管理）。
7. 请选择 Enable。
8. 选择更新区域组。

使用 Amazon CLI 启用 Wavelength 区域

使用 modify-availability-zone-group 命令。

在 Wavelength 区域中启动实例

启动实例时，您可以指定位于 Wavelength 区域中的子网。您还可以从网络边界组分配运营商 IP 地址，该组是一组唯一的可用区、Local Zones 或 Wavelength 区域（Amazon 可从中通告 IP 地址，例如 `us-east-1-wl1-bos-wlz-1`）。

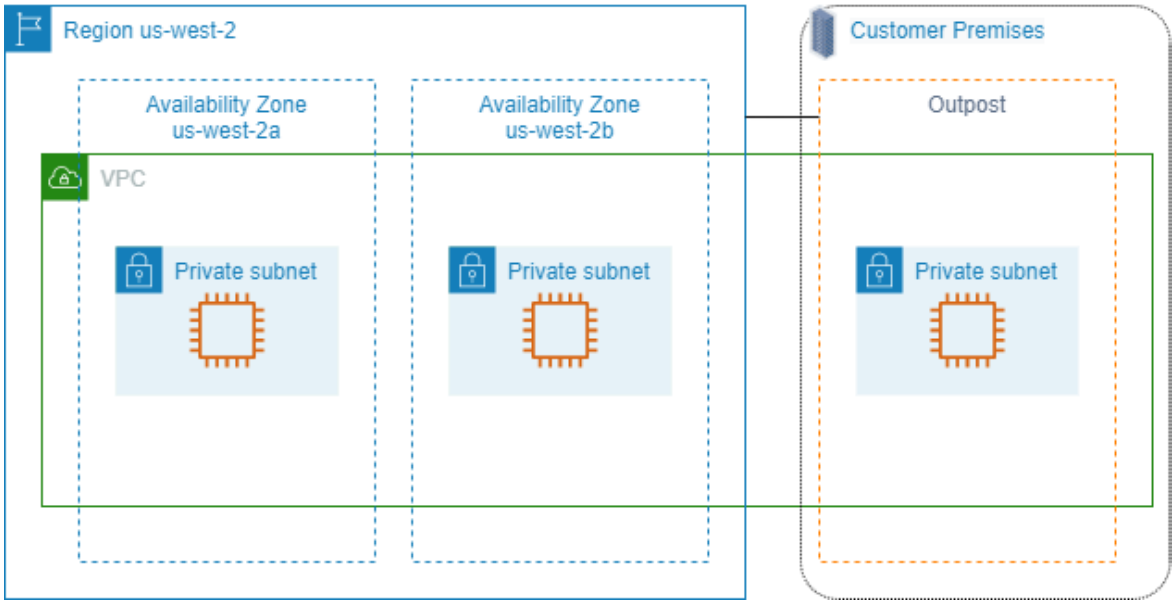
有关如何在 Wavelength 区域中启动实例的信息，请参阅 Amazon Wavelength 开发人员指南中的 Amazon Wavelength 入门。

Amazon Outposts

Amazon Outposts 是一项完全托管的服务，可将 Amazon 基础设施、服务、API 和工具扩展到客户场所。通过提供对 Amazon 托管基础设施的本地访问，Amazon Outposts 使客户能够使用与 Amazon 区域中相同的编程接口在本地构建和运行应用程序，同时使用本地计算和存储资源来满足更低的延迟和本地数据处理需求。

Outpost 是部署在客户站点的 Amazon 计算和存储容量池。Amazon 作为 Amazon 区域的一部分运营、监控和管理此容量。您可以在 Outpost 上创建子网，并在创建 Amazon 资源时指定这些子网。Outpost 子网中的实例使用私有 IP 地址与 Amazon 区域中的其他实例通信，全部都在相同 VPC 内进行。

下图说明了 Amazon 区域 `us-west-2`、其两个可用区及 Outpost。VPC 跨多个可用区和 Outpost。Outpost 位于本地部署的客户数据中心。VPC 中的每个区域都有一个子网，每个子网都有一个实例。



要开始使用 Amazon Outposts，您必须创建一个 Outpost 并订购 Outpost 容量。有关 Outposts 配置的更多信息，请参阅我们的目录。安装 Outpost 设备后，当您在 Outpost 上启动 Amazon EC2 实例时，可以使用计算和存储容量。

在 Outpost 上启动实例

您可以在您创建的 Outpost 子网中启动 EC2 实例。安全组控制 Outpost 子网中具有弹性网络接口的实例的入站和出站流量，就像对待可用区子网中的实例一样。要连接到 Obpost 子网中的 EC2 实例，您可以在启动实例时指定密钥对，就像对待可用区子网中的实例一样。

Outpost 机架上实例的根卷必须小于或等于 30 GB。您可以在 AMI 或实例的块储存设备映射中指定数据卷以提供额外存储。要从引导卷中裁剪未使用的块，请参阅 Amazon 合作伙伴网络博客中的如何构建稀疏 EBS 卷。

我们建议您增加根卷的 NVMe 超时。有关更多信息，请参阅I/O 操作超时 (p. 1522)。

有关如何创建 Outpost 的信息，请参阅 Amazon Outposts 用户指南中的 Amazon Outposts 入门。

在 Outpost 机架上创建卷

Amazon Outposts 提供机架和服务器外形尺寸。如果容量位于 Outpost 机架上，则您可以在所创建的 Outpost 子网中创建 EBS 卷。创建卷时，请指定 Outpost 的 Amazon Resource Name (ARN)。

以下 create-volume 命令在指定的 Outpost 上创建一个空的 50 GB 卷。

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-
east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

您可以在不分离卷的情况下动态修改 Amazon EBS gp2 卷的大小。有关在不分离卷的情况下修改卷的更多信息，请参阅 请求对您的 EBS 卷进行修改 (p. 1495)。

Amazon EC2 实例 IP 寻址

Amazon EC2 和 Amazon VPC 支持 IPv4 和 IPv6 寻址协议。默认情况下，Amazon VPC 使用 IPv4 寻址协议；您无法禁用此行为。创建 VPC 时，您必须指定 IPv4 CIDR 块 (一系列私有 IPv4 地址)。您可以选择将 IPv6 CIDR 块分配给您的 VPC，并将来自该块的 IPv6 地址分配给您子网中的实例。

目录

- 私有 IPv4 地址 (p. 1053)
- 公有 IPv4 地址 (p. 1054)
- 弹性 IP 地址 (IPv4) (p. 1055)
- IPv6 地址 (p. 1055)
- 使用实例的 IPv4 地址 (p. 1055)
- 使用实例的 IPv6 地址 (p. 1057)
- 多个 IP 地址 (p. 1059)
- EC2 实例主机名 (p. 1066)

私有 IPv4 地址

私有 IPv4 地址是指无法通过 Internet 访问的 IP 地址。您可以使用私有 IPv4 地址在同一 VPC 中实现实例之间的通信。有关私有 IPv4 地址标准和规范的更多信息，请参阅 RFC 1918。我们会使用 DHCP 将私有 IPv4 地址分配到实例。

Note

您可以创建一个具有公共可路由的 CIDR 块 (不在 RFC 1918 中指定的私有 IPv4 地址范围内) 的 VPC。但是，出于本文档的写作目的，我们的私有 IPv4 地址 (或"私有 IP 地址") 指的是位于 VPC 的 IPv4 CIDR 范围内的 IP 地址。

VPC 子网可以是以下类型之一：

- 仅 IPv4 子网：您只能在这些子网中创建已分配 IPv4 地址的资源。
- 仅 IPv6 子网：您只能在这些子网中创建已分配 IPv6 地址的资源。
- IPv4 和 IPv6 子网：您可以在这些子网中创建已分配 IPv4 或 IPv6 地址的资源。

在仅 IPv4 或双协议堆栈（IPv4 和 IPv6）子网中启动 EC2 实例时，该实例将在子网的 IPv4 地址范围内收到一个主要私有 IP 地址。有关更多信息，请参阅《Amazon VPC 用户指南》中的 IP 寻址。如果您在启动实例时未指定主要私有 IP 地址，我们会在子网的 IPv4 范围内为您选择一个可用的 IP 地址。每个实例都具有分配了主要私有 IPv4 地址的默认网络接口 (eth0)。您还可以指定其他私有 IPv4 地址，即辅助私有 IPv4 地址。与主要私有 IP 地址不同的是，辅助私有 IP 地址可以从一个实例重新分配到另一个实例。有关更多信息，请参阅多个 IP 地址 (p. 1059)。

私有 IPv4 地址（无论是主地址还是辅助地址）会在实例停止和重新启动或休眠和启动时保持与网络接口的关联，并在实例终止时释放。

公有 IPv4 地址

公有 IP 地址是指可通过 Internet 访问的 IPv4 地址。您可以使用公用 地址在您的实例和 Internet 之间进行通信。

在默认 VPC 中启动实例时，默认情况下，我们会为实例分配公有 IP 地址。当您在非默认 VPC 中启动实例时，子网的一个属性会确定在该子网中启动的实例是否从公有 IPv4 地址池接收公有 IP 地址。默认情况下，我们不会将公有 IP 地址分配到非默认子网中启动的实例。

您可以按如下所示控制实例是否接收公有 IP 地址：

- 修改子网的公有 IP 寻址属性。有关更多信息，请参阅 Amazon VPC 用户指南 中的修改子网的公有 IPv4 寻址属性。
- 在启动过程中启用或禁用公有 IP 寻址功能，以覆盖子网的公有 IP 寻址属性。有关更多信息，请参阅在实例启动期间分配公有 IPv4 地址 (p. 1057)。

公有 IP 地址将从 Amazon 的公有 IPv4 地址池分配给实例，不与您的 Amazon 账户关联。在取消公有 IP 地址与实例的关联后，该地址即会释放回公有 IPv4 地址池中，并且您无法重新使用该地址。

您不能从实例手动关联或取消关联公有 IP (IPv4) 地址。在某些情况下，我们会从您的实例释放公有 IP 地址，或为其分配新的地址：

- 当您的实例已停止、休眠或终止后，我们会释放它的公有 IP 地址。已停止或休眠的实例在启动时会收到一个新的公有 IP 地址。
- 当您将弹性 IP 地址与您实例的公有 IP 地址关联时，我们会释放该公有 IP 地址。当您从实例取消与弹性 IP 地址的关联时，实例会收到新的公有 IP 地址。
- 如果 VPC 中的实例的公有 IP 地址已释放，则在多个网络接口了附加到实例的情况下，该实例不会接收新地址。
- 如果您实例的公有 IP 地址在其辅助私有 IP 地址与弹性 IP 地址关联时被释放，则该实例不会接收新的公有 IP 地址。

如果您需要可根据需要关联到实例并从实例进行关联的永久公有 IP 地址，可改为使用弹性 IP 地址。

如果您使用动态 DNS 来将现有 DNS 名称映射到新实例的公有 IP 地址，可能需要 24 小时，以便 IP 地址可以传递到整个 Internet。其结果是，新的实例可能无法接收流量，而已终止实例继续接收请求。要解决此问题，请使用弹性 IP 地址。您可以分配自己的弹性 IP 地址，并将其与您的实例相关联。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

Note

通过公有 NAT IP 地址访问其他实例的实例需要支付区域或 Internet 数据传输费用，具体取决于这些实例是否在同一区域内。

弹性 IP 地址 (IPv4)

弹性 IP 地址是指可分配给您的账户的公有 IPv4 地址。您可以根据需要将其与实例关联或取消其与实例的关联。它会分配给您的账户，直到您选择释放它。有关弹性 IP 地址及其使用方法的更多信息，请参阅弹性 IP 地址 (p. 1094)。

我们不支持对 IPv6 使用弹性 IP 地址。

IPv6 地址

您可以选择将 IPv6 CIDR 块与 VPC 关联，并将 IPv6 CIDR 块与子网关联。我们将自动从 Amazon 的 IPv6 地址池中为您的 VPC 分配 IPv6 CIDR 块，因此您无法自行选择范围。有关更多信息，请参阅 Amazon VPC 用户指南 中的以下主题：

- 适用于 IPv6 的 VPC 定型
- 将 IPv6 CIDR 块与 VPC 关联
- 将 IPv6 CIDR 块与子网关联

IPv6 地址具有全局唯一性，可以配置为保持私有或通过互联网进行访问。有关 IPv6 的更多信息，请参阅 Amazon VPC 用户指南中的 IP 寻址。如果您的 VPC 和子网关联了 IPv6 CIDR 块，并且满足以下条件之一，则您的实例会收到 IPv6 地址：

- 您的子网配置为在启动期间向实例自动分配 IPv6 地址。有关更多信息，请参阅修改子网的 IPv6 寻址属性。
- 您在启动期间为实例分配了 IPv6 地址。
- 您在启动后为实例的主网络接口分配了 IPv6 地址。
- 您向同一子网中的某个网络接口分配 IPv6 地址，并在启动后将此网络接口附加到您的实例。

当实例在启动期间收到 IPv6 地址时，此地址将与实例的主网络接口 (eth0) 关联。您可以取消 IPv6 地址与该网络接口的关联。

IPv6 地址会在您停止和启动或休眠和启动实例时保留下来，并在您终止实例时释放出来。您无法重新分配已分配给某个网络接口的 IPv6 地址；您必须先取消分配此 IPv6 地址。

通过将 IPv6 地址分配给附加到实例的网络接口，您可以为实例分配更多的 IPv6 地址。可以分配给网络接口的 IPv6 地址数量以及可以附加到实例的网络接口数量因实例类型而异。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。

使用实例的 IPv4 地址

您可以在启动实例时为其分配公有 IPv4 地址。您可以在控制台中通过 Instances（实例）或 Network Interfaces（网络接口）页面查看实例的 IPv4 地址。

目录

- 查看 IPv4 地址 (p. 1056)
- 在实例启动期间分配公有 IPv4 地址 (p. 1057)

查看 IPv4 地址

您可以使用 Amazon EC2 控制台查看实例的公有和私有 IPv4 地址。您还可以通过使用实例元数据，从实例内确定实例的公有 IPv4 地址和私有 IPv4 地址。有关更多信息，请参阅实例元数据和用户数据 (p. 754)。

公有 IPv4 地址在控制台中显示为网络接口的属性，但它通过 NAT 映射到主要私有 IPv4 地址。因此，如果您检查实例网络接口的属性 (例如，通过 `ifconfig` [Linux] 或 `ipconfig` [Windows])，则不会显示公有 IPv4 地址。要从实例确定您的实例的公有 IPv4 地址，请使用实例元数据。

使用控制台查看实例的 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 联网选项卡上提供以下信息：
   - 公有 IPv4 地址 - 公有 IPv4 地址。如果您将弹性 IP 地址与实例或主网络接口相关联，则这是弹性 IP 地址。
   - 私有 IPv4 地址 - 私有 IPv4 地址。
   - 辅助私有 IPv4 地址 - 任何辅助私有 IPv4 地址。
4. 或者，在联网选项卡上的网络接口下，选择主网络接口的接口 ID（例如 eni-123abc456def78901）。界面中会提供以下信息：
   - Private IPv4 address（私有 IPv4 地址）– 主要私有 IPv4 地址。
   - 公有 IPv4 地址 - 公有 IPv4 地址。如果您将弹性 IP 地址与实例或主网络接口相关联，则这是弹性 IP 地址。
   - 辅助私有 IPv4 地址 - 任何辅助私有 IPv4 地址。

使用命令行查看实例的 IPv4 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-instances (Amazon CLI)
- Get-EC2InstanceAmazon Tools for Windows PowerShell

使用实例元数据确定实例的 IPv4 地址

1. 连接到您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 使用以下命令访问私有 IP 地址：

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

3. 使用以下命令访问公有 IP 地址：

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
   ```

   如果弹性 IP 地址与实例相关联，则返回的值是弹性 IP 地址。

在实例启动期间分配公有 IPv4 地址

所有子网都有一个属性可确定在子网中启动的实例是否分配了公有 IP 地址。默认情况下，非默认子网的此属性设置为 false，默认子网的此属性设置为 true。启动实例时，您也可以通过公有 IPv4 寻址功能来控制是否为实例分配公有 IPv4 地址；您可以覆盖子网 IP 寻址属性的默认行为。公有 IPv4 地址从 Amazon 的公有 IPv4 地址池进行分配，并分配给设备索引为 eth0 的网络接口。此功能取决于启动实例时的特定条件。

注意事项

- 启动后，即无法手动将该公有 IP 地址与您的实例取消关联。在某些情况下，它会自动释放，之后无法重新使用。有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。如果需要可以随意关联或取消关联的永久公有 IP 地址，请在启动后向实例分配弹性 IP 地址。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。
- 如果您指定多个网络接口，则不能自动分配公有 IP 地址。此外，如果您将某个现有网络接口指定为 eth0，则无法使用自动分配公有 IP 功能覆盖子网设置。
- 公有 IP 地址分配功能只在启动时可用。然而，无论您是否在启动时为实例分配公有 IP 地址，您都可以在启动后将弹性 IP 地址与实例相关联。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。您还可以修改子网的公有 IPv4 寻址行为。有关更多信息，请参阅修改子网的公有 IPv4 寻址属性。

在实例启动期间使用控制台分配公有 IPv4 地址

请按照步骤启动实例 (p. 577)，并在配置网络设置 (p. 579)时选择 Auto-assign Public IP（自动分配公有 IP）。

使用命令行启用或禁用公有 IP 寻址功能

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- 将 `--associate-public-ip-address` 或 `--no-associate-public-ip-address` 选项与 run-instances 命令 (Amazon CLI) 结合使用
- 将 `-AssociatePublicIp` 参数与 New-EC2Instance 命令 (Amazon Tools for Windows PowerShell) 结合使用

使用实例的 IPv6 地址

您可以查看分配给实例的 IPv6 地址，为实例分配公有 IPv6 地址，或取消分配给实例的 IPv6 地址。您可以在控制台中通过实例或网络接口页面查看这些地址。

目录

- 查看 IPv6 地址 (p. 1058)
- 向实例分配 IPv6 地址 (p. 1058)
- 取消分配给实例的 IPv6 地址 (p. 1059)

查看 IPv6 地址

您可以使用 Amazon EC2 控制台、Amazon CLI 和实例元数据查看实例的 IPv6 地址。

使用控制台查看实例的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 在联网选项卡上，找到 IPv6 地址。
5. 或者，在联网选项卡上的网络接口下，选择网络接口的接口 ID（例如 eni-123abc456def78901）。找到 IPv6 addresses（IPv6 地址）。

使用命令行查看实例的 IPv6 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-instances (Amazon CLI)
- Get-EC2InstanceAmazon Tools for Windows PowerShell

使用实例元数据查看实例的 IPv6 地址

1. 连接到您的 实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 使用以下命令查看 IPv6 地址 (您可以从 `http://169.254.169.254/latest/meta-data/network/interfaces/macs/` 中获取 MAC 地址)：

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

向实例分配 IPv6 地址

如果您的 VPC 和子网有与之关联的 IPv6 CIDR 块，则您可以在启动期间或之后向实例分配 IPv6 地址。IPv6 地址从子网的 IPv6 地址范围进行分配，并分配给设备索引为 eth0 的网络接口。

在实例启动期间分配 IPv6 地址

请按照步骤启动实例 (p. 577)，并在配置网络设置 (p. 579)时选择 Auto-assign IPv6 IP（自动分配 IPv6 IP）。

在启动实例后分配 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的实例，然后依次选择操作、联网和管理 IP 地址。
4. 展开网络接口。在 IPv6 地址下，选择分配新 IP 地址。输入子网范围内的 IPv6 地址，或将该字段留空，让 Amazon 为您选择 IPv6 地址。
5. 选择 Save。

使用命令行分配 IPv6 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- 将 `--ipv6-addresses` 选项与 run-instances 命令 (Amazon CLI) 结合使用
- 将 `Ipv6Addresses` 属性用于 New-EC2Instance 命令 (`-NetworkInterface`) 中的 Amazon Tools for Windows PowerShell
- assign-ipv6-addresses (Amazon CLI)
- Register-EC2Ipv6AddressList (Amazon Tools for Windows PowerShell)

取消分配给实例的 IPv6 地址

您可以随时取消分配给实例的 IPv6 地址。

使用控制台取消分配给实例的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的实例，然后依次选择操作、联网和管理 IP 地址。
4. 展开网络接口。在 IPv6 地址下方，选择 IPv6 地址旁边的取消分配。
5. 选择 Save。

使用命令行取消分配给实例的 IPv6 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- unassign-ipv6-addresses (Amazon CLI)
- Unregister-EC2Ipv6AddressList (Amazon Tools for Windows PowerShell)。

多个 IP 地址

您可以为实例指定多个私有 IPv4 和 IPv6 地址。您可为实例指定的网络接口和私有 IPv4 和 IPv6 地址的数量取决于该实例的类型。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。

在执行以下操作时，为 VPC 中的实例分配多个 IP 地址会非常有用：

- 在单个服务器上使用多个 SSL 证书，并为每个证书关联一个指定的 IP 地址，以在单个服务器上托管多个网站。
- 操作每个网络接口有多个 IP 地址的网络应用，如防火墙或负载均衡器。
- 当实例发生故障时，可将内部流量重定向到备用实例，方法是为备用实例重新分配辅助 IP 地址。

目录

- 多个 IP 地址的工作方式 (p. 1060)
- 使用多个 IPv4 地址 (p. 1060)
- 使用多个 IPv6 地址 (p. 1064)

多个 IP 地址的工作方式

下表说明了多个 IP 地址如何与网络接口配合工作：

- 您可以为任何网络接口分配辅助私有 IPv4 地址。网络接口不需要附加到实例。
- 您可以将多个 IPv6 地址分配给拥有关联 IPv6 CIDR 块的子网中的网络接口。
- 您必须从子网的 IPv4 CIDR 块范围内为网络接口选择辅助 IPv4 地址。
- 您必须从子网的 IPv6 CIDR 块范围内为网络接口选择辅助 IPv6。
- 将安全组与网络接口关联，而不是与各 IP 地址关联。因此，网络接口中指定的每个 IP 地址均受其网络接口的安全组约束。
- 可将多个 IP 地址分配给附加到正在运行或已停止实例的网络接口，也可以取消分配操作。
- 如果您明确允许，已分配给某个网络接口的辅助私有 IPv4 地址可重新分配给其他网络接口。
- 无法将 IPv6 地址重新分配给其他网络接口；您必须先取消分配给现有网络接口的 IPv6 地址。
- 当使用命令行工具或 API 将多个 IP 地址分配给某个网络接口时，如果其中有一个 IP 地址无法分配，整个操作都会失败。
- 当网络接口与实例分离或附加到实例时，主要私有 IPv4 地址、辅助私有 IPv4 地址、弹性 IP 地址以及 IPv6 地址将仍然属于此辅助网络接口。
- 尽管您无法从实例分离主要网络接口，但是您可以将主要网络接口的辅助私有 IPv4 地址重新分配给另一个网络接口。

下表说明了如何将多个 IP 地址与弹性 IP 地址配合使用 (仅限 IPv4)：

- 每个私有 IPv4 地址只能与一个弹性 IP 地址关联，反之亦然。
- 当辅助私有 IPv4 地址重新分配给其他接口时，该辅助私有 IPv4 地址会保留与弹性 IP 地址的相关性。
- 当您取消分配给接口的辅助私有 IPv4 地址时，相关的弹性 IP 地址会自动取消与该辅助私有 IPv4 地址的关联。

使用多个 IPv4 地址

您可以将一个辅助私有 IPv4 地址分配给实例，将弹性 IPv4 地址与辅助私有 IPv4 地址关联，并且取消分配辅助私有 IPv4 地址。

目录

- 分配辅助私有 IPv4 地址 (p. 1060)
- 在实例上配置操作系统以识别辅助私有 IPv4 地址 (p. 1062)
- 将弹性 IP 地址与辅助私有 IPv4 地址关联 (p. 1062)
- 查看辅助私有 IPv4 地址 (p. 1063)
- 取消分配辅助私有 IPv4 地址 (p. 1063)

分配辅助私有 IPv4 地址

您可以在启动实例时或在实例运行后为实例的网络接口分配辅助私有 IPv4 地址。本节包括以下过程。

- 启动实例时分配辅助私有 IPv4 地址 (p. 1061)
- 使用命令行在启动期间分配辅助 IPv4 地址 (p. 1061)

- 为网络接口分配辅助私有 IPv4 地址 (p. 1062)
- 使用命令行为现有实例分配辅助私有 IPv4 (p. 1062)

New console

启动实例时分配辅助私有 IPv4 地址

1. 按照步骤启动实例 (p. 577)，在配置网络设置 (p. 579)时，选择 Advanced network configuration（高级网络配置）。
2. 在 Secondary IP（辅助 IP）下，选择 Automatically assign（自动分配）以让 Amazon 自动分配辅助 IPv4 地址，或选择 Manually assign（手动分配）以手动输入 CIDR。
3. 完成剩余步骤以启动实例 (p. 577)。

Old console

启动实例时分配辅助私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Launch Instance（启动实例）。
3. 选择一个 AMI，然后选择实例类型并选择 Next: Configure Instance Details。
4. 在配置实例详细信息页面中，为网络选择一个 VPC，为子网选择一个子网。
5. 在 Network Interfaces 部分中，执行以下操作，然后选择 Next: Add Storage：
   - 要添加其他网络接口，请选择添加设备。当您启动实例时，控制台允许您指定最多两个网络接口。启动实例后，选择导航窗格中的 Network Interfaces 以添加其他网络接口。您可以附加的网络接口总数因实例类型而有所差异。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。

     Important

     当您添加第二个网络接口时，系统将无法再自动分配公有 IPv4 地址。除非您将弹性 IP 地址分配给主网络接口 (eth0)，否则将无法通过 IPv4 连接到实例。您可在完成启动向导后分配弹性 IP 地址。有关更多信息，请参阅使用弹性 IP 地址 (p. 1095)。
   - 对于每个网络接口，在辅助 IP 地址下，选择添加 IP，然后输入一个处于子网范围内的私有 IP 地址，或接受默认值 `Auto-assign`，从而让 Amazon 选择一个地址。
6. 在接下来的 Add Storage 页面上，除了 AMI 指定的卷 (如根设备卷) 外，您可指定要挂载到实例的卷，然后选择 Next: Add Tags。
7. 在 Add Tags 页面上，为实例指定标签 (例如，便于用户识别的名称)，然后选择 Next: Configure Security Group。
8. 在 Configure Security Group (配置安全组) 页面上，选择一个现有安全组或创建新安全组。选择 Review and Launch。
9. 在 Review Instance Launch 页面上，检查您的设置，然后选择 Launch 以选择一个密钥对并启动您的实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

   Important

   向网络接口添加辅助私有 IP 地址后，您必须连接到实例并在该实例上配置辅助私有 IP 地址。有关更多信息，请参阅在实例上配置操作系统以识别辅助私有 IPv4 地址 (p. 1062)。

使用命令行在启动期间分配辅助 IPv4 地址

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- 用于 `--secondary-private-ip-addresses`run-instances 命令 (Amazon CLI) 的 选项
- 使用 New-EC2Instance 命令 (`-NetworkInterface`) 定义 `PrivateIpAddresses` 并指定 Amazon Tools for Windows PowerShell 参数。

为网络接口分配辅助私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces，然后选择附加到实例的网络接口。
3. 依次选择 Actions、Manage IP Addresses。
4. 在 IPv4 Addresses 下，选择 Assign new IP。
5. 输入一个处于实例子网范围内的特定 IPv4 地址，或者将该字段保留空白，以便让 Amazon 为您选择一个 IP 地址。
6. (可选) 选择 Allow reassignment，以允许已分配到另一个网络接口的辅助私有 IP 地址能够重新分配。
7. 选择是，请更新。

或者，您也可以为实例分配辅助私有 IPv4 地址。在导航窗格中选择实例，选择相应实例，然后依次选择操作、联网、管理 IP 地址。您可以按上述步骤进行操作，以配置相同的内容。该 IP 地址将分配给实例的主网络接口 (eth0)。

使用命令行为现有实例分配辅助私有 IPv4

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。
  - assign-private-ip-addresses (Amazon CLI)
  - Register-EC2PrivateIpAddress (Amazon Tools for Windows PowerShell)

在实例上配置操作系统以识别辅助私有 IPv4 地址

为实例分配辅助私有 IPv4 地址后，您需要在实例上配置操作系统，以识别辅助私有 IP 地址。

- 如果您使用的是 Amazon Linux，ec2-net-utils 包可以在此步骤上为您提供帮助。它能在实例运行期间配置您附加的其他网络接口，在 DHCP 租约续订期间更新辅助 IPv4 地址，并更新相关的路由规则。您可以使用 `sudo service network restart` 命令立即刷新接口列表，然后使用 `ip addr li` 查看最新列表。如果您需要手动控制网络配置，可以删除 ec2-net-utils 包。有关更多信息，请参阅使用 ec2-net-utils 为 Amazon Linux 配置网络接口 (p. 1137)。
- 如果您正在使用其他 Linux 分配，请参阅有关 Linux 分配的文档。您可以搜索有关配置其他网络接口和辅助 IPv4 地址的信息。如果实例在同一子网中有两个或更多接口，请搜索有关利用路由规则解决非对称路由的信息。

有关配置 Windows 实例的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的为 VPC 中的 Windows 实例配置辅助私有 IP 地址。

将弹性 IP 地址与辅助私有 IPv4 地址关联

将弹性 IP 地址与辅助私有 IPv4 地址关联

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Actions，然后选择 Associate address。
4. 对于 Network interface，选择网络接口，然后从 Private IP 列表中选择辅助 IP 地址。
5. 选择 Associate。

使用命令行将弹性 IP 地址与辅助私有 IPv4 地址关联

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。
  - associate-address (Amazon CLI)
  - Register-EC2Address (Amazon Tools for Windows PowerShell)

查看辅助私有 IPv4 地址

查看分配给网络接口的私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择您要查看其私有 IP 地址的网络接口。
4. 在详细信息窗格中的 Details 选项卡上，查看 Primary private IPv4 IP 和 Secondary private IPv4 IP 字段，了解分配给该网络接口的主要私有 IPv4 地址和任何辅助私有 IPv4 地址。

查看分配给实例的私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择要查看其私有 IPv4 地址的实例。
4. 在详细信息窗格的 Description 选项卡上，查看 Private IPs 和 Secondary private IPs 字段，了解通过实例的网络接口分配给实例的主要私有 IPv4 地址和任何辅助私有 IPv4 地址。

取消分配辅助私有 IPv4 地址

如果您不再需要辅助私有 IPv4 地址，则可取消分配给实例或网络接口的这类地址。当取消分配给网络接口的辅助私有 IPv4 地址后，弹性 IP 地址 (如果存在) 也会断开相关联系。

取消分配给实例的辅助私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例，然后依次选择操作、联网和管理 IP 地址。
4. 在 IPv4 Addresses 下，选择要取消分配的 IPv4 地址对应的 Unassign。
5. 选择是，请更新。

取消分配给网络接口的辅助私有 IPv4 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv4 Addresses 下，选择要取消分配的 IPv4 地址对应的 Unassign。
5. 选择是，请更新。

使用命令行取消分配辅助私有 IPv4 地址

- 您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- unassign-private-ip-addresses (Amazon CLI)
- Unregister-EC2PrivateIpAddress (Amazon Tools for Windows PowerShell)

使用多个 IPv6 地址

您可以将多个 IPv6 地址分配给实例、查看分配给实例的 IPv6 地址以及取消分配给实例的 IPv6 地址。

目录

- 分配多个 IPv6 地址 (p. 1064)
- 查看您的 IPv6 地址 (p. 1065)
- 取消分配 IPv6 地址 (p. 1066)

分配多个 IPv6 地址

您可以在启动期间或之后将一个或多个 IPv6 地址分配给实例。要将 IPv6 地址分配给实例，您在其中启动实例的 VPC 和子网都必须有一个关联的 IPv6 CIDR 块。有关更多信息，请参阅《Amazon VPC 用户指南》中的 IPv6 地址。

New console

在启动期间分配多个 IPv6 地址

1. 按照步骤启动实例 (p. 577)，在配置网络设置 (p. 579)时，选择 Advanced network configuration（高级网络配置）。
2. 若要分配辅助 IPv6 地址，请在 IPv6 IP 下选择 Automatically assign（自动分配）以让 Amazon 自动分配辅助 IPv6 地址，或选择 Manually assign（手动分配）以手动输入 CIDR。
3. 完成剩余步骤以启动实例 (p. 577)。

Old console

在启动期间分配多个 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制面板中，选择 Launch Instance。
3. 选择一个 AMI 和实例类型，然后选择 Next: Configure Instance Details。请确保您选择的实例类型支持 IPv6。有关更多信息，请参阅实例类型 (p. 238)。
4. 在 Configure Instance Details (配置实例详细信息) 页上，从 Network (网络) 列表中选择一个 VPC，然后从 Subnet (子网) 列表中选择一个子网。
5. 在 Network Interfaces 部分中，执行以下操作，然后选择 Next: Add Storage：
   - 要将单个 IPv6 地址分配给主网络接口 (eth0)，请在 IPv6 IP 下选择 Add IP。要添加一个辅助 IPv6 地址，请再次选择 Add IP。您可以输入子网范围内的 IPv6 地址，或保留默认值 Auto-assign，这样 Amazon 会从子网中为您选择一个 IPv6 地址。
   - 选择 Add Device，以添加另一个网络接口，并重复上述步骤，将一个或多个 IPv6 地址添加到该网络接口。当您启动实例时，控制台允许您指定最多两个网络接口。启动实例后，选择导航窗格中的 Network Interfaces 以添加其他网络接口。您可以附加的网络接口总数因实例类型而有所差异。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。
6. 按照向导中的后续步骤附加卷并标记您的实例。
7. 在 Configure Security Group (配置安全组) 页面上，选择一个现有安全组或创建新安全组。如果您想让实例可通过 IPv6 访问，请确保您的安全组拥有允许从 IPv6 地址访问的规则。有关更多信息，请参阅针对不同使用案例的安全组规则 (p. 1315)。选择 Review and Launch。

8. 在 Review Instance Launch 页面上，检查您的设置，然后选择 Launch 以选择一个密钥对并启动您的实例。如果您不熟悉 Amazon EC2 并且还没有创建任何密钥对，向导会提示您创建一个。

您可以使用 Amazon EC2 控制台的 Instances (实例) 屏幕将多个 IPv6 地址分配给现有实例。该做法可将 IPv6 地址分配给实例的主网络接口 (eth0)。要将特定 IPv6 地址分配给实例，请确保 IPv6 地址尚未分配给其他实例或网络接口。

将多个 IPv6 地址分配给现有实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的实例，然后依次选择 Actions (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
4. 在 IPv6 Addresses 下，选择您要添加的每个 IPv6 地址对应的 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择是，请更新。

或者，您可以将多个 IPv6 地址分配给现有网络接口。网络接口必须是在具有关联的 IPv6 CIDR 块的子网中创建的。要将特定 IPv6 地址分配给网络接口，请确保该 IPv6 地址尚未分配给其他网络接口。

将多个 IPv6 地址分配给网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择您的网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择您要添加的每个 IPv6 地址对应的 Assign new IP。您可以指定一个处于子网范围内的 IPv6 地址，也可以保留 Auto-assign 值，从而让 Amazon 为您选择一个 IPv6 地址。
5. 选择是，请更新。

CLI 概览

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- 在启动期间分配 IPv6 地址：
  - 将 `--ipv6-addresses` 或 `--ipv6-address-count` 选项与 run-instances 命令 (Amazon CLI) 结合使用
  - 使用 New-EC2Instance 命令 (`-NetworkInterface`) 定义 `Ipv6Addresses` 并指定 `Ipv6AddressCount` 或 Amazon Tools for Windows PowerShell 参数。
- 将 IPv6 地址分配给网络接口：
  - assign-ipv6-addresses (Amazon CLI)
  - Register-EC2Ipv6AddressList (Amazon Tools for Windows PowerShell)

查看您的 IPv6 地址

您可以查看实例或网络接口的 IPv6 地址。

查看分配给实例的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。在详细信息窗格中，查看 IPv6 IPs 字段。

查看分配给网络接口的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择您的网络接口。在详细信息窗格中，查看 IPv6 IPs 字段。

CLI 概览

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- 查看实例的 IPv6 地址：
  - describe-instances (Amazon CLI)
  - Get-EC2InstanceAmazon Tools for Windows PowerShell
- 查看网络接口的 IPv6 地址：
  - describe-network-interfaces (Amazon CLI)
  - Get-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

取消分配 IPv6 地址

您可以取消分配给实例主网络接口的 IPv6 地址，也可以取消分配给网络接口的 IPv6 地址。

取消分配给实例的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的实例，然后依次选择 Actions (操作)、Networking (联网) 和 Manage IP Addresses (管理 IP 地址)。
4. 在 IPv6 Addresses 下，选择要取消分配的 IPv6 地址对应的 Unassign。
5. 选择是，请更新。

取消分配给网络接口的 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择您的网络接口，然后依次选择 Actions、Manage IP Addresses。
4. 在 IPv6 Addresses 下，选择要取消分配的 IPv6 地址对应的 Unassign。
5. 选择 Save。

CLI 概览

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- unassign-ipv6-addresses (Amazon CLI)
- Unregister-EC2Ipv6AddressList (Amazon Tools for Windows PowerShell)。

EC2 实例主机名

当您创建 EC2 实例时，Amazon 为该实例创建主机名。有关主机名类型及其 Amazon 预置方式的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。Amazon 提供了 DNS 服务器，可将 Amazon 提供的

主机名解析为 IPv4 和 IPv6 地址。Amazon DNS 服务器位于 VPC 网络范围起始地址 + 2 的位置。有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 中的 DNS 支持。

Amazon EC2 实例主机名类型

本节介绍在 VPC 子网中启动实例时可用的 Amazon EC2 实例来宾操作系统主机名类型。

主机名区分网络中的 EC2 实例。例如，如果您想运行脚本，以与网络上的部分或全部实例进行通信，则可以使用实例的主机名。

目录

- EC2 主机名的类型 (p. 1067)
- 查看资源名称和 IP 名称的位置 (p. 1068)
- 如何决定是选择资源名称还是 IP 名称 (p. 1069)
- 修改主机名类型和 DNS 主机名配置 (p. 1069)

EC2 主机名的类型

在 VPC 中启动 EC2 实例时，来宾操作系统主机名有两种主机名类型：

- IP name（IP 名称）：传统命名方案，当您启动实例时，实例的私有 IPv4 地址包含在实例的主机名中。IP 名称在 EC2 实例的生命周期内存在。当用作私有 DNS 主机名时，它只会返回私有 IPv4 地址（A 记录）。
- Resource name（资源名称）：当您启动实例时，EC2 instance ID（EC2 实例 ID）包含在实例的主机名中。资源的名称在 EC2 实例的生命周期内存在。当用作私有 DNS 主机名时，它可以返回私有 IPv4 地址（A 记录）和/或 IPv6 全局单播地址（AAAA 记录）。

EC2 实例来宾操作系统主机名类型取决于子网设置：

- 如果在仅 IPv4 子网中启动实例，则可以选择 IP 名称或资源名称。
- 如果在双堆栈（IPv4+IPv6）子网中启动实例，则可以选择 IP 名称或资源名称。
- 如果在仅 IPv6 子网中启动实例，则会自动使用资源名称。

目录

- IP 名称 (p. 1067)
- 资源名称 (p. 1068)
- IP 名称和资源名称之间的区别 (p. 1068)

IP 名称

当您启动具有 IP name（IP 名称）的 Hostname type（主机名类型）的 EC2 实例时，来宾操作系统主机名将配置为使用私有 IPv4 地址。

- us-east-1 中的实例的格式：*private-ipv4-address*.ec2.internal
- 示例：*ip-10-24-34-0*.ec2.internal
- 任何其它Amazon区域中的实例的格式：*private-ipv4-address.region*.compute.internal
- 示例：*ip-10-24-34-0.us-west-2*.compute.internal

资源名称

当您在仅 IPv6 子网中启动 EC2 实例时，Resource name（资源名称）的 Hostname type（主机名类型）默认处于选中状态。当您在仅 IPv4 子网或双堆栈（IPv4+IPv6）子网中启动实例时，Resource name（资源名称）是您可以选择的选项。启动实例后，您可以管理主机名配置。有关更多信息，请参阅修改主机名类型和 DNS 主机名配置 (p. 1069)。

当您启动具有 Resource name（资源名称）的Hostname type（主机名类型）的 EC2 实例时，来宾操作系统主机名将配置为使用 EC2 实例 ID。

- us-east-1 中的实例的格式：*ec2-instance-id*.ec2.internal
- 示例：*i-0123456789abcdef*.ec2.internal
- 任何其它Amazon区域中的实例的格式：*ec2-instance-id.region*.compute.internal
- 示例：*i-0123456789abcdef.us-west-2*.compute.internal

IP 名称和资源名称之间的区别

IP 名称和资源名称的 DNS 查询共存，以确保向后兼容并允许您从基于 IP 的主机名命名迁移到基于资源的命名。对于基于 IP 名称的私有 DNS 主机名，您无法配置是否响应实例的 DNS A 记录查询。无论客户操作系统主机名设置如何，DNS A 记录查询始终得到响应。相反，对于基于资源名称的私有 DNS 主机名，您可以配置是否响应实例的 DNS A 和/或 DNS AAAA 查询。当您启动实例或修改子网时，您可以配置响应行为。有关更多信息，请参阅修改主机名类型和 DNS 主机名配置 (p. 1069)。

查看资源名称和 IP 名称的位置

本节介绍您会在 EC2 控制台中的什么位置看到主机名类型、资源名称和 IP 名称。

目录

- 创建 EC2 实例时 (p. 1068)
- 查看现有 EC2 实例的详细信息时 (p. 1069)

创建 EC2 实例时

当您创建 EC2 实例时，根据您选择的子网类型，Resource name（资源名称）的 Hostname type（主机名类型）可能是可用的，也可能已选中且无法修改。本节介绍您会在什么场景中看到主机名类型、资源名称和 IP 名称。

方案 1

您在向导中创建 EC2 实例（参阅 使用新启动实例向导启动实例 (p. 575)），然后配置详细信息时，您选择配置为仅 IPv6 的子网。

在这种情况下，Resource name（资源名称）的 Hostname type（主机名类型）已自动选中且无法修改。将自动取消选择 Enable IP name IPv4 (A record) DNS requests（启用 IP 名称 IPv4（A 记录）DNS 请求）和 Enable resource-based IPv4 (A record) DNS requests（启用基于资源的 IPv4（A 记录）DNS 请求）的 DNS Hostname（DNS 主机名）选项且不可修改。Enable resource-based IPv6 (AAAA record) DNS requests（启用基于资源的 IPv6（AAAA 记录）DNS 请求）默认处于选中状态，但是可修改。如果选择该选项，对资源名称的 DNS 请求将解析为此 EC2 实例的 IPv6 地址（AAAA 记录）。

方案 2

您在向导中创建 EC2 实例（见 使用新启动实例向导启动实例 (p. 575)），然后配置详细信息时，您选择配置为 IPv4 CIDR 块或同时配置 IPv4 和 IPv6 CIDR 块（“双堆栈”）的子网。

在此情况下，Enable IP name IPV4 (A record) DNS requests（启用 IP 名称 IPv4（A 记录）DNS 请求）已自动选中且无法更改。这意味着对 IP 名称的请求将解析为此 EC2 实例的 IPv4 地址（A 记录）。

选项默认为子网的配置，但是您可以根据子网设置修改此实例的选项：

- Hostname type（主机名类型）：确定您希望 EC2 实例的来宾操作系统主机名是资源名称还是 IP 名称。默认值是 IP name（IP 名称）。
- Enable resource-based IPv4 (A record) DNS requests（启用基于资源的 IPV4（A 记录）DNS 请求）：确定对您的资源名称的请求是否解析为此 EC2 实例的私有 IPv4 地址（A 记录）。此选项非默认选定。
- Enable resource-based IPV6 (AAAA record) DNS requests（启用基于资源的 IPV6（AAAA 记录）DNS 请求）：确定对您的资源名称的请求是否解析为此 EC2 实例的 IPv6 GUA 地址（AAAA 记录）。此选项非默认选定。

查看现有 EC2 实例的详细信息时

您可以在 EC2 实例的 Details（详细信息）选项卡中查看现有 EC2 实例的主机名值：

- Hostname type（主机名类型）：IP 名称或资源名称格式的主机名。
- Private IP DNS name (IPv4 only)（私有 IP DNS 名称（仅 IPv4））：将始终解析为实例的私有 IPv4 地址的 IP 名称。
- Private resource DNS name（私有资源 DNS 名称）：解析为为此实例选择的 DNS 记录的资源名称。
- Answer private resource DNS name（回答私有资源 DNS 名称）：资源名称解析为 IPv4（A）、IPv6（AAAA）或 IPv4 和 IPv6（A 和 AAAA）DNS 记录。

此外，如果您直接通过 SSH 连接到 EC2 实例，然后输入 `hostname` 命令，您将看到 IP 名称或资源名称格式的主机名。

如何决定是选择资源名称还是 IP 名称

当您启动 EC2 实例时（请参阅使用新启动实例向导启动实例 (p. 575)），如果选择 Resource name（资源名称）的 Hostname type（主机名类型），EC2 实例将使用资源名称格式的主机名启动。在这种情况下，此 EC2 实例的 DNS 记录也可以指向资源名称。这使您可以灵活地选择该主机名是解析为实例的 IPv4 地址、IPv6 地址，还是同时解析实例的 IPv4 和 IPv6 地址。如果您计划在未来使用 IPv6，或者如果您现在使用双堆栈子网，最好使用 Resource name（资源名称）的 Hostname type（主机名类型），以便在不对 DNS 记录本身进行任何更改的情况下更改实例主机名的 DNS 解析。资源名称允许您在 EC2 实例上添加和删除 IPv4 和 IPv6 DNS 解析。

如果选择了 IP name（IP 名称）的 Hostname type（主机名类型），并将其用作 DNS 主机名，则只能解析为实例的 IPv4 地址。即使实例同时具有与之关联 IPv4 地址和 IPv6 地址，它也不会解析为实例的 IPv6 地址。

修改主机名类型和 DNS 主机名配置

按照本节中的步骤，在启动后修改子网或 EC2 实例的主机名类型和 DNS 主机名配置。

目录

- 子网 (p. 1069)
- EC2 实例 (p. 1070)

子网

通过在 VPC 控制台中选择子网并选择 Actions（操作）、Edit subnet settings（编辑子网设置）来修改子网的配置。

Note

更改子网设置不会更改子网中已启动的 EC2 实例的配置。

- Hostname type（主机名类型）：确定您希望在子网中启动的 EC2 实例的来宾操作系统主机名的默认设置是资源名称还是 IP 名称。
- Enable DNS hostname IPv4 (A record) requests [启用 DNS 主机名 IPv4（A 记录）请求]：确定是否将对资源名称的 DNS 请求/查询解析为此 EC2 实例的私有 IPv4 地址（A 记录）。
- Enable DNS hostname IPv6 (AAAA record) requests（启用 DNS 主机名 IPv6（AAAA 记录）请求）：确定对您的资源名称的 DNS 请求/查询是否解析为此 EC2 实例的 IPv6 地址（AAAA 记录）。

EC2 实例

按照本节中的步骤修改 EC2 实例的主机名类型和 DNS 主机名配置。

Important

- 更改 Use resource based naming as guest OS hostname（将基于资源的命名用作来宾操作系统主机名）设置时，您必须先停止该实例。更改 Answer DNS hostname IPv4 (A record) request（回答 DNS 主机名 IPv4（记录）请求）或 Answer DNS hostname IPv6 (AAAA record) requests（回答 DNS 主机名 IPv6（AAAA 记录）请求）设置时，您无需停止该实例。
- 修改非 EBS 支持的 EC2 实例类型的任何设置时，您无法停止该实例。您必须终止该实例，然后启动包含所需主机名类型和 DNS 主机名配置的新实例。

修改 EC2 实例的主机名类型和 DNS 主机名配置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 如果您要更改 Use resource based naming as guest OS hostname（将基于资源的命名用作来宾操作系统主机名）设置，首先停止该 EC2 实例。否则，请跳过此步骤。

   要停止实例，请选择该实例，然后依次选择 Instance state（实例状态）、Stop instance（停止实例）。
3. 选择实例，然后依次选择 Actions（操作）、Instance settings（实例设置）、Change resource based naming options（更改基于资源的命名选项）。

   - Use resource based naming as guest OS hostname（将基于资源的命名用作来宾操作系统主机名）：确定您希望 EC2 实例的来宾操作系统主机名是资源名称还是 IP 名称。
   - Answer DNS hostname IPv4 (A record) requests [回答 DNS 主机名 IPv4（A 记录）请求]：确定是否将对资源名称的 DNS 请求/查询解析为此 EC2 实例的私有 IPv4 地址。
   - Answer DNS hostname IPv6 (AAAA record) requests（回答 DNS 主机名 IPv6（AAAA 记录）请求）：确定对您的资源名称的 DNS 请求/查询是否解析为此 EC2 实例的 IPv6 地址（AAAA 记录）。
4. 选择 Save（保存）。
5. 如果您已经停止实例，可以重新启动它。

在 Amazon EC2 中使用您自己的 IP 地址 (BYOIP)

您可将自己的全部或部分可公开路由的 IPv4 或 IPv6 地址从本地网络引入到 Amazon 账户中。您继续控制该地址范围，但 Amazon 默认将其通告到互联网。在将地址范围引入 Amazon 中之后，它会在您的 Amazon 账户中显示为地址池。

BYOIP 仅对部分区域和资源可用。有关受支持区域和资源的列表，请参阅自带 IP 常见问题。

Note

下面的步骤说明了如何将您自己的 IP 地址范围仅用于 Amazon EC2。有关在 Amazon Global Accelerator 中使用自己的 IP 地址范围的步骤，请参阅 Amazon Global Accelerator 开发人员指南中的自带 IP 地址 (BYOIP)。

目录

- BYOIP 定义 (p. 1071)
- 要求和配额 (p. 1071)
- BYOIP 地址范围的载入先决条件 (p. 1072)
- 载入 BYOIP (p. 1077)
- 使用地址范围 (p. 1079)
- 验证 BYOIP (p. 1080)

BYOIP 定义

- X.509 自签名证书：最常用于加密和验证网络内数据的证书标准。这是 Amazon 用来验证从 RDAP 记录控制 IP 空间的证书。有关 X.509 证书的更多信息，请参阅 RFC 3280。
- 注册数据访问协议 (RDAP)：查询注册数据的资源。其由客户更新，并由 Amazon 用来验证对区域互联网注册机构 (RIR) 中地址空间的控制。
- 路由来源授权 (ROA)：由 RIR 创建的对象，供客户对特定自治系统中的 IP 播发进行身份验证。如需相关概览，请参阅 ARIN 网站上的路由来源授权 (ROA)。
- 本地互联网注册机构 (LIR)：网络服务提供商等企业，从 RIR 为其客户分配 IP 地址数据块。

要求和配额

- 必须在区域互联网注册表 (RIR) 中注册地址范围，例如 American Registry for Internet Numbers (ARIN)、Réseaux IP Européens Network Coordination Centre (RIPE) 或 Asia-Pacific Network Information Centre (APNIC)。它必须由企业或机构实体注册，而不能由个人注册。
- 您可以引入的最具体 IPv4 地址范围是 /24。
- 对于公开发布的 CIDR，您可以引入的最具体 IPv6 地址范围是 /48，对于不公开发布 (p. 1078)的 CIDR，您可以引入的最具体 IPv6 地址范围是 /56。
- 不公开通告的 CIDR 范围不需要 ROA，但 RDAP 记录仍需更新。
- 您可以将每个地址范围一次添加到一个区域中。
- 对于每个区域，您可以将总共 5 个 BYOIP IPv4 和 IPv6 地址范围引入到您的 Amazon 账户中。您无法使用“Service Quotas”（服务限额）控制台调整 BYOIP CIDR 的限额，但您可以通过 Amazon 支持中心，按照 Amazon 服务限额 中的说明联系 Amazon《General Reference》 内，以请求提高限额。
- 您无法使用 Amazon RAM 与其它账户共享您的 IP 地址范围，除非您使用 Amazon VPC IP 地址管理器 (IPAM) 并将 IPAM 与 Amazon Organizations 集成。有关更多信息，请参阅 Amazon VPC IPAM 用户指南中的将 IPAM 与 Amazon Organizations 集成。
- IP 地址范围中的地址必须具有干净的历史记录。我们可能会调查 IP 地址范围的声誉，并保留权利以拒绝包含的 IP 地址具有不良声誉或与恶意行为关联的 IP 地址范围。
- Amazon 不支持旧式分配。
- 如果为 LIR，常见做法是通过手动过程更新记录。这可能需要几天的时间来部署，具体取决于 LIR。
- 大型 CIDR 块需要单个 ROA 对象和 RDAP 记录。您可以使用单个对象和记录，将多个较小的 CIDR 块从该范围添加到 Amazon，甚至可以跨多个区域添加。
- Local Zones、Wavelength Zones 或 Amazon Outposts 上不支持 BYOIP。

BYOIP 地址范围的载入先决条件

BYOIP 的载入过程分为两个阶段，您必须为此执行三个步骤。这些步骤与下图中描述的步骤相对应。我们在本文档中包含了手动操作步骤，但您的 RIR 可能会提供托管服务来帮助您完成这些步骤。

准备阶段

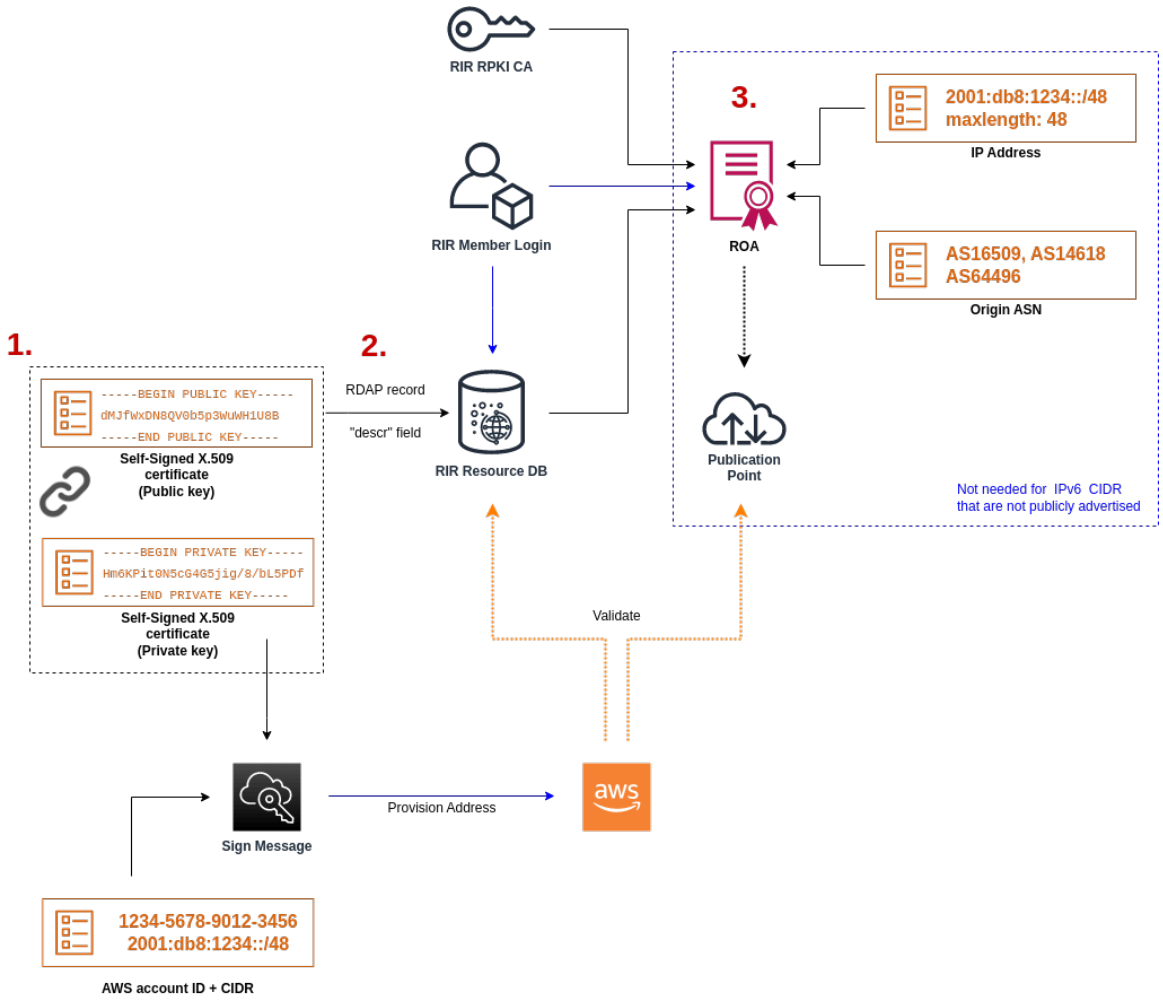
1. 为进行身份验证，请创建 RSA 密钥对 (p. 1073)并用其生成自签名 X.509 证书。此证书仅用于预调配阶段。

RIR 配置阶段

2. 将自签名证书上传 (p. 1076)到 RDAP 记录注释。

3. 在 RIR 中创建 ROA 对象 (p. 1076)。ROA 定义了所需的地址范围、允许通告地址范围的自治系统编号 (ASN) 以及向您 RIR 的资源公有密钥基础设施 (RPKI) 进行注册的到期日期。

> **Note**
>
> 不公开发布的 IPv6 地址空间不需要 ROA。



要引入多个不连续地址范围，您必须对每个地址范围重复此过程。不过，如果在几个不同区域之间拆分连续数据块，则无需执行重复准备和 RIR 配置步骤。

引入地址范围不会影响您之前引入的任何地址范围。

载入地址范围之前，请完成以下先决条件。对于某些任务，您可以运行 Linux 命令。在 Windows 上，您可以使用适用于 Linux 的 Windows 子系统运行 Linux 命令。

1. 为 Amazon 身份验证创建密钥对

使用以下过程创建自签名 X.509 证书，并将其添加到您的 RIR 的 RDAP 记录。此密钥对用于向 RIR 对地址范围进行身份验证。openssl 命令需要 OpenSSL 版本 1.0.2 或更高版本。

复制以下命令并仅替换占位符值（以彩色斜体文本显示）。

创建自签名 X.509 证书并将其添加到 RDAP 记录

此过程遵循加密私有 RSA 密钥并要求使用通行短语来访问该密钥的最佳实践。

1. 生成 RSA 2048 位密钥对，如下所示。

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out private-
key.pem
```

-aes256 参数指定用于加密私有密钥的算法。该命令返回以下输出，包括设置通行短语的提示：

```
......+++
.+++
Enter PEM pass phrase: xxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxx
```

您可以使用以下命令检查密钥：

```
$ openssl pkey -in private-key.pem -text
```

这会返回通行短语提示和密钥内容，应类似于以下内容：

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
```

```
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
```

```
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

当您的私有密钥不用时，请将其保存在安全位置。

2. 从私有密钥生成您的公有密钥，如下所示。稍后您将使用此功能来测试您的签名授权消息是否已正确验证。

```
$ openssl rsa -in private-key.pem -pubout > public-key.pem
```

检查时，您的公有密钥应如下所示：

```
$ cat public-key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxQVx0SOB1SgIYd7HonIq
KIswkU2yXtfmLMTU42uF8isqVRiBVgxoWbOOBQh5Tzjk1Sfjaj++MPeqDOwz0t8a
PZGkMmQRZ9mBKdhAaub399OyhzUZmWVJpJ9MxzkhKTZmNnzMSEgcXsJcURQJ4sJk
nf/Ew7xyTGPRbwCL1rk7L+ZdLSSpPmvdSuPrTt1HQ0e0p6OVlxMX7Aa1t4NcnaN0
wbMfIuf2IlTnDQKcu4HtvxYsGN2glyQeq+p7heh/JkYCOK+L5DEbDpQISQ52TzXs
Hm6KPit0N5cG4G5jig/8/bL5PDf/oVEwbSF9H0bWxvjyyMN8VkRxqzEp9gc7D1bg
ywIDAQAB
-----END PUBLIC KEY-----
```

3. 使用之前创建的密钥对生成 X.509 证书。在此示例中，该证书在 365 天后过期，在此日期后它将不能是受信任的。请务必相应地设置到期时间。`tr -d "\n"` 命令从输出中删除换行符。您需要在出现提示时提供公用名称，但其他字段可以留空。

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" > certificate.pem
```

这会产生类似于下述信息的输出：

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

Note

Amazon 预置不需要公用名。其可以是任何内部或公有域名。

您可以使用以下命令检查证书：

```
$ cat certificate.pem
```

输出应该是一个没有换行符的 PEM 编码的长字符串，前面是 `-----BEGIN CERTIFICATE-----`，后面是 `-----END CERTIFICATE-----`。

2. 将 RDAP 记录上传到 RIR

将之前创建的证书添加到 RIR 的 RDAP 记录。请务必在编码部分前后包含 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----` 字符串。所有这些内容必须都在单个长线上。更新 RDAP 的过程取决于您的 RIR：

- 对于 ARIN，在地址范围的“Public Comments (公共注释)”部分中添加证书。请勿将其添加到您组织的注释部分。
- 对于 RIPE，将证书添加为地址范围的“描述”字段。请勿将其添加到您组织的注释部分。
- 对于 APNIC，通过电子邮件将证书发送到 helpdesk@apnic.net，以手动将其添加到您的地址范围的“remarks”（备注）字段中。请以 IP 地址的 APNIC 授权联系人身份发送电子邮件。

完成下方预调配阶段后，可从 RIR 的记录中删除证书。

3. 在 RIR 中创建 ROA 对象

创建 ROA 对象以授权 Amazon ASN 16509 和 14618 来发布您的地址范围，以及当前授权的 ASN 来发布该地址范围。对于 Amazon GovCloud (US) Region，授权 ASN 8987。您必须将最大长度设置为您要引入的 CIDR 的大小。您可以引入的最具体 IPv4 前缀是 /24。对于公开发布的 CIDR，您可以引入的最具体 IPv6 地址范围是 /48，对于不公开发布的 CIDR，您可以引入的最具体 IPv6 地址范围是 /56。

Important

如果您正在为 Amazon VPC IP Address Manager (IPAM) 创建 ROA 对象，则在创建 ROA 时，对于 IPv4 CIDR，必须将 IP 地址前缀的最大长度设置为 /24。对于 IPv6 CIDR，如果要将它们添加到可传播池中，IP 地址前缀的最大长度必须为 /48。这可以确保您有充分的灵活性来跨 Amazon 区域划分您的公有 IP 地址。IPAM 强制执行您设置的最大长度。有关通向 IPAM 的 BYOIP 地址的更多信息，请参阅《Amazon VPC IPAM 用户指南》中的教程：通向 IPAM 的 BYOIP 地址 CIDR。

若要 ROA 可用于 Amazon，可能需要多达 24 小时的时间。有关更多信息，请参阅 RIR：

- ARIN — ROA 请求
- RIPE — 管理 ROA
- APNIC - 路由管理

将广告从本地工作负载迁移到 Amazon 时，在为 Amazon 的 ASN 创建 ROA 之前，您必须为现有的 ASN 创建 ROA。否则，您可能会看到对现有路由和广告的影响。

Note

不公开通告的 IPv6 地址空间不需要此步骤。

载入 BYOIP

根据您的需求，BYOIP 的载入过程具有以下任务：

主题

- 在 Amazon 中预置公开通告的地址范围 (p. 1077)
- 预置不公开发布的 IPv6 地址范围 (p. 1078)
- 通过 Amazon 发布地址范围 (p. 1078)
- 取消预配置地址范围 (p. 1079)

在 Amazon 中预置公开通告的地址范围

预置地址范围与 Amazon 配合使用时，您需要确认您控制该地址范围，并授权亚马逊发布该地址范围。我们还会通过签名授权消息验证您控制该地址范围。该消息是使用在通过 X.509 证书更新 RDAP 记录时使用的自签名 X.509 密钥对签名的。Amazon 需要提供给 RIR 的加密签名授权消息。RIR 根据您添加到 RDAP 的证书验证签名，并根据 ROA 检查授权详细信息。

要预置地址范围

1. 撰写消息

   撰写明文授权消息。消息的格式如下所示，其中，日期是消息的到期日期：

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   将账号、地址范围和到期日期替换为您自己的值，以创建类似于以下内容的消息：

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   这不能与外观类似的 ROA 消息混淆。

2. 对消息进行签名

   使用之前创建的私有密钥对明文消息进行签名。此命令返回的签名是一个长字符串，您需要在下一步中使用。

   Important

   我们建议您复制并粘贴此命令。除消息内容之外，不要修改或替换任何值。

   ```
   signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
    rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM |
    openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
   ```

3. 预置地址

   使用 Amazon CLI provision-byoip-cidr 命令预置地址范围。`--cidr-authorization-context` 选项使用之前创建的消息和签名字符串。

Important

如果 BYOIP 范围与 Amazon CLI 配置 `Default region name` 不同，您必须指定应在其中预配 BYOIP 范围的 Amazon 区域。

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --region us-east-1
```

预配置地址范围是一项异步操作，因此该调用会立即返回，但地址范围未准备就绪，直到其状态从 `pending-provision` 更改为 `provisioned` 才可供使用。

4. 监控进度

完成可公开通告范围的调配过程最多可能需要一周时间。使用 describe-byoip-cidrs 命令来监视进度，如下例所示：

```
aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
```

如果在预置过程中出现问题，并且状态变为 `failed-provision`，则您必须在解决问题后再次运行 `provision-byoip-cidr` 命令。

预置不公开发布的 IPv6 地址范围

默认情况下，将预置一个地址范围以公开发布到 Internet 上。您可以预置不公开发布的 IPv6 地址范围。对于不可公开通告的路由，预置过程通常在几分钟内完成。如果将非公有地址范围的 IPv6 CIDR 块与 VPC 关联，则只能通过支持 IPv6 的混合连接选项（Amazon Direct Connect、Amazon Site-to-Site VPN 或 Amazon VPC Transit Gateway）访问 IPv6 CIDR。

不需要使用 ROA 以预调配非公有地址范围。

Important

您只能指定在预置期间是否公开发布地址范围。您以后无法更改可发布状态。

要预置不公开发布的 IPv6 地址范围，请使用以下 provision-byoip-cidr 命令。

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

通过 Amazon 发布地址范围

预配置地址范围后，即可对其进行发布。您必须发布预配置的确切地址范围。您不能只发布预配置的地址范围的一部分。

如果您预置不公开发布的 IPv6 地址范围，则无需完成该步骤。

在通过 Amazon 发布地址范围之前，我们建议您停止从其他位置发布它。如果您一直从其他位置发布 IP 地址范围，我们将无法可靠地为其提供支持或解决问题。具体来说，我们无法保证到地址范围的流量将进入我们的网络。

为最大限度地减少停机时间，您可以在发布之前将 Amazon 资源配置为使用地址池中的某一地址，然后停止从当前位置发布该地址并同时开始通过 Amazon 发布该地址。有关从地址池分配弹性 IP 地址的更多信息，请参阅分配弹性 IP 地址 (p. 1095)。

限制

- 您最多只能每 10 秒运行一次 advertise-byoip-cidr 命令，即使每次指定不同的地址范围也是如此。

- 您最多只能每 10 秒运行一次 withdraw-byoip-cidr 命令，即使每次指定不同的地址范围也是如此。

要发布地址范围，请使用以下 advertise-byoip-cidr 命令。

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

要停止发布地址范围，请使用以下 withdraw-byoip-cidr 命令。

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

取消预配置地址范围

要停止在 Amazon 上使用您的地址范围，请先释放任何弹性 IP 地址，并取消关联仍从地址池中分配的任何 IPv6 CIDR 块。接下来，停止发布该地址范围，并最终取消预置该地址范围。

您无法取消预置地址范围的一部分。如果要在 Amazon 上使用更具体的地址范围，请取消预置整个地址范围，并预置一个更具体的地址范围。

(IPv4) 要释放每个弹性 IP 地址，请使用以下 release-address 命令。

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) 要取消关联 IPv6 CIDR 块，请使用以下 disassociate-vpc-cidr-block 命令。

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1 --
region us-east-1
```

要停止发布地址范围，请使用以下 withdraw-byoip-cidr 命令。

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

要取消预置地址范围，请使用以下 deprovision-byoip-cidr 命令。

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

取消预置地址范围最多可能需要一天的时间。

使用地址范围

您可以查看和使用在您的账户中预置的 IPv4 和 IPv6 地址范围。

IPv4 地址范围

您可以从 IPv4 地址池中创建弹性 IP 地址，并将其用于您的 Amazon 资源，如 EC2 实例、NAT 网关和 Network Load Balancer。

要查看有关在您的账户中预置的 IPv4 地址池的信息，请使用以下 describe-public-ipv4-pools 命令。

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

要从 IPv4 地址池中创建弹性 IP 地址，请使用 allocate-address 命令。您可以使用 `--public-ipv4-pool` 选项指定 `describe-byoip-cidrs` 返回的地址池的 ID。或者，您可以使用 `--address` 选项从您预置的地址范围中指定一个地址。

IPv6 地址范围

要查看有关在您的账户中预置的 IPv6 地址池的信息，请使用以下 describe-ipv6-pools 命令。

```
aws ec2 describe-ipv6-pools --region us-east-1
```

要创建 VPC 并从 IPv6 地址池中指定 IPv6 CIDR，请使用以下 create-vpc 命令。要让 Amazon 从 IPv6 地址池中选择 IPv6 CIDR，请省略 `--ipv6-cidr-block` 选项。

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-pool pool-id
 --region us-east-1
```

要将 IPv6 地址池中的 IPv6 CIDR 块与 VPC 关联，请使用以下 associate-vpc-cidr-block 命令。要让 Amazon 从 IPv6 地址池中选择 IPv6 CIDR，请省略 `--ipv6-cidr-block` 选项。

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-cidr
 --ipv6-pool pool-id --region us-east-1
```

要查看 VPC 和关联的 IPv6 地址池信息，请使用 describe-vpcs 命令。要查看有关特定 IPv6 地址池中的关联 IPv6 CIDR 块的信息，请使用以下 get-associated-ipv6-pool-cidrs 命令。

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

如果将 IPv6 CIDR 块与 VPC 取消关联，则会将其释放回 IPv6 地址池中。

有关在 VPC 控制台中使用 IPv6 CIDR 块的更多信息，请参阅 Amazon VPC 用户指南 中的使用 VPC 和子网。

验证 BYOIP

1. 验证自签名 x.509 密钥对

   通过 whois 命令验证证书是否已上传且有效。

   对于 ARIN，使用 `whois -h whois.arin.net r + 2001:0DB8:6172::/48` 查找地址范围的 RDAP 记录。检查命令输出中 NetRange（网络范围）的 Public Comments 部分。应将证书添加到地址范围的 Public Comments 部分。

   您可以使用以下命令检查包含证书的 Public Comments：

   ```
   whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
   ```

   这会返回包含密钥内容的输出，应类似于以下内容：

   ```
   Public Comments:
   -----BEGIN CERTIFICATE-----
   MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
   LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
   hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
   wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
   NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
   rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
   VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
   W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
   R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
   prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
   mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
   ```

```
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

对于 RIPE，使用 `whois -r -h whois.ripe.net` *2001:0DB8:7269::/48* 查找地址范围的 RDAP 记录。检查命令输出中 `inetnum` 对象（网络范围）的 `descr` 部分。应将证书添加为地址范围的新 `descr` 字段。

您可以使用以下命令检查包含证书的 `descr`：

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

这会返回包含密钥内容的输出，应类似于以下内容：

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

对于 APNIC，使用 `whois -h whois.apnic.net` *2001:0DB8:6170::/48* 查找 BYOIP 地址范围的 RDAP 记录。检查命令输出中 `inetnum` 对象（网络范围）的 `remarks` 部分。应将证书添加为地址范围的新 `remarks` 字段。

您可以使用以下命令检查包含证书的 `remarks`：

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

这会返回包含密钥内容的输出，应类似于以下内容：

```
remarks:
-----BEGIN CERTIFICATE-----
```

```
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. 验证 ROA 对象创建

   使用 RIPEstat Data API 验证 ROA 对象是否成功创建。请务必根据 Amazon ASN 16509 和 14618 以及当前授权通告地址范围的 ASN 来测试地址范围。

   您可以使用以下命令，通过地址范围检查不同 Amazon ASN 的 ROA 对象：

   ```
   curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
   resource=ASN&prefix=CIDR
   ```

   在此示例输出中，Amazon ASN 16509 的响应结果为 `"status": "valid"`。这表示该地址范围的 ROA 对象已成功创建：

   ```
   {
       "messages": [],
       "see_also": [],
       "version": "0.3",
       "data_call_name": "rpki-validation",
       "data_call_status": "supported",
       "cached": false,
       "data": {
           "validating_roas": [
               {
                   "origin": "16509",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "valid"
               },
               {
                   "origin": "14618",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "invalid_asn"
               },
               {
                   "origin": "64496",
                   "prefix": "2001:0DB8::/32",
                   "max_length": 48,
                   "validity": "invalid_asn"
               }
   ```

```
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```


“unknown” 状态表示该地址范围的 ROA 对象尚未创建。“invalid_asn” 状态表示该地址范围的 ROA 对象尚未成功创建。

为 Amazon EC2 网络接口分配前缀

您可以自动或手动为网络接口分配私有 IPv4 或 IPv6 CIDR 范围。通过分配前缀，您可以扩展和简化应用程序的管理，包括一个实例上需要多个 IP 地址的容器和网络应用程序。

可用的分配选项如下：

- Automatic assignment（自动分配）– Amazon 从 VPC 子网的 IPv4 或 IPv6 CIDR 块中选择前缀，并将其分配给您的网络接口。
- Manual Assignment（手动分配）– 您可以从 VPC 子网的 IPv4 或 IPv6 CIDR 块中指定前缀，Amazon 会在将前缀分配给您的网络接口之前，验证该前缀是否尚未分配给其他资源。

分配前缀具有以下优势：

- 增加了网络接口上的 IP 地址 – 使用前缀时，您可以分配一个 IP 地址块，而不是单个 IP 地址。这会增加网络接口的 IP 地址数量。
- 简化了容器的 VPC 管理 – 在容器应用程序中，每个容器都需要一个唯一的 IP 地址。为您的实例分配前缀可简化 VPC 的管理，因为您可以启动和终止容器，而无需为单个 IP 分配调用 Amazon EC2 API。

主题

- 分配前缀的基础知识 (p. 1083)
- 前缀的注意事项和限制 (p. 1084)
- 使用前缀 (p. 1084)

分配前缀的基础知识

- 您可以为新的或现有网络接口分配前缀。
- 要使用前缀，请为您的网络接口分配前缀，将该网络接口连接至您的实例，然后配置您的操作系统。
- 选择指定前缀的选项时，前缀必须满足以下要求：
  - 您可以指定的 IPv4 前缀为 /28。
  - 您可以指定的 IPv6 前缀为 /80。
  - 前缀位于网络接口的子网 CIDR 中，并且不会与分配给子网中现有资源的其他前缀或 IP 地址重叠。

- 您可以为主网络接口或辅助网络接口分配前缀。
- 您可以将弹性 IP 地址分配给有前缀的网络接口。
- 您也可以将弹性 IP 地址分配给已分配前缀的 IP 地址。
- 我们将实例的私有 DNS 主机名解析为主私有 IPv4 地址。
- 我们使用以下格式为网络接口分配每个私有 IPv4 地址，包括前缀中的地址：
  - us-east-1 区域

```
ip-private-ipv4-address.ec2.internal
```

  - 所有其他区域

```
ip-private-ipv4-address.region.compute.internal
```

前缀的注意事项和限制

使用前缀时请注意以下事项：

- 基于 Nitro 系统构建的实例 (p. 246)支持带有前缀的网络接口。
- 网络接口的前缀仅限为 IPv6 地址和私有 IPv4 地址。
- 您可以分配给网络接口的 IP 地址的最大数量取决于实例类型。您分配给网络接口的每个前缀都算作一个 IP 地址。例如，c5.large 实例具有每个网络接口 10 个 IPv4 地址的限制。此实例的每个网络接口都有一个主 IPv4 地址。如果网络接口没有辅助 IPv4 地址，则您最多可以为网络接口分配 9 个前缀。您每为网络接口多分配一个 IPv4 地址，则您就可以为网络接口少分配一个前缀。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。
- 前缀包含在源/目标检查中。

使用前缀

主题

- 在网络接口创建过程中分配前缀 (p. 1084)
- 分配前缀至现有网络接口 (p. 1089)
- 为带有前缀的网络接口配置操作系统 (p. 1091)
- 查看分配至您的网络接口的前缀 (p. 1091)
- 从网络接口中移除前缀 (p. 1093)

在网络接口创建过程中分配前缀

如果使用自动分配选项，则可以在子网中预留 IP 地址块。Amazon 会从此块中选择前缀。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网 CIDR 预留。

创建网络接口后，使用 attach-network-interface Amazon CLI 命令将网络接口连接到您的实例。您必须配置操作系统，才能使用带有前缀的网络接口。有关更多信息，请参阅为带有前缀的网络接口配置操作系统 (p. 1091)。

主题

- 在网络接口创建过程中自动分配前缀 (p. 1085)
- 在网络接口创建过程中分配特定前缀 (p. 1087)

在网络接口创建过程中自动分配前缀

您可以使用下列方法之一在网络接口创建过程中自动分配前缀。

Console

在网络接口创建过程中自动分配前缀

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口），然后选择 Create network interface（创建网络接口）。
3. 指定网络接口的描述，选择要在其中创建网络接口的子网，并配置私有 IPv4 和 IPv6 地址。
4. 展开 Advanced settings（高级设置），并执行以下操作：
   a. 要自动分配 IPv4 前缀，对于 IPv4 prefix delegation（IPv4 前缀委派），选择 Auto-assign（自动分配）。然后对于 Number of IPv4 prefixes（IPv4 前缀的数量），指定要分配的前缀数。
   b. 要自动分配 IPv6 前缀，对于 IPv6 prefix delegation（IPv6 前缀委派），选择 Auto-assign（自动分配）。然后对于 Number of IPv6 prefixes（IPv6 前缀的数量），指定要分配的前缀数。

      Note

      IPv6 prefix delegation（IPv6 前缀委派）仅当为 IPv6 启用了选定的子网时才会显示。
5. 选择要与网络接口关联的安全组，并根据需要分配资源标签。
6. 选择创建网络接口。

Amazon CLI

在网络接口创建过程中自动分配 IPv4 前缀

使用 create-network interface 命令并将 `--ipv4-prefix-count` 设置为您希望 Amazon 分配的前缀数。在下面的示例中，Amazon 分配 1 前缀。

```
$ aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

输出示例

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
```

```
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

在网络接口创建过程中自动分配 IPv6 前缀

使用 create-network interface 命令并将 `--ipv6-prefix-count` 设置为您希望 Amazon 分配的前缀数。在下面的示例中，Amazon 分配 1 前缀。

```
$ aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

输出示例

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
```

```
}
```

在网络接口创建过程中分配特定前缀

您可以使用下列方法之一在网络接口创建过程中分配特定前缀。

Console

在网络接口创建过程中分配特定前缀

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口），然后选择 Create network interface（创建网络接口）。
3. 指定网络接口的描述，选择要在其中创建网络接口的子网，并配置私有 IPv4 和 IPv6 地址。
4. 展开 Advanced settings（高级设置），并执行以下操作：
   a. 要分配特定 IPv4 前缀，对于 IPv4 prefix delegation（IPv4 前缀委派），选择 Custom（自定义）。然后选择 Add new prefix（添加新前缀），并输入要使用的前缀。
   b. 要分配特定 IPv6 前缀，对于 IPv6 prefix delegation（IPv6 前缀委派），选择 Custom（自定义）。然后选择 Add new prefix（添加新前缀），并输入要使用的前缀。

      Note

      IPv6 prefix delegation（IPv6 前缀委派）仅当为 IPv6 启用了选定的子网时才会显示。
5. 选择要与网络接口关联的安全组，并根据需要分配资源标签。
6. 选择创建网络接口。

Amazon CLI

在网络接口创建过程中分配特定 IPv4 前缀

使用 create-network interface 命令并设置 `--ipv4-prefixes` 至前缀。Amazon 会从此范围中选择 IP 地址。在下面的示例中，前缀 CIDR 为 `10.0.0.208/28`。

```
$ aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

输出示例

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 manual example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
```

```
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

在网络接口创建过程中分配特定 IPv6 前缀

使用 create-network interface 命令并设置 `--ipv6-prefixes` 至前缀。Amazon 会从此范围中选择 IP 地址。在下面的示例中，前缀 CIDR 为 `2600:1f13:fc2:a700:1768::/80`。

```
$ aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

输出示例

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
```

```
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

分配前缀至现有网络接口

分配前缀后，使用 attach-network-interface Amazon CLI 命令将网络接口连接到您的实例。您必须配置操作系统，才能使用带有前缀的网络接口。有关更多信息，请参阅为带有前缀的网络接口配置操作系统 (p. 1091)。

自动分配前缀至现有网络接口

您可以使用下列方法之一向现有网络接口自动分配前缀。

Console

自动分配前缀至现有网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择要为其分配前缀的网络接口，然后选择 Actions（操作）、Manage prefixes（管理前缀）。
4. 要自动分配 IPv4 前缀，对于 IPv4 prefix delegation（IPv4 前缀委派），选择 Auto-assign（自动分配）。然后对于 Number of IPv4 prefixes（IPv4 前缀的数量），指定要分配的前缀数。
5. 要自动分配 IPv6 前缀，对于 IPv6 prefix delegation（IPv6 前缀委派），选择 Auto-assign（自动分配）。然后对于 Number of IPv6 prefixes（IPv6 前缀的数量），指定要分配的前缀数。

   Note

   IPv6 prefix delegation（IPv6 前缀委派）仅当为 IPv6 启用了选定的子网时才会显示。
6. 选择 Save（保存）。

Amazon CLI

您可以使用 assign-ipv6-addresses 命令来分配 IPv6 前缀，使用 assign-private-ip-addresses 命令将 IPv4 前缀分配给现有网络接口。

自动分配 IPv4 前缀至现有网络接口

使用 assign-private-ip-addresses 命令并将 `--ipv4-prefix-count` 设置为您希望 Amazon 分配的前缀数。在下面的示例中，Amazon 分配 1 IPv4 前缀。

```
$ aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

输出示例

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
        }
    ]
}
```

自动分配 IPv6 前缀至现有网络接口

使用 assign-ipv6-addresses 命令并将 `--ipv6-prefix-count` 设置为您希望 Amazon 分配的前缀数。在下面的示例中，Amazon 分配 1 IPv6 前缀。

```
$ aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

输出示例

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

分配特定前缀至现有网络接口

您可以使用下列方法之一分配特定前缀至现有网络接口。

Console

分配特定前缀至现有网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择要为其分配前缀的网络接口，然后选择 Actions（操作）、Manage prefixes（管理前缀）。
4. 要分配特定 IPv4 前缀，对于 IPv4 prefix delegation（IPv4 前缀委派），选择 Custom（自定义）。然后选择 Add new prefix（添加新前缀），并输入要使用的前缀。
5. 要分配特定 IPv6 前缀，对于 IPv6 prefix delegation（IPv6 前缀委派），选择 Custom（自定义）。然后选择 Add new prefix（添加新前缀），并输入要使用的前缀。

   Note

   IPv6 prefix delegation（IPv6 前缀委派）仅当为 IPv6 启用了选定的子网时才会显示。
6. 选择 Save（保存）。

Amazon CLI

分配特定 IPv4 前缀至现有网络接口

使用 assign-private-ip-addresses 命令并设置 `--ipv4-prefixes` 至前缀。Amazon 会从此范围中选择 IPv4 地址。在下面的示例中，前缀 CIDR 为 `10.0.0.208/28`。

```
$ aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

输出示例

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
```

```
            "Ipv4Prefix": "10.0.0.208/28"
        }
    ]
}
```

分配特定 IPv6 前缀至现有网络接口

使用 assign-ipv6-addresses 命令并设置 `--ipv6-prefixes` 至前缀。Amazon 会从此范围中选择 IPv6 地址。在下面的示例中，前缀 CIDR 为 `2600:1f13:fc2:a700:18bb::/80`。

```
$ aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

输出示例

```
{
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",
    "AssignedIpv6Prefixes": [
        {
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"
        }
    ]
}
```

为带有前缀的网络接口配置操作系统

Amazon Linux AMI 可能包含由 Amazon 安装的其他脚本，它们称为 `ec2-net-utils`。这些脚本可以选择性地自动配置您的网络接口。它们仅适用于 Amazon Linux。

如果您没有使用 Amazon Linux，您可以将容器网络接口 (CNI) 用于 Kubernetes 插件或 `dockerd`（如果您使用 Docker 管理容器）。

查看分配至您的网络接口的前缀

您可以使用下列方法之一查看分配至您的网络接口的前缀。

Console

查看分配至现有网络接口的自动前缀

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择要查看其前缀的网络接口，然后选择 Details（详细信息）选项卡。
4. IPv4 Prefix Delegation（IPv4 前缀委派）字段列出了分配的 IPv4 前缀，IPv6 Prefix Delegation（IPv6 前缀委派）字段列出了分配的 IPv6 前缀。

Amazon CLI

您可以使用 describe-network-interfaces Amazon CLI 命令查看分配给网络接口的前缀。

```
$ aws ec2 describe-network-interfaces
```

输出示例

```
{
```

```
    "NetworkInterfaces": [
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "Ipv6Prefixes": [],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b2146bf252"
        },
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c411c91b5"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:bb:e4:31:fe:09",
            "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.73",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.73"
                }
            ],
            "Ipv4Prefixes": [],
            "Ipv6Prefixes": [
                {
                    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
```

```
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    ]
}
```

从网络接口中移除前缀

您可以使用下列方法之一从网络接口中移除前缀。

Console

从网络接口中移除前缀

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择要从中移除前缀的网络接口，然后选择 Actions（操作）、Manage prefixes（管理前缀）。
4. 请执行下列操作之一：
   - 要移除所有分配的前缀，对于 IPv4 prefix delegation（IPv4 前缀委派）和 IPv6 prefix delegation（IPv6 前缀委派），选择 Do not assign（不分配）。
   - 要移除特定分配的前缀，对于 IPv4 prefix delegation（IPv4 前缀委派）和 IPv6 prefix delegation（IPv6 前缀委派），选择 Custom（自定义），然后选择要移除的前缀旁的 Unassign（取消分配）。

     Note

     IPv6 prefix delegation（IPv6 前缀委派）仅当为 IPv6 启用了选定的子网时才会显示。
5. 选择 Save（保存）。

Amazon CLI

您可以使用 unassign-ipv6-addresses 命令来移除 IPv6 前缀，使用 unassign-private-ip-addresses 命令将 IPv4 前缀从现有网络接口中移除。

从网络接口中移除 IPv4 前缀

使用 unassign-private-ip-addresses 命令并将 `--ipv4-prefix` 设置为要删除的地址。

```
$ aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

从网络接口中移除 IPv6 前缀

使用 unassign-ipv6-addresses 命令并将 `--ipv6-prefix` 设置为要删除的地址。

```
$ aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

弹性 IP 地址

弹性 IP 地址是专为动态云计算设计的静态 IPv4 地址。弹性 IP 地址会分配给您的 Amazon 账户，并且在您释放它之前一直属于您。使用弹性 IP 地址，您可以快速将地址重新映射到您的账户中的另一个实例，从而屏蔽实例故障。或者，您可以在域的 DNS 记录中指定弹性 IP 地址，以使域指向您的实例。有关更多信息，请参阅您的域注册商或在 Amazon Linux 实例上设置动态 DNS (p. 747)的文档。

弹性 IP 地址是公有 IPv4 地址，可通过 Internet 访问。如果您的实例没有公有 IPv4 地址，则可以将弹性 IP 地址与您的实例关联以启用与 Internet 的通信。例如，这允许您从本地计算机连接到您的实例。

目录

- 弹性 IP 地址定价 (p. 1094)
- 弹性 IP 地址基本信息 (p. 1094)
- 使用弹性 IP 地址 (p. 1095)
- 弹性 IP 地址限制 (p. 1104)

弹性 IP 地址定价

为确保弹性 IP 地址的有效使用，如果弹性 IP 地址未与正在运行的实例关联，或者它已与停止的实例或未附加的网络接口关联，我们将强制收取小额的小时费用。当您的实例正在运行时，您无需为与该实例关联的某个弹性 IP 地址付费，但需为与该实例关联的所有其他弹性 IP 地址付费。

有关更多信息，请参阅上的弹性 IP 地址。

弹性 IP 地址基本信息

下面是弹性 IP 地址的基本特征：

- 弹性 IP 地址是静态地址，不会随着时间的推移而改变。
- 一个弹性 IP 地址只能在一个特定区域中使用，不能移动到其他区域。
- 弹性 IP 地址来自 Amazon 的 IPv4 地址池，或来自已引入到您的 Amazon 账户的自定义 IPv4 地址池。
- 要使用弹性 IP 地址，您应首先向您的账户分配这样一个地址，然后将其与您的实例或网络接口关联。
- 当您将弹性 IP 地址与实例关联时，该地址也会与实例的主网络接口相关联。当您将弹性 IP 地址与连接到实例的网络接口关联时，它也与该实例关联。
- 当您将弹性 IP 地址与实例或其主网络接口关联时，实例的公有 IPv4 地址 (如果有) 将释放回 Amazon 的公有 IPv4 地址池中。您不能重用公有 IPv4 地址，并且不能将公有 IPv4 地址转换为弹性 IP 地址。有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。
- 您可以取消弹性 IP 地址与资源的关联，然后重新将此地址与其他资源关联。为避免意外行为，请确保在进行更改之前关闭到现有关联中指定资源的所有活动连接。将弹性 IP 地址关联到其他资源后，可以重新打开与新关联的资源的连接。
- 取消关联的弹性 IP 地址保持分配到您的账户，直至您明确释放它。如果弹性 IP 地址未与正在运行的实例关联，我们会按小时收取少量费用。
- 在将弹性 IP 地址与之前具有公有 IPv4 地址的实例关联时，该实例的公有 DNS 主机名将发生更改以匹配弹性 IP 地址。
- 我们会将公有 DNS 主机名解析为实例所在网络外部的该实例的公有 IPv4 地址或弹性 IP 地址，以及实例所在网络内部的该实例的私有 IPv4 地址。
- 从已引入到您 Amazon 账户的 IP 地址池分配弹性 IP 地址时，该地址不会计入弹性 IP 地址限制。有关更多信息，请参阅弹性 IP 地址限制 (p. 1104)。
- 分配弹性 IP 地址时，您可以将弹性 IP 地址与网络边界组关联。这是我们通告 CIDR 块的位置。设置网络边界组会将 CIDR 块限制到此组。如果您未指定网络边界组，我们将设置包含区域中所有可用区的边界组（例如，`us-west-2`）。

- 弹性 IP 地址仅用于特定网络边界组。

使用弹性 IP 地址

以下部分介绍如何使用弹性 IP 地址。

任务

- 分配弹性 IP 地址 (p. 1095)
- 描述您的弹性 IP 地址 (p. 1096)
- 为弹性 IP 地址添加标签 (p. 1096)
- 将弹性 IP 地址与实例或网络接口关联起来 (p. 1097)
- 解除弹性 IP 地址的关联 (p. 1098)
- 转移弹性 IP 地址 (p. 1098)
- 释放弹性 IP 地址 (p. 1101)
- 恢复弹性 IP 地址 (p. 1102)
- 将反向 DNS 用于电子邮件应用程序 (p. 1102)

分配弹性 IP 地址

您可以从 Amazon 的公有 IPv4 地址池分配弹性 IP 地址，也可以从已引入到您 Amazon 账户的自定义 IP 地址池分配该地址。有关将您自己的 IP 地址范围引入到您 Amazon 账户的更多信息，请参阅 在 Amazon EC2 中使用您自己的 IP 地址 (BYOIP) (p. 1070)。

您可以使用以下方法之一分配弹性 IP 地址。

Console

分配弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network & Security（网络与安全）下的Elastic IPs（弹性 IP）。
3. 选择 Allocate Elastic IP address (分配弹性 IP 地址)。
4. 对于Public IPv4 address pool（公有 IPv4 地址池），选择以下选项之一：
   - Amazon 的 IPv4 地址池—如果要从 Amazon 的 IPv4 地址池中分配 IPv4 地址。
   - Public IPv4 address that you bring to your Amazon account - 如果您想从已引入到您的 Amazon 账户的 IP 地址池中分配 IPv4 地址。如果您没有任何 IP 地址池，则此选项将被禁用。
   - Customer owned pool of IPv4 addresses (客户拥有的 IPv4 地址池) – 如果要从在本地网络创建的池中分配 IPv4 地址以供 Amazon Outpost 使用。如果您没有 Amazon Outpost，则此选项将被禁用。
5. （可选）添加或删除标签。

   [添加标签] 选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于 Value（值），输入键值。

   [删除标签] 选择标签的“键”和“值”右侧的删除。
6. 选择 Allocate。

Amazon CLI

分配弹性 IP 地址

使用 allocate-address Amazon CLI 命令。

PowerShell

分配弹性 IP 地址

使用 New-EC2Address Amazon Tools for Windows PowerShell 命令。

描述您的弹性 IP 地址

您可以使用以下方法之一描述弹性 IP 地址。

Console

描述您的弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要查看的弹性 IP 地址，然后依次选择 Actions (操作)、View details (查看详细信息)。

Amazon CLI

描述您的弹性 IP 地址

使用 describe-addresses Amazon CLI 命令。

PowerShell

描述您的弹性 IP 地址

使用 Get-EC2Address Amazon Tools for Windows PowerShell 命令。

为弹性 IP 地址添加标签

可以为您的弹性 IP 地址分配自定义标签，以不同的方式对它们分类，例如按用途、所有者或环境。这有助于您根据所分配的自定义标签快速查找特定弹性 IP 地址。

不支持使用弹性 IP 地址标签跟踪成本分配。

您可以使用以下方法之一标记弹性 IP 地址。

Console

为弹性 IP 地址添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要标记的弹性 IP 地址，然后依次选择 Actions (操作)、View details (查看详细信息)。
4. 在 Tags (标签) 部分中，选择 Manage tags (管理标签)。
5. 指定标签键值对。
6. （可选）选择 Add tag (添加标签) 以添加其他标签。
7. 选择 Save。

Amazon CLI

为弹性 IP 地址添加标签

使用 create-tags Amazon CLI 命令。

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

为弹性 IP 地址添加标签

使用 New-EC2Tag Amazon Tools for Windows PowerShell 命令。

New-EC2Tag 命令需要 Tag 参数，来指定弹性 IP 地址标签要使用的键值对。以下命令创建 Tag 参数。

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
 PS C:\> $tag.Key = "Owner"
 PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

将弹性 IP 地址与实例或网络接口关联起来

如果要将弹性 IP 地址与您的实例关联以启用与 Internet 的通信，您还必须确保您的实例在公有子网中。有关更多信息，请参阅 Amazon VPC 用户指南 中的 Internet 网关。

您可以使用以下方法之一将弹性 IP 地址与实例或网络接口关联。

Console

要关联弹性 IP 地址和实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要关联的弹性 IP 地址，然后依次选择 Actions (操作)、Associate Elastic IP address (关联弹性 IP 地址)。
4. 对于 Resource type (资源类型)，选择 Instance (实例)。
5. 例如，选择要将弹性 IP 地址关联到的实例。您还可以输入文本以搜索特定实例。
6. （可选）对于 Private IP address (私有 IP 地址)，请指定要将弹性 IP 地址关联到的私有 IP 地址。
7. 选择 Associate。

将弹性 IP 地址与网络接口相关联

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要关联的弹性 IP 地址，然后依次选择 Actions (操作)、Associate Elastic IP address (关联弹性 IP 地址)。
4. 对于 Resource type (资源类型)，选择 Network interface (网络接口)。
5. 对于 Network interface (网络接口)，请选择要将弹性 IP 地址关联到的网络接口。您还可以输入文本来搜索特定网络接口。
6. （可选）对于 Private IP address (私有 IP 地址)，请指定要将弹性 IP 地址关联到的私有 IP 地址。
7. 选择 Associate。

Amazon CLI

关联弹性 IP 地址

使用 associate-address Amazon CLI 命令。

PowerShell

关联弹性 IP 地址

使用 Register-EC2Address Amazon Tools for Windows PowerShell 命令。

解除弹性 IP 地址的关联

您可以随时取消弹性 IP 地址与实例或网络接口的关联。取消关联弹性 IP 地址后，您可以将其与其他资源重新关联。

您可以使用下列方法之一取消关联弹性 IP 地址。

Console

取消关联和重新关联弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要取消关联的弹性 IP 地址，然后依次选择 Actions (操作)、Disassociate Elastic IP address (取消关联弹性 IP 地址)。
4. 选择取消关联。

Amazon CLI

撤销弹性 IP 地址的关联

使用 disassociate-address Amazon CLI 命令。

PowerShell

撤销弹性 IP 地址的关联

使用 Unregister-EC2Address Amazon Tools for Windows PowerShell 命令。

转移弹性 IP 地址

本节介绍如何将弹性 IP 地址从一个 Amazon Web Services 账户 转移到另一个账户。在以下情况下，转移弹性 IP 地址可能会很有用：

- 组织调整 – 使用弹性 IP 地址转移在 Amazon Web Services 账户 之间快速转移工作负载。您不必等待新弹性 IP 地址被列入安全组和 NACL 的允许名单。
- 集中式安全管理 – 使用集中式 Amazon 安全账户跟踪和转移已通过安全合规性审查的弹性 IP 地址。
- 灾难恢复 – 在紧急事件期间使用弹性 IP 地址转移，为面向公众的互联网工作负载快速重新映射 IP。

转移弹性 IP 地址不收取任何费用。

任务

- 启用弹性 IP 地址转移 (p. 1099)
- 禁用弹性 IP 地址转移 (p. 1100)
- 接受转移的弹性 IP 地址 (p. 1100)

启用弹性 IP 地址转移

本节介绍如何接受转移的弹性 IP 地址。请注意以下与启用弹性 IP 地址转移相关的限制：

- 您可以将弹性 IP 地址从任何 Amazon Web Services 账户（源账户）转移到同一 Amazon 区域的任何其他 Amazon 账户（转移账户）。
- 在转移弹性 IP 地址时，Amazon Web Services 账户 账户之间有两步握手。当源账户开始转移时，转移账户有七天的时间来接受这个弹性 IP 地址转移。在那七天之内，从源账户可以看得见有待转移的那个弹性 IP 地址，比如：在亚马逊控制台中，或通过使用 describe-address-transfers 这个 Amazon CLI 命令即可看到。七天之后，转移将过期，而且弹性 IP 地址的所有权将被返回给其原始账户。
- Amazon 不会向转移账户通知待处理的弹性 IP 地址转移请求。源账户的所有者必须通知转移账户的所有者：他们必须接受弹性 IP 地址转移请求。
- 转移完成后，与正在转移的弹性 IP 地址关联的所有标签都将被重置。
- 您无法将从自带的公有 IPv4 地址池 [通常称为自带 IP（BYOIP）地址池] 分配的弹性 IP 地址转移到您的 Amazon Web Services 账户。
- 如果已启用并配置了 Amazon Outposts，则您可能已从客户拥有的 IP 地址池（CoIP）中分配了弹性 IP 地址。您无法转移从 CoIP 分配的弹性 IP 地址。但是，您可以使用 Amazon RAM 与其他账户共享 CoIP。有关更多信息，请参阅《Amazon Outposts 用户指南》中的客户拥有的 IP 地址。
- 您可以使用 Amazon VPC IPAM 跟踪向 Amazon Organizations 组织中的账户转移弹性 IP 地址的情况。有关更多信息，请参阅查看 IP 地址历史记录。但是，如果将弹性 IP 地址转移到组织外部的 Amazon Web Services 账户，则弹性 IP 地址的 IPAM 审核历史记录将丢失。

这些步骤必须由源账户完成。

Console

启用弹性 IP 地址转移

1. 确保您使用的是源 Amazon 账户。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择 Elastic IPs。
4. 选择一个或多个要启用转移的弹性 IP 地址，然后选择 Actions（操作）、Enable transfer（启用转移）。
5. 如果要转移多个弹性 IP 地址，则会看到 Transfer type（转移类型）选项。请选择以下任一选项：
   - 如果要将弹性 IP 地址转移到单个 Amazon 账户，请选择 Single account（单个账户）。
   - 如果要将弹性 IP 地址转移到多个 Amazon 账户，请选择 Multiple accounts（多个账户）。
6. 在 Transfer account ID（转移账户 ID）下，输入要向其转移弹性 IP 地址的 Amazon 账户的 ID。
7. 在文本框中输入 **enable** 以确认转移。
8. 选择 Submit（提交）。
9. 若要接受转移，请参阅 接受转移的弹性 IP 地址 (p. 1100)。若要禁用转移，请参阅 禁用弹性 IP 地址转移 (p. 1100)。

Amazon CLI

启用弹性 IP 地址转移

使用 enable-address-transfer 命令。

PowerShell

启用弹性 IP 地址转移

使用 Enable-EC2AddressTransfer 命令。

禁用弹性 IP 地址转移

本节介绍如何在启用转移后禁用弹性 IP 转移。

这些步骤必须由启用转移的源账户完成。

Console

禁用弹性 IP 地址转移

1. 确保您使用的是源 Amazon 账户。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择 Elastic IPs。
4. 在弹性 IP 的资源列表中，确保启用了显示 Transfer status（转移状态）列的属性。
5. 选择一个或多个 Transfer status（转移状态）为 Pending（待处理）的弹性 IP 地址，然后选择 Actions（操作）、Disable transfer（禁用转移）。
6. 在文本框中输入 **disable** 以确认。
7. 选择 Submit（提交）。

Amazon CLI

禁用弹性 IP 地址转移

使用 disable-address-transfer 命令。

PowerShell

禁用弹性 IP 地址转移

使用 Disable-EC2AddressTransfer 命令。

接受转移的弹性 IP 地址

本节介绍如何接受转移的弹性 IP 地址。

在转移弹性 IP 地址时，Amazon 账户之间有两步握手：源账户（标准 Amazon 账户或 Amazon Organizations 账户）和转移账户。当源账户开始转移时，转移账户有七个小时接受弹性 IP 地址转移，否则弹性 IP 地址将返回给其原始所有者。

接受转移时，请注意可能发生的以下异常情况以及如何解决这些异常：

- AddressLimitExceeded：如果您的转移账户已超过弹性 IP 地址配额，则源账户可以启用弹性 IP 地址转移，但是当转移账户尝试接受转移时，会发生此异常。默认情况下，所有 Amazon 账户限制为每个区域使用 5 个弹性 IP 地址。有关提高限制的说明，请参阅 弹性 IP 地址限制 (p. 1104)。
- InvalidTransfer.AddressCustomPtrSet：如果您或组织中的某人已将您正在尝试转移的弹性 IP 地址配置为使用反向 DNS 查找，则源账户可以启用弹性 IP 地址转移，但是当转移账户尝试接受转移时，会发生此异常。若要解决此问题，源账户必须删除弹性 IP 地址的 DNS 记录。有关更多信息，请参阅将反向 DNS 用于电子邮件应用程序 (p. 1102)。
- InvalidTransfer.AddressAssociated：如果弹性 IP 地址与 ENI 或 EC2 实例相关联，则源帐户可以启用弹性 IP 地址转移，但是当转移帐户尝试接受转移时，会发生此异常。若要解决此问题，源帐户必须解除弹性 IP 地址的关联。有关更多信息，请参阅解除弹性 IP 地址的关联 (p. 1098)。

对于任何其他异常，请联系 Amazon Web Services Support。

这些步骤必须由转移账户完成。

Console

接受弹性 IP 地址转移

1. 确保您使用的是转移账户。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择 Elastic IPs。
4. 选择 Actions（操作）、Accept transfer（接受转移）。
5. 当您接受转移时，与要转移的弹性 IP 地址关联的标签不会随弹性 IP 地址一起转移。如果要为所接受的弹性 IP 地址定义 Name（名称）标签，请选择 Create a tag with a key of 'Name' and a value that you specify（创建具有“Name”键以及您指定的值的标签）。
6. 输入要转移的弹性 IP 地址。
7. 如果您接受多个转移的弹性 IP 地址，请选择 Add address（添加地址）以输入附加弹性 IP 地址。
8. 选择 Submit（提交）。

Amazon CLI

接受弹性 IP 地址转移

使用 accept-address-transfer 命令。

PowerShell

接受弹性 IP 地址转移

使用 Approve-EC2AddressTransfer 命令。

释放弹性 IP 地址

如果您不再需要弹性 IP 地址，我们建议您使用以下方法之一释放该地址。要发布的地址当前不得与 Amazon 资源关联，例如 EC2 实例、NAT 网关或 Network Load Balancer。

Note

如果您联系了 Amazon Support 为弹性 IP（EIP）地址设置反向 DNS，您可以删除该反向 DNS，但不能释放弹性 IP 地址，因为它已被 Amazon Support 锁定。要解锁弹性 IP 地址，请联系 Amazon Web Services Support。解锁弹性 IP 地址后，您就可以释放弹性 IP 地址。

Console

释放弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择要释放的弹性 IP 地址，然后依次选择 Actions (操作)、Release Elastic IP addresses (释放弹性 IP 地址)。
4. 选择 Release (释放)。

Amazon CLI

释放弹性 IP 地址

使用 release-address Amazon CLI 命令。

PowerShell

释放弹性 IP 地址

使用 Remove-EC2Address Amazon Tools for Windows PowerShell 命令。

恢复弹性 IP 地址

如果您已释放您的弹性 IP 地址，则可能能够恢复它。以下规则适用：

- 如果弹性 IP 地址已分配至其他 Amazon 账户，或者该地址将导致您超出弹性 IP 地址限制，则您无法恢复该地址。
- 您不能恢复与弹性 IP 地址关联的标签。
- 您只能使用 Amazon EC2 API 或命令行工具恢复弹性 IP 地址。

Amazon CLI

恢复弹性 IP 地址

使用 allocate-address Amazon CLI 命令，并使用 `--address` 参数指定 IP 地址，如下所示。

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

恢复弹性 IP 地址

使用 New-EC2Address Amazon Tools for Windows PowerShell 命令，并使用 `-Address` 参数指定 IP 地址，如下所示。

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

将反向 DNS 用于电子邮件应用程序

如果您打算从实例向第三方发送电子邮件，我们建议您调配一个或多个弹性 IP 地址，并向您用于发送电子邮件的弹性 IP 地址分配静态反向 DNS 记录。这样有助于避免电子邮件被一些反垃圾电子邮件组织标记为垃圾电子邮件。Amazon 与 ISP 以及 Internet 反垃圾电子邮件组织合作，减少从这些地址发送的电子邮件被标记为垃圾电子邮件的几率。

注意事项

- 在创建反向 DNS 记录之前，您必须设置指向您的弹性 IP 地址的对应的正向 DNS 记录（记录类型 A）。
- 如果反向 DNS 记录与弹性 IP 地址关联，则该弹性 IP 地址将锁定到您的账户中且无法从您的账户中释放，直至删除记录。
- Amazon GovCloud (US) Region

  您不能使用控制台或 Amazon CLI 创建反向 DNS 记录。Amazon 必须为您分配静态反向 DNS 记录。打开 Request to remove reverse DNS and email sending limitations（请求删除反向 DNS 和电子邮件发送限制），向我们提供您的弹性 IP 地址和反向 DNS 记录。

创建反向 DNS 记录

要创建反向 DNS 记录，请选择与您的首选方法匹配的选项卡。

Console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Elastic IPs。
3. 选择弹性 IP 地址，然后依次选择 Actions（操作）和 Update reverse DNS（更新反向 DNS）。
4. 对于 Reverse DNS domain name（反向 DNS 域名），输入域名。
5. 输入 **update** 以确认。
6. 选择更新。

Amazon CLI

在 Amazon CLI 中使用 modify-address-attribute 命令，如以下示例中所示：

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --domain-
name example.com
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
        }
    ]
}
```

删除反向 DNS 记录

要删除反向 DNS 记录，请选择与您的首选方法匹配的选项卡。

Console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择弹性 IP 地址，然后依次选择 Actions（操作）和 Update reverse DNS（更新反向 DNS）。
4. 对于 Reverse DNS domain name（反向 DNS 域名），清除域名。
5. 输入 **update** 以确认。
6. 选择更新。

Amazon CLI

在 Amazon CLI 中使用 reset-address-attribute 命令，如以下示例中所示：

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
    ]
}
```

Note

如果您在运行该命令时收到以下错误消息，则您可以向客户支持部门提交删除电子邮件发送限制的请求以获得帮助。
无法释放带有分配 ID 的地址，因为它已锁定到您的账户。

弹性 IP 地址限制

默认情况下，所有 Amazon 账户在每个区域最多可拥有五 (5) 个弹性 IP 地址，因为公有 (IPv4) Internet 地址是稀缺的公有资源。我们强烈鼓励您主要使用弹性 IP 地址，以便在实例发生故障的情况下能够将该地址映射到另一实例，并能够将 DNS 主机名用于所有其他节点间通信。

验证正在使用的弹性 IP 地址数量

访问 https://console.aws.amazon.com/ec2/，打开 Amazon EC2 控制台，然后从导航窗格中选择 Elastic IPs (弹性 IP)。

验证弹性 IP 地址的当前账户限制

您可以在 Amazon EC2 控制台或 Service Quotas 控制台中验证您的限制。请执行下列操作之一：

- 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

  从导航窗格中选择限制，然后在搜索字段中输入 **IP**。限制为 EC2-VPC 弹性 IP。如果您有权访问 EC2-Classic，还有一个额外的限制，即 EC2-Classic 弹性 IP。
- 访问 https://console.aws.amazon.com/servicequotas/，打开 Service Quotas 控制台。

  在控制面板中，选择 Amazon Elastic Compute Cloud (Amazon EC2)。如果控制面板中未列出 Amazon Elastic Compute Cloud (Amazon EC2)，请选择 Amazon services (亚马逊云科技服务)，在搜索字段中输入 **EC2**，然后选择 Amazon Elastic Compute Cloud (Amazon EC2)。

  在 Amazon EC2 Service Quotas 页面上，在搜索字段中输入 **IP**。限制为 EC2-VPC 弹性 IP。如果您有权访问 EC2-Classic，还有一个额外的限制，即 EC2-Classic 弹性 IP。有关更多信息，请选择限制。

如果您认为您的架构需要额外的弹性 IP 地址，则可直接从 Service Quotas 控制台请求提高配额。

弹性网络接口

弹性网络接口 是 VPC 中表示虚拟网卡的逻辑网络组件。它可以包含以下属性：

- 您的 VPC 的 IPv4 地址范围内的一个主要私有 IPv4 地址
- 您的 VPC 的 IPv4 地址范围内的一个或多个辅助私有 IPv4 地址
- 每个私有 IPv4 地址一个弹性 IP 地址 (IPv4)
- 一个公有 IPv4 地址
- 一个或多个 IPv6 地址
- 一个或多个安全组
- 一个 MAC 地址
- 一个源/目标检查标记
- 一个描述

您可以创建并配置网络接口，并将其连接到同一可用区中的实例。您的账户也可能具有请求者托管的网络接口，这些网络接口是由 Amazon 服务创建和管理的，让您可以使用其他资源和服务。您自己无法管理这些网络接口。有关更多信息，请参阅请求者托管的网络接口 (p. 1140)。

该 Amazon 资源在 Amazon Web Services Management Console 和 Amazon EC2 API 中称为网络接口。因此，我们在本文档中使用“网络接口”，而不是“弹性网络接口”。本文档中的“网络接口”术语始终表示“弹性网络接口”。

目录

- 网络接口基础知识 (p. 1105)
- 网卡 (p. 1106)
- 每种实例类型的每个网络接口的 IP 地址数 (p. 1107)
- 使用网络接口 (p. 1129)
- 配置网络接口的最佳实践 (p. 1136)
- 网络接口方案 (p. 1138)
- 请求者托管的网络接口 (p. 1140)

网络接口基础知识

您可以创建一个网络接口，将其连接到某个实例，将其与实例分离，再连接到另一个实例。将网络接口附加到一个实例或者从一个实例分离并重新附加到另一实例时，网络接口的属性不会变化。当您将一个网络接口从一个实例移动到另一个实例时，网络流量也会重导向到新的实例。

主网络接口

每个实例都有一个默认网络接口，称为主网络接口。您无法从实例断开主网络接口。您可以创建并附加额外的网络接口。您可以使用的网络接口的数量上限因实例类型而不同。有关更多信息，请参阅每种实例类型的每个网络接口的 IP 地址数 (p. 1107)。

网络接口的公有 IPv4 地址

在 VPC 中，所有子网都有一个可以修改的属性，该属性可以确定在子网中创建的网络接口 (以及在该子网中启动的实例) 是否会分配到一个公有 IPv4 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的子网的 IP 寻址行为。公有 IPv4 地址从 Amazon 的公有 IPv4 地址池分配。在启动实例时，将为创建的主网络接口分配 IP 地址。

当您创建一个网络接口时，它会继承子网的公有 IPv4 寻址属性。如果您日后修改了子网的公有 IPv4 寻址属性，网络接口仍会继续使用在其创建时生效的设置。如果启动一个实例并将现有的网络接口指定为主网络接口，则公有 IPv4 地址属性是由该网络接口确定的。

有关更多信息，请参阅公有 IPv4 地址 (p. 1054)。

网络接口的弹性 IP 地址

如果您有弹性 IP 地址，则可将其与网络接口的某个私有 IPv4 地址相关联。您可以为每个私有 IPv4 地址关联一个弹性 IP 地址。

如果解除弹性 IP 地址与网络接口的关联，则可以将其释放回地址池。这是将弹性 IP 地址与其他子网或 VPC 中的实例关联的唯一方法，因为网络接口是特定于子网的。

网络接口的 IPv6 地址

如果您将 IPv6 CIDR 块与您的 VPC 和子网关联，则可以将子网范围内的一个或多个 IPv6 地址分配给一个网络接口。每个 IPv6 地址可以分配给一个网络接口。

所有子网都有一个可以修改的属性，该属性可以确定在子网中创建的网络接口 (以及在该子网中启动的实例) 是否会自动分配到一个处于子网范围内的 IPv6 地址。有关更多信息，请参阅 Amazon VPC 用户指南中的子网的 IP 寻址行为。在启动实例时，将为创建的主网络接口分配 IPv6 地址。

有关更多信息，请参阅IPv6 地址 (p. 1055)。

前缀委派

前缀委派指预留的私有 IPv4 或 IPv6 CIDR 范围，用于自动或手动分配给与实例关联的网络接口。通过使用委派前缀，您可以通过将一系列 IP 地址分配为单个前缀来更快启动服务。

终止操作

您可以设置附加到实例的网络接口的终止操作。您可以指定在终止网络接口附加到的实例时是否自动删除该接口。

源/目标检查

您可以启用或禁用源/目标检查，以确保实例是其接收的任何流量的源或目标。默认情况下会启用源/目标检查。如果实例运行网络地址转换、路由或防火墙等服务，您必须禁用源/目标检查。

监控 IP 流量

您可以在网络接口上启用 VPC 流日志以捕获有关出入该网络接口的 IP 流量的信息。创建流日志后，您可以在 Amazon CloudWatch Logs 中查看和检索其数据。有关更多信息，请参阅 Amazon VPC 用户指南 中的 VPC 流日志。

网卡

具有多个网卡的实例可提供更高的网络性能，包括 100 Gbps 以上的带宽能力和更高的数据包速率性能。每个网络接口都连接到一个网卡上。必须将主网络接口分配给网卡索引 0。

如果在启动支持多个网卡的实例时启用 Elastic Fabric Adapter (EFA)，则所有网卡都可用。您最多可以为每张网卡分配一个 EFA。一个 EFA 计为一个网络接口。

以下实例支持多个网卡。所有其他实例类型都支持一个网卡。

实例类型	网卡数
c6in.32xlarge	2
c6in.metal	2
dl1.24xlarge	4
hpc6id.32xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8

每种实例类型的每个网络接口的 IP 地址数

下表列出了每个实例类型的网络接口的最大数量，以及每个网络接口的私有 IPv4 地址和 IPv6 地址的最大数量。每个网络接口的 IPv6 地址与私有 IPv4 地址有不同的限制并且分别列出。并非所有实例类型都支持 IPv6 寻址。

主题

- 通用 (p. 1107)
- 计算优化 (p. 1113)
- 内存优化 (p. 1118)
- 存储优化 (p. 1125)
- 加速计算 (p. 1127)

通用

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
a1.medium	2	4	4
a1.large	3	10	10
a1.xlarge	4	15	15
a1.2xlarge	4	15	15
a1.4xlarge	8	30	30
a1.metal	8	30	30
m1.small	2	4	不支持 IPv6
m1.medium	2	6	不支持 IPv6
m1.large	3	10	不支持 IPv6
m1.xlarge	4	15	不支持 IPv6
m2.xlarge	4	15	不支持 IPv6
m2.2xlarge	4	30	不支持 IPv6
m2.4xlarge	8	30	不支持 IPv6
m3.medium	2	6	不支持 IPv6
m3.large	3	10	不支持 IPv6
m3.xlarge	4	15	不支持 IPv6
m3.2xlarge	4	30	不支持 IPv6
m4.large	2	10	10
m4.xlarge	4	15	15
m4.2xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
m4.4xlarge	8	30	30
m4.10xlarge	8	30	30
m4.16xlarge	8	30	30
m5.large	3	10	10
m5.xlarge	4	15	15
m5.2xlarge	4	15	15
m5.4xlarge	8	30	30
m5.8xlarge	8	30	30
m5.12xlarge	8	30	30
m5.16xlarge	15	50	50
m5.24xlarge	15	50	50
m5.metal	15	50	50
m5a.large	3	10	10
m5a.xlarge	4	15	15
m5a.2xlarge	4	15	15
m5a.4xlarge	8	30	30
m5a.8xlarge	8	30	30
m5a.12xlarge	8	30	30
m5a.16xlarge	15	50	50
m5a.24xlarge	15	50	50
m5ad.large	3	10	10
m5ad.xlarge	4	15	15
m5ad.2xlarge	4	15	15
m5ad.4xlarge	8	30	30
m5ad.8xlarge	8	30	30
m5ad.12xlarge	8	30	30
m5ad.16xlarge	15	50	50
m5ad.24xlarge	15	50	50
m5d.large	3	10	10
m5d.xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
m5d.2xlarge	4	15	15
m5d.4xlarge	8	30	30
m5d.8xlarge	8	30	30
m5d.12xlarge	8	30	30
m5d.16xlarge	15	50	50
m5d.24xlarge	15	50	50
m5d.metal	15	50	50
m5dn.large	3	10	10
m5dn.xlarge	4	15	15
m5dn.2xlarge	4	15	15
m5dn.4xlarge	8	30	30
m5dn.8xlarge	8	30	30
m5dn.12xlarge	8	30	30
m5dn.16xlarge	15	50	50
m5dn.24xlarge	15	50	50
m5dn.metal	15	50	50
m5n.large	3	10	10
m5n.xlarge	4	15	15
m5n.2xlarge	4	15	15
m5n.4xlarge	8	30	30
m5n.8xlarge	8	30	30
m5n.12xlarge	8	30	30
m5n.16xlarge	15	50	50
m5n.24xlarge	15	50	50
m5n.metal	15	50	50
m5zn.large	3	10	10
m5zn.xlarge	4	15	15
m5zn.2xlarge	4	15	15
m5zn.3xlarge	8	30	30
m5zn.6xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
m5zn.12xlarge	15	50	50
m5zn.metal	15	50	50
m6a.large	3	10	10
m6a.xlarge	4	15	15
m6a.2xlarge	4	15	15
m6a.4xlarge	8	30	30
m6a.8xlarge	8	30	30
m6a.12xlarge	8	30	30
m6a.16xlarge	15	50	50
m6a.24xlarge	15	50	50
m6a.32xlarge	15	50	50
m6a.48xlarge	15	50	50
m6a.metal	15	50	50
m6g.medium	2	4	4
m6g.large	3	10	10
m6g.xlarge	4	15	15
m6g.2xlarge	4	15	15
m6g.4xlarge	8	30	30
m6g.8xlarge	8	30	30
m6g.12xlarge	8	30	30
m6g.16xlarge	15	50	50
m6g.metal	15	50	50
m6gd.medium	2	4	4
m6gd.large	3	10	10
m6gd.xlarge	4	15	15
m6gd.2xlarge	4	15	15
m6gd.4xlarge	8	30	30
m6gd.8xlarge	8	30	30
m6gd.12xlarge	8	30	30
m6gd.16xlarge	15	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
m6gd.metal	15	50	50
m6i.large	3	10	10
m6i.xlarge	4	15	15
m6i.2xlarge	4	15	15
m6i.4xlarge	8	30	30
m6i.8xlarge	8	30	30
m6i.12xlarge	8	30	30
m6i.16xlarge	15	50	50
m6i.24xlarge	15	50	50
m6i.32xlarge	15	50	50
m6i.metal	15	50	50
m6id.large	3	10	10
m6id.xlarge	4	15	15
m6id.2xlarge	4	15	15
m6id.4xlarge	8	30	30
m6id.8xlarge	8	30	30
m6id.12xlarge	8	30	30
m6id.16xlarge	15	50	50
m6id.24xlarge	15	50	50
m6id.32xlarge	15	50	50
m6id.metal	15	50	50
m6idn.large	3	10	10
m6idn.xlarge	4	15	15
m6idn.2xlarge	4	15	15
m6idn.4xlarge	8	30	30
m6idn.8xlarge	8	30	30
m6idn.12xlarge	8	30	30
m6idn.16xlarge	15	50	50
m6idn.24xlarge	15	50	50
m6idn.32xlarge	14	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
m6idn.metal	14	50	50
m6in.large	3	10	10
m6in.xlarge	4	15	15
m6in.2xlarge	4	15	15
m6in.4xlarge	8	30	30
m6in.8xlarge	8	30	30
m6in.12xlarge	8	30	30
m6in.16xlarge	15	50	50
m6in.24xlarge	15	50	50
m6in.32xlarge	14	50	50
m6in.metal	14	50	50
m7g.medium	2	4	4
m7g.large	3	10	10
m7g.xlarge	4	15	15
m7g.2xlarge	4	15	15
m7g.4xlarge	8	30	30
m7g.8xlarge	8	30	30
m7g.12xlarge	8	30	30
m7g.16xlarge	15	50	50
m7g.metal	15	50	50
mac1.metal	8	30	30
mac2.metal	8	30	30
t1.micro	2	2	不支持 IPv6
t2.nano	2	2	2
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
t2.large	3	12	12
t2.xlarge	3	15	15
t2.2xlarge	3	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
t3.nano	2	2	2
t3.micro	2	2	2
t3.small	3	4	4
t3.medium	3	6	6
t3.large	3	12	12
t3.xlarge	4	15	15
t3.2xlarge	4	15	15
t3a.nano	2	2	2
t3a.micro	2	2	2
t3a.small	2	4	4
t3a.medium	3	6	6
t3a.large	3	12	12
t3a.xlarge	4	15	15
t3a.2xlarge	4	15	15
t4g.nano	2	2	2
t4g.micro	2	2	2
t4g.small	3	4	4
t4g.medium	3	6	6
t4g.large	3	12	12
t4g.xlarge	4	15	15
t4g.2xlarge	4	15	15

计算优化

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c1.medium	2	6	不支持 IPv6
c1.xlarge	4	15	不支持 IPv6
c3.large	3	10	10
c3.xlarge	4	15	15
c3.2xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c3.4xlarge	8	30	30
c3.8xlarge	8	30	30
c4.large	3	10	10
c4.xlarge	4	15	15
c4.2xlarge	4	15	15
c4.4xlarge	8	30	30
c4.8xlarge	8	30	30
c5.large	3	10	10
c5.xlarge	4	15	15
c5.2xlarge	4	15	15
c5.4xlarge	8	30	30
c5.9xlarge	8	30	30
c5.12xlarge	8	30	30
c5.18xlarge	15	50	50
c5.24xlarge	15	50	50
c5.metal	15	50	50
c5a.large	3	10	10
c5a.xlarge	4	15	15
c5a.2xlarge	4	15	15
c5a.4xlarge	8	30	30
c5a.8xlarge	8	30	30
c5a.12xlarge	8	30	30
c5a.16xlarge	15	50	50
c5a.24xlarge	15	50	50
c5ad.large	3	10	10
c5ad.xlarge	4	15	15
c5ad.2xlarge	4	15	15
c5ad.4xlarge	8	30	30
c5ad.8xlarge	8	30	30
c5ad.12xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c5ad.16xlarge	15	50	50
c5ad.24xlarge	15	50	50
c5d.large	3	10	10
c5d.xlarge	4	15	15
c5d.2xlarge	4	15	15
c5d.4xlarge	8	30	30
c5d.9xlarge	8	30	30
c5d.12xlarge	8	30	30
c5d.18xlarge	15	50	50
c5d.24xlarge	15	50	50
c5d.metal	15	50	50
c5n.large	3	10	10
c5n.xlarge	4	15	15
c5n.2xlarge	4	15	15
c5n.4xlarge	8	30	30
c5n.9xlarge	8	30	30
c5n.18xlarge	15	50	50
c5n.metal	15	50	50
c6a.large	3	10	10
c6a.xlarge	4	15	15
c6a.2xlarge	4	15	15
c6a.4xlarge	8	30	30
c6a.8xlarge	8	30	30
c6a.12xlarge	8	30	30
c6a.16xlarge	15	50	50
c6a.24xlarge	15	50	50
c6a.32xlarge	15	50	50
c6a.48xlarge	15	50	50
c6a.metal	15	50	50
c6g.medium	2	4	4

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c6g.large	3	10	10
c6g.xlarge	4	15	15
c6g.2xlarge	4	15	15
c6g.4xlarge	8	30	30
c6g.8xlarge	8	30	30
c6g.12xlarge	8	30	30
c6g.16xlarge	15	50	50
c6g.metal	15	50	50
c6gd.medium	2	4	4
c6gd.large	3	10	10
c6gd.xlarge	4	15	15
c6gd.2xlarge	4	15	15
c6gd.4xlarge	8	30	30
c6gd.8xlarge	8	30	30
c6gd.12xlarge	8	30	30
c6gd.16xlarge	15	50	50
c6gd.metal	15	50	50
c6gn.medium	2	4	4
c6gn.large	3	10	10
c6gn.xlarge	4	15	15
c6gn.2xlarge	4	15	15
c6gn.4xlarge	8	30	30
c6gn.8xlarge	8	30	30
c6gn.12xlarge	8	30	30
c6gn.16xlarge	15	50	50
c6i.large	3	10	10
c6i.xlarge	4	15	15
c6i.2xlarge	4	15	15
c6i.4xlarge	8	30	30
c6i.8xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c6i.12xlarge	8	30	30
c6i.16xlarge	15	50	50
c6i.24xlarge	15	50	50
c6i.32xlarge	15	50	50
c6i.metal	15	50	50
c6id.large	3	10	10
c6id.xlarge	4	15	15
c6id.2xlarge	4	15	15
c6id.4xlarge	8	30	30
c6id.8xlarge	8	30	30
c6id.12xlarge	8	30	30
c6id.16xlarge	15	50	50
c6id.24xlarge	15	50	50
c6id.32xlarge	15	50	50
c6id.metal	15	50	50
c6in.large	3	10	10
c6in.xlarge	4	15	15
c6in.2xlarge	4	15	15
c6in.4xlarge	8	30	30
c6in.8xlarge	8	30	30
c6in.12xlarge	8	30	30
c6in.16xlarge	15	50	50
c6in.24xlarge	15	50	50
c6in.32xlarge	14	50	50
c6in.metal	14	50	50
c7g.medium	2	4	4
c7g.large	3	10	10
c7g.xlarge	4	15	15
c7g.2xlarge	4	15	15
c7g.4xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
c7g.8xlarge	8	30	30
c7g.12xlarge	8	30	30
c7g.16xlarge	15	50	50
c7g.metal	15	50	50
cc2.8xlarge	8	30	不支持 IPv6
hpc6a.48xlarge	2	50	50

内存优化

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
cr1.8xlarge	8	30	不支持 IPv6
hpc6id.32xlarge	2	50	50
r3.large	3	10	10
r3.xlarge	4	15	15
r3.2xlarge	4	15	15
r3.4xlarge	8	30	30
r3.8xlarge	8	30	30
r4.large	3	10	10
r4.xlarge	4	15	15
r4.2xlarge	4	15	15
r4.4xlarge	8	30	30
r4.8xlarge	8	30	30
r4.16xlarge	15	50	50
r5.large	3	10	10
r5.xlarge	4	15	15
r5.2xlarge	4	15	15
r5.4xlarge	8	30	30
r5.8xlarge	8	30	30
r5.12xlarge	8	30	30
r5.16xlarge	15	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
r5.24xlarge	15	50	50
r5.metal	15	50	50
r5a.large	3	10	10
r5a.xlarge	4	15	15
r5a.2xlarge	4	15	15
r5a.4xlarge	8	30	30
r5a.8xlarge	8	30	30
r5a.12xlarge	8	30	30
r5a.16xlarge	15	50	50
r5a.24xlarge	15	50	50
r5ad.large	3	10	10
r5ad.xlarge	4	15	15
r5ad.2xlarge	4	15	15
r5ad.4xlarge	8	30	30
r5ad.8xlarge	8	30	30
r5ad.12xlarge	8	30	30
r5ad.16xlarge	15	50	50
r5ad.24xlarge	15	50	50
r5b.large	3	10	10
r5b.xlarge	4	15	15
r5b.2xlarge	4	15	15
r5b.4xlarge	8	30	30
r5b.8xlarge	8	30	30
r5b.12xlarge	8	30	30
r5b.16xlarge	15	50	50
r5b.24xlarge	15	50	50
r5b.metal	15	50	50
r5d.large	3	10	10
r5d.xlarge	4	15	15
r5d.2xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
r5d.4xlarge	8	30	30
r5d.8xlarge	8	30	30
r5d.12xlarge	8	30	30
r5d.16xlarge	15	50	50
r5d.24xlarge	15	50	50
r5d.metal	15	50	50
r5dn.large	3	10	10
r5dn.xlarge	4	15	15
r5dn.2xlarge	4	15	15
r5dn.4xlarge	8	30	30
r5dn.8xlarge	8	30	30
r5dn.12xlarge	8	30	30
r5dn.16xlarge	15	50	50
r5dn.24xlarge	15	50	50
r5dn.metal	15	50	50
r5n.large	3	10	10
r5n.xlarge	4	15	15
r5n.2xlarge	4	15	15
r5n.4xlarge	8	30	30
r5n.8xlarge	8	30	30
r5n.12xlarge	8	30	30
r5n.16xlarge	15	50	50
r5n.24xlarge	15	50	50
r5n.metal	15	50	50
r6a.large	3	10	10
r6a.xlarge	4	15	15
r6a.2xlarge	4	15	15
r6a.4xlarge	8	30	30
r6a.8xlarge	8	30	30
r6a.12xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
r6a.16xlarge	15	50	50
r6a.24xlarge	15	50	50
r6a.32xlarge	15	50	50
r6a.48xlarge	15	50	50
r6a.metal	15	50	50
r6g.medium	2	4	4
r6g.large	3	10	10
r6g.xlarge	4	15	15
r6g.2xlarge	4	15	15
r6g.4xlarge	8	30	30
r6g.8xlarge	8	30	30
r6g.12xlarge	8	30	30
r6g.16xlarge	15	50	50
r6g.metal	15	50	50
r6gd.medium	2	4	4
r6gd.large	3	10	10
r6gd.xlarge	4	15	15
r6gd.2xlarge	4	15	15
r6gd.4xlarge	8	30	30
r6gd.8xlarge	8	30	30
r6gd.12xlarge	8	30	30
r6gd.16xlarge	15	50	50
r6gd.metal	15	50	50
r6i.large	3	10	10
r6i.xlarge	4	15	15
r6i.2xlarge	4	15	15
r6i.4xlarge	8	30	30
r6i.8xlarge	8	30	30
r6i.12xlarge	8	30	30
r6i.16xlarge	15	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
r6i.24xlarge	15	50	50
r6i.32xlarge	15	50	50
r6i.metal	15	50	50
r6idn.large	3	10	10
r6idn.xlarge	4	15	15
r6idn.2xlarge	4	15	15
r6idn.4xlarge	8	30	30
r6idn.8xlarge	8	30	30
r6idn.12xlarge	8	30	30
r6idn.16xlarge	15	50	50
r6idn.24xlarge	15	50	50
r6idn.32xlarge	14	50	50
r6idn.metal	14	50	50
r6in.large	3	10	10
r6in.xlarge	4	15	15
r6in.2xlarge	4	15	15
r6in.4xlarge	8	30	30
r6in.8xlarge	8	30	30
r6in.12xlarge	8	30	30
r6in.16xlarge	15	50	50
r6in.24xlarge	15	50	50
r6in.32xlarge	14	50	50
r6in.metal	14	50	50
r6id.large	3	10	10
r6id.xlarge	4	15	15
r6id.2xlarge	4	15	15
r6id.4xlarge	8	30	30
r6id.8xlarge	8	30	30
r6id.12xlarge	8	30	30
r6id.16xlarge	15	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
r6id.24xlarge	15	50	50
r6id.32xlarge	15	50	50
r6id.metal	15	50	50
r7g.medium	2	4	4
r7g.large	3	10	10
r7g.xlarge	4	15	15
r7g.2xlarge	4	15	15
r7g.4xlarge	8	30	30
r7g.8xlarge	8	30	30
r7g.12xlarge	8	30	30
r7g.16xlarge	15	50	50
r7g.metal	15	50	50
u-3tb1.56xlarge	8	30	30
u-6tb1.56xlarge	15	50	50
u-6tb1.112xlarge	15	50	50
u-6tb1.metal	5	30	30
u-9tb1.112xlarge	15	50	50
u-9tb1.metal	5	30	30
u-12tb1.112xlarge	15	50	50
u-12tb1.metal	5	30	30
u-18tb1.metal	15	50	50
u-24tb1.metal	15	50	50
x1.16xlarge	8	30	30
x1.32xlarge	8	30	30
x2gd.medium	2	4	4
x2gd.large	3	10	10
x2gd.xlarge	4	15	15
x2gd.2xlarge	4	15	15
x2gd.4xlarge	8	30	30
x2gd.8xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
x2gd.12xlarge	8	30	30
x2gd.16xlarge	15	50	50
x2gd.metal	15	50	50
x2idn.16xlarge	15	50	50
x2idn.24xlarge	15	50	50
x2idn.32xlarge	15	50	50
x2idn.metal	15	50	50
x2iedn.xlarge	4	15	15
x2iedn.2xlarge	4	15	15
x2iedn.4xlarge	8	30	30
x2iedn.8xlarge	8	30	30
x2iedn.16xlarge	15	50	50
x2iedn.24xlarge	15	50	50
x2iedn.32xlarge	15	50	50
x2iedn.metal	15	50	50
x2iezn.2xlarge	4	15	15
x2iezn.4xlarge	8	30	30
x2iezn.6xlarge	8	30	30
x2iezn.8xlarge	8	30	30
x2iezn.12xlarge	15	50	50
x2iezn.metal	15	50	50
x1e.xlarge	3	10	10
x1e.2xlarge	4	15	15
x1e.4xlarge	4	15	15
x1e.8xlarge	4	15	15
x1e.16xlarge	8	30	30
x1e.32xlarge	8	30	30
z1d.large	3	10	10
z1d.xlarge	4	15	15
z1d.2xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
z1d.3xlarge	8	30	30
z1d.6xlarge	8	30	30
z1d.12xlarge	15	50	50
z1d.metal	15	50	50

存储优化

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
d2.xlarge	4	15	15
d2.2xlarge	4	15	15
d2.4xlarge	8	30	30
d2.8xlarge	8	30	30
d3.xlarge	4	3	3
d3.2xlarge	4	5	5
d3.4xlarge	4	10	10
d3.8xlarge	3	20	20
d3en.xlarge	4	3	3
d3en.2xlarge	4	5	5
d3en.4xlarge	4	10	10
d3en.6xlarge	4	15	15
d3en.8xlarge	4	20	20
d3en.12xlarge	3	30	30
h1.2xlarge	4	15	15
h1.4xlarge	8	30	30
h1.8xlarge	8	30	30
h1.16xlarge	15	50	50
hs1.8xlarge	8	30	不支持 IPv6
i2.xlarge	4	15	15
i2.2xlarge	4	15	15
i2.4xlarge	8	30	30

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
i2.8xlarge	8	30	30
i3.large	3	10	10
i3.xlarge	4	15	15
i3.2xlarge	4	15	15
i3.4xlarge	8	30	30
i3.8xlarge	8	30	30
i3.16xlarge	15	50	50
i3.metal	15	50	50
i3en.large	3	10	10
i3en.xlarge	4	15	15
i3en.2xlarge	4	15	15
i3en.3xlarge	4	15	15
i3en.6xlarge	8	30	30
i3en.12xlarge	8	30	30
i3en.24xlarge	15	50	50
i3en.metal	15	50	50
i4i.large	3	10	10
i4i.xlarge	4	15	15
i4i.2xlarge	4	15	15
i4i.4xlarge	8	30	30
i4i.8xlarge	8	30	30
i4i.16xlarge	15	50	50
i4i.32xlarge	15	50	50
i4i.metal	15	50	50
im4gn.large	3	10	10
im4gn.xlarge	4	15	15
im4gn.2xlarge	4	15	15
im4gn.4xlarge	8	30	30
im4gn.8xlarge	8	30	30
im4gn.16xlarge	15	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
is4gen.medium	2	4	4
is4gen.large	3	10	10
is4gen.xlarge	4	15	15
is4gen.2xlarge	4	15	15
is4gen.4xlarge	8	30	30
is4gen.8xlarge	8	30	30

加速计算

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
dl1.24xlarge	60	50	50
f1.2xlarge	4	15	15
f1.4xlarge	8	30	30
f1.16xlarge	8	50	50
g2.2xlarge	4	15	不支持 IPv6
g2.8xlarge	8	30	不支持 IPv6
g3.4xlarge	8	30	30
g3.8xlarge	8	30	30
g3.16xlarge	15	50	50
g4ad.xlarge	2	4	4
g4ad.2xlarge	2	4	4
g4ad.4xlarge	3	10	10
g4ad.8xlarge	4	15	15
g4ad.16xlarge	8	30	30
g4dn.xlarge	3	10	10
g4dn.2xlarge	3	10	10
g4dn.4xlarge	3	10	10
g4dn.8xlarge	4	15	15
g4dn.12xlarge	8	30	30
g4dn.16xlarge	4	15	15

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
g4dn.metal	15	50	50
g5.xlarge	4	15	15
g5.2xlarge	4	15	15
g5.4xlarge	8	30	30
g5.8xlarge	8	30	30
g5.12xlarge	15	50	50
g5.16xlarge	8	30	30
g5.24xlarge	15	50	50
g5.48xlarge	7	50	50
g5g.xlarge	4	15	15
g5g.2xlarge	4	15	15
g5g.4xlarge	8	30	30
g5g.8xlarge	8	30	30
g5g.16xlarge	15	50	50
g5g.metal	15	50	50
inf1.xlarge	4	10	10
inf1.2xlarge	4	10	10
inf1.6xlarge	8	30	30
inf1.24xlarge	11	30	30
p2.xlarge	4	15	15
p2.8xlarge	8	30	30
p2.16xlarge	8	30	30
p3.2xlarge	4	15	15
p3.8xlarge	8	30	30
p3.16xlarge	8	30	30
p3dn.24xlarge	15	50	50
p4d.24xlarge	60	50	50
p4de.24xlarge	60	50	50
trn1.2xlarge	4	15	15
trn1.32xlarge	40	50	50

实例类型	最大网络接口数	每个接口的私有 IPv4 地址数	每个接口的 IPv6 地址数
vt1.3xlarge	4	15	15
vt1.6xlarge	8	30	30
vt1.24xlarge	15	50	50

您可以使用 describe-instance-types Amazon CLI 命令来显示有关实例类型的信息，例如支持的网络接口和每个接口的 IP 地址。以下示例显示了所有 C5 实例的此类信息。

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query
 "InstanceTypes[].{Type: InstanceType, MaxENI: NetworkInfo.MaximumNetworkInterfaces,
 IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" --output table
-------------------------------------
|        DescribeInstanceTypes        |
+----------+----------+---------------+
| IPv4addr | MaxENI   |     Type      |
+----------+----------+---------------+
|  30      |  8       |  c5.4xlarge   |
|  50      |  15      |  c5.24xlarge  |
|  15      |  4       |  c5.xlarge    |
|  30      |  8       |  c5.12xlarge  |
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

使用网络接口

您可以通过 Amazon EC2 控制台或命令行使用网络接口。

目录

- 创建网络接口 (p. 1129)
- 查看有关网络接口的详细信息 (p. 1130)
- 将网络接口连接至实例 (p. 1131)
- 将网络接口与实例分离 (p. 1132)
- 管理 IP 地址 (p. 1133)
- 修改网络接口属性 (p. 1134)
- 添加或编辑标签 (p. 1135)
- 删除网络接口 (p. 1136)

创建网络接口

您可以在子网中创建一个网络接口。您不能在创建网络接口之后将其移动至另一子网。您必须将网络接口连接到同一可用区中的实例。

New console

使用控制台创建网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择创建网络接口。
4. （可选）对于描述，请输入一个描述性的名称。
5. 对于 Subnet (子网)，选择一个子网。后续步骤中可用的选项根据您选择的子网类型（仅 IPv4、仅 IPv6 或双堆栈（IPv4 和 IPv6））而有所变化。
6. 对于私有 IPv4 地址，执行以下操作之一：
   - 选择自动分配允许 Amazon EC2 从子网中选择 IPv4 地址。
   - 选择自定义然后输入从子网中选择的 IPv4 地址。
7. （仅具有 IPv6 地址的子网）对于 IPv6 地址，请执行以下操作之一：
   - 如果您不想为网络接口分配 IPv6 地址，选择没有。
   - 选择自动分配允许 Amazon EC2 从子网中选择 IPv6 地址。
   - 选择自定义然后输入从子网中选择的 IPv6 地址。
8. （可选）要创建 Elastic Fabric Adapter，请选择 Elastic Fabric Adapter，启用。
9. 对于 Security groups，选择一个或多个安全组。
10. （可选）对于每个标签，请选择添加新标签，然后输入标签键和可选的标签值。
11. 选择创建网络接口。

Old console

使用控制台创建网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择 Create Network Interface。
4. 对于 Description，输入一个描述性名称。
5. 对于 Subnet，选择子网。
6. 对于私有 IP (或 IPv4 私有 IP)，请输入主要私有 IPv4 地址。如果您未指定 IPv4 地址，我们将在所选子网中选择一个可用的私有 IPv4 地址。
7. (仅限 IPv6) 如果您选择了一个拥有相关联的 IPv6 CIDR 块的子网，那么可以选择性地在 IPv6 IP 字段中指定一个 IPv6 地址。
8. 要创建 Elastic Fabric Adapter，请选择 Elastic Fabric Adapter。
9. 对于 Security groups，选择一个或多个安全组。
10. （可选）选择添加标签，然后输入标签键和标签值。
11. 选择 Yes, Create。

使用命令行创建网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-network-interface (Amazon CLI)
- New-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

查看有关网络接口的详细信息

您可以查看您账户中的所有网络接口。

New console

使用控制台描述网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 要查看网络接口的详细信息页面，请选择该网络接口的 ID。或者，要在不离开网络接口页面的情况下查看信息，请选中该网络接口的复选框。

Old console

使用控制台描述网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择网络接口。
4. 要查看详细信息，请选择详细信息。

使用命令行描述网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-network-interfaces (Amazon CLI)
- Get-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

使用命令行描述网络接口属性

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-network-interface-attribute (Amazon CLI)
- Get-EC2NetworkInterfaceAttribute (Amazon Tools for Windows PowerShell)

将网络接口连接至实例

您可以使用 Amazon EC2 控制台的 Instances (实例) 或 Network Interfaces (网络接口) 页面，将网络接口连接至相同可用区中的任何实例。或者，您可以在启动实例 (p. 575)时指定现有的网络接口。

Important

对于仅 IPv6 子网中的 EC2 实例，如果您将辅助网络接口附加到该实例，则第二个网络接口的私有 DNS 主机名将解析为实例第一个网络接口上的第一个 IPv6 地址。有关 EC2 实例私有 DNS 主机名的更多信息，请参阅 Amazon EC2 实例主机名类型 (p. 1067)。

如果您的实例上的公有 IPv4 地址已释放，并且有多个网络接口附加到实例，那么该实例不会收到新地址。有关公有 IPv4 地址行为的更多信息，请参阅公有 IPv4 地址 (p. 1054)。

Instances page

使用 Instances（实例）页面将网络接口附加到实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选中该实例的复选框。

4. 依次选择操作、联网、附加网络接口。
5. 选择网络接口。如果实例支持多个网卡，则可以选择网卡。
6. 选择 Attach。

Network Interfaces page

使用 Network Interfaces（网络接口）页面将网络接口附加到实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 依次选择操作、附加。
5. 选择一个实例。如果实例支持多个网卡，则可以选择网卡。
6. 选择 Attach。

使用命令行将网络接口附加到实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- attach-network-interface (Amazon CLI)
- Add-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

将网络接口与实例分离

您可以随时使用 Amazon EC2 控制台的 Instances (实例) 或 Network Interfaces (网络接口) 页面，分离附加到 EC2 实例的辅助网络接口。

如果试图将连接至资源的网络接口从另一个服务（如 Elastic Load Balancing 负载均衡器、Lambda 函数、WorkSpace 或 NAT 网关）中分离，您将收到错误消息，提示您无权访问资源。要查找哪个服务创建了连接到网络接口的资源，请检查网络接口的说明。如果删除资源，则其网络接口将被删除。

Instances page

使用实例页面将网络接口与实例分离

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选中该实例的复选框。检查联网选项卡的网络接口部分，以验证网络接口是否作为辅助网络接口附加到实例。
4. 依次选择操作、联网、分离网络接口。
5. 选择网络接口，然后选择分离。

Network Interfaces page

使用网络接口页面将网络接口与实例分离

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。检查详细信息选项卡的实例详细信息部分，以验证网络接口是否作为辅助网络接口附加到实例。

4. 依次选择操作、分离。
5. 当系统提示进行确认时，选择分离。
6. 如果网络接口未能与实例分离，请选择强制分离、启用，然后重试。我们建议仅将强制分离用作最后手段。强制分离可以防止您在重新启动实例之前在同一索引上附加不同的网络接口。它还可以防止实例元数据反映网络接口在您重新启动实例已分离。

使用命令行分离网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- detach-network-interface (Amazon CLI)
- Dismount-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

管理 IP 地址

您可以管理网络接口的以下 IP 地址：

- 弹性 IP 地址（每个私有 IPv4 地址一个）
- IPv4 地址
- IPv6 地址

使用控制台管理网络接口的弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 要关联弹性 IP 地址，请执行以下操作：
   a. 依次选择操作、关联地址。
   b. 对于弹性 IP 地址，选择弹性 IP 地址。
   c. 对于私有 IPv4 地址，选择要与弹性 IP 地址关联的私有 IPv4 地址。
   d. （可选）如果网络接口当前已与其他实例或网络接口关联，选择允许重新关联弹性 IP 地址。
   e. 选择 Associate。
5. 要取消关联弹性 IP 地址，请执行以下操作：
   a. 选择 Actions、Disassociate address。
   b. 对于公有 IP 地址，选择弹性 IP 地址。
   c. 选择取消关联。

使用控制台管理网络接口的 IPv4 和 IPv6 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择网络接口。
4. 依次选择操作、管理 IP 地址。
5. 展开网络接口。
6. 对于 IPv4 地址，根据需要修改 IP 地址。要分配 IPv4 地址，请选择分配新 IP 地址，然后从子网范围内指定一个 IPv4 地址，或者让 Amazon 为您选择一个。要取消分配 IPv4 地址，请选择该地址旁边的取消分配。

7. 对于 IPv6 地址，根据需要修改 IP 地址。要分配 IPv6 地址，请选择分配新 IP 地址，然后从子网范围内指定一个 IPv6 地址，或者让 Amazon 为您选择一个。要取消分配 IPv6 地址，请选择该地址旁边的取消分配。
8. 选择 Save。

使用 Amazon CLI 管理网络接口的 IP 地址

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- assign-ipv6-addresses
- associate-address
- disassociate-address
- unassign-ipv6-addresses

使用 Tools for Windows PowerShell 管理网络接口的 IP 地址

您可以使用以下任一命令。

- Register-EC2Address
- Register-EC2Ipv6AddressList
- Unregister-EC2Address
- Unregister-EC2Ipv6AddressList

修改网络接口属性

您可以更改以下网络接口属性：

- 描述 (p. 1134)
- 安全组 (p. 1134)
- 终止时删除 (p. 1135)
- 源/目标检查 (p. 1135)

使用控制台更改网络接口的描述

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 依次选择操作、更改描述。
5. 对于描述，输入网络接口的描述。
6. 选择 Save。

使用控制台更改网络接口的安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 依次选择操作、更改安全组。

5. 对于关联的安全组，选择要使用的安全组，然后选择保存。

   安全组和网络接口必须针对相同 VPC 创建。要更改其他服务（如 Elastic Load Balancing）所拥有的接口的安全组，请通过该服务进行更改。

使用控制台更改网络接口的终止操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 依次选择操作、更改终止行为。
5. 根据需要选择或清除终止时删除、启用，然后选择保存。

使用控制台更改网络接口的源/目标检查

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 依次选择操作、更改源/目标检查。
5. 根据需要选择或清除源/目标检查、启用，然后选择保存。

使用命令行修改网络接口属性

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- modify-network-interface-attribute (Amazon CLI)
- Edit-EC2NetworkInterfaceAttribute (Amazon Tools for Windows PowerShell)

添加或编辑标签

标签是您可以添加到网络接口的元数据。标签是私有的，只有您的账户可见。每一个标签都包含一个键和一个可选值。有关标签的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

New console

使用控制台编辑或添加网络接口的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中该网络接口的复选框。
4. 在标签选项卡上，选择管理标签。
5. 对于要创建的每个标签，请选择添加新标签然后输入键和可选值。完成此操作后，选择 Save。

Old console

使用控制台编辑或添加网络接口的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择网络接口。
4. 在详细信息窗格中，选择 Tags、Add/Edit Tags。
5. 在 Add/Edit Tags 对话框中，对于每个要创建的标签选择 Create Tag，然后输入键和可选值。完成此操作后，选择 Save。

使用命令行添加或编辑网络接口的标签

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-tags（Amazon CLI）
- New-EC2Tag（Amazon Tools for Windows PowerShell）

删除网络接口

删除网络接口之后，所有与该接口关联的属性都会被释放，而且所有私有 IP 地址或弹性 IP 地址也都会被释放以供另一个实例使用。

您无法删除正在使用的网络接口。首先，您必须分离网络接口 (p. 1132)。

New console

使用控制台删除网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选中网络接口的复选框，然后依次选择操作、删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

Old console

使用控制台删除网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 选择一个网络接口，然后选择删除。
4. 在 Delete Network Interface 对话框中，选择 Yes, Delete。

使用命令行删除网络接口

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- delete-network-interface (Amazon CLI)
- Remove-EC2NetworkInterface (Amazon Tools for Windows PowerShell)

配置网络接口的最佳实践

- 您可以在实例运行时 (热附加)、实例停止时 (暖附加) 或实例启动时 (冷附加) 将网络接口连接到实例。
- 您可以在实例运行时或停止时分离次要网络接口。不过，您无法分离主网络接口。

- 如果实例位于相同可用区和 VPC 但位于不同子网，您可以将网络接口从一个实例移动到另一个实例。
- 在使用 CLI、API 或开发工具包启动实例时，您可以指定主网络接口和额外的网络接口。
- 启动具有多个网络接口的 Amazon Linux 或 Windows Server 实例会自动在该实例的操作系统上配置接口、私有 IPv4 地址和路由表。
- 如果要通过暖附加或热附加方式连接一个额外的网络接口，您可能需要手动添加第二个接口、配置私有 IPv4 地址并相应修改路由表。运行 Amazon Linux 或 Windows Server 的实例会自动识别暖附加或热附加，并自行进行配置。
- 您无法通过将另一个网络接口附加到实例（例如一种网卡绑定配置）以增加或加倍双主机实例的网络带宽。
- 如果将来自同一子网的两个或多个网络接口连接到一个实例，可能会遇到非对称路由等联网问题。请尽可能在主网络接口上改用辅助私有 IPv4 地址。

使用 ec2-net-utils 为 Amazon Linux 配置网络接口

Amazon Linux AMI 可能包含由 Amazon 安装的其他脚本，它们称为 ec2-net-utils。这些脚本可以选择性地自动配置您的网络接口。这些脚本仅适用于 Amazon Linux。

使用以下命令可在 Amazon Linux 上安装该程序包 (如果尚未安装) 或对其进行更新 (如果已安装且存在可用的其他更新)：

```
$ yum install ec2-net-utils
```

以下组件属于 ec2-net-utils 的一部分；

udev 规则 (`/etc/udev/rules.d`)

在网络接口附加、分离或重新附加正在运行的实例时识别它们，并确保 hotplug 脚本运行 (`53-ec2-network-interfaces.rules`)。将 MAC 地址映射到设备名称 (生成 `75-persistent-net-generator.rules` 的 `70-persistent-net.rules`)。

hotplug 脚本

生成一个适用于 DHCP 的接口配置文件 (`/etc/sysconfig/network-scripts/ifcfg-ethN`)。并生成一个路由配置文件 (`/etc/sysconfig/network-scripts/route-ethN`)。

DHCP 脚本

每当网络接口收到一个新的 DHCP 租约时，此脚本会查询弹性 IP 地址的实例元数据。对于每个弹性 IP 地址，它会为路由策略数据库添加一个规则，确保来自该地址的出站流量使用正确的网络接口。它还会将每个私有 IP 地址作为辅助地址添加至网络接口。

ec2ifup ethN

扩展标准 ifup 的功能。在此脚本重写配置文件 `ifcfg-ethN` 和 `route-ethN` 之后，它将运行 ifup。

ec2ifdown ethN

扩展标准 ifdown 的功能。当此脚本从路由策略数据库中删除网络接口的任何规则后，它将运行 ifdown。

ec2ifscan

检查尚未配置的网络接口并对它们进行配置。

此脚本在初始版本的 ec2-net-utils 中不可用。

要列出任何由 ec2-net-utils 生成的配置文件，请使用以下命令：

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

要禁用自动化，您可以将 EC2SYNC=no 添加至相应的 ifcfg-ethN 文件。例如，您可以使用以下命令为 eth1 接口禁用自动化：

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

要彻底禁用自动化，可以使用以下命令删除该包：

```
$ yum remove ec2-net-utils
```

网络接口方案

当您想执行以下操作时，将多个网络接口附加到一个实例很有帮助：

- 创建管理网络。
- 在虚拟私有云（VPC）中使用网络和安全设备。
- 创建双主机实例，并在不同子网间分配工作负载/任务。
- 创建一个低预算的高可用性解决方案。

创建管理网络

此方案说明了如何在满足以下条件和设置的情况下，创建带有网络接口的管理网络（如下图所示）。

标准

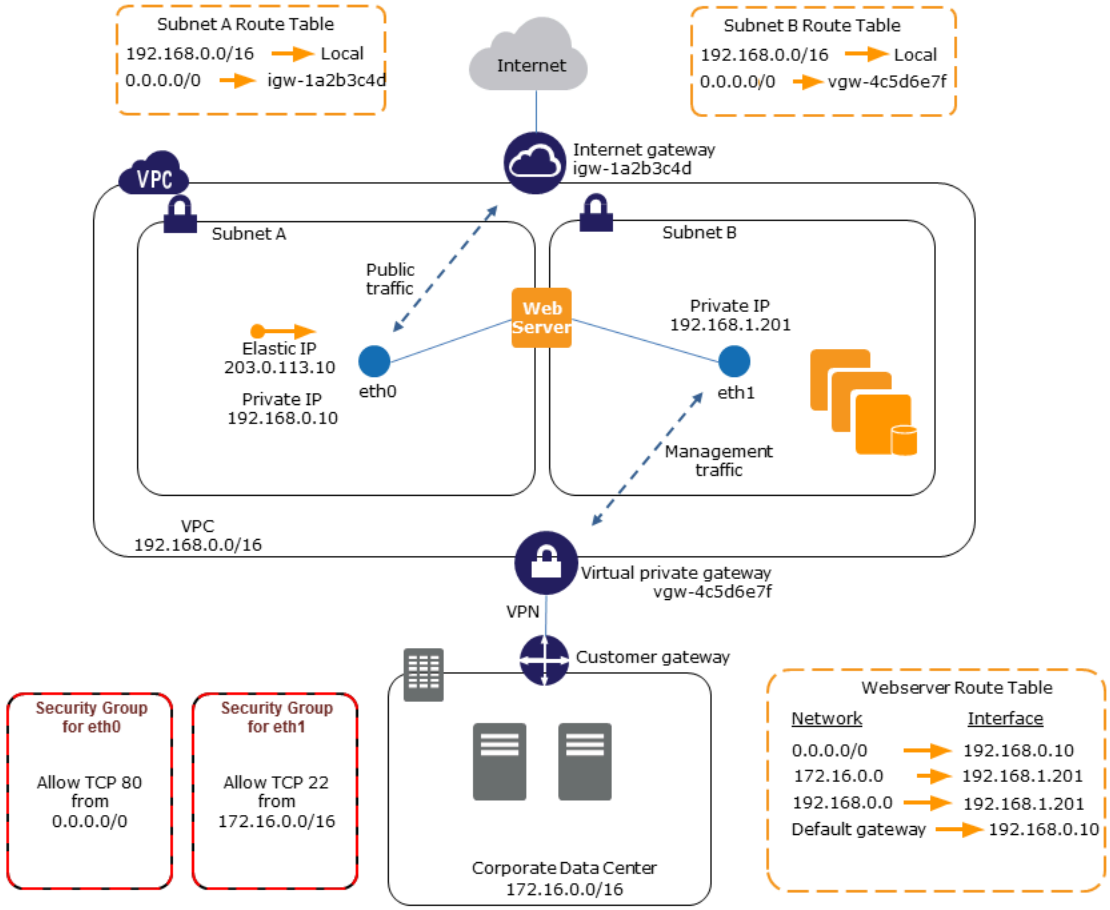
- 实例上的主网络接口（eth0）处理公有流量。
- 实例上的辅助网络接口（eth1）处理后端管理流量。它连接到具有更严格的访问控制的单独子网，并作为主网络接口位于可用区（AZ）内。

设置

- 主网络接口（可能配置或未配置负载均衡器）具有允许从 Internet 访问服务器的关联的安全组。例如，允许来自 0.0.0.0/0 或来自负载均衡器的 TCP 端口 80 和 443。
- 辅助网络接口具有一个关联的安全组，该安全组仅允许 SSH 访问，该安全组从以下位置之一启动：
  - 允许的 IP 地址范围，可以是 VPC 之内，也可以是来自互联网。
  - 与主网络接口位于同一可用区内的私有子网。
  - 虚拟私有网关。

  Note

  为确保故障转移功能，可以考虑针对网络接口上的传入流量使用辅助私有 IPv4。在某个实例失效时，您可以将接口和/或辅助私有 IPv4 地址移动到备用实例中。



在 VPC 中使用网络和安全设备

负载均衡器、网络地址转换 (NAT) 服务器和代理服务器等网络和安全设备更偏向于配置多个网络接口。您可以创建并附加辅助网络接口至正在运行这些类型的应用程序的实例中，并用实例自己的公用和私有 IP 地址、安全组和源/目标检查设置其他接口。

创建在不同子网上具有工作负载/角色的双主机实例

您可以将网络接口放置到每一个与承载应用程序服务器的中间层网络相连接的 Web 服务器。应用程序服务器也可以用双主机连接至承载数据库服务器的后端网络（子网）。每一个双主机实例都在前端接收和处理请求、启动与后端的连接，然后将请求发送至后端网络上的服务器，而不是通过双主机实例路由网络数据包。

创建低预算的高可用性解决方案

如果您的一个提供特定功能的实例失效，则其网络接口可附加到一个针对同一种角色预配置的替代或热备用实例，以快速恢复服务。例如，您可以将一个网络接口用作连接数据库实例或 NAT 实例等关键服务的主要或辅助网络接口。如果实例失效，您 (或更有可能是代表您运行的代码) 可以将网络接口附加到热备用实例。由于接口保持其私有 IP 地址、弹性 IP 地址和 MAC 地址，因此只要您将网络接口附加到替代实例，网络流量就会立即开始流向备用实例。在实例失效之后、网络接口附加到备用实例之前，用户会暂时失去连接，但不需要更改路由表或您的 DNS 服务器。

请求者托管的网络接口

请求者托管式网络接口是 Amazon Web Service 代表您在 VPC 中创建的网络接口。网络接口与其他服务的资源相关联，例如 Amazon RDS 的数据库实例、NAT 网关或 Amazon PrivateLink 的接口 VPC 终端节点。

注意事项

- 您可以查看自己账户中的请求者托管的网络接口。您可以添加或删除标签，但不能更改请求者托管式网络接口的其他属性。
- 您无法断开请求者托管式网络接口。
- 如果您删除与请求者托管式网络接口关联的资源，Amazon Web Service 会断开网络接口并将其删除。如果服务断开了网络接口但没有将其删除，您可以删除断开的网络接口。

使用控制台查看请求者托管的网络接口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Network & Security（网络与安全）、Network Interfaces（网络接口）。
3. 选择网络接口的 ID 以打开其详细信息页面。
4. 以下是可用于确定网络接口用途的关键字段：
   - Description（描述）：由创建接口的 Amazon 服务提供的描述。例如，“VPC Endpoint Interface vpce 089f2123488812123（VPC 终端节点接口 vpce 089f2123488812123）”。
   - Requester-managed（请求者托管式）：指明网络接口是否由 Amazon 托管。
   - Requester ID（请求者 ID）：创建网络接口的主体或服务的别名或 Amazon 账户 ID。如果您创建了网络接口，这便是您的 Amazon Web Services 账户 ID。如果没有，则由其他主体或服务创建。

使用 Amazon CLI 查看请求者托管式网络接口

按如下方式使用 describe-network-interfaces 命令。

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

以下示例输出显示了可用于确定网络接口用途的关键字段 Description 和 InterfaceType。

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

使用适用于 Windows PowerShell 的工具查看请求者托管式网络接口

按如下所示使用 Get-EC2NetworkInterface cmdlet。

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

以下示例输出显示了可用于确定网络接口用途的关键字段 Description 和 InterfaceType。

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType      : vpc_endpoint
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Amazon EC2 实例网络带宽

实例带宽规格适用于实例的入站和出站流量。例如，如果实例指定高达 10Gbps 的带宽，则意味着其具有高达 10Gbps 的入站流量带宽和 10Gbps 的出站流量带宽。EC2 实例可用的网络带宽取决于多个因素，如下所示。

多流流量

实例可用的聚合多流流量带宽取决于流量的目标。

- 在区域内 - 流量可以利用实例可用的全部网络带宽。
- 到其他区域、互联网网关、Direct Connect 或本地网关 (LGW) – 流量可以利用至少具有 32 个 vCPU 的 current generation instance (p. 239)（当前一代实例）可用网络带宽的高达 50%。具有少于 32 个 vCPU 的当前一代实例的带宽限制为 5 Gbps。

单流流量

如果实例不在同一个集群置放群组 (p. 1177)中，单流（5 元组）流量的基准带宽限制为 5 Gbps。要减少延迟并增加单流带宽，请尝试以下任一操作：

- 使用集群置放群组，使同一置放群组内的实例具有高达 10 Gbps 的带宽。
- 在任意两个端点之间设置多条路径，以通过多路径 TCP（MPTCP）实现更高带宽。
- 为同一子网内符合条件的实例配置 ENA Express，以在这些实例之间实现高达 25 Gbps 的带宽。

可用实例带宽

实例的可用网络带宽取决于其拥有的 vCPU 数量。例如，`m5.8xlarge` 实例有 32 个 vCPU 和 10 Gbps 的网络带宽，`m5.16xlarge` 实例有 64 个 vCPU 和 20 Gbps 的网络带宽。但是，如果实例超过实例级别的网络限额（例如每秒数据包或跟踪的连接数），则实例可能无法实现此带宽。流量可以利用多少可用带宽取决于 vCPU 的数量和目的地。例如，`m5.16xlarge` 实例具有 64 个 vCPU，因此到该区域中另一个实例的流量可以利用完整的可用带宽 (20 Gbps)。但是，到不同区域中另一个实例的流量只能利用 50% 的可用带宽 (10 Gbps)。

通常，有 16 个或更少 vCPU 的实例（大小为 `4xlarge` 或更小）被记录为具有“高达”的指定带宽；例如，“高达 10 Gbps”。这些实例具备基准带宽。为满足其他需求，可以使用网络 I/O 积分机制，以突增超出其基准带宽。实例可以在有限时间内使用突增带宽，通常为 5 到 60 分钟，具体取决于实例的大小。

实例在启动时接收最大数量的网络 I/O 积分。如果实例耗尽了其网络 I/O 积分，则返回至其基准带宽。正在运行的实例只要使用少于其基准带宽的网络带宽，就会获得网络 I/O 积分。已停止的实例不会获得网络 I/O 积分。即使实例有可用积分，实例突增也已尽了最大努力，因为突增带宽是一个共享资源。

基本和爆发网络性能

以下文档介绍了所有实例的网络性能，以及可以使用突增带宽的实例可用的基准网络带宽。

- 通用实例 (p. 260)
- 计算优化型实例 (p. 305)
- 内存优化型实例 (p. 322)
- 存储优化型实例 (p. 347)
- 加速计算实例 (p. 364)

使用 Amazon CLI 查看网络性能

您可以使用 describe-instance-types Amazon CLI 命令来显示有关实例类型的信息。以下示例显示了所有 C5 实例的网络性能信息。

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query
 "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance]" --output table
------------------------------------
|       DescribeInstanceTypes       |
+--------------+--------------------+
|  c5.4xlarge  |  Up to 10 Gigabit  |
|  c5.xlarge   |  Up to 10 Gigabit  |
|  c5.12xlarge |  12 Gigabit        |
|  c5.24xlarge |  25 Gigabit        |
|  c5.9xlarge  |  10 Gigabit        |
|  c5.2xlarge  |  Up to 10 Gigabit  |
|  c5.large    |  Up to 10 Gigabit  |
|  c5.metal    |  25 Gigabit        |
|  c5.18xlarge |  25 Gigabit        |
+--------------+--------------------+
```

监控实例带宽

您可以使用 CloudWatch 指标监控实例网络带宽以及发送和接收的数据包。您可以使用弹性网络适配器 (ENA) 驱动程序提供的网络性能指标来监控流量何时超过 Amazon EC2 在实例级别定义的网络限额。

您可以配置 Amazon EC2 是使用 1 分钟还是 5 分钟时段将实例的指标数据发送到 CloudWatch。网络性能指标可能会显示超出限额并丢弃数据包，而 CloudWatch 实例指标不会显示。当实例对网络资源的需求出现短暂峰值（称为微爆发），但 CloudWatch 指标的精细程度不足以反映这些微秒峰值时，就会发生这种情况。

了解更多信息

- 实例指标 (p. 1003)
- 网络性能指标 (p. 1164)

Linux 上的增强联网

增强联网使用单个根 I/O 虚拟化 (SR-IOV) 在支持的实例类型 (p. 1143)上提供高性能的联网功能。SR-IOV 是一种设备虚拟化方法，与传统虚拟化网络接口相比，它不仅能提高 I/O 性能，还能降低 CPU 使用率。增强联网可以提高带宽，提高每秒数据包数 (PPS) 性能，并不断降低实例间的延迟。使用增强联网不收取任何额外费用。

有关每个实例类型支持的网络速度的信息，请参阅 Amazon EC2 实例类型。

目录

- 增强联网支持 (p. 1143)
- 在实例上启用增强联网 (p. 1143)

- 在 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网 (p. 1143)
- 在 Linux 实例上使用 ENA Express 提高网络性能 (p. 1152)
- 在 Linux 实例上启用 Intel 82599 VF 接口增强联网。 (p. 1158)
- 操作系统优化 (p. 1164)
- 监控 EC2 实例的网络性能 (p. 1164)
- 对 Elastic Network Adapter (ENA) 进行问题排查 (p. 1169)

增强联网支持

除了 T2 实例外，所有当前一代 (p. 239)实例类型都支持增强联网。

您可以使用以下某种机制启用增强联网：

Elastic Network Adapter (ENA)

对于支持的实例类型，Elastic Network Adapter (ENA) 最多支持 100 Gbps 的网络速度。

除了小于 `m4.16xlarge` 的 C4、D2 和 M4 实例外，当前一代实例均使用 ENA 以实现增强联网。

Intel 82599 虚拟功能 (VF) 接口

对于受支持的实例类型，Intel 82599 虚拟功能接口最多支持 10 Gbps 的网络速度。

以下实例类型使用 Intel 82599 VF 接口来实现增强联网：C3、C4、D2、I2、M4（不包括 m4.16xlarge）和 R3。

有关按实例类型分列的增强联网机制的摘要，请参阅联网和存储功能摘要 (p. 247)。

在实例上启用增强联网

如果您的实例类型支持使用 Elastic Network Adapter 实现增强联网，请执行在 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网 (p. 1143)中的步骤。

如果您的实例类型支持使用 Intel 82599 VF 接口实现增强联网，请执行在 Linux 实例上启用 Intel 82599 VF 接口增强联网。 (p. 1158)中的步骤。

在 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网

Amazon EC2 通过 Elastic Network Adapter (ENA) 提供增强联网功能。要使用增强型联网，您必须安装所需的 ENA 模块并启用 ENA 支持。

目录

- 要求 (p. 1144)
- 增强联网性能 (p. 1144)
- 测试是否启用了增强联网功能 (p. 1144)
- 在 Amazon Linux AMI 上启用增强联网 (p. 1146)
- 在 Ubuntu 上启用增强联网 (p. 1147)
- 在 Linux 上启用增强联网 (p. 1148)
- 利用 DKMS 在 Ubuntu 上启用增强联网 (p. 1150)

- 驱动程序发行说明 (p. 1152)
- 问题排查 (p. 1152)

要求

要使用 ENA 准备增强联网，请按如下方式设置您的实例：

- 使用当前一代 (p. 239)实例类型启动实例，但小于 `m4.16xlarge` 的 C4、D2、M4 实例或 T2 除外。
- 使用支持的 Linux 内核版本及支持的发行版启动实例，以便为实例自动启用 ENA 增强联网。有关更多信息，请参阅 ENA Linux 内核驱动程序发行说明。
- 确保实例具有 Internet 连接。
- 使用 Amazon Web Services Management Console 的 Amazon CloudShell，或者将 Amazon CLI 或 Amazon Tools for Windows PowerShell 安装到您选择的任意电脑上（最好是本地台式机或笔记本电脑）并进行配置。有关的更多信息，请参阅 访问 Amazon EC2 (p. 3) 或 Amazon CloudShell 用户指南。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留，则应立即从您的实例创建 AMI，来备份这些数据。更新内核和内核模块以及启用 `enaSupport` 属性可能会导致实例不兼容或无法访问操作系统。如果您有最新备份，则发生此情况时仍将保留数据。

增强联网性能

以下文档汇总了支持 ENA 增强联网的实例类型的网络性能：

- 加速计算实例的网络性能 (p. 364)
- 计算优化型实例的网络性能 (p. 312)
- 通用型实例的网络性能 (p. 260)
- 内存优化型实例的网络性能 (p. 332)
- 存储优化型实例的网络性能 (p. 351)

测试是否启用了增强联网功能

以下 AMI 包含所需的 ENA 模块并启用了 ENA 支持：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

  Note

  Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

若要测试是否已启用了增强联网，请确认实例上已安装 `ena` 模块且设置了 `enaSupport` 属性。如果实例满足这两个条件，则 ethtool -i eth*n* 命令应显示该模块已在网络接口上使用。

内核模块 (ena)

要确认已安装 ena 模块，请使用 modinfo 命令，如以下示例中所示。

```
[ec2-user ~]$ modinfo ena
filename:       /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:        1.5.0g
license:        GPL
description:    Elastic Network Adapter (ENA)
author:         Amazon.com, Inc. or its affiliates
srcversion:     692C7C68B8A9001CB3F31D0
alias:          pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:      Y
intree:         Y
name:           ena
...
```

在上述 Amazon Linux 情况中，ena 模块已安装。

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

在上述 Ubuntu 实例中，此模块未安装，因此您必须首先安装它。有关更多信息，请参阅在 Ubuntu 上启用增强联网 (p. 1147)。

实例属性 (enaSupport)

要检查实例是否设置了增强联网 enaSupport 属性，请使用以下任一命令。如果该属性已设置，则响应为 true。

- describe-instances (Amazon CLI/Amazon CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance（适用于 Windows PowerShell 的工具）

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

映像属性（enaSupport）

要检查 AMI 是否设置了增强联网 enaSupport 属性，请使用以下任一命令。如果该属性已设置，则响应为 true。

- describe-images (Amazon CLI/Amazon CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image（适用于 Windows PowerShell 的工具）

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

网络接口驱动程序

使用以下命令验证是否在特定接口上使用了 ena 模块（替代要检查的接口名称）。如果您使用单个接口（默认设置），则它是 eth0。如果操作系统支持可预测的网络名称 (p. 1149)，这可以是 ens5 等名称。

在以下示例中，ena 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

在此示例中，ena 模块进行加载并具有推荐的最低版本。此实例正确配置了增强联网。

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

在 Amazon Linux AMI 上启用增强联网

Amazon Linux 2 和最新版本的 Amazon Linux AMI 包括安装了 ENA 的增强联网所需的模块并启用了 ENA 支持。因此，如果使用 HVM 版本的 Amazon Linux 在支持的实例类型上启动实例，则已为您的实例启用增强联网。有关更多信息，请参阅测试是否启用了增强联网功能 (p. 1144)。

如果您使用较旧的 Amazon Linux AMI 启动了实例，并且实例尚未启用增强联网，请通过以下步骤启用增强联网。

在 Amazon Linux AMI 上启用增强联网

1. 连接到您的 实例。
2. 从实例运行以下命令以使用最新内核和内核模块 (包括 ena) 更新实例：

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机重启实例：reboot-instances（Amazon CLI）、Restart-EC2Instance（Amazon Tools for Windows PowerShell）。
4. 再次连接到您的实例，并使用ena中的 modinfo ena 命令验证 测试是否启用了增强联网功能 (p. 1144) 模块是否已安装并具有推荐的最低版本。
5. [由 EBS 支持的实例] 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances（Amazon CLI）、Stop-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

[实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：在 Amazon Linux AMI 上启用增强联网（实例存储支持的实例）(p. 1147)。

6. 使用以下任一命令从本地电脑启用增强联网属性：

   - modify-instance-attribute (Amazon CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
   ```

   - Edit-EC2InstanceAttribute（适用于 Windows PowerShell 的工具）

   ```
   Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
   ```

7. (可选) 从实例创建 AMI，如 中所述创建一个由 Amazon EBS 支持的 Linux AMI (p. 137) 该 AMI 从实例继承增强联网 `enaSupport` 属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。
8. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances（Amazon CLI）、Start-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
9. 连接到您的实例，并使用`ena`中的 ethtool -i eth*n* 命令验证是否在网络接口上安装并加载了 测试是否启用了增强联网功能 (p. 1144) 模块。

   如果您在启用增强联网之后无法连接到实例，请参阅对 Elastic Network Adapter (ENA) 进行问题排查 (p. 1169)。

在 Amazon Linux AMI 上启用增强联网（实例存储支持的实例）

按照上述过程操作，直到您停止实例的步骤。按照创建由实例存储支持的 Linux AMI (p. 142)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- register-image (Amazon CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

在 Ubuntu 上启用增强联网

最新的 Ubuntu HVM AMI 包括安装了 ENA 的增强联网所需的模块并启用了 ENA 支持。因此，如果使用最新的 Ubuntu HVM AMI 在支持的实例类型上启动实例，则已为您的实例启用增强联网。有关更多信息，请参阅测试是否启用了增强联网功能 (p. 1144)。

如果您使用较旧的 AMI 启动了实例，并且实例尚未启用增强联网，则可以安装 `linux-aws` 内核程序包以获取最新的增强联网驱动程序并更新所需的属性。

安装 **`linux-aws`** 内核程序包（Ubuntu 16.04 或更高版本）

Ubuntu 16.04 和 18.04 随附 Ubuntu 自定义内核（`linux-aws` 内核程序包）。要使用其他内核，请联系 Amazon Web Services Support。

安装 **`linux-aws`** 内核程序包（Ubuntu Trusty 14.04）

1. 连接到您的 实例。

2. 更新包缓存和包。

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

   Important

   如果在更新过程中系统提示您安装 grub，请使用 /dev/xvda 安装 grub，然后选择保留当前版本的 /boot/grub/menu.lst。

3. [由 EBS 支持的实例] 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances（Amazon CLI）、Stop-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

   [实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：在 Ubuntu 上启用增强联网（由实例存储支持的实例）(p. 1148)。

4. 使用以下任一命令从本地电脑启用增强联网属性：

   - modify-instance-attribute (Amazon CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

   - Edit-EC2InstanceAttribute（适用于 Windows PowerShell 的工具）

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

5. (可选) 从实例创建 AMI，如 中所述创建一个由 Amazon EBS 支持的 Linux AMI (p. 137) 该 AMI 从实例继承增强联网 enaSupport 属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。

6. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances（Amazon CLI）、Start-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。

在 Ubuntu 上启用增强联网（由实例存储支持的实例）

按照上述过程操作，直到您停止实例的步骤。按照创建由实例存储支持的 Linux AMI (p. 142)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- register-image (Amazon CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

在 Linux 上启用增强联网

用于 Red Hat Enterprise Linux、SUSE Linux Enterprise Server 和 CentOS 的最新 AMI 包括使用 ENA 增强联网所需的模块并启用了 ENA 支持。因此，如果使用最新的 AMI 在支持的实例类型上启动实例，则已为您的实例启用增强联网。有关更多信息，请参阅测试是否启用了增强联网功能 (p. 1144)。

下面的过程提供了在 Amazon Linux AMI 或 Ubuntu 之外的 Linux 发行版上启用增强联网的一般步骤。有关更多信息（如命令的详细语法、文件位置或包和工具支持），请参阅您的 Linux 发行版的文档。

对 Linux 启用增强联网

1. 连接到您的 实例。
2. 从位于以下网址的 GitHub 克隆您实例上的 ena 模块的源代码：https://github.com/amzn/amzn-drivers。（默认情况下，SUSE Linux Enterprise Server 12 SP2 及更高版本包含 ENA 2.02，因此不需要下载和编译 ENA 驱动程序。对于 SUSE Linux Enterprise Server 12 SP2 及更高版本，您应该提交一个请求，将您想要的驱动程序版本添加到存储内核中）。
3. 在实例上编译并安装 ena 模块。这些步骤取决于 Linux 发行版。有关在 Red Hat Enterprise Linux 上编译模块的更多信息，请参阅 Amazon 知识中心文章。
4. 运行 sudo depmod 命令以更新模块依赖项。
5. 在实例上更新 `initramfs` 以确保在启动时加载新模块。例如，如果您的发行版支持 dracut，则可使用以下命令。

   ```
   dracut -f -v
   ```

6. 确定您的系统是否默认使用可预测的网络接口名称。使用 systemd 或 udev 版本 197 或更高版本的系统可以重命名以太网设备，它们不保证单个网络接口将命名为 `eth0`。此行为可能导致连接到实例时出现问题。要获取更多信息并查看其他配置选项，请参阅 freedesktop.org 网站上的可预测的网络接口名称。

   a. 您可以使用以下命令在基于 RPM 的系统上检查 systemd 或 udev 版本。

      ```
      rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
      systemd-208-11.el7_0.2.x86_64
      ```

      在以上 Red Hat Enterprise Linux 7 示例中，systemd 版本是 208，因此必须禁用可预测的网络接口名称。

   b. 通过将 `net.ifnames=0` 选项添加到 `GRUB_CMDLINE_LINUX` 中的 `/etc/default/grub` 行，可禁用可预测的网络接口名称。

      ```
      sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/grub
      ```

   c. 重新构建 grub 配置文件。

      ```
      sudo grub2-mkconfig -o /boot/grub2/grub.cfg
      ```

7. [由 EBS 支持的实例] 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances（Amazon CLI）、Stop-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

   [实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：在 Linux 上启用增强联网（由实例存储支持的实例）(p. 1150)。
8. 使用以下任一命令从本地计算机启用增强联网 `enaSupport` 属性：

   - modify-instance-attribute (Amazon CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute（适用于 Windows PowerShell 的工具）

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

9. (可选) 从实例创建 AMI，如 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137) 中所述。该 AMI 从实例继承增强联网 `enaSupport` 属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。

Important

如果您的实例操作系统包含 `/etc/udev/rules.d/70-persistent-net.rules` 文件，则必须在创建 AMI 之前将其删除。此文件包含原始实例的以太网适配器 MAC 地址。如果其他实例使用此文件启动，操作系统将找不到设备，`eth0` 会失败，从而导致启动问题。此文件将在下次启动过程中重新生成，从 AMI 启动的任意实例都会创建这个文件的自有版本。

10. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances（Amazon CLI）、Start-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
11. (可选) 连接到实例并确认已安装模块。

    如果您在启用增强联网之后无法连接到实例，请参阅对 Elastic Network Adapter (ENA) 进行问题排查 (p. 1169)。

在 Linux 上启用增强联网（由实例存储支持的实例）

按照上述过程操作，直到您停止实例的步骤。按照创建由实例存储支持的 Linux AMI (p. 142)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- register-image (Amazon CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

利用 DKMS 在 Ubuntu 上启用增强联网

此方法仅用于测试和反馈目的。它不供生产部署使用。有关生产部署，请参阅在 Ubuntu 上启用增强联网 (p. 1147)。

Important

使用 DKMS 可避免您的订阅的支持协议。不得将其用于生产部署。

在 Ubuntu 上启用 ENA 增强联网 (EBS 支持的实例)

1. 按照在 Ubuntu 上启用增强联网 (p. 1147)中的步骤 1 和 2 操作。
2. 安装 `build-essential` 包以编译内核模块和 `dkms` 包，这样每次更新内核时都会重建 `ena` 模块。

```
ubuntu:~$ sudo apt-get install -y build-essential dkms
```

3. 从位于以下网址的 GitHub 克隆您实例上的 `ena` 模块的源代码：https://github.com/amzn/amzn-drivers。

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

4. 将 `amzn-drivers` 包移动到 `/usr/src/` 目录，以便 DKMS 可以在每次内核更新中找到并构建该模块。将源代码的版本号 (您可在发行说明中找到当前版本号) 附加到目录名称。例如，版本 `1.0.0` 显示在以下示例中。

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. 使用以下值创建 DKMS 配置文件（替代您的 `ena` 版本）。

创建 文件。

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

编辑文件并添加以下值。

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. 使用 DKMS 在实例上添加、构建和安装 ena 模块。

   将该模块添加到 DKMS。

   ```
   ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
   ```

   使用 dkms 命令构建该模块。

   ```
   ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
   ```

   使用 dkms 安装该模块。

   ```
   ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
   ```

7. 重新构建 `initramfs`，以便在启动时加载正确的模块。

   ```
   ubuntu:~$ sudo update-initramfs -u -k all
   ```

8. 使用ena中的 modinfo ena 命令验证是否安装了 测试是否启用了增强联网功能 (p. 1144) 模块。

   ```
   ubuntu:~$ modinfo ena
   filename:       /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
   version:        1.0.0
   license:        GPL
   description:    Elastic Network Adapter (ENA)
   author:         Amazon.com, Inc. or its affiliates
   srcversion:     9693C876C54CA64AE48F0CA
   alias:          pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
   alias:          pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
   alias:          pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
   alias:          pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
   depends:
   vermagic:       3.13.0-74-generic SMP mod_unload modversions
   parm:           debug:Debug level (0=none,...,16=all) (int)
   parm:           push_mode:Descriptor / header push mode
    (0=automatic,1=disable,3=enable)
        0 - Automatically choose according to device capability (default)
        1 - Don't push anything to device memory
        3 - Push descriptors and header buffer to device memory (int)
   parm:           enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1)
    (int)
   ```

```
parm:           enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:           numa_node_override_array:Numa node override map
 (array of int)
parm:           numa_node_override:Enable/Disable numa node override (0=disable)
 (int)
```

9. 继续执行在 Ubuntu 上启用增强联网 (p. 1147)中的步骤 3。

驱动程序发行说明

有关 Linux ENA 驱动程序版本的信息，请参阅 ENA Linux 内核驱动程序发行说明。

问题排查

有关故障排除信息，请参阅对 Elastic Network Adapter (ENA) 进行问题排查 (p. 1169)。

在 Linux 实例上使用 ENA Express 提高网络性能

ENA Express 由 Amazon 可扩展的可靠数据报（SRD）技术提供支持。SRD 是一种高性能网络传输协议，使用动态路由来提高吞吐量并最大限度地减少尾部延迟。使用 ENA Express，您可在同一子网中的两个 EC2 实例之间通信。

ENA Express 的优势

- 将子网内单流可以使用的最大带宽从 5 Gbps 增加至 25Gbps。
- 减少 EC2 实例之间网络流量的尾部延迟，尤其是在网络高负载期间。
- 检测并避开拥塞的网络路径。
- 直接在网络层处理某些任务，比如接收端的数据包重新排序以及所需的大部分重传。这样可以腾出应用层用于其他工作。

> **Note**
>
> 如果您的应用程序每秒发送或接收大量数据包，并且大部分时间都需要优化延迟，尤其是在网络不拥塞的时段，那么 增强联网 (p. 1142) 可能更适合您的网络。

在网络流量较少的时段内，当数据包使用 ENA Express 时，您可能会注意到数据包延迟略有增加（数十微秒）。在此期间，优先考虑特定网络性能特征的应用程序可以从 ENA Express 中受益，如下所示：

- 同一子网内的最大单流带宽从 5 Gbps 提高到 25 Gbps 时，进程可以从中受益。
- 在网络拥塞时段，运行时间较长的进程会减少尾部延迟。
- 网络响应时间分配更流畅、更标准时，进程可以从中受益。

先决条件

为确保 ENA Express 能够有效运行，请为您的实例更新以下设置。

- 如果您的实例使用巨型帧，请运行以下命令，以将最大传输单元（MTU）设置为 8900。

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- 增加接收器（Rx）环的大小，如下所示：

```
[ec2-user ~]$ ethtool -G device rx 8192
```

ENA Express 的工作原理

SRD 技术使用数据包散射机制来分配负载并避免网络拥塞。该技术通过不同的 Amazon 网络路径为每个网络流分配数据包，并在检测到拥塞迹象时动态调整分配。它还能管理接收端的数据包重新排序。

为确保 ENA Express 能够按预期方式管理网络流量，实例的发送和接收以及实例之间的通信必须满足以下所有要求：

- 同时支持发送和接收实例类型。有关更多信息，请参阅 ENA Express 支持的实例类型 (p. 1153) 表。
- 发送和接收实例都必须配置 ENA Express。如配置存在差异，则可能会遇到流量默认为标准 ENA 传输的情况。以下方案显示了可能发生的情况。

  方案：配置差异

实例	已启用 ENA Express	UDP 使用 ENA Express
实例 1	是	是
实例 2	是	否

  在这种情况下，两个实例之间的 TCP 流量可以使用 ENA Express，因为两个实例均已启用该功能。但是，由于其中一个实例不将 ENA Express 用于 UDP 流量，因此这两个实例之间通过 UDP 进行的通信则使用标准 ENA 传输。
- 发送和接收实例必须在同一子网中运行。
- 实例之间的网络路径不得包含中间件。ENA Express 目前不支持中间件。
- 要充分利用带宽潜力，请使用驱动程序版本 2.2.9 或更高版本。
- 要生成指标，请使用驱动程序版本 2.8 或更高版本。

如果未满足任何要求，实例将使用标准 TCP/UDP 协议，但不使用 SRD 进行通信。

为确保您的实例网络驱动程序配置为最佳性能，请查看 ENA 驱动程序的最佳实践推荐。这些最佳实践同样适用于 ENA Express。有关更多信息，请参阅 GitHub 网站上的 ENA Linux Driver Best Practices and Performance Optimization Guide（ENA Linux 驱动程序最佳实践和性能优化指南）。

> **Note**
>
> Amazon EC2 是指实例与作为附件附加到该实例的网络接口之间的关系。ENA Express 设置适用于该附件。如果网络接口从实例中分离，则该附件将不再存在，应用于它的 ENA Express 设置将不再生效。终止实例时也是如此，即使网络接口仍然存在。

ENA Express 支持的实例类型

下表包含支持 ENA Express 的实例类型。

实例系列	实例类型	实例大小	架构
通用型	m6i	m6i.32xl、m6i.metal	x86_64
通用型	m6id	m6id.32xl、m6id.metal	x86_64
计算优化	c6gn	c6gn.16xl	arm64
计算优化	c6i	c6i.32xl、c6i.metal	x86_64
计算优化	c6id	c6id.32xl、c6id.metal	x86_64

实例系列	实例类型	实例大小	架构
内存优化	r6i	r6i.32xl、r6i.metal	x86_64
内存优化	r6id	r6id.32xl、r6id.metal	x86_64
存储优化	i4i	i4i.32xl、i4i.metal	x86_64
存储优化	im4gn	im4gn.16xl	arm64

列出并查看 ENA Express 设置

本节介绍如何通过 Amazon Web Services Management Console 或 Amazon CLI 列出和查看 ENA Express 信息。有关更多信息，请选择与要使用的方法匹配的选项卡。

Console

该选项卡介绍如何在 Amazon Web Services Management Console 中查找有关当前 ENA Express 设置的信息以及如何查看实例类型支持。

查看实例类型支持

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instance Types（实例类型）。
3. 选择实例类型以查看该实例的详细信息。您可以选择 Instance type（实例类型）链接以打开详情页面，也可以选择列表左侧的复选框，在页面底部的详情窗格中查看详细信息。
4. 在 Networking（网络）选项卡或详情页面的该部分中，ENA Express support（ENA Express 支持）显示真值或假值，以显示该实例类型是否支持此功能。

从网络接口列表中查看设置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Network interfaces（网络接口）。
3. 选择一个网络接口以查看该实例的详细信息。您可以选择 Network interface ID（网络接口 ID）链接以打开详情页面，也可以选择列表左侧的复选框，在页面底部的详情窗格中查看详细信息。
4. 在 Details（详细信息）选项卡或详情页面的 Network interface attachment（网络接口附件）部分中，查看 ENA Express 和 ENA Express UDP 的设置。

从实例中查看设置

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择实例以查看该实例的详细信息。您可以选择 Instance ID（实例类型）链接以打开详情页面，也可以选择列表左侧的复选框，在页面底部的详情窗格中查看详细信息。
4. 在 Networking（网络）选项卡的 Network interfaces（网络接口）部分中，向右滚动查看 ENA Express 和 ENA Express UDP 的设置。

Amazon CLI

该选项卡介绍如何在 Amazon CLI 中查找有关当前 ENA Express 设置的信息以及如何查看实例类型支持。

描述实例类型

有关特定实例类型的实例类型设置信息，请在 Amazon CLI 中运行 describe-instance-types 命令，然后替换实例类型，如下所示：

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
"InstanceTypes": [
    {
        "InstanceType": "m6i.metal",
        "CurrentGeneration": true,
        ...
        },
        "NetworkInfo": {
            ...
            "EnaSrdSupported": true
        },
        ...
    }
]
}
```

描述网络接口

有关实例类型设置的信息，请在 Amazon CLI 中运行 describe-network-interfaces 命令，如下所示：

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
    {
        "Association": {
            ....IPs, DNS...
        },
        "Attachment": {
            "AttachTime": "2022-11-17T09:04:28+00:00",
            "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
            "DeleteOnTermination": true,
            "DeviceIndex": 0,
            "NetworkCardIndex": 0,
            "InstanceId": "i-0abcd123e456fabcd",
            "InstanceOwnerId": "111122223333",
            "Status": "attached",
            "EnaSrdSpecification": {
                "EnaSrdEnabled": true,
                "EnaSrdUdpSpecification": {
                    "EnaSrdUdpEnabled": true
                }
            }
        },
        ...
        "NetworkInterfaceId": "eni-0d1234e5f6a78901b",
        "OwnerId": "111122223333",
        ...
    }
]
}
```

配置 ENA Express 设置

您可为支持的 EC2 实例类型配置 ENA Express，而无需安装任何其他软件。本节介绍如何从 Amazon Web Services Management Console 或 Amazon CLI 中配置 ENA Express。有关更多信息，请选择与要使用的方法匹配的选项卡。

Console

此选项卡介绍如何管理附加到实例的网络接口的 ENA Express 设置。

从网络接口列表中管理 ENA Express

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Network interfaces（网络接口）。
3. 选择附加到实例的网络接口。您可以选择 Network interface ID（网络接口 ID）链接以打开详情页面，也可以选择列表左侧的复选框。
4. 从页面右上角的 Action（操作）菜单中选择 Manage ENA Express（管理 ENA Express）。这样将打开 Manage ENA Express（管理 ENA Express）对话框，显示选定的网络接口 ID 和当前设置。

   Note

   如果您选择的网络接口未附加到实例，则菜单中不会出现此操作。
5. 要使用 ENA Express，请选择 Enable（启用）复选框。
6. 启用 ENA Express 后，您可以配置 UDP 设置。要使用 ENA Express UDP，请选择 Enable（启用）复选框。
7. 选择 Save（保存）以保存您的设置。

从实例列表中管理 ENA Express

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择想要管理的实例。您可以选择 Instance ID（实例 ID）以打开详情页面，也可以选择列表左侧的复选框。
4. 选择要为您的实例配置的 Network interface（网络接口）。
5. 从页面右上角的 Action（操作）菜单中选择 Manage ENA Express（管理 ENA Express）。
6. 要为附加到实例的网络接口配置 ENA Express，请从 Network interface（网络接口）列表中进行选择。
7. 要对选定的网络接口附件使用 ENA Express，请选择 Enable（启用）复选框。
8. 启用 ENA Express 后，您可以配置 UDP 设置。要使用 ENA Express UDP，请选择 Enable（启用）复选框。
9. 选择 Save（保存）以保存您的设置。

将网络接口附加到 EC2 实例时配置 ENA Express

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Network interfaces（网络接口）。
3. 选择未附加到实例的网络接口 [Status（状态）为可用]。您可以选择 Network interface ID（网络接口 ID）链接以打开详情页面，也可以选择列表左侧的复选框。
4. 选择要附加到的 Instance（实例）。
5. 将网络接口附加到实例后要使用 ENA Express，请选择 Enable（启用）复选框。
6. 启用 ENA Express 后，您可以配置 UDP 设置。要使用 ENA Express UDP，请选择 Enable（启用）复选框。
7. 要将网络接口附加到实例并保存 ENA Express 设置，请选择 Attach（附加）。

Amazon CLI

此选项卡介绍如何在 Amazon CLI 中配置 ENA Express 设置。

附加网络接口时配置 ENA Express

要在将网络接口附加到实例时配置 ENA Express，请在 Amazon CLI 中运行 attach-network-interface 命令，如以下示例所示：

示例 1：将 ENA Express 用于 TCP 流量，而非 UDP 流量

在此示例中，我们将 EnaSrdEnabled 配置为 true，并允许 EnaSrdUdpEnabled 默认为 false。

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-srd-
specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

示例 2：将 ENA Express 用于 TCP 流量和 UDP 流量

在此示例中，我们将 EnaSrdEnabled 和 EnaSrdUdpEnabled 均配置为 true。

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-srd-
specification 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

更新网络接口附件的 ENA Express 设置

要更新附加到实例的网络接口的 ENA Express 设置，请在 Amazon CLI 中运行 modify-network-interface-attribute 命令，如以下示例所示：

示例 1：将 ENA Express 用于 TCP 流量，而非 UDP 流量

在此示例中，我们将 EnaSrdEnabled 配置为 true，如果之前从未设置过，则允许 EnaSrdUdpEnabled 默认为 false。

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

示例 2：将 ENA Express 用于 TCP 流量和 UDP 流量

在此示例中，我们将 EnaSrdEnabled 和 EnaSrdUdpEnabled 均配置为 true。

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

示例 3：停止将 ENA Express 用于 UDP 流量

在此示例中，我们将 EnaSrdUdpEnabled 配置为 false。

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

监控 ENA Express 性能

在为发送和接收实例上的网络接口附件启用 ENA Express 后，您可以使用 ENA Express 指标来帮助确保实例充分利用 SRD 技术所提供的性能改进。

要查看针对 ENA Express 筛选的指标列表，请对您的网络接口（此处显示为 `eth0`）运行以下 ethtool 命令：

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 pena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

验证实例的 ENA Express 设置

要验证实例上的网络接口附件的当前 ENA Express 设置，请运行 `ethtool` 命令，以列出 ENA Express 指标，并记下 `ena_srd_mode` 指标的值。值如下所示：

- `0` = ENA Express 关闭，UDP 关闭
- 1 = ENA Express 开启，UDP 关闭
- 2 = ENA Express 关闭，UDP 开启

  Note

  仅在最初启用 ENA Express 并将 UDP 配置为使用该功能时，才会发生这种情况。UDP 流量将保留先前值。
- 3 = ENA Express 开启，UDP 开启

为实例上的网络接口附件启用 ENA Express 后，发送实例会启动与接收实例的通信，SRD 会检测 ENA Express 是否同时在发送实例和接收实例上运行。如果 ENA Express 正在运行，则通信可以使用 SRD 传输。如果 ENA Express 未在运行，则通信将退回到标准 ENA 传输。要确认数据包传输是否使用 SRD，您可以将符合条件的数据包数量（`ena_srd_eligible_tx_pkts` 指标）与指定时间段内传输的 SRD 数据包数量（`ena_srd_tx_pkts` 指标）进行比较。

您可以使用该 `ena_srd_resource_utilization` 指标监控 SRD 资源利用率。如果实例即将耗尽其 SRD 资源，则是时候横向扩展该实例了。

有关 ENA Express 指标的更多信息，请参阅 ENA Express 指标 (p. 1165)。

在 Linux 实例上启用 Intel 82599 VF 接口增强联网。

Amazon EC2 通过使用 Intel `ixgbevf` 驱动程序的 Intel 82599 VF 接口提供增强联网功能。

目录

- 要求 (p. 1159)
- 测试是否启用了增强联网功能 (p. 1159)
- 在 Amazon Linux 上启用增强联网 (p. 1160)
- 在 Ubuntu 上启用增强联网 (p. 1161)
- 在其他 Linux 发行版上启用增强联网 (p. 1162)
- 对连接问题进行故障排除 (p. 1163)

要求

要使用 Intel 82599 VF 接口准备增强联网，请按如下方式设置您的实例：

- 从以下支持的实例类型中选择：C3、C4、D2、I2、M4（不包括 `m4.16xlarge`）和 R3。
- 从使用 Linux 内核版本 2.6.32 或更高版本的 HVM AMI 启动实例。最新的 Amazon Linux HVM AMI 安装有增强联网所需的模块，并已设置所需的属性。因此，如果使用最新 Amazon Linux HVM AMI 启动由 Amazon EBS 提供支持且支持增强联网的实例，则已为您的实例启用增强联网。

  Warning

  仅 HVM 实例支持增强联网。使用半虚拟化实例启用增强联网会让该实例无法访问。在模块或模块版本不正确的情况下设置此属性还可能导致您的实例不可访问。
- 确保实例具有 Internet 连接。
- 使用 Amazon Web Services Management Console 的 Amazon CloudShell，或者将 Amazon CLI 或 Amazon Tools for Windows PowerShell 安装到您选择的任意电脑上（最好是本地台式机或笔记本电脑）并进行配置。有关的更多信息，请参阅 访问 Amazon EC2 (p. 3) 或 Amazon CloudShell 用户指南。不能从 Amazon EC2 控制台管理增强联网。
- 如果您的实例上有重要的数据需要保留，则应立即从您的实例创建 AMI，来备份这些数据。更新内核和内核模块以及启用 `sriovNetSupport` 属性可能会导致实例不兼容或无法访问操作系统。如果您有最新备份，则发生此情况时仍将保留数据。

测试是否启用了增强联网功能

如果已在您的实例上安装 `ixgbevf` 模块且设置了 `sriovNetSupport` 属性，请启用 Intel 82599 VF 接口增强联网。

实例属性 (sriovNetSupport)

要检查实例是否设置了增强联网 `sriovNetSupport` 属性，请使用以下任一命令：

- describe-instance-attribute (Amazon CLI/Amazon CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute sriovNetSupport
```

- Get-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

如果未设置此属性，则 `SriovNetSupport` 为空。如果设置了此属性，则值很简单，如以下示例输出所示。

```
"SriovNetSupport": {
    "Value": "simple"
},
```

映像属性 (sriovNetSupport)

要检查 AMI 是否设置了增强联网 `sriovNetSupport` 属性，请使用以下任一命令：

- describe-images (Amazon CLI/Amazon CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (Amazon Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

如果未设置此属性，则 SriovNetSupport 为空。如果设置了此属性，则值很简单。

网络接口驱动程序

使用以下命令验证是否在特定接口上使用了该模块（替代要检查的接口名称）。如果您使用单个接口（默认设置），则为 eth0。如果操作系统支持可预测的网络名称 (p. 1162)，这可以是 ens5 等名称。

在以下示例中，ixgbevf 模块未加载，因为列出的驱动程序是 vif。

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

在此示例中，已加载 ixgbevf 模块。此实例正确配置了增强联网。

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

在 Amazon Linux 上启用增强联网

最新的 Amazon Linux HVM AMI 安装有增强联网所需的 ixgbevf 模块，并已设置所需的 sriovNetSupport 属性。因此，如果使用最新的 Amazon Linux HVM AMI 启动实例类型，则已为您的实例启用增强联网。有关更多信息，请参阅测试是否启用了增强联网功能 (p. 1159)。

如果您使用较旧的 Amazon Linux AMI 启动了实例，并且实例尚未启用增强联网，请通过以下步骤启用增强联网。

> Warning
>
> 增强联网属性启用之后将无法禁用。

启用增强联网

1. 连接到您的实例。
2. 从实例运行以下命令以使用最新内核和内核模块 (包括 ixgbevf) 更新实例：

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机重启实例：reboot-instances（Amazon CLI）、Restart-EC2Instance（Amazon Tools for Windows PowerShell）。

4. 再次连接到您的实例，并使用`ixgbevf`中的 modinfo ixgbevf 命令验证 测试是否启用了增强联网功能 (p. 1159) 模块是否已安装并具有推荐的最低版本。
5. [由 EBS 支持的实例] 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances（Amazon CLI）、Stop-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

   [实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：启用增强联网（由实例存储支持的实例）(p. 1161)。
6. 使用以下任一命令从本地电脑启用增强联网属性：

   - modify-instance-attribute (Amazon CLI/Amazon CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   - Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```
7. (可选) 从实例创建 AMI，如 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137) 中所述。该 AMI 从实例继承增强联网属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。
8. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances（Amazon CLI）、Start-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
9. 连接到您的实例，并使用`ixgbevf`中的 ethtool -i eth*n* 命令验证是否在网络接口上安装并加载了 测试是否启用了增强联网功能 (p. 1159) 模块。

启用增强联网（由实例存储支持的实例）

按照上述过程操作，直到您停止实例的步骤。按照创建由实例存储支持的 Linux AMI (p. 142)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- register-image (Amazon CLI/Amazon CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

在 Ubuntu 上启用增强联网

在开始之前，在您的实例上检查是否已启用增强联网 (p. 1159)。

Quick Start Ubuntu HVM AMI 包含实现增强联网所需的驱动程序。如果您的 `ixgbevf` 版本早于 2.16.4，则可以安装 `linux-aws` 内核程序包以获取最新增强的联网功能驱动程序。

以下过程提供了在 Ubuntu 实例上编译 `ixgbevf` 模块的一般步骤。

安装 `linux-aws` 内核程序包

1. 连接到您的 实例。
2. 更新包缓存和包。

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

Important

如果在更新过程中系统提示您安装 grub，请使用 /dev/xvda 安装 grub，然后选择保留当前版本的 /boot/grub/menu.lst。

在其他 Linux 发行版上启用增强联网

在开始之前，在您的实例上检查是否已启用增强联网 (p. 1159)。最新 Quick Start HVM AMI 包含实现增强联网所需的驱动程序，因此您无需执行其他步骤。

下面的过程提供了在 Amazon Linux 或 Ubuntu 之外的 Linux 发行版上启用 Intel 82599 VF 接口增强联网所需的一般步骤。有关更多信息 (如命令的详细语法、文件位置或包和工具支持)，请参阅您的 Linux 发行版的特定文档。

对 Linux 启用增强联网

1. 连接到您的 实例。
2. 从 Sourceforge 上的 ixgbevfhttps://sourceforge.net/projects/e1000/files/%20stable/ 位置在实例上下载 ixgbevf 模块的源代码。

   早于 2.16.4 的 ixgbevf 版本 (包括版本 2.14.2) 在某些 Linux 发行版 (包括某些 Ubuntu 版本) 上构建不正确。
3. 在实例上编译并安装 ixgbevf 模块。

   Warning

   如果您为当前内核编译 ixgbevf 模块，然后升级内核而不为新内核重新构建驱动程序，则系统会在下次重新启动时恢复为特定于发行版的 ixgbevf 模块。这可能会在特定于发行版的版本与增强联网不兼容时使您的系统无法访问。
4. 运行 sudo depmod 命令以更新模块依赖项。
5. 在实例上更新 initramfs 以确保在启动时加载新模块。
6. 确定您的系统是否默认使用可预测的网络接口名称。使用 systemd 或 udev 版本 197 或更高版本的系统可以重命名以太网设备，它们不保证单个网络接口将命名为 eth0。此行为可能导致连接到实例时出现问题。要获取更多信息并查看其他配置选项，请参阅 freedesktop.org 网站上的可预测的网络接口名称。

   a. 您可以使用以下命令在基于 RPM 的系统上检查 systemd 或 udev 版本：

   ```
   [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   在以上 Red Hat Enterprise Linux 7 示例中，systemd 版本是 208，因此必须禁用可预测的网络接口名称。

   b. 通过将 net.ifnames=0 选项添加到 GRUB_CMDLINE_LINUX 中的 /etc/default/grub 行，可禁用可预测的网络接口名称。

   ```
   [ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/grub
   ```

   c. 重新构建 grub 配置文件。

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. [由 EBS 支持的实例] 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances（Amazon CLI/Amazon CloudShell）、Stop-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

   [实例存储支持的实例] 您无法停止实例来修改属性。请执行此过程：启用增强联网（由实例存储支持的实例）(p. 1163)。
8. 使用以下任一命令从本地电脑启用增强联网属性：

   - modify-instance-attribute (Amazon CLI/Amazon CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   - Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```
9. (可选) 从实例创建 AMI，如 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137) 中所述。该 AMI 从实例继承增强联网属性。因此，您可以使用此 AMI 启动默认情况下启用了增强联网功能的其他实例。

   Important

   如果您的实例操作系统包含 `/etc/udev/rules.d/70-persistent-net.rules` 文件，则必须在创建 AMI 之前将其删除。此文件包含原始实例的以太网适配器 MAC 地址。如果其他实例使用此文件启动，操作系统将找不到设备，`eth0` 会失败，从而导致启动问题。此文件将在下次启动过程中重新生成，从 AMI 启动的任意实例都会创建这个文件的自有版本。
10. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances（Amazon CLI）、Start-EC2Instance（Amazon Tools for Windows PowerShell）。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
11. (可选) 连接到实例并确认已安装模块。

启用增强联网（由实例存储支持的实例）

按照上述过程操作，直到您停止实例的步骤。按照创建由实例存储支持的 Linux AMI (p. 142)中所述创建新 AMI，确保在注册 AMI 时启用增强联网属性。

- register-image (Amazon CLI/Amazon CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

对连接问题进行故障排除

如果您在启用增强联网期间丢失连接，则 `ixgbevf` 模块可能与内核不兼容。请尝试安装用于您的实例的 Linux 发行版所附带的 `ixgbevf` 模块版本。

如果您为半虚拟化实例或 AMI 启用增强网络，则这可能会使您的实例无法访问。

有关更多信息，请参阅我如何在我的 EC2 实例上启用和配置增强联网功能？。

操作系统优化

若要在具有增强联网的实例上实现最高网络性能，您可能需要修改原定设置操作系统配置。有关更多信息，请参阅 GitHub 上的 ENA Linux Driver Best Practices and Performance Optimization Guide（ENA Linux 驱动程序最佳实践和性能优化指南）。

监控 EC2 实例的网络性能

Elastic Network Adapter (ENA) 驱动程序从启用这些指标的实例发布网络性能指标。您可以使用这些指标来排查实例性能问题、为工作负载选择合适的实例大小、主动计划扩展活动以及对应用程序进行基准测试，以确定它们是否最大限度地提高了实例的可用性能。

Amazon EC2 定义实例级别的网络最大值，以确保高质量的联网体验，包括不同大小实例间一致的网络性能。Amazon 为每个实例提供以下最大值：

- 带宽功能 – 根据实例类型和大小，每个 EC2 实例都具有聚合入站和出站流量的最大带宽。一些实例使用一种网络 I/O 积分机制，根据平均带宽使用率分配网络带宽。Amazon EC2 还拥有最大的带宽，可用于流向 Amazon Direct Connect 和互联网的流量。有关更多信息，请参阅Amazon EC2 实例网络带宽 (p. 1141)。
- 每秒数据包 (PPS) 性能 – 根据实例类型和大小，每个 EC2 实例都具有最大的 PPS 性能。
- 跟踪连接 – 安全组会跟踪建立的每个连接，以确保返回数据包按预期交付。每个实例都有可以跟踪的最大连接数量。有关更多信息，请参阅 安全组连接跟踪 (p. 1306)
- 链接本地服务访问 – Amazon EC2 为流向 DNS 服务、实例元数据服务和 Amazon Time Sync Service 等服务的流量提供每个网络接口的最大 PPS。

当实例的网络流量超过最大值时，Amazon 将通过排队然后丢弃网络数据包来调整超过最大值的流量。您可以使用网络性能指标监控流量何时超过最大值。这些指标可以实时告知您对网络流量的影响以及可能的网络性能问题。

目录

- 要求 (p. 1164)
- ENA 驱动程序的指标 (p. 1165)
- 查看 Linux 实例的网络性能指标 (p. 1165)
- ENA Express 指标 (p. 1165)
- ENA 的 DPDK 驱动程序的网络性能指标 (p. 1167)
- 运行 FreeBSD 的实例的指标 (p. 1168)

要求

以下要求适用于 Linux 实例。

- 安装 ENA 驱动程序版本 2.2.10 或更高版本。要验证安装的版本，请使用 ethtool 命令。在以下示例中，版本符合最低要求。

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  要升级 ENA 驱动程序，请参阅增强联网 (p. 1143)。
- 要将这些指标导入到 Amazon CloudWatch，请安装 CloudWatch 代理。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的收集网络性能指标。

- 要支持 `conntrack_allowance_available` 指标，请安装 ENA 驱动程序版本 2.8.1。

ENA 驱动程序的指标

ENA 驱动程序实时向实例传送以下指标。它们提供了自上次驱动程序重置以来在每个网络接口上排队或丢弃的累计数据包数。

以下指标适用于 Linux 实例、FreeBSD 实例和 DPDK 环境。

指标	描述	在以下实例上受支持：
bw_in_allowance_exceeded	因入站聚合带宽超过实例的最大值而排队或丢弃的数据包的数量。	所有实例类型
bw_out_allowance_exceeded	因出站聚合带宽超过实例的最大值而排队或丢弃的数据包的数量。	所有实例类型
conntrack_allowance_exceeded	由于连接跟踪超过实例的最大值且无法建立新连接而丢弃的数据包的数量。这可能会导致进出实例的流量丢失数据包。	所有实例类型
conntrack_allowance_available	在达到该实例类型的跟踪连接限额之前，实例可以建立的跟踪连接数。	仅限基于 Nitro 的实例类型 (p. 246)
linklocal_allowance_exceeded	由于到本地代理服务的流量的 PPS 超出网络接口的最大值而丢弃的数据包数量。这会影响流向 DNS 服务、实例元数据服务和 Amazon Time Sync Service 的流量。	所有实例类型
pps_allowance_exceeded	因双向 PPS 超过实例的最大值而排队或丢弃的数据包的数量。	所有实例类型

查看 Linux 实例的网络性能指标

您可以将指标发布到自己的收藏夹工具以可视化指标数据。例如，您可以使用 CloudWatch 代理将指标发布到 Amazon CloudWatch。代理使您能够选择单个指标并控制发布。

您还可以使用 ethtool 按如下方式检索每个网络接口的指标，例如 eth0。

```
[ec2-user ~]$ ethtool -S eth0
     bw_in_allowance_exceeded: 0
     bw_out_allowance_exceeded: 0
     pps_allowance_exceeded: 0
     conntrack_allowance_exceeded: 0
     linklocal_allowance_exceeded: 0
     conntrack_allowance_available: 136812
```

ENA Express 指标

ENA Express 由 Amazon 可扩展的可靠数据报（SRD）技术提供支持。SRD 是一种高性能网络传输协议，使用动态路由来提高吞吐量并最大限度地减少尾部延迟。您可以使用 ENA Express 指标来帮助确保您的实例充分利用 SRD 技术所提供的性能改进，例如：

- 评估您的资源，确保其有足够的容量来建立更多的 SRD 连接。
- 确定哪些位置存在阻止符合条件的传出数据包使用 SRD 的潜在问题。
- 计算实例使用 SRD 的传出流量的百分比。

- 计算实例使用 SRD 的传入流量的百分比。

  Note

  要生成指标，请使用驱动程序版本 2.8 或更高版本。

对于基于 Linux 的实例，使用 ethtool 命令可获得以下 ENA Express 指标。

- `ena_srd_mode` – 描述启用了哪些 ENA Express 功能。值如下所示：
  - `0` = ENA Express 关闭，UDP 关闭
  - `1` = ENA Express 开启，UDP 关闭
  - `2` = ENA Express 关闭，UDP 开启

    Note

    仅在最初启用 ENA Express 并将 UDP 配置为使用该功能时，才会发生这种情况。UDP 流量将保留先前值。
  - `3` = ENA Express 开启，UDP 开启
- `ena_srd_eligible_tx_pkts` – 在指定时间段内发送的符合 SRD 资格要求的网络数据包的数量，如下所示：
  - 同时支持发送和接收实例类型。有关更多信息，请参阅 ENA Express 支持的实例类型 (p. 1153) 表。
  - 发送和接收实例都必须配置 ENA Express。
  - 发送和接收实例必须在同一子网中运行。
  - 实例之间的网络路径不得包含中间件。ENA Express 目前不支持中间件。

    Note

    ENA Express 资格指标包括源和目标要求以及两个端点之间的网络。符合条件的数据包在已计数后仍可取消资格。例如，如果某个符合条件的数据包超过了最大传输单元（MTU）的限制，则尽管该数据包在计数器中仍显示为符合条件，但其仍会退回到标准 ENA 传输。
- `ena_srd_tx_pkts` – 指定时间段内传输的 SRD 数据包数量。
- `ena_srd_rx_pkts` – 指定时间段内接收的 SRD 数据包数量。
- `ena_srd_resource_utilization` – 实例已消耗的 SRD 并发连接的最大允许内存利用率的百分比。

要查看针对 ENA Express 筛选的指标列表，请对您的网络接口（此处显示为 `eth0`）运行以下 ethtool 命令：

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 pena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
 ena_srd_resource_utilization: 0
```

出口流量（传出数据包）

为确保您的出口流量按预期使用 SRD，请将符合条件的 SRD 数据包数量（`ena_srd_eligible_tx_pkts`）与指定时间段内发送的 SRD 数据包数量（`ena_srd_tx_pkts`）进行比较。

符合条件的数据包数量和发送的 SRD 数据包数量之间的显著差异通常是由资源利用率问题引起的。当附加到实例的网卡已用尽其最大资源时，或如果数据包超过 MTU 限制，则符合条件的数据包将无法通过 SRD 传输，必须退回到标准 ENA 传输。在实时迁移或实时批量更新期间，数据包也可能出现这种问题。要确定根本原因，还需进行额外的故障排除。

Note

您可以忽略符合条件的数据包数量与 SRD 数据包数量之间偶尔的细微差异。例如，当您的实例为 SRD 流量与另一个实例建立连接时，就会发生这种情况。

要找出在给定时间段内使用 SRD 的总出口流量百分比，请将该时间段内发送的 SRD 数据包数（`ena_srd_tx_pkts`）与针对该实例发送的数据包总数（`NetworkPacketOut`）进行比较。

入口流量（传入数据包）

要找出入口流量使用 SRD 的百分比，请将在给定时间段内接收的 SRD 数据包数（`ena_srd_rx_pkts`）与该时间段内针对该实例接收的数据包总数（`NetworkPacketIn`）进行比较。

资源利用率

资源利用率基于单个实例在指定时间可以容纳的 SRD 并发连接的数量。资源利用率指标（`ena_srd_resource_utilization`）会持续跟踪您当前对实例的利用率。当利用率接近 100% 时，可能会出现性能问题。ENA Express 从 SRD 退回到标准 ENA 传输，丢弃数据包的可能性也随之增加。高资源利用率表明是时候向外扩展实例以提高网络性能了。

Note

当实例的网络流量超过最大值时，Amazon 将通过排队然后丢弃网络数据包来调整超过最大值的流量。

持久性

为实例启用 ENA Express 时，会累积出口和入口指标。如果停用 ENA Express，指标就会停止累积，但只要实例仍在运行，指标就会一直存在。如果实例重启或终止，或网络接口与实例分离，则指标将重置。

ENA 的 DPDK 驱动程序的网络性能指标

ENA 驱动程序版本 2.2.0 及更高版本支持网络指标报告。DPDK 20.11 包括 ENA 驱动程序 2.2.0，它是第一个支持此功能的 DPDK 版本。

您可以使用示例应用程序查看 DPDK 统计信息。要启动示例应用程序的交互式版本，请运行以下命令。

```
./app/dpdk-testpmd -- -i
```

在此交互式会话中，您可以输入命令来检索端口的扩展统计信息。以下示例命令将检索端口 0 的统计信息。

```
show port xstats 0
```

以下是与 DPDK 示例应用程序进行交互式会话的示例。

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected
```

```
        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

有关示例应用程序以及使用它检索扩展统计信息的更多信息。请参阅 DPDK 文档中的 Testpmd 应用程序用户指南。

运行 FreeBSD 的实例的指标

从 2.3.0 版开始，ENA FreeBSD 驱动程序支持在运行 FreeBSD 的实例上收集网络性能指标。要启用 FreeBSD 指标的收集，请输入以下命令并将 *interval*（间隔）设置为 1 到 3600 之间的值。这指定了收集 FreeBSD 指标的频率（以秒为单位）。

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

例如，以下命令将驱动程序设置为每 10 秒在网络接口 1 上收集 FreeBSD 指标：

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

要关闭 FreeBSD 指标集合，您可以运行上述命令并将 `0` 指定为`##`。

收集 FreeBSD 指标后，您可以通过运行以下命令来检索最新收集的指标集。

```
sysctl dev.ena.network_interface.eni_metrics
```

对 Elastic Network Adapter (ENA) 进行问题排查

Elastic Network Adapter (ENA) 旨在改进操作系统运行状况和降低因意外硬件行为或故障而导致长期中断的几率。ENA 架构保持设备或驱动程序故障对系统尽可能透明。本主题提供了关于 ENA 的故障排除信息。

如果您不能连接到实例，请先从对连接问题进行故障排除 (p. 1169)部分开始。

如果您在迁移到第六代实例类型后遇到性能下降，请参阅 Amazon 知识中心的文章：What do I need to do before migrating my EC2 instance to a sixth generation instance to make sure that I get maximum network performance?（在将 EC2 实例迁移到第六代实例之前，我需要采取哪些措施来确保自己获得最大的网络性能？）。

如果您能连接到实例，则可以使用本主题后面部分中涵盖的故障检测和恢复机制收集诊断信息。

目录

- 对连接问题进行故障排除 (p. 1169)
- 保持活动机制 (p. 1170)
- 注册表读取超时 (p. 1171)
- 统计数据 (p. 1171)
- syslog 中的驱动程序错误日志 (p. 1176)

对连接问题进行故障排除

如果您在启用增强联网时丢失连接，则 `ena` 模块可能与您的实例当前运行的内核不兼容。如果您为特定内核版本安装该模块（不使用 dkms，或使用配置错误的 dkms.conf 文件），然后更新您的实例内核，则会发生这种情况。如果在启动时加载的实例内核未正确安装 `ena` 模块，则您的实例将无法识别网络适配器，并且您的实例将变得无法访问。

如果您为 PV 实例或 AMI 启用增强联网，这也会使您的实例无法访问。

如果在启用 ENA 增强联网后您的实例变得无法访问，可以为您的实例禁用 `enaSupport` 属性，这将回退到库存网络适配器。

禁用 ENA 增强联网 (EBS 支持的实例)

1. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机停止实例：stop-instances (Amazon CLI)、Stop-EC2Instance (Amazon Tools for Windows PowerShell)。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中停止该实例，以便使实例状态保持同步。

   Important

   如果您使用的是实例存储支持的实例，则不能停止实例，而应继续禁用 ENA 增强联网 (实例存储支持的实例) (p. 1170)。

2. 从本地计算机中，使用以下命令禁用增强联网属性。

   - modify-instance-attribute (Amazon CLI)

   ```
   $ aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
   ```

3. 使用 Amazon EC2 控制台或以下任一命令从您的本地计算机启动实例：start-instances (Amazon CLI)、Start-EC2Instance (Amazon Tools for Windows PowerShell)。如果您的实例由 Amazon OpsWorks 管理，则应在 Amazon OpsWorks 控制台中启动该实例，以便使实例状态保持同步。
4. (可选) 连接到您的实例，并按照ena中的步骤尝试重新安装具有当前内核版本的 在 Linux 实例上启用 Elastic Network Adapter (ENA) 增强联网 (p. 1143) 模块。

禁用 ENA 增强联网 (实例存储支持的实例)

如果您的实例是实例存储支持的实例，则创建新的 AMI，如创建由实例存储支持的 Linux AMI (p. 142) 中所述。在注册 AMI 时，请确保禁用增强联网 `enaSupport` 属性。

- register-image (Amazon CLI)

```
$ aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (Amazon Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

保持活动机制

ENA 设备按固定速度 (通常每秒一次) 发布保持活动事件。ENA 驱动程序实施一种监视机制，用于检查是否存在这些保持活动消息。如果存在一条或多条消息，则重新启动监视，否则此驱动程序将认为设备出现故障，然后执行以下操作：

- 将当前统计数据转储到 syslog
- 重置 ENA 设备
- 重置 ENA 驱动程序状态

上述重置过程可能会在短时间内导致一些流量丢失 (TCP 连接应该能恢复)，但应该不会影响到用户。

例如，如果 ENA 设备在加载无法恢复的配置后进入未知状态，ENA 设备也可能会间接请求设备重置过程，而不发送保持活动通知。

下面是重置过程示例：

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog process
 initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
```

```
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the end
 of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The driver
 begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date [Wed
 Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset process
 is complete
```

注册表读取超时

ENA 架构建议使用有限的内存映射的 I/O (MMIO) 读取操作。ENA 设备驱动程序仅在其初始化过程中访问 MMIO 注册表。

如果驱动程序日志（在 dmesg 输出中可用）指示读取操作失败，这可能是由驱动程序不兼容或编译错误、硬件设备繁忙或硬件故障所导致的。

指示读取操作失败的间歇性日志条目不应视为问题；在这种情况下，驱动程序将重试读取操作。但是，一系列包含读取失败的日志条目则指示驱动程序或硬件问题。

下面是指示读取操作因超时而失败的驱动程序日志条目示例：

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
 req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
 req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

统计数据

如果您遇到网络性能差或延迟问题，您应该检索设备统计数据并检查这些数据。可以使用 ethtool 获取这些统计数据，如下所示：

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
    tx_timeout: 0
    suspend: 0
    resume: 0
    wd_expired: 0
    interface_up: 1
    interface_down: 0
    admin_q_pause: 0
    bw_in_allowance_exceeded: 0
```

```
    bw_out_allowance_exceeded: 0
    pps_allowance_exceeded: 0
    conntrack_allowance_available: 450878
    conntrack_allowance_exceeded: 0
    linklocal_allowance_exceeded: 0
    queue_0_tx_cnt: 4329
    queue_0_tx_bytes: 1075749
    queue_0_tx_queue_stop: 0
    ...
```

命令输出参数如下所述：

`tx_timeout`: *N*

Netdev 监视的激活次数。

`suspend`: *N*

驱动程序执行挂起操作的次数。

`resume`: *N*

驱动程序执行恢复操作的次数。

`wd_expired`: *N*

驱动程序在过去的 3 秒内未收到保持活动事件的次数。

`interface_up`: *N*

ENA 接口启动的次数。

`interface_down`: *N*

ENA 接口关闭的次数。

`admin_q_pause`: *N*

在运行状态下找不到管理员队列的次数。

`bw_in_allowance_exceeded`: *N*

由于超过带宽限制而丢弃的 rx 数据包的数量。

`bw_out_allowance_exceeded`: *N*

由于超过带宽限额限制而丢弃的 tx 数据包的数量。

`pps_allowance_exceeded`: *N*

由于超过 pps（每秒数据包数）限额限制而丢弃的数据包的数量。

`conntrack_allowance_available`: *N*

在超出该实例类型的最大跟踪连接数之前，实例可以建立的跟踪连接数。

`linklocal_allowance_exceeded`: *N*

由于超过 pps（每秒数据包）限额限制而丢弃的代理数据包的数量。

`queue_`*N*`_tx_cnt`: *N*

为此队列传输的数据包数。

`queue_`*N*`_tx_bytes`: *N*

为此队列传输的字节数。

queue_*N*_tx_queue_stop: *N*

队列 *N* 已满并停止的次数。

queue_*N*_tx_queue_wakeup: *N*

队列 *N* 在停止后恢复的次数。

queue_*N*_tx_dma_mapping_err: *N*

直接内存访问错误计数。如果此值不为 0，则表示系统资源不足。

queue_*N*_tx_linearize: *N*

此对队列尝试 SKB 线性化处理的次数。

queue_*N*_tx_linearize_failed: *N*

此队列的 SKB 线性化处理失败的次数。

queue_*N*_tx_napi_comp: *N*

napi 处理程序为此队列调用 napi_complete 的次数。

queue_*N*_tx_tx_poll: *N*

为此队列 计划 napi 处理程序的次数。

queue_*N*_tx_doorbells: *N*

此队列的传输门铃数。

queue_*N*_tx_prepare_ctx_err: *N*

此队列的 ena_com_prepare_tx 失败的次数。

queue_*N*_tx_bad_req_id: *N*

此队列的 req_id 无效。有效的 req_id = 0 - queue_size - 1。

queue_*N*_tx_llq_buffer_copy: *N*

此队列的报头大小大于 llq 条目的数据包的数量。

queue_*N*_tx_missed_tx: *N*

此队列剩下未完成的数据包数。

queue_*N*_tx_unmask_interrupt: *N*

此队列的 tx 中断被揭开的次数。

queue_*N*_rx_cnt: *N*

为此队列接收的数据包数。

queue_*N*_rx_bytes: *N*

为此队列接收的字节数。

queue_*N*_rx_rx_copybreak_pkt: *N*

rx 队列收到小于此队列的 rx_copybreak 数据包大小的数据包的次数。

queue_*N*_rx_csum_good: *N*

rx 队列收到数据包的次数，其中检查校验和并且对此队列是正确的。

`queue_N_rx_refil_partial`: *N*

驱动程序未成功使用此队列的缓冲区重填空的 rx 队列部分的次数。如果此值不为零，则表示内存资源不足。

`queue_N_rx_bad_csum`: *N*

`rx` 队列具有此队列的错误校验和的次数（仅当支持 rx 校验和卸载时）。

`queue_N_rx_page_alloc_fail`: *N*

此队列的页分配失败的次数。如果此值不为零，则表示内存资源不足。

`queue_N_rx_skb_alloc_fail`: *N*

此队列的 SKB 分配失败的次数。如果此值不为零，则表示系统资源不足。

`queue_N_rx_dma_mapping_err`: *N*

直接内存访问错误计数。如果此值不为 0，则表示系统资源不足。

`queue_N_rx_bad_desc_num`: *N*

每个数据包使用的缓冲区太多。如果此值不为 0，则表示使用的缓冲区非常小。

`queue_N_rx_bad_req_id`: *N*

此队列的 req_id 无效。有效的 req_id 来自 [0, queue_size-1]。

`queue_N_rx_empty_rx_ring`: *N*

此队列的 rx 队列为空的次数。

`queue_N_rx_csum_unchecked`: *N*

rx 队列收到未检查此队列校验和的数据包的次数。

`queue_N_rx_xdp_aborted`: *N*

XDP 数据包被归类为 XDP_ABORT 的次数。

`queue_N_rx_xdp_drop`: *N*

XDP 数据包被归类为 XDP_DROP 的次数。

`queue_N_rx_xdp_pass`: *N*

XDP 数据包被归类为 XDP_PASS 的次数。

`queue_N_rx_xdp_tx`: *N*

XDP 数据包被归类为 XDP_TX 的次数。

`queue_N_rx_xdp_invalid`: *N*

数据包的 XDP 返回代码无效的次数。

`queue_N_rx_xdp_redirect`: *N*

XDP 数据包被归类为 XDP_REDIRECT 的次数。

`queue_N_xdp_tx_cnt`: *N*

为此队列传输的数据包数。

`queue_N_xdp_tx_bytes`: *N*

为此队列传输的字节数。

`queue_N_xdp_tx_queue_stop`: *N*

此队列已满并停止的次数。

`queue_N_xdp_tx_queue_wakeup`: *N*

此队列在停止后恢复的次数。

`queue_N_xdp_tx_dma_mapping_err`: *N*

直接内存访问错误计数。如果此值不为 0，则表示系统资源不足。

`queue_N_xdp_tx_linearize`: *N*

此队列尝试 XDP 缓冲区线性化的次数。

`queue_N_xdp_tx_linearize_failed`: *N*

此队列的 XDP 缓冲区线性化失败的次数。

`queue_N_xdp_tx_napi_comp`: *N*

为此队列调用 napi_complete 的 napi 处理程序的次数。

`queue_N_xdp_tx_tx_poll`: *N*

为此队列安排了 napi 处理程序的次数。

`queue_N_xdp_tx_doorbells`: *N*

此队列的传输门铃数。

`queue_N_xdp_tx_prepare_ctx_err`: *N*

此队列 ena_com_prepare_tx 失败的次数。此值应始终为零；否则，请查看驱动程序日志。

`queue_N_xdp_tx_bad_req_id`: *N*

此队列的 req_id 无效。有效的 req_id 来自 [0, queue_size-1]。

`queue_N_xdp_tx_llq_buffer_copy`: *N*

使用此队列的 llq 缓冲区副本复制了其标头的数据包的数量。

`queue_N_xdp_tx_missed_tx`: *N*

tx 队列条目错过此队列的完成超时的次数。

`queue_N_xdp_tx_unmask_interrupt`: *N*

此队列的 tx 中断被揭开的次数。

`ena_admin_q_aborted_cmd`: *N*

已中止的管理命令数。这通常发生在自动恢复过程中。

`ena_admin_q_submitted_cmd`: *N*

管理队列门铃数。

`ena_admin_q_completed_cmd`: *N*

管理队列完成数。

`ena_admin_q_out_of_space`: *N*

驱动程序尝试提交新管理命令但队列已满的次数。

`ena_admin_q_no_completion: N`

驱动程序未获得命令的管理完成的次数。

syslog 中的驱动程序错误日志

ENA 驱动程序会在系统启动期间将日志消息写入到 syslog 中。如果您遇到问题，则可以查看这些日志以检查错误。下面是 ENA 驱动程序在系统启动期间记录在 syslog 中的信息示例以及一些选择消息注释。

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM: ena_com_validate_version]
 ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM: ena_com_validate_version]
 ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device watchdog is
 Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation is
 not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM: ena_com_get_feature_ex]
 Feature 10 isn't supported // RSS HASH function configuration is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM: ena_com_get_feature_ex]
 Feature 18 isn't supported //RSS HASH input source configuration is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic Network
 Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted. Opts:
 (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family 10
```

可以忽略哪些错误？

可以忽略以下可能出现在系统错误日志中的关于 Elastic Network Adapter 的警告：

Set host attribute isn't supported

此设备不支持主机属性。

failed to alloc buffer for rx queue

这是可恢复的错误，引发此错误时，表示可能存在内存压力问题。

Feature *X* isn't supported

Elastic Network Adapter 不支持引用的功能。*X* 的可能值包括：

- **10**：此设备不支持 RSS 哈希函数配置。
- **12**：此设备不支持 RSS 间接表配置。
- **18**：此设备不支持 RSS 哈希输入配置。
- **20**：此设备不支持中断裁决。
- **27**：Elastic Network Adapter 驱动程序不支持从 snmpd 轮询以太网功能。

Failed to config AENQ

Elastic Network Adapter 不支持 AENQ 配置。

Trying to set unsupported AENQ events

此错误表示尝试设置 Elastic Network Adapter 不支持的 AENQ 事件组。

置放群组

在您启动新的 EC2 实例时，EC2 服务会尝试以某种方式放置实例，以便将所有实例分布在基础硬件上以最大限度减少相关的故障。您可以使用置放群组影响如何放置一组相互依赖的实例，从而满足您的工作负载需求。根据工作负载类型，您可以使用以下置放策略之一创建置放群组：

- 集群 – 将一个可用区中靠近的实例打包在一起。通过使用该策略，工作负载可以实现所需的低延迟网络性能，以满足高性能计算（HPC）应用程序通常使用的紧密耦合的节点到节点通信的要求。
- 分区 – 将实例分布在不同的逻辑分区上，以便一个分区中的实例组不会与不同分区中的实例组使用相同的基础硬件。该策略通常为大型分布式和重复的工作负载所使用，例如，Hadoop、Cassandra 和 Kafka。
- 分布 – 将一小组实例严格放置在不同的基础硬件上以减少相关的故障。

创建置放群组无需支付费用。

置放群组策略

您可以使用以下一种置放策略创建置放群组。

集群置放群组

集群置放群组是单个可用区中的实例的逻辑分组。集群置放群组可横跨同一区域中的对等虚拟专用网络（VPC）。同一集群置放群组中的实例可针对 TCP/IP 流量享受更高的每流吞吐量限制，并且这些实例将处于网络的同一高等分带宽段中。

下图显示放入集群置放群组中的实例。



建议将集群置放群组用于可受益于低网络延迟和/或高网络吞吐量的应用程序。如果大部分网络流量在组中的实例之间进行，也建议使用集群置放群组。要为置放群组提供最低延迟和最高每秒数据包数的网络性能，请选择支持增强联网的实例类型。有关更多信息，请参阅增强联网 (p. 1142)。

我们建议您按照以下方法启动您的实例：

- 使用单个启动请求在置放群组中启动所需的实例数。
- 对置放群组中的所有实例使用相同的实例类型。

如果您以后尝试将更多实例添加到置放群组，或者如果您尝试在置放群组中启动多个实例类型，都会增大发生容量不足错误的可能性。

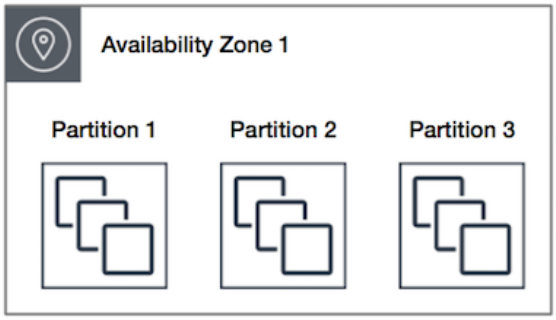
如果您停止置放群组中的某个实例，然后重启该实例，则其仍将在该置放群组中运行。但是，如果没有足够容量可用于该实例，则启动将会失败。

如果您在已有正在运行的实例的置放群组中启动实例时接收到容量错误信息，请在该置放群组中停止并启动所有实例，然后尝试再次启动。启动实例可能会将实例迁移至具有针对所有请求实例的容量的硬件。

分区置放群组

分区置放群组可帮助您的应用程序减少相关硬件故障的可能性。在使用分区置放群组时，Amazon EC2 将每个群组划分为多个逻辑段（称为“分区”）。Amazon EC2 确保置放群组中的每个分区具有自己的一组机架。每个机架具有自己的网络和电源。置放群组中的任何两个分区将不会分享相同的机架，从而让您可以在您的应用程序中隔离硬件故障的影响。

下图是单个可用区中的分区置放群组简单的直观表示。它显示了放入到一个分区置放群组的实例，该置放群组具有三个分区 — 分区 1、分区 2 和 分区 3。每个分区均包含多个实例。一个分区中的实例不与其他分区中的实例共享机架，这使您可以将单一硬件故障的影响限定在相关的分区内。



可使用分区置放群组跨不同机架部署大型分布式和重复的工作负载，例如 HDFS、HBase 和 Cassandra。当您在分区置放群组中启动实例时，Amazon EC2 将尝试跨您指定数量的分区均匀分发实例。您还可以在特定分区中启动实例，以更好地控制实例的放置位置。

分区置放群组可以在同一区域的多个可用区中具有分区。对于每个可用区，一个分区置放群组最多可具有 7 个分区。可在分区置放群组启动的实例的数量仅受账户限制的限制。

此外，分区置放群组提供对分区的可见性，您可以查看哪些实例位于哪些分区中。您可以与具有感知技术能力的应用程序共享此信息，例如 HDFS、HBase 和 Cassandra。这些应用程序使用此信息做出智能数据复制决策，用于提升数据的可用性和持久性。

如果在一个分区置放群组中启动一个实例，而没有足够的独特硬件来满足请求，则请求将失败。Amazon EC2 会随着时间的推移提供更多不同的硬件，因此，您稍后可以重试请求。

分布置放群组

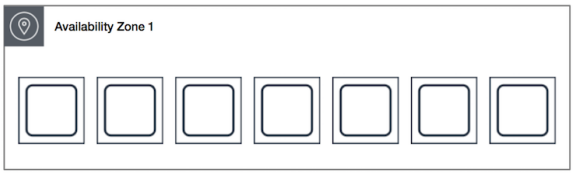
分布置放群组是将实例分别置放在不同硬件上的实例群组。

建议在具有少量应单独放置的重要实例的应用程序中使用分布置放群组。通过在分布置放群组中启动实例，可以降低在实例位于同一设备中时同时出现故障的风险。分布置放群组使用不同的硬件，因而适合混用不同类型的实例或随着时间推移逐步启动实例的场景。

如果在一个排列置放群组中启动一个实例，而没有足够的独特硬件来满足请求，则请求将失败。Amazon EC2 会随着时间的推移提供更多不同的硬件，因此，您稍后可以重试请求。置放群组可以跨机架或主机分布实例。主机级别分布置放群组只能用于 Amazon Outposts。

机架级别分布置放群组

下图显示单个可用区中的 7 个实例，这些实例已放入一个分布置放群组。将七个实例置放在七个不同的机架上，每个机架都具有自己的网络和电源。



机架分布置放群组可以跨越同一区域中的多个可用区。对于机架分布置放群组，每个群组在每个可用区中最多可以运行七个实例。

主机级别分布置放群组

主机级别置放群组仅适用于 Amazon Outposts。对于主机级别分布置放群组，每个 Outpost 上可运行的实例数量没有限制。有关更多信息，请参阅the section called “Amazon Outposts 上的置放群组” (p. 1191)。

置放群组规则和限制

主题

- 一般规则和限制 (p. 1179)
- 集群置放群组规则和限制 (p. 1179)
- 分区置放群组规则和限制 (p. 1180)
- 分布置放群组规则和限制 (p. 1180)

一般规则和限制

在使用置放群组之前，请注意以下规则：

- 在每个区域中，最多可以为每个账户创建 500 个置放群组。
- 您为置放群组指定的名称在您的区域 Amazon 账户中必须是唯一的。
- 不能合并置放群组。
- 一次可在一个置放群组中启动一个实例；实例不能跨多个置放群组。
- 按需容量预留 (p. 540) 和 zonal 预留实例 (p. 410) 为特定的可用区中的 EC2 实例提供容量预留。置放群组中的实例可以使用容量预留。使用带有容量预留的集群置放群组时，建议您在集群置放群组内预留容量。有关更多信息，请参阅集群置放群组中的容量预留。

  可用区预留实例 (p. 410)在特定的可用区中提供实例容量预留。置放群组中的实例可以使用容量预留。但是，您无法使用可用区预留实例为置放群组显式预留容量。
- 您无法在置放群组中启动专用主机。

集群置放群组规则和限制

以下规则适用于集群置放群组：

- 支持以下实例类型：

  - 当前一代 (p. 239)实例，但可突增性能 (p. 274)实例（例如 T2）除外。
  - 以下上一代 (p. 244)实例：A1、C3、cc2.8xlarge、cr1.8xlarge、G2、hs1.8xlarge、I2 和 R3。
- 一个集群置放群组不能跨过多个可用区。
- 集群置放群组中的两个实例之间的最大网络吞吐量流量速度受两个实例中的较慢实例限制。对于具有高吞吐量要求的应用程序，请选择其网络连接满足您要求的实例类型。
- 对于启用了增强联网的实例，以下规则适用：
  - 对于单个流的流量，集群置放群组中的实例最多可以使用 10 Gbps。对于单个流的流量，不在集群置放群组中的实例最多可以使用 5 Gbps。
  - 在同一个区域中，通过公有 IP 地址空间或者通过 VPC 终端节点往返于 Amazon S3 存储桶之间的流量可以使用所有可用的实例聚合带宽。
- 您可以将多种类型的实例启动到集群置放群组中。不过，这会降低提供所需容量以成功完成启动的可能性。我们建议集群置放群组中的所有实例使用相同的实例类型。
- 指向 Internet 的网络流量以及通过 Amazon Direct Connect 连接指向本地资源的流量限制为 5 Gbps。

分区置放群组规则和限制

以下规则适用于分区置放群组：

- 对于每个可用区，一个分区置放群组最多支持 7 个分区。您可在分区置放群组中启动的实例的数量仅受账户限制的限制。
- 当您在分区置放群组中启动实例时，Amazon EC2 将尝试跨所有分区均匀分发实例。Amazon EC2 不保证跨所有分区均匀分发实例。
- 具有 专用实例 的分区置放群组最多可具有 2 个分区。
- 容量预留不会在分区放置组中预留容量。

分布置放群组规则和限制

以下规则适用于分布置放群组：

- 机架分布置放群组最多支持在每个可用区运行七个实例。例如，在具有三个可用区的区域中，您可以在组中总共运行 21 个实例，每个可用区 7 个实例。如果您尝试在同一可用区和同一个分布置放群组中启动第八个实例，则该实例将无法启动。如果需要在一个可用区中运行超过七个实例，则建议使用多个分布置放群组。使用多个分布置放群组并不能保证实例在群组之间分布，但可帮助确保每个群组内的分布，从而限制某些故障类别的影响。
- 专用实例 不支持分布置放群组。
- 主机级别分布置放群组仅适用于 Amazon Outposts 上的置放群组。主机级别分布置放群组对于可运行的实例数量没有限制。
- 容量预留不会在分布放置组中预留容量。

使用置放群组

目录

- 创建置放群组 (p. 1181)
- 标记置放群组 (p. 1182)
- 在置放群组中启动实例 (p. 1184)
- 描述置放群组中的实例 (p. 1185)

- 更改实例的置放群组 (p. 1186)
- 删除置放群组 (p. 1187)

创建置放群组

您可以使用以下一种方法创建置放群组。

Note

您只能在创建时使用命令行工具标记置放群组。

Console

使用控制台创建置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Placement Groups (置放群组)，然后选择 Create placement group (创建置放群组)。
3. 指定群组的名称。
4. 选择适用于群组的置放策略。如果选择 Partition (分区)，则选择群组中的分区数。

   选择适用于群组的置放策略。

   - 如果选择 Spread（分布），则需要选择分布级别。
     - Rack（机架）– 无限制
     - Host（主机）– 仅适用于 Outposts
   - 如果选择 Partition (分区)，则选择群组中的分区数。
5. 要标记置放群组，请选择 Add tag（添加标签），然后输入键和值。为每个要添加的标签选择 Add tag（添加标签）。
6. 选择创建组。

Amazon CLI

使用 Amazon CLI 创建置放群组

使用 create-placement-group 命令。以下示例创建一个名为 `my-cluster` 的置放群组，它使用 `cluster` 放置策略，并应用键为 `purpose` 且值为的 `production` 标签。

```
aws ec2 create-placement-group --group-name my-cluster --strategy cluster --tag-
specifications 'ResourceType=placement-group,Tags={Key=purpose,Value=production}'
```

使用 Amazon CLI 创建分区置放群组

使用 create-placement-group 命令。使用 `--strategy` 值指定 `partition` 参数，并使用所需分区数指定 `--partition-count` 参数。在此示例中，分区置放群组名为 `HDFS-Group-A`，并包含 5 个分区。

```
aws ec2 create-placement-group --group-name HDFS-Group-A --strategy partition --
partition-count 5
```

PowerShell

使用 Amazon Tools for Windows PowerShell 创建置放群组

使用 New-EC2PlacementGroup 命令。

标记置放群组

要对现有置放群组进行分类和管理，可以使用自定义元数据标记它们。有关标签的工作原理的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

当您标记置放群组时，不会自动标记启动到置放群组中的实例。您需要显式标记启动到置放群组中的实例。有关更多信息，请参阅在启动实例时添加标签 (p. 1671)。

您可以使用新 的控制台和命令行工具查看、添加和删除标签。

New console

您可以使用以下方法之一查看、添加和删除标签。

Console

查看、添加或删除现有置放群组的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
3. 在导航窗格中，选择 Placement Groups。
4. 选择置放群组，然后依次选择 Actions (操作)、Manage tags (管理标签)。
5. Manage tags (管理标签) 部分显示分配给置放群组的所有标签。执行以下操作以添加或删除标签：
   - 要添加标签，请选择 Add tag (添加标签)，然后输入标签键和值。每个置放群组最多可添加 50 个标签。有关更多信息，请参阅标签限制 (p. 1668)。
   - 要删除标签，请选择要删除的标签旁边的 Remove (删除)。
6. 选择 Save changes（保存更改）。

Amazon CLI

查看置放群组标签

使用 describe-tags 命令可查看指定资源的标签。在以下示例中，您描述所有置放群组的标签。

```
aws ec2 describe-tags \
    --filters Name=resource-type,Values=placement-group
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        },
        {
            "Key": "Environment",
            "ResourceId": "pg-9876543210EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
```

```
}
```

还可以使用 describe-tags 命令通过指定置放群组 ID 来查看置放群组的标签。在以下示例中，您将描述 pg-0123456789EXAMPLE 的标签。

```
aws ec2 describe-tags \

    --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

还可以通过描述置放群组来查看置放群组的标签。

使用 describe-placement-groups 命令可查看指定置放群组的配置，其中包括为置放群组指定的任何标签。

```
aws ec2 describe-placement-groups \
    --group-name my-cluster
```

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

使用 Amazon CLI 标记现有置放群组

可以使用 create-tags 命令标记现有的资源。在以下示例中，使用 Key=Cost-Center 和 Value=CC-123 标记现有置放群组。

```
aws ec2 create-tags \
    --resources pg-0123456789EXAMPLE \
    --tags Key=Cost-Center,Value=CC-123
```

使用 Amazon CLI 从置放群组中删除标签

您可以使用 delete-tag 命令从现有资源中删除标签。有关示例，请参阅 Amazon CLI Command Reference 中的示例。

PowerShell

查看置放群组标签

使用 Get-EC2Tag 命令。

描述特定置放群组的标签

使用 Get-EC2PlacementGroup 命令。

标记现有置放群组

使用 New-EC2Tag 命令。

从置放群组中删除标签

使用 Remove-EC2Tag 命令。

在置放群组中启动实例

如果使用以下一种方法满足置放群组规则和限制 (p. 1180)，则可以在置放群组中启动实例。

Console

使用控制台将实例启动到置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从 EC2 控制台控制面板中，在 Launch instance（启动实例）框中，选择 Launch instance（启动实例），然后从显示的选项中选择Launch instance（启动实例）。根据提示填写表单，注意完成以下操作：
   - 在 Instance type（实例类型）下，选择可以启动到置放群组中的实例类型。
   - 在 Number of instances（实例数）下的 Summary（汇总）框中，输入该置放群组中需要的实例总数，因为此后可能无法向其中添加实例。
   - 在 Advanced details（高级详细信息）下，对于 Placement group name（置放群组名称），您可以选择将实例添加到某个新置放群组或现有置放群组。如果选择具有分区策略的置放群组，则对于 Target partition（目标分区），选择要在其中启动实例的分区。

Old Console

使用控制台将实例启动到置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择 Launch Instance（启动实例）。按指示完成向导，注意执行以下操作：

   从 EC2 控制台控制面板中，在 Launch instance（启动实例）框中，选择 Launch instance（启动实例），然后从显示的选项中选择Launch instance（启动实例）。按指示完成向导，注意执行以下操作：

   - 在 Choose an Instance Type 页面上，选择可以启动到置放群组中的实例类型。
   - 在 Configure Instance Details (配置实例详细信息) 页面上，以下字段适用于置放群组：
     - 在 Number of instances (实例数) 中，输入您在该置放群组中所需的实例总数，因为您以后可能无法向其中添加实例。
     - 对于 Placement group (置放群组)，选择 Add instance to placement group (向置放群组添加实例) 复选框。如果您在此页面上没有看到置放群组，请确认您是否已选择可启动到置放群组的实例类型。否则，此选项不可用。

- 对于 Placement group name (置放群组名称)，您可以选择将实例添加到现有置放群组，或者添加到您创建的新置放群组。
- 对于 Placement group strategy (置放群组策略)，选择适当的策略。如果您选择 partition (分区)，则对于 Target partition (目标分区)，选择 Auto distribution (自动分配) 以让 Amazon EC2 尽可能在群组的所有分区中平均地分配实例。或者指定要在其中启动实例的分区。

Amazon CLI

使用 Amazon CLI 在置放群组中启动实例

使用 run-instances 命令，并使用 `--placement "GroupName = my-cluster"` 参数指定置放群组名称。在此示例中，置放群组名为 `my-cluster`。

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

使用 Amazon CLI 在分区置放群组的特定部分中启动实例

使用 run-instances 命令，并使用 `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"` 参数指定置放群组名称和分区。在此示例中，置放群组名为 `HDFS-Group-A`，分区编号为 `3`。

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

使用 Amazon Tools for Windows PowerShell 在置放群组中启动实例

使用 New-EC2Instance 命令并使用 `-Placement_GroupName` 参数指定置放群组名称。

描述置放群组中的实例

您可以使用以下一种方法查看实例的置放信息。您还可以使用 Amazon CLI 按分区编号筛选分区置放群组。

Console

使用控制台查看实例的置放群组和分区编号

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 在 Details (详细信息) 选项卡中的 Host and placement group (主机和置放群组) 下，找到 Placement group (置放群组)。如果实例未在任何置放群组中，则此字段为空。否则，此字段将包含相应置放群组的名称。如果该置放群组是分区置放群组，则分区编号中将包含该实例的分区编号。

Amazon CLI

使用 Amazon CLI 查看分区置放群组中实例的分区编号

使用 describe-instances 命令并指定 `--instance-id` 参数。

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

响应包含置放信息，其中包含实例的置放群组名称和分区编号。

```
"Placement": {
     "AvailabilityZone": "us-east-1c",
     "GroupName": "HDFS-Group-A",
     "PartitionNumber": 3,
     "Tenancy": "default"
}
```

使用 Amazon CLI 筛选特定分区置放群组和分区编号的实例

使用 describe-instances 命令并指定具有 `--filters` 和 `placement-group-name` 筛选条件的 `placement-partition-number` 参数。在此示例中，置放群组名为 `HDFS-Group-A`，分区编号为 `7`。

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-Group-A" "Name = placement-partition-number, Values = 7"
```

响应列出了位于指定置放群组的指定分区中的所有实例。以下示例输出仅显示所返回实例的实例 ID、实例类型和置放信息。

```
"Instances": [
                {
                    "InstanceId": "i-0a1bc23d4567e8f90",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
                    }

                {
                    "InstanceId": "i-0a9b876cd5d4ef321",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
                    }
             ],
```

更改实例的置放群组

您可以通过以下任一方法更改实例的置放群组：

- 将现有实例移动到置放群组
- 将实例从一个置放群组移动到另一个置放群组
- 从置放群组中删除实例

在移动或删除实例之前，实例必须处于 `stopped` 状态。您可以使用 Amazon CLI 或 Amazon 开发工具包移动或删除实例。

Amazon CLI

使用 Amazon CLI 将实例移动到置放群组

1. 使用 stop-instances 命令停止实例。
2. 使用 modify-instance-placement 命令，并指定要将实例移到的置放群组的名称。

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-
name MySpreadGroup
```

3. 使用 start-instances 命令启动实例。

PowerShell

使用 Amazon Tools for Windows PowerShell 将实例移动到置放群组

1. 使用 Stop-EC2Instance 命令停止实例。
2. 使用 Edit-EC2InstancePlacement 命令，并指定要将实例移到的置放群组的名称。
3. 使用 Start-EC2Instance 命令启动实例。

Amazon CLI

使用 Amazon CLI 从置放群组中删除实例

1. 使用 stop-instances 命令停止实例。
2. 使用 modify-instance-placement 命令，并为置放群组名称指定一个空字符串。

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name ""
```

3. 使用 start-instances 命令启动实例。

PowerShell

使用 Amazon Tools for Windows PowerShell 从置放群组中删除实例

1. 使用 Stop-EC2Instance 命令停止实例。
2. 使用 Edit-EC2InstancePlacement 命令，并为置放群组名称指定一个空字符串。
3. 使用 Start-EC2Instance 命令启动实例。

删除置放群组

如果您需要替换或不再需要某个置放群组，您可以将其删除。您可以使用以下一种方法删除置放群组。

要求

在删除置放群组之前，该群组中不能包含任何实例。您可以终止 (p. 636)在置放群组中启动的所有实例，将这些实例移动 (p. 1187)到另一个置放群组，或者将其从置放群组中删除 (p. 1187)。

Console

使用控制台删除置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Placement Groups。
3. 选择该置放群组，然后依次选择操作、删除。
4. 提示进行确认时，输入 **Delete**，然后选择 Delete（删除）。

Amazon CLI

使用 Amazon CLI 删除置放群组

使用 delete-placement-group 命令并指定置放群组名称以删除置放群组。在此示例中，置放群组名称为 my-cluster。

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

使用 Amazon Tools for Windows PowerShell 删除置放群组

使用 Remove-EC2PlacementGroup 命令删除置放群组。

共享置放群组

通过置放群组共享，您可以影响由单独 Amazon 账户拥有的相互依赖实例的置放。您可在多个 Amazon 账户之间或在您的 Amazon Organizations 内共享一个置放群组。您可在共享的置放群组中启动实例。

置放群组所有者可与以下人员共享置放群组：

- 其 Amazon 组织内部或外部的特定 Amazon 账户
- 其 Amazon 组织内的组织部门
- 其整个 Amazon 组织

Note

您要共享置放群组的 Amazon 账户必须在 IAM policy 中具有以下权限。

- `ec2:PutResourcePolicy`
- `ec2:DeleteResourcePolicy`

主题

- 规则和限制 (p. 1188)
- 跨可用区共享 (p. 1189)
- 共享置放群组 (p. 1189)
- 识别共享的置放群组 (p. 1189)
- 在共享的置放群组中启动实例 (p. 1190)
- 将共享置放群组取消共享 (p. 1191)

规则和限制

当您共享置放群组或与您共享置放群组时，请遵循以下规则和限制。

- 要共享置放群组，您必须在您的 Amazon 账户中拥有该置放群组。无法共享已与您共享的置放群组。
- 共享分区或扩展分布置放群组时，置放群组限制不会改变。共享分区置放群组支持每个可用区最多七个分区，共享分布置放群组支持每个可用区最多七个运行实例。
- 要与您的 Amazon 组织或 Amazon 组织内的组织部门共享置放群组，您必须允许与 Amazon Organizations 共享。有关更多信息，请参阅共享 Amazon 资源。
- 您负责管理共享置放群组中您拥有的实例。
- 您无法查看或修改与共享置放群组有关但不属于您的实例和容量预留。

跨可用区共享

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的名称。这可能会导致账户之间的可用区命名差异。例如，您的 `us-east-1a` 账户的可用区 Amazon 可能与另一 `us-east-1a` 账户的 Amazon 不在同一位置。

要确定专用主机相对于账户的位置，您必须使用可用区 ID (AZ ID)。可用区 ID 是跨所有 Amazon 账户的可用区的唯一且一致的标识符。例如，`use1-az1` 是 `us-east-1` 区域的可用区 ID，它在每个 Amazon 账户中的位置均相同。

查看账户中的可用区的可用区 ID：

1. 通过以下网址打开 Amazon RAM 控制台：https://console.aws.amazon.com/ram。
2. 当前区域的可用区 ID 显示在右侧面板的 Your AZ ID（您的可用区 ID）下。

共享置放群组

要共享置放群组，您必须将其添加到资源共享。资源共享是一项 Amazon RAM 资源，可让您跨 Amazon 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。

如果您属于 Amazon Organizations 中的某个组织并且已在您的组织中启用共享，则组织中的使用者将获得对共享置放群组的访问权限。

如果将置放群组与您组织以外的 Amazon 账户共享，则 Amazon 账户所有者将会收到加入资源共享的邀请。他们可在接受邀请后访问共享的置放群组。

您可以使用 https://console.aws.amazon.com/ram 或 Amazon CLI，跨 Amazon 账户共享置放群组。

Amazon RAM console

要使用 https://console.aws.amazon.com/ram 共享您拥有的置放群组，请参阅 Creating a resource share（创建资源共享）。

Amazon CLI

要共享您拥有的置放群组，请使用 create-resource-share 命令。

识别共享的置放群组

您可通过 https://console.aws.amazon.com/ec2/ 或 Amazon CLI 识别与您共享的置放群组。

Amazon EC2 console

1. 打开：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Placement Groups（置放群组）。

3. 右侧的 Placement Groups（置放群组）屏幕列出了您拥有的和与您共享的所有置放群组。置放群组的 Amazon Resource Name（ARN）[Amazon 资源名称（ARN）] 包含其所有者的详细信息。

Amazon CLI

describe-placement-groups 命令列出了您拥有的和与您共享的所有置放群组。置放群组的 Amazon Resource Name（ARN）[Amazon 资源名称（ARN）] 包含其所有者的详细信息。

在共享的置放群组中启动实例

Important

您必须指定置放群组的 Group Id（群组 ID），才能在共享置放群组中启动实例。

只有当您是正在共享的置放群组的所有者时，才能使用置放群组名称。我们建议使用置放群组 Group Id（群组 ID）来避免 Amazon 账户之间潜在的置放群组名称冲突。

您可使用 describe-placement-groups 命令，也可在 Network & Security（网络与安全）下的 Placement Groups（置放群组）屏幕上的 https://console.aws.amazon.com/ec2/ 中找到置放群组的群组 ID。

Amazon EC2 Console

使用控制台将实例启动到置放群组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择 Launch Instance（启动实例）。按指示完成向导，注意执行以下操作：
   - 在 Choose an Instance Type 页面上，选择可以启动到置放群组中的实例类型。
   - 在 Configure Instance Details (配置实例详细信息) 页面上，以下字段适用于置放群组：
     - 在 Number of instances (实例数) 中，输入您在该置放群组中所需的实例总数，因为您以后可能无法向其中添加实例。
     - 对于 Placement group (置放群组)，选择 Add instance to placement group (向置放群组添加实例) 复选框。如果您在此页面上没有看到置放群组，请确认您是否已选择可启动到置放群组的实例类型。否则，此选项不可用。
     - 对于 Placement group name (置放群组名称)，您可以选择将实例添加到现有置放群组，或者添加到您创建的新置放群组。
     - 对于 Placement group strategy (置放群组策略)，选择适当的策略。如果您选择 partition (分区)，则对于 Target partition (目标分区)，选择 Auto distribution (自动分配) 以让 Amazon EC2 尽可能在群组的所有分区中平均地分配实例。或者指定要在其中启动实例的分区。

Amazon CLI

在共享置放群组中启动实例

使用 run-instances 命令并指定置放群组的 Group Id（群组 ID）。

```
aws ec2 run-instances –placement "GroupId = pg-01234567891011121"
```

在分区置放群组的特定分区中启动实例

使用 run-instances 命令并指定共享置放群组的 Group Id（群组 ID）和 PartitionNumber。

```
aws ec2 run-instances –placement "GroupId = pg-01234567891011121, PartitionNumber = 3"
```

Tip

使用 VPC 对等连接独立 Amazon 账户拥有的实例，并获得共享集群置放群组提供的全部延迟优势。有关更多信息，请参阅什么是 VPC 对等连接？

将共享置放群组取消共享

置放群组所有者随时可以将共享置放群组取消共享。

将共享置放群组取消共享时，以下更改将生效。

- 与之共享置放群组的 Amazon 账户将无法再启动实例或预留容量。
- 如果您的实例正在共享置放群组中运行，则其将与该置放群组断开关联，但会继续在您的 Amazon 账户中正常运行。
- 如果您在共享置放群组中进行了容量预留，则这些预留容量将与该置放群组断开关联，但您可以继续在您的 Amazon 账户中对其进行访问。

您可以使用以下方法之一将共享置放群组取消共享。

Amazon RAM console

要使用 https://console.aws.amazon.com/ram 将共享置放群组取消共享，请参阅 Deleting a resource share（删除资源共享）。

Amazon CLI

要使用 Amazon Command Line Interface 将共享置放群组取消共享，请使用 `disassociate-resource-share` 命令。

Amazon Outposts 上的置放群组

Amazon Outposts 是一项完全托管的服务，可将 Amazon 基础设施、服务、API 和工具扩展到客户场所。通过提供对 Amazon 托管基础设施的本地访问，Amazon Outposts 使客户能够使用与 Amazon 区域中相同的编程接口在本地构建和运行应用程序，同时使用本地计算和存储资源来满足更低的延迟和本地数据处理需求。

Outpost 是部署在客户站点的 Amazon 计算和存储容量池。Amazon 作为 Amazon 区域的一部分运营、监控和管理此容量。

您可以在您在账户中创建的 Outpost 上创建置放群组。从而将实例分布在您站点中的 Outpost 上的底层硬件上。在 Outpost 上创建和使用置放群组的方式与您在常规可用区中创建和使用置放群组时相同。当您在 Outpost 上创建具有分布策略的置放群组时，您可以选择让置放群组跨主机或机架分布实例。跨主机分布实例允许您使用具有单个机架 Outpost 的分布策略。

先决条件

您的站点必须安装一个 Outpost。有关更多信息，请参阅 Amazon Outposts 用户指南中的创建 Outpost 并订购 Outpost 容量。

在 Outpost 上使用置放群组

1. 在 Outpost 上创建子网。有关更多信息，请参阅 Amazon Outposts 用户指南中的创建子网。
2. 在与该 Outpost 关联的区域中创建一个置放群组。如果您创建具有分布策略的置放群组，则可以选择主机或机架分布级别，以确定该群组将如何在 Outpost 上的底层硬件之间分布实例。有关更多信息，请参阅the section called “创建置放群组” (p. 1181)。

3. 将一个实例启动到置放群组。对于 Subnet（子网），选择您在第 1 步中创建的子网，然后对于 Placement group name（置放群组名称），选择您在第 2 步中创建的置放群组。有关更多信息，请参阅 Amazon Outposts 用户指南中的在 Outpost 中启动实例。

EC2 实例的网络最大传输单位 (MTU)

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小 (以字节为单位)。连接的 MTU 越大，可在单个数据包中传递的数据越多。以太网帧由数据包（即您发送的实际数据）以及相关网络开销信息组成。

以太网帧有不同的格式，最常见的格式是标准以太网 v2 帧格式。它支持 1500 MTU，这是大部分 Internet 上支持的最大以太网数据包大小。实例支持的最大 MTU 取决于其实例类型。

以下规则适用于 Wavelength 区域中的实例：

- 在同一个 Wavelength 区域中的 VPC 内，从一个实例到另一个实例的流量的 MTU 为 1300。
- 在 Wavelength 区域内，从一个实例到另一个使用运营商 IP 的实例的流量的 MTU 为 1500。
- 在 Wavelength 区域和使用公有 IP 地址的区域之间从一个实例到另一个实例的流量的 MTU 为 1500。
- 在 Wavelength 区域和使用私有 IP 地址的区域之间从一个实例到另一个实例的流量的 MTU 为 1300。

要查看 Windows 实例的网络 MTU 信息，请转到 Amazon EC2 用户指南（适用于 Windows 实例）指南中的此页面：EC2 实例的网络最大传输单位 (MTU)。

目录

- 巨型帧 (9001 MTU) (p. 1192)
- 路径 MTU 发现 (p. 1193)
- 查看两个主机之间的路径 MTU (p. 1193)
- 在您的 Linux 实例上检查并设置 MTU (p. 1194)
- 问题排查 (p. 1194)

巨型帧 (9001 MTU)

巨型帧通过增加每个数据包的负载大小，从而增加数据包中不属于数据包开销的百分比来支持 1500 个字节以上的数据。发送等量的可用数据所需要的数据包更少。但是，在以下情况下，流量限制为最大 MTU 为 1500：

- 互联网网关流量
- 区域间 VPC 对等连接中的流量
- VPN 连接的流量
- EC2-Classic 给定 Amazon 区域外的流量

如果数据包大于 1500 字节，则对数据包进行分段；如果在 IP 标头中设置了 `Don't Fragment` 标记，则丢弃数据包。

对于面向 Internet 的流量或离开 VPC 的任何流量，应谨慎使用巨型帧。中间系统会对数据包进行分段，从而减缓此流量。要使用 VPC 中的巨型帧而不减慢 VPC 外部的绑定流量的速度，您可按路由配置 MTU 大小，或者将弹性网络接口与不同 MTU 大小和不同路由结合使用。

对于在集群置放群组中并置的实例，巨型帧有助于实现可能的最大网络吞吐量，建议在这种情况下使用这些帧。有关更多信息，请参阅置放群组 (p. 1177)。

您可以通过 Amazon Direct Connect 使用巨型帧在 VPC 与本地网络之间进行通信。有关更多信息以及如何验证巨型帧功能，请参阅 Amazon Direct Connect 用户指南中的设置网络 MTU。

所有 Amazon EC2 实例类型都支持 1500 MTU，所有当前一代实例类型 (p. 247)都支持巨型帧。下列前一代实例类型支持巨型帧：A1、C3、G2、I2、M3 和 R3。

有关中转网关支持的 MTU 大小的更多信息，请参阅 Amazon VPC 中转网关 中的 MTU。

路径 MTU 发现

路径 MTU 发现 (PMTUD) 用于确定两台设备之间的路径 MTU。路径 MTU 是原始主机和接收主机之间的路径所支持的最大数据包大小。当两个主机的网络中 MTU 大小存在差异时，PMTUD 使接收主机能够使用 ICMP 消息响应原始主机。此 ICMP 消息将指示原始主机在网络路径中使用最低 MTU 大小并重新发送请求。若无此协商，当请求过大，导致接收主机无法接收时，数据包可能会丢失。

对于 IPv4，如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机或设备将删除此数据包，然后返回以下 ICMP 消息：`Destination Unreachable: Fragmentation Needed and Don't Fragment was Set`（类型 3，代码 4）。这将指示传输主机将有效负载拆分为多个较小的数据包，然后重新传输。

IPv6 协议不支持网络中的分段。如果主机发送一个大于接收主机的 MTU 或大于路径上某台设备的 MTU 的数据包，则接收主机或设备将删除此数据包，然后返回以下 ICMP 消息：`ICMPv6 Packet Too Big (PTB)`（类型 2）。这将指示传输主机将有效负载拆分为多个较小的数据包，然后重新传输。

默认情况下，安全组不允许任何入站 ICMP 流量。如果您没有为安全组显式配置 ICMP 入站规则，PMTUD 则将被阻止。有关在网络 ACL 中配置 ICMP 规则的更多信息，请参阅 Amazon VPC 用户指南 中的路径 MTU 发现。

> **Important**
>
> 路径 MTU 发现不能保证某些路由器不丢弃巨型帧。您 VPC 中的互联网网关仅将转发最多 1500 字节的数据包。建议对 Internet 流量使用 1500 MTU 数据包。

查看两个主机之间的路径 MTU

您可使用 tracepath 命令查看两个主机之间的路径 MTU，此命令是很多 Linux 发行版默认情况下提供的 `iputils` 程序包的一部分，包括 Amazon Linux）。

使用 tracepath 检查路径 MTU

使用以下命令检查您的 EC2 实例与另一个主机之间的路径 MTU。可以使用 DNS 名称或 IP 地址作为目的地。如果目的地是另一个 EC2 实例，则验证安全组是否允许入站 UDP 流量。本例检查 EC2 实例和 `amazon.com` 之间的路径 MTU。

```
[ec2-user ~]$ tracepath amazon.com
 1?: [LOCALHOST]      pmtu 9001
 1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  100.64.16.241 (100.64.16.241)                              0.574ms
 5:  72.21.222.221 (72.21.222.221)                             84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                           79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                             96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                             79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                           91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

在此示例中，路径 MTU 为 1500。

在您的 Linux 实例上检查并设置 MTU

一些实例配置为使用巨型帧，另一些则配置为使用标准帧大小。您可能希望将巨型帧用于您的 VPC 内的网络流量，或希望将标准帧用于 Internet 流量。无论您的使用案例如何，我们建议验证您的实例是否会按您的预期运行。您可以使用本部分中的过程查看您的网络接口的 MTU 设置并按需对其进行修改。

查看 Linux 实例上的 MTU 设置

您可使用以下 ip 命令检查当前 MTU 值。请注意，在示例输出中，*mtu 9001* 指示此实例使用了巨型帧。

```
[ec2-user ~]$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode DEFAULT
 group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

在 Linux 实例上设置 MTU 值

1. 可以使用 ip 命令设置 MTU 值。以下命令将预期 MTU 值设置为 1500，但是您可以使用 9001 代替。

   ```
   [ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
   ```

2. (可选) 要在重启后保留您的网络 MTU 设置，请根据您的操作系统类型修改配置文件。

   - 对于 Amazon Linux 2，将以下一行添加到 `/etc/sysconfig/network-scripts/ifcfg-eth0` 文件：

     ```
     MTU=1500
     ```

     将以下行添加到 `/etc/dhcp/dhclient.conf` 文件：

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name, domain-
     search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-servers;
     ```

   - 对于 Amazon Linux，将以下几行添加到 `/etc/dhcp/dhclient-eth0.conf` 文件。

     ```
     interface "eth0" {
     supersede interface-mtu 1500;
     }
     ```

   - 对于其他 Linux 发行版，请参阅其具体文档。

3. (可选) 重启实例并验证 MTU 设置是否正确。

问题排查

如果在使用巨型帧时您的 EC2 实例和 Amazon Redshift 集群之间出现连接问题，请参阅《Amazon Redshift Management 指南》中的查询挂起

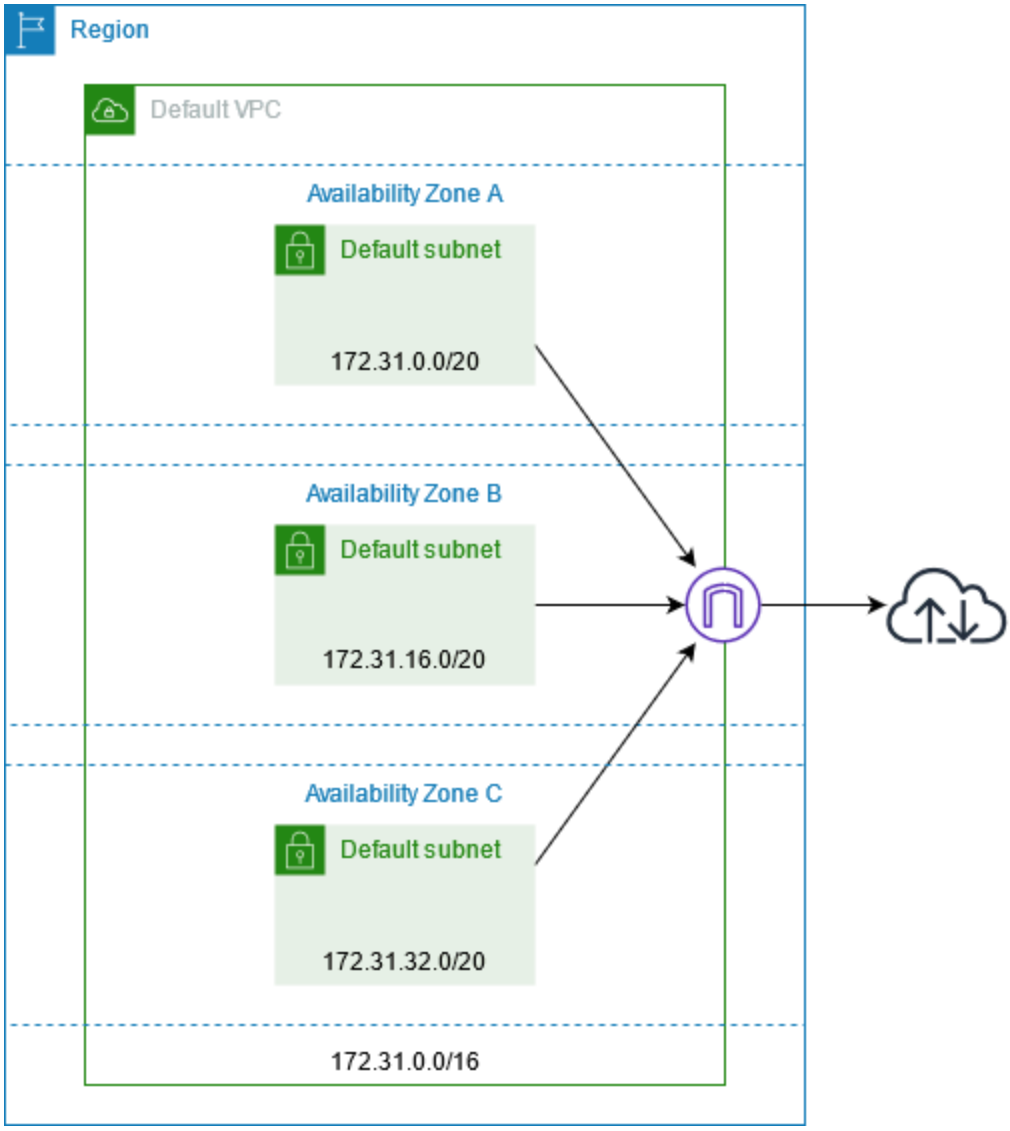
Virtual Private Cloud

通过 Amazon Virtual Private Cloud (Amazon VPC)，您可以在 Amazon 云内您自己的逻辑隔离区域中定义虚拟网络，我们称之为 Virtual Private Cloud 或 VPC。您可将 Amazon 资源（如 Amazon EC2 实例）创建

到 VPC 的子网中。您的 VPC 与您在自己的数据中心中运行的传统网络可能极为相似，同时享有使用来自 Amazon 的可扩展基础设施的优势。您可以配置您的 VPC；您可以选择它的 IP 地址范围、创建子网并配置路由表、网关和安全设置。现在您可以将您的 VPC 中的实例连接到 Internet 或您自己的数据中心。

您的默认 VPC

在您创建 Amazon 账户时，我们会在每个区域中创建一个默认 VPC。默认 VPC 是已配置好可供您使用的 VPC。例如，在每个默认 VPC 中，每个可用区都有一个默认子网，一个连接到 VPC 的互联网网关，并且主路由表中有一条将所有流量 (0.0.0.0/0) 发送到互联网网关的路由。或者，您也可以创建自己的 VPC 并对其进行配置，以满足您的需要。



创建额外的 VPC

使用以下过程创建具有所需子网、网关和路由配置的 VPC。

创建 VPC

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。

2. 选择 Create VPC（创建 VPC）。
3. 在要创建的 Resources（资源）下，选择 VPC and more（VPC 等）。
4. 对于 Name tag auto-generation（名称标签自动生成），为 VPC 输入名称。
5. 对于 IPv4 CIDR block（IPv4 CIDR 块），要么保留默认建议，要么输入应用程序或网络所需的 CIDR 块。
6. 对于 Number of Availability Zones（可用区数量），选择 2，以便您可以在多个可用区中启动实例，以确保高可用性。
7. 如果必须可从互联网访问您的实例，请执行以下操作之一：
   - 如果您的实例可以位于公共子网中，请为 Number of public subnets（公共子网数量）选择一个非零值。保持 DNS options（DNS 选项）下的两个选项处于选中状态。您可以选择立即或稍后添加私有子网。
   - 如果您的实例必须位于私有子网中，请为 Number of public subnets（公共子网数量）选择 0。对于 Number of private subnets（私有子网数量），根据您的需要选择一个数字（可能的值对应于每个可用区 1 或 2 个私有子网）。对于 NAT gateways（NAT 网关），如果您的两个可用区中的实例跨可用区发送或接收大量流量，请选择 1 per AZ（每个可用区 1 个）。否则，请选择 In 1 AZ（在 1 个可用区中），并启动在与 NAT 网关相同的可用区中发送或接收跨区域流量的实例。
8. 展开 Customize subnet CIDR blocks（自定义子网 CIDR 块）。要么保留默认建议，要么为每个子网输入一个 CIDR 块。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网大小调整。
9. 查看 Preview（预览）窗格，该窗格显示将根据您的选择创建的 VPC 资源。
10. 选择 Create VPC（创建 VPC）。

从您的实例访问互联网

启动到默认子网的实例可以访问 Internet，因为 VPC 配置为分配公有 IP 地址和 DNS 主机名，而且主路由表配置了通往连接到 VPC 的互联网网关的路由。

对于在 VPC 中创建的子网，请执行以下操作之一，以确保在这些子网中启动的实例可以访问 Internet：

- 配置互联网网关。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关将子网连接到互联网。
- 配置公有 NAT 网关。有关更多信息，请参阅 Amazon VPC 用户指南中的从私有子网访问互联网。

对您的实例进行 SSH 访问

要连接到实例，您必须将 SSH 流量授权给来自您网络的实例。您还必须在启动实例时指定密钥对，并在连接到实例时指定 `.pem` 文件。有关更多信息，请参阅设置以连接到实例 (p. 645)。

EC2-Classic

> 我们即将停用 EC2-Classic。我们建议您从 EC2-Classic 迁移到 VPC (p. 1211)。

通过使用 EC2-Classic，您的实例会在一个可与其他客户共享的扁平化网络中运行。通过使用 Amazon VPC，您的实例会在一个逻辑上与 Amazon 账户分离的 Virtual Private Cloud（VPC）中运行。

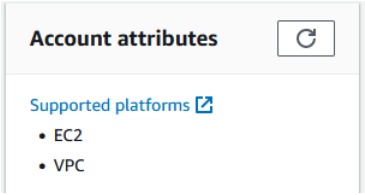
EC2-Classic 平台是在 Amazon EC2 的初始版本中引入的。如果您的 Amazon 账户是在 2013 年 12 月 4 日之后创建的，它不支持 EC2-Classic，因此您必须在 VPC 中启动您的 Amazon EC2 实例。

检测支持的平台

Amazon EC2 控制台会显示您在所选区域中可以启动实例的平台，以及您在该区域是否拥有默认 VPC。或者，您也可以使用 Amazon CLI 中的 describe-account-attributes 命令。

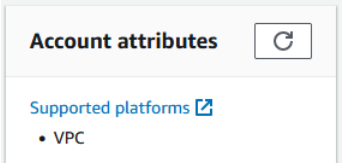
支持 EC2-Classic 的账户

选择区域并在控制面板上找到账户属性。下面的内容表示该账户支持 EC2-Classic。



需要 VPC 的账户

选择区域并在控制面板上找到账户属性。下面的内容表示该账户不支持 EC2-Classic。



EC2-Classic 中提供的实例类型

多数较新的实例类型都需要 VPC。以下是 EC2-Classic 中支持的唯一实例类型：

- 通用：M1、M3 和 T1
- 计算优化：C1、C3 和 CC2
- 内存优化：CR1、M2 和 R3
- 存储优化：D2、HS1 和 I2
- 加速计算：G2

如果您的账户支持 EC2-Classic，但您尚未创建非默认 VPC，您可以执行以下操作之一来启动需要 VPC 的实例：

- 在请求中指定子网 ID 或网络接口 ID，以便创建非默认 VPC 并将您的仅 VPC 实例启动至该 VPC。请注意，如果您没有默认的 VPC 并且使用 Amazon CLI、Amazon EC2 API 或 Amazon 软件开发工具包来启动仅限 VPC 的实例，则必须创建非默认 VPC。
- 使用 Amazon EC2 控制台启动仅 VPC 实例。Amazon EC2 控制台在您的账户中创建非默认 VPC 并将实例启动至第一个可用区中的子网。控制台将创建具有以下属性的 VPC：
  - 每个可用区中有一个子网，其公有 IPv4 地址属性设置为 `true`，因此实例会收到一个公有 IPv4 地址。有关更多信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 中的 IP 地址。
  - 一个 Internet 网关，以及一个将 VPC 中的流量路由到该 Internet 网关的主路由表。这使您在 VPC 中启动的实例可以在 Internet 上通信。有关更多信息，请参阅 Amazon VPC 用户指南 中的 Internet 网关。
  - VPC 的默认安全组和与每个子网关联的默认网络 ACL。有关更多信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 的安全组。

如果您在 EC2-Classic 中有其他资源，则可以采取措施将它们迁移到 VPC。有关更多信息，请参阅从 EC2-Classic 迁移到 VPC (p. 1211)。

EC2-Classic 和 VPC 中的实例之间的区别

下表总结了在 EC2-Classic、默认 VPC 以及非默认 VPC 这三种平台中启动的实例之间的区别。

特征	EC2-Classic	默认 VPC	非默认 VPC
公有 IPv4 地址 (来自 Amazon 的公有 IP 地址池)	您的实例从 EC2-Classic 公有 IPv4 地址池接收公有 IPv4 地址。	默认情况下，在默认子网中启动的实例会收到公有 IPv4 地址，除非您在启动过程中另行指定，或者您修改子网的公有 IPv4 地址属性。	默认情况下，您的实例不会收到公有 IPv4 地址，除非您在启动过程中另行指定，或者您修改子网的公有 IPv4 地址属性。
私有 IPv4 地址	您的实例会在每次启动时收到一个处于 EC2-Classic 范围内的私有 IPv4 地址。	您的实例会收到一个处于默认 VPC 地址范围内的静态私有 IPv4 地址。	您的实例会收到一个处于 VPC 地址范围内的静态私有 IPv4 地址。
多个私有 IPv4 地址	我们会为您的实例选择一个私有 IP 地址；不支持多个 IP 地址。	您可以将多个私有 IPv4 地址分配给您的实例。	您可以将多个私有 IPv4 地址分配给您的实例。
弹性 IP 地址 (IPv4)	当您停止实例时，弹性 IP 会取消与实例的关联。	当您停止实例时，弹性 IP 会保持与实例的关联。	当您停止实例时，弹性 IP 会保持与实例的关联。
分配弹性 IP 地址	将弹性 IP 地址与实例相关联。	弹性 IP 地址是网络接口的一个属性。您可以通过更新附加到实例的网络接口，将弹性 IP 地址与该实例关联起来。	弹性 IP 地址是网络接口的一个属性。您可以通过更新附加到实例的网络接口，将弹性 IP 地址与该实例关联起来。
取消关联弹性 IP 地址	如果弹性 IP 地址已经与其他实例关联，该地址会自动与新实例关联。	如果弹性 IP 地址已经与其他实例关联，该地址会自动与新实例关联。	如果弹性 IP 地址已经与其他实例关联，则只有您允许重新关联时该操作才会成功。
标记弹性 IP 地址	您不能将标签应用于弹性 IP 地址。	您可以将标签应用于弹性 IP 地址。	您可以将标签应用于弹性 IP 地址。
DNS 主机名	DNS 主机名默认处于启用状态。	DNS 主机名默认处于启用状态。	DNS 主机名默认处于禁用状态。
安全组	安全组可以引用属于其他 Amazon 账户的安全组。	安全组可以引用您的 VPC 的安全组，或者引用 VPC 对等连接中的对等 VPC 的安全组。	安全组只能引用您的 VPC 的安全组。
安全组关联	您不能更改正在运行的实例的安全组。您可以修改已分配的安全组的规则，或使用新实例予以替换 (从该实例中创建 AMI，通过此 AMI 启动带有您所需的安全组的新实例，取消任意弹性 IP 地址与原有实例的关联并将其与新实例关联起来，然后终止原有实例)。	您最多可以为一个实例分配 5 个安全组。 您可以在启动实例时和实例运行过程中为其分配安全组。	您最多可以为一个实例分配 5 个安全组。 您可以在启动实例时和实例运行过程中为其分配安全组。
安全组规则	您只能为入站流量添加规则。	您可以为入站和出站流量添加规则。	您可以为入站和出站流量添加规则。

特征	EC2-Classic	默认 VPC	非默认 VPC
Tenancy	您的实例在共享硬件上运行。	您可以在共享硬件或单租户硬件上运行您的实例。	您可以在共享硬件或单租户硬件上运行您的实例。
正在访问 Internet	您的实例可以访问 Internet。您的实例会自动接收公有 IP 地址，并且可以直接通过 Amazon 网络边界访问 Internet。	默认情况下，您的实例可以访问 Internet。您的实例默认会接收一个公有 IP 地址。一个 Internet 网关附加到您的默认 VPC，并且您的默认子网有一个到 Internet 网关的路由。	默认情况下，您的实例不能访问 Internet。您的实例默认不会接收公有 IP 地址。您的 VPC 可能有一个 Internet 网关，具体取决于它的创建方式。
IPv6 寻址	不支持 IPv6 寻址。您无法将 IPv6 地址分配给您的实例。	您可以选择将一个 IPv6 CIDR 块与 VPC 关联，并将 IPv6 地址分配给 VPC 中的实例。	您可以选择将一个 IPv6 CIDR 块与 VPC 关联，并将 IPv6 地址分配给 VPC 中的实例。

EC2-Classic 的安全组

如果要使用 EC2-Classic，则必须使用为 EC2-Classic 专门创建的安全组。当您在 EC2-Classic 中启动实例时，您必须在实例所在的相同区域内指定一个安全组。在 EC2-Classic 中启动实例时，您无法指定为 VPC 创建的安全组。

在 EC2-Classic 中启动实例后，您就不能再更改其安全组。不过，您可以向安全组添加或从中删除规则，并且这些更改会在经过一小段时间之后自动应用于与该安全组关联的所有实例。

您的 Amazon 账户在每个区域中都自动拥有一个 EC2-Classic 默认安全组。如果您尝试删除默认安全组，会显示以下错误：Client.InvalidGroup.Reserved: The security group 'default' is reserved (Client.InvalidGroup.Reserved: 保留“默认”安全组)。

您可以创建自定义安全组。安全组名称在您的区域账户中必须是唯一的。要创建在 EC2-Classic 中使用的安全组，请对 VPC 选择 No VPC (无 VPC)。

您可以对默认和自定义安全组添加入站规则。您无法更改 EC2-Classic 安全组的出站规则。创建安全组规则时，您可以在与源或目标相同的区域中使用其他 EC2-Classic 安全组。要为其他 Amazon 账户指定安全组，请添加 Amazon 账户 ID 作为前缀；例如 `111122223333/sg-edcd9784`。

在 EC2-Classic 中，您可以在每个区域为每个账户创建多达 500 个安全组。您最多可以为一个安全组添加 100 条规则。每个实例最多可拥有 800 个安全组规则。其计算方式为：每个安全组的规则数乘以每个实例的安全组数量。如果您在安全组规则中引用其他安全组，我们建议您使用长度不超过 22 个字符的安全组名称。

IP 寻址和 DNS

Amazon 提供了 DNS 服务器，可将 Amazon 提供的 IPv4 DNS 主机名解析为 IPv4 地址。在 EC2-Classic 中，此 Amazon DNS 服务器位于 `172.16.0.23`。

如果您在 EC2-Classic 中创建自定义防火墙配置，那么必须在您的防火墙中创建规则，以允许来自 Amazon DNS 服务器地址的端口 53 (DNS)（目标端口在临时范围内）的入站流量，否则，实例的内部 DNS 解析会失败。如果您的防火墙无法自动允许 DNS 查询响应，那么您就需要允许来自 Amazon DNS 服务器的 IP 地址的流量。要获取 Amazon DNS 服务器的 IP 地址，请在您的实例中使用以下命令：

```
grep nameserver /etc/resolv.conf
```

弹性 IP 地址

如果您的账户支持 EC2-Classic，则其中一个弹性 IP 地址池可用于 EC2-Classic 平台，而另一个可用于 VPC。您不能将已分配与 VPC 配合使用的弹性 IP 地址与 EC2-Classic 中的实例相关联，反之亦然。

分配可在 EC2-Classic 中使用的弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate Elastic IP address (分配弹性 IP 地址)。
4. 对于 Scope（范围），选择 EC2-Classic。
5. 选择 Allocate。

在 EC2-Classic 与 VPC 之间共享和访问资源

您的 Amazon 账户中的一些资源和功能可以在 EC2-Classic 与 VPC 平台之间共享或访问（例如，通过 ClassicLink）。有关更多信息，请参阅ClassicLink (p. 1201)。

如果您的账户支持 EC2-Classic，您可能已经设置在 EC2-Classic 中使用的资源。如果您要从 EC2-Classic 迁移到 VPC，则必须在 VPC 中重新创建这些资源。有关从 EC2-Classic 迁移到 VPC 的更多信息，请参阅从 EC2-Classic 迁移到 VPC (p. 1211)。

以下资源可在 EC2-Classic 与 VPC 之间共享或访问。

资源	备注
AMI	
捆绑任务	
EBS 卷	
弹性 IP 地址 (IPv4)	您可将弹性 IP 地址从 EC2-Classic 迁移至 VPC。您无法将本来分配为在 VPC 中使用的弹性 IP 地址迁移至 EC2-Classic。有关更多信息，请参阅the section called “弹性 IP 地址” (p. 1213)。
实例	EC2-Classic 实例可以使用公有 IPv4 地址与 VPC 中的实例通信，或者您可以使用 ClassicLink 通过私有 IPv4 地址实现通信。 您不能将实例从 EC2-Classic 迁移到 VPC。不过，您可以将应用程序从 EC2-Classic 中的实例迁移到 VPC 中的实例。有关更多信息，请参阅从 EC2-Classic 迁移到 VPC (p. 1211)。
密钥对	
负载均衡器	如果您使用了 ClassicLink，则可以将一个链接的 EC2-Classic 实例注册到某个 VPC 中的负载均衡器，前提是该 VPC 具有与实例位于同一可用区的子网。 您不能将负载均衡器从 EC2-Classic 迁移到 VPC。您无法在 EC2-Classic 的负载均衡器中注册 VPC 中的实例。

资源	备注
置放群组	
Reserved Instance	可以将 预留实例 的网络平台从 EC2-Classic 更改为 VPC。有关更多信息，请参阅修改 预留实例 (p. 434)。
安全组	链接的 EC2-Classic 实例可通过 ClassicLink 使用 VPC 安全组以控制进出 VPC 的流量。VPC 实例不能使用 EC2-Classic 安全组。 您不能将安全组从 EC2-Classic 迁移到 VPC。您可以将规则从 EC2-Classic 安全组复制到 VPC 安全组。有关更多信息，请参阅创建安全组 (p. 1309)。
快照	

以下资源不能在 EC2-Classic 与 VPC 之间共享或移动：

- 竞价型实例

ClassicLink

我们即将停用 EC2-Classic。我们建议您从 EC2-Classic 迁移到 VPC (p. 1211)。

ClassicLink 允许您将 EC2-Classic 实例链接到账户中位于同一区域内的 VPC。如果您将 VPC 安全组与 EC2-Classic 实例相关联，这允许 EC2-Classic 实例与 VPC 中的实例使用私有 IPv4 地址进行通信。通过 ClassicLink，无需使用公有 IPv4 地址或弹性 IP 地址即可在这些平台中的实例之间进行通信。

ClassicLink 可用于账户支持 EC2-Classic 平台的所有用户，并且可以与任何 EC2-Classic 实例一起使用。使用 ClassicLink 不收取任何额外费用。采用标准的数据传输和实例使用计费方式。

目录

- ClassicLink 基本知识 (p. 1201)
- ClassicLink 限制 (p. 1203)
- 使用 ClassicLink (p. 1204)
- ClassicLink 的 IAM policy 示例 (p. 1207)
- 示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 (p. 1209)

ClassicLink 基本知识

使用 ClassicLink 将 EC2-Classic 实例链接到 VPC 分两步进行。首先，您必须为 VPC 启用 ClassicLink。默认情况下，您的账户中的所有 VPC 都未启用 ClassicLink，目的是保持其隔离状态。为 ClassicLink 启用 VPC 之后，您可以将账户中位于同一区域的任何运行的 EC2-Classic 实例链接到该 VPC。链接实例的过程中，要从将与您的 EC2-Classic 实例关联的 VPC 中选择安全组。在您链接实例之后，只要 VPC 安全组允许，实例可以使用其私有 IP 地址与您的 VPC 中的实例通信。EC2-Classic 实例在链接到 VPC 时不会丢失其私有 IP 地址。

将实例链接到 VPC 有时称为连接 实例。

链接的 EC2-Classic 实例可以与 VPC 中的实例通信，但它并不构成 VPC 的一部分。如果您列出自己的实例并按 VPC 筛选，例如，通过 `DescribeInstances` API 请求或使用 Amazon EC2 控制台中的 Instances

(实例) 屏幕执行此操作，则结果不会返回任何链接到 VPC 的 EC2-Classic 实例。有关如何查看链接的 EC2-Classic 实例的更多信息，请参阅查看启用了 ClassicLink 的 VPC 和链接的实例 (p. 1205)。

默认情况下，如果您使用公有 DNS 主机名从链接的 EC2-Classic 实例对 VPC 中的实例进行定位，则该主机名会解析为该实例的公有 IP 地址。如果使用公有 DNS 主机名从 VPC 中的实例对一个链接的 EC2-Classic 实例进行定位，也是同样的情况。如果您希望公有 DNS 主机名解析为私有 IP 地址，可以对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅启用 ClassicLink DNS 支持 (p. 1206)。

如果您不再需要实例与 VPC 之间的 ClassicLink 连接，可以从 VPC 取消与 EC2-Classic 实例的链接。这将断开 VPC 安全组与 EC2-Classic 实例的连接。链接的 EC2-Classic 实例一旦停止，会自动取消与 VPC 的链接。从 VPC 取消链接的所有 EC2-Classic 实例的链接后，您可以为 VPC 禁用 ClassicLink。

将 VPC 中的其他 Amazon 服务与 ClassicLink 结合使用

链接的 EC2-Classic 实例可以访问 VPC 中的以下 Amazon 服务：Amazon Redshift、Amazon ElastiCache、Elastic Load Balancing 和 Amazon RDS。但是，VPC 中的实例无法通过 ClassicLink 访问 EC2-Classic 平台预置的 Amazon 服务。

如果使用 Elastic Load Balancing，您可以向负载均衡器注册链接的 EC2-Classic 实例。您必须在启用了 ClassicLink 的 VPC 中创建负载均衡器，并启用在其中运行实例的可用区。当您终止链接的 EC2-Classic 实例时，负载均衡器会注销该实例。

如果您使用 Amazon EC2 Auto Scaling，则可以创建一个 Amazon EC2 Auto Scaling 组，其中包含在启动时自动链接到启用了 ClassicLink 的指定 VPC 的实例。有关更多信息，请参阅Amazon EC2 Auto Scaling 用户指南中的将 EC2-Classic 实例链接到 VPC。

如果您在 VPC 中使用 Amazon RDS 实例或 Amazon Redshift 集群，并且它们可以公开访问（可通过 Internet 访问），则您用于从链接的 EC2-Classic 实例定位这些资源的终端节点会默认解析为公有 IP 地址。如果这些资源不可公开访问，则终端节点会解析为私有 IP 地址。要使用 ClassicLink 通过私有 IP 定位可公共访问的 RDS 实例或 Redshift 集群，您必须使用其私有 IP 地址或私有 DNS 主机名，或者必须对 VPC 启用 ClassicLink DNS 支持。

如果使用私有 DNS 主机名或私有 IP 地址对 RDS 实例寻址，则链接的 EC2-Classic 实例将无法使用多可用区部署可用的故障转移支持。

您可以使用 Amazon EC2 控制台查找 Amazon Redshift、Amazon ElastiCache 或 Amazon RDS 资源的私有 IP 地址。

查找您的 VPC 中的 Amazon 资源的私有 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Network Interfaces（网络接口）。
3. 在 Description (描述) 列中查看网络接口的描述。Amazon Redshift、Amazon ElastiCache 或 Amazon RDS 所使用网络接口的描述中将包含服务名称。例如，连接到 Amazon RDS 实例的网络接口的描述如下：`RDSNetworkInterface`。
4. 选择所需的网络接口。
5. 在详细信息窗格中，从 Primary private IPv4 IP 字段中获取私有 IP 地址。

控制 ClassicLink 的使用

默认情况下，用户无权使用 ClassicLink。您可以创建 IAM 角色和 IAM policy，授予用户以下权限：为 VPC 启用或禁用 ClassicLink，将实例链接到启用了 ClassicLink 的 VPC 或取消此链接，查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例。有关用于 Amazon EC2 的 IAM policy 的更多信息，请参阅 适用于 Amazon EC2 的 IAM policy (p. 1225)。

有关使用 ClassicLink 的策略的更多信息，请参阅以下示例：ClassicLink 的 IAM policy 示例 (p. 1207)。

ClassicLink 中的安全组

将 EC2-Classic 实例链接到 VPC 不会对您的 EC2-Classic 安全组造成影响。它们会继续控制实例的所有传入和传出流量。这不包括 VPC 中实例的传入和传出流量，这些流量由与 EC2-Classic 实例关联的 VPC 安全组控制。链接到同一 VPC 的 EC2-Classic 实例无论是否与同一 VPC 安全组关联，都不能通过该 VPC 相互通信。EC2-Classic 实例之间的通信由与这些实例关联的 EC2-Classic 安全组控制。有关安全组配置的示例，请参阅示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置 (p. 1209)。

在您将实例链接到 VPC 之后，不可再更改与该实例关联的 VPC 安全组。要将不同安全组与您的实例关联，必须先取消实例链接，然后再将其链接到 VPC 并选择所需的安全组。

ClassicLink 的路由

在您为 VPC 启用 ClassicLink 时，会向所有 VPC 路由表添加一个静态路由，其目的地为 `10.0.0.0/8`，目标为 `local`。这允许 VPC 中的实例与后来链接到该 VPC 的任意 EC2-Classic 实例之间进行通信。如果您向启用了 ClassicLink 的 VPC 添加自定义路由表，则会自动添加一个静态路由，其目的地为 `10.0.0.0/8`，目标为 `local`。在您为 VPC 禁用 ClassicLink 时，会从所有 VPC 路由表中自动删除此路由。

可以为处于 `10.0.0.0/16` 和 `10.1.0.0/16` IP 地址范围内的 VPC 启用 ClassicLink，但仅当这些 VPC 的路由表中没有任何 `10.0.0.0/8` IP 地址范围内的现有静态路由时才能如此，并且在创建 VPC 时自动添加的本地路由除外。同样，如果您已经为 VPC 启用了 ClassicLink，那么您不能在路由表中再添加 `10.0.0.0/8` IP 地址范围内的任何其他特定路由。

> **Important**
>
> 如果您的 VPC CIDR 块为公共可路由 IP 地址范围，则在您将 EC2-Classic 实例链接到 VPC 之前，应考虑安全方面的问题。例如，如果链接的 EC2-Classic 实例从处于 VPC IP 地址范围内的源 IP 地址收到传入的拒绝服务 (DoS) 请求洪流攻击，则响应流量将发送到您的 VPC。我们强烈建议您使用私有 IP 地址范围创建 VPC，具体说明见 RFC 1918。

有关 VPC 中的路由表和路由的更多信息，请参阅 Amazon VPC 用户指南 中的路由表。

为 ClassicLink 启用 VPC 对等连接

如果您在两个 VPC 之间有 VPC 对等连接，而且存在一个或多个 EC2-Classic 实例（这些实例通过 ClassicLink 链接到这两个 VPC 中的一个或两个），则可以扩展 VPC 对等连接以启用 EC2-Classic 实例与 VPC 对等连接另一端的 VPC 中的实例之间的通信。这将使 EC2-Classic 实例和 VPC 中的实例能够通过私有 IP 地址进行通信。为此，您可允许本地 VPC 与对等 VPC 中链接的 EC2-Classic 实例通信，也可允许本地链接的 EC2-Classic 实例与对等 VPC 中的实例通信。

如果您允许本地 VPC 与对等 VPC 中的链接 EC2-Classic 实例通信，则将自动向您的路由表添加一个静态路由（目的地为 `10.0.0.0/8`，目标为 `local`）。

有关更多信息和示例，请参阅Amazon VPC Peering Guide中的使用 ClassicLink 进行配置。

ClassicLink 限制

要使用 ClassicLink 功能，您需要了解以下限制：

- EC2-Classic 实例一次只能链接到一个 VPC。
- 如果您停止链接的 EC2-Classic 实例，它会自动取消与 VPC 的链接，并且 VPC 安全组不再与实例关联。您可以在重新启动之后，再次将实例链接到 VPC。
- 不能将 EC2-Classic 实例链接到不同区域或不同 Amazon 账户中的 VPC。
- 您不能使用 ClassicLink 将一个 VPC 实例链接到另一个 VPC 或 EC2-Classic 资源。要在 VPC 之间建立私有连接，可以使用 VPC 对等连接。有关更多信息，请参阅 Amazon VPC 对等连接指南。
- 您不能将 VPC 弹性 IP 地址与链接的 EC2-Classic 实例关联。

- 您不能允许 EC2-Classic 实例进行 IPv6 通信。您可以将 IPv6 CIDR 块与 VPC 关联，然后将 IPv6 地址分配给 VPC 中的资源，但是，VPC 中的 ClassicLinked 实例和资源之间仅通过 IPv4 进行通信。
- 路由与 EC2-Classic 私有 IP 地址范围 `10/8` 冲突的 VPC 不能启用 ClassicLink。这不包括在路由表中已有本地路由的 `10.0.0.0/16` 和 `10.1.0.0/16` IP 地址范围的 VPC。有关更多信息，请参阅ClassicLink 的路由 (p. 1203)。
- 对于配置用于专用租赁的 VPC，无法启用 ClassicLink。您可以联系 Amazon Web Services 支持，申请允许为您的专用租期 VPC 启用 ClassicLink。

  Important

  EC2-Classic 实例运行在共享硬件上。如果您因法规或安全要求已将 VPC 租赁设置为 `dedicated`，那么将 EC2-Classic 实例链接到 VPC 可能并不符合这些要求，因为您可以利用共享的租赁资源，使用私有 IP 地址直接对隔离的资源进行寻址。如果您需要为专用 VPC 启用 ClassicLink，请在 Amazon Web Services 支持请求中提供这么做的详细原因。
- 如果您将 EC2-Classic 实例链接到 `172.16.0.0/16` 范围中的某个 VPC，并在该 VPC 中的 `172.16.0.23/32` IP 地址上运行了一个 DNS 服务器，那么您所链接的 EC2-Classic 实例将无法访问 VPC DNS 服务器。要解决此问题，请在该 VPC 中的其他 IP 地址上运行您的 DNS 服务器。
- ClassicLink 不支持 VPC 外的传递关系。链接的 EC2-Classic 实例不能访问与 VPC 关联的任何 VPN 连接、VPC 网关终端节点、NAT 网关或 Internet 网关。同样，VPN 连接或 Internet 网关另一端的资源也不能访问链接的 EC2-Classic 实例。

使用 ClassicLink

您可以通过 Amazon EC2 和 Amazon VPC 控制台使用 ClassicLink 功能。您可以为 VPC 启用或禁用 ClassicLink，也可以将 EC2-Classic 实例链接到 VPC 或取消其链接。

Note

ClassicLink 功能仅在支持 EC2-Classic 的账户和区域的控制台中显示。

任务

- 为 VPC 启用 ClassicLink (p. 1204)
- 将实例链接到 VPC (p. 1205)
- 在启动时将实例链接到 VPC (p. 1205)
- 查看启用了 ClassicLink 的 VPC 和链接的实例 (p. 1205)
- 启用 ClassicLink DNS 支持 (p. 1206)
- 禁用 ClassicLink DNS 支持 (p. 1206)
- 从 VPC 取消链接一个实例 (p. 1206)
- 为 VPC 禁用 ClassicLink (p. 1207)

为 VPC 启用 ClassicLink

要将 EC2-Classic 实例链接到某个 VPC，您必须先为该 VPC 启用 ClassicLink。如果 VPC 的路由与 EC2-Classic 私有 IP 地址范围冲突，则不能为该 VPC 启用 ClassicLink。有关更多信息，请参阅ClassicLink 的路由 (p. 1203)。

为 VPC 启用 ClassicLink

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs（您的 VPC）。
3. 选择 VPC。

4. 选择 Actions（操作）、Edit VPC settings（编辑 VPC 设置）。
5. 对于 ClassicLink，选择 Enable（启用）。
6. （可选）如果您希望公有 DNS 主机名解析为私有 IP 地址，请在链接任何实例之前先对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅启用 ClassicLink DNS 支持 (p. 1206)。

将实例链接到 VPC

为 ClassicLink 启用 VPC 后，您可以将 EC2-Classic 实例与其链接。该实例必须处于 `running` 状态。

（可选）如果您希望公有 DNS 主机名解析为私有 IP 地址，请在链接实例之前先对 VPC 启用 ClassicLink DNS 支持。有关更多信息，请参阅启用 ClassicLink DNS 支持 (p. 1206)。

将实例链接到 VPC

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择一个或多个正在运行的 EC2-Classic 实例。
4. 依次选择操作、ClassicLink、链接到 VPC。
5. 选择 VPC。控制台只会显示启用了 ClassicLink 的 VPC。
6. 选择要与您的实例关联的一个或多个安全组。控制台只会显示启用了 ClassicLink 的 VPC 的安全组。
7. 选择链接。

在启动时将实例链接到 VPC

您可以在 Amazon EC2 控制台中使用启动向导启动 EC2-Classic 实例，然后立即将其链接到启用了 ClassicLink 的 VPC。

在启动时将实例链接到 VPC

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从 Amazon EC2 仪表板中，选择 Launch Instance。
3. 选择 AMI，然后选择 EC2-Classic 支持的实例类型。有关更多信息，请参阅EC2-Classic 中提供的实例类型 (p. 1197)。
4. 在 Configure Instance Details (配置实例详细信息) 页面中，执行以下操作：
   a. 对于网络，选择在 EC2-Classic 中启动。如果此选项处于禁用状态，则表示 EC2-Classic 不支持该实例类型。
   b. 展开链接到 VPC (ClassicLink)，然后从链接到 VPC 中选择一个 VPC。控制台只会显示启用了 ClassicLink 的 VPC。
5. 完成向导中的剩余步骤即可启动实例。有关更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。

查看启用了 ClassicLink 的 VPC 和链接的实例

您可以在 Amazon VPC 控制台中查看启用了 ClassicLink 的所有 VPC，在 Amazon EC2 控制台中查看链接的 EC2-Classic 实例。

查看启用了 ClassicLink 的 VPC

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs（您的 VPC）。

3. 选择 VPC。
4. 如果 ClassicLink 的值为已启用，则表示 VPC 已启用 ClassicLink。

启用 ClassicLink DNS 支持

您可以对您的 VPC 启用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例与 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。要使此功能起作用，必须对您的 VPC 启用 DNS 主机名和 DNS 解析。

> Note
>
> 如果您对 VPC 启用 ClassicLink DNS 支持，则链接的 EC2-Classic 实例可以访问与 VPC 关联的所有私有托管区。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的私有托管区域的使用。

启用 ClassicLink DNS 支持

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs（您的 VPC）。
3. 选择 VPC。
4. 选择 Actions（操作）、Edit VPC settings（编辑 VPC 设置）。
5. 对于 ClassicLink DNS 支持，请选择启用。
6. 选择 Save changes（保存更改）。

禁用 ClassicLink DNS 支持

您可以对您的 VPC 禁用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例和 VPC 中的实例之间的 DNS 主机名解析为公有 IP 地址而不是私有 IP 地址。

禁用 ClassicLink DNS 支持

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs（您的 VPC）。
3. 选择 VPC。
4. 选择 Actions（操作）、Edit VPC settings（编辑 VPC 设置）。
5. 对于 ClassicLink DNS 支持，请清除启用。
6. 选择 Save changes（保存更改）。

从 VPC 取消链接一个实例

如果您不再需要 EC2-Classic 实例与 VPC 之间的 ClassicLink 连接，可以从 VPC 取消与该实例的链接。取消实例链接会从实例解除与 VPC 安全组的关联。

停止的实例会从 VPC 自动取消链接。

从 VPC 取消链接一个实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的一个或多个实例。
4. 依次选择操作、ClassicLink、从 VPC 取消链接。

5. 当系统提示进行确认时，选择取消链接。

为 VPC 禁用 ClassicLink

如果您不再需要 EC2-Classic 实例与 VPC 之间的连接，可以禁用 VPC 的 ClassicLink。您必须先取消链接到 VPC 的所有链接的 EC2-Classic 实例的链接。

为 VPC 禁用 ClassicLink

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Your VPCs（您的 VPC）。
3. 选择您的 VPC。
4. 选择 Actions（操作）、Edit VPC settings（编辑 VPC 设置）。
5. 对于 ClassicLink，取消选择 Enable（启用）。

ClassicLink 的 IAM policy 示例

您可以为 VPC 启用 ClassicLink，然后将 EC2-Classic 实例链接到 VPC。您还可以查看启用了 ClassicLink 的 VPC 和所有链接到 VPC 的 EC2-Classic 实例。可以为 `ec2:EnableVpcClassicLink`、`ec2:DisableVpcClassicLink`、`ec2:AttachClassicLinkVpc` 和 `ec2:DetachClassicLinkVpc` 操作创建包含资源级权限的策略，以控制用户对这些操作的使用。`ec2:Describe*` 操作不支持资源级权限。

示例

- 使用 ClassicLink 的完全权限 (p. 1207)
- 为 VPC 启用和禁用 ClassicLink (p. 1207)
- 链接实例 (p. 1208)
- 断开关联实例 (p. 1209)

使用 ClassicLink 的完全权限

以下策略授予用户如下权限：查看启用了 ClassicLink 的 VPC 和链接的 EC2-Classic 实例，为 VPC 启用和禁用 ClassicLink，以及从启用了 ClassicLink 的 VPC 链接实例和取消与实例的链接。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeClassicLinkInstances", "ec2:DescribeVpcClassicLink",
        "ec2:EnableVpcClassicLink", "ec2:DisableVpcClassicLink",
        "ec2:AttachClassicLinkVpc", "ec2:DetachClassicLinkVpc"
      ],
      "Resource": "*"
    }
   ]
}
```

为 VPC 启用和禁用 ClassicLink

以下策略允许用户为具有特定标签“purpose=classiclink”的 VPC 启用和禁用 ClassicLink。用户不能为其他任何 VPC 启用或禁用 ClassicLink。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcClassicLink",
      "Resource": "arn:aws:ec2:region:account:vpc/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose":"classiclink"
        }
      }
    }
  ]
}
```

链接实例

以下策略为用户授予将实例链接到 VPC 的权限，但前提是实例具有 m3.large 实例类型。第二条语句允许用户使用 VPC 以及将实例链接到 VPC 所需的安全组资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": "arn:aws:ec2:region:account:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceType":"m3.large"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": [
        "arn:aws:ec2:region:account:vpc/*",
        "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

以下策略为用户授予以下权限：仅将实例链接到特定 VPC (vpc-1a2b3c4d) 以及仅将 VPC 中的特定安全组 (sg-1122aabb 和 sg-aabb2233) 与实例相关联。用户不能将实例链接到任何其他 VPC，因此他们不能在请求中指定任何 VPC 其他安全组与实例关联。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": [
         "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",
         "arn:aws:ec2:region:account:instance/*",
         "arn:aws:ec2:region:account:security-group/sg-1122aabb",
         "arn:aws:ec2:region:account:security-group/sg-aabb2233"
       ]
```

```
    }
  ]
}
```

断开关联实例

以下策略授予用户从 VPC 取消与任何链接的 EC2-Classic 实例的链接的权限，但仅当实例具有标签“unlink=true”时才有效。第二条语句为用户授予使用 VPC 资源的权限，需要具有该权限才能从 VPC 中取消链接实例。

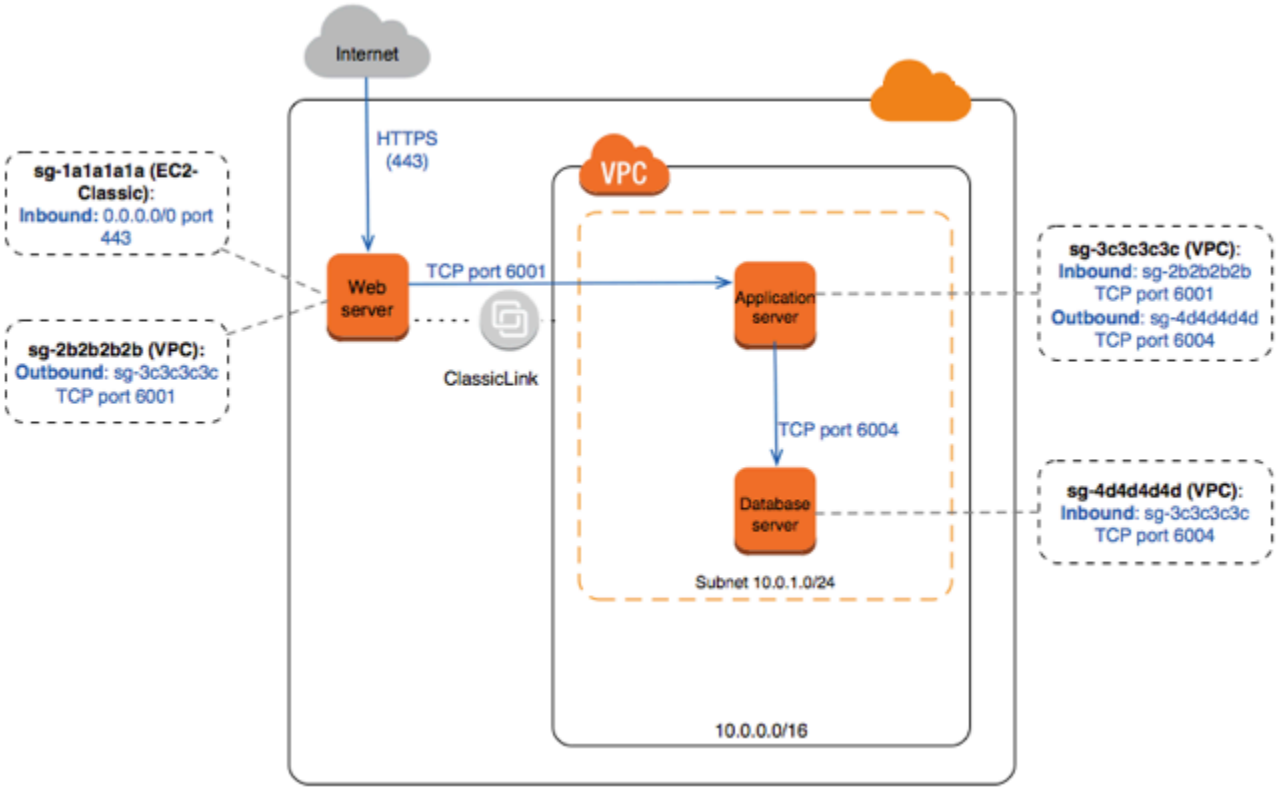
```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:DetachClassicLinkVpc",
      "Resource": [
         "arn:aws:ec2:region:account:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/unlink":"true"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:DetachClassicLinkVpc",
      "Resource": [
         "arn:aws:ec2:region:account:vpc/*"
         ]
      }
   ]
}
```

示例：适用于三层 Web 应用程序的 ClassicLink 安全组配置

在此示例中，您有具有以下三个实例的应用程序：面向公众的 Web 服务器、应用程序服务器和数据库服务器。您的 Web 服务器接收来自 Internet 的 HTTPS 流量，然后通过 TCP 端口 6001 与应用程序服务器通信。然后，您的应用程序服务器通过 TCP 端口 6004 与数据库服务器通信。您正在进行将整个应用程序迁移到账户中的 VPC 的过程。已将您的应用程序服务器和数据库服务器迁移到 VPC。您的 Web 服务器仍在 EC2-Classic 中而且已通过 ClassicLink 链接到 VPC。

您需要一个安全组配置，该配置仅允许流量在这些实例间流动。您具有 4 个安全组：其中两个安全组用于 Web 服务器 (sg-1a1a1a1a 和 sg-2b2b2b2b)、一个安全组用于应用程序服务器 (sg-3c3c3c3c)，一个安全组用于数据库服务器 (sg-4d4d4d4d)。

下图显示了实例的架构及其安全组配置。



适用于 Web 服务器的安全组（**sg-1a1a1a1a** 和 **sg-2b2b2b2b**）

您的一个安全组位于 EC2-Classic 中，另一个安全组位于 VPC 中。当通过 ClassicLink 将您的 Web 服务器实例链接到 VPC 时，是将 VPC 安全组与该实例关联。VPC 安全组使您能够控制从 Web 服务器到应用程序服务器的出站流量。

以下是适用于 EC2-Classic 安全组的安全组规则 (sg-1a1a1a1a)。

Inbound			
源	类型	端口范围	注释
0.0.0.0/0	HTTPS	443	允许 Internet 流量到达您的 Web 服务器。

以下是适用于 VPC 安全组的安全组规则 (sg-2b2b2b2b)。

Outbound			
目的地	类型	端口范围	注释
sg-3c3c3c3c	TCP	6001	在您的 VPC 中允许从 Web 服务器到应用程序服务器 (或到与 sg-3c3c3c3c 关联的任何其他实例) 的出站流量。

适用于您的应用程序服务器的安全组 (**sg-3c3c3c3c**)

以下是适用于与您的应用程序服务器关联的 VPC 安全组的安全组规则。

Inbound			
源	类型	端口范围	注释
sg-2b2b2b2b	TCP	6001	允许来自 Web 服务器 (或与 sg-2b2b2b2b 关联的任何其他实例) 的指定类型的流量到达应用程序服务器。
Outbound			
目的地	类型	端口范围	注释
sg-4d4d4d4d	TCP	6004	Allows outbound traffic from the application server to the database server (or to any other instance associated with sg-4d4d4d4d).

适用于数据库服务器的安全组 (**sg-4d4d4d4d**)

以下是适用于与您的数据库服务器关联的 VPC 安全组的安全组规则。

Inbound			
源	类型	端口范围	注释
sg-3c3c3c3c	TCP	6004	允许来自应用程序服务器 (或与 sg-3c3c3c3c 关联的任何其他实例) 的指定类型的流量到达数据库服务器。

从 EC2-Classic 迁移到 VPC

我们即将停用 EC2-Classic。有关更多信息，请参阅博客文章 EC2-Classic Networking is Retiring - Here's How to Prepare。

要从 EC2-Classic 迁移到 VPC，您必须在 VPC 中迁移或重新创建 EC2-Classic 资源。

目录

- 将资源迁移到 VPC (p. 1212)
- 使用 Amazon Web Services Support-MigrateEC2ClassicToVPC 运行手册 (p. 1216)
- 示例：迁移简单的 Web 应用程序 (p. 1216)

将资源迁移到 VPC

您可以将部分资源迁移或移动到 VPC。某些资源只能从 EC2-Classic 迁移到位于同一区域和同一 Amazon 账户中的 VPC。如果无法迁移资源，则必须创建新资源以供在 VPC 中使用。

先决条件

开始之前，您必须拥有 VPC。如果您没有默认 VPC，则可以创建非默认 VPC。有关更多信息，请参阅创建 VPC。

资源

- 安全组 (p. 1212)
- 弹性 IP 地址 (p. 1213)
- AMI 和实例 (p. 1213)
- Amazon RDS 数据库实例 (p. 1215)
- 经典负载均衡器 (p. 1216)

安全组

如果您希望 VPC 中的实例具有与 EC2-Classic 实例相同的安全组规则，则可以使用 Amazon EC2 控制台将现有 EC2-Classic 安全组规则复制到新的 VPC 安全组。您可以将 EC2-Classic 中的任何安全组复制到符合要求的 VPC。默认安全组无法删除，将由系统在 EC2-Classic 停用时代表您删除。

您只能将安全组规则复制到相同区域内相同 Amazon 账户中的新安全组。如果您使用不同的区域或不同的 Amazon 账户，则必须创建新的安全组并自行手动添加规则。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

先决条件

在开始复制安全组之前，您应该检查 EC2-Classic 安全组在其中引用 EC2-Classic 内的另一个安全组的规则。您应该移除这些规则，因为无法将它们复制到 VPC 中。有关更多信息，请参阅从安全组中删除规则。

将您的安全组规则复制到新安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择与您 EC2-Classic 实例关联的安全组，再选择 Actions（操作），然后选择Copy to new security group（复制到新安全组）。

   Note

   要标识 EC2-Classic 安全组，请检查 VPC ID 列。对于每个 EC2-Classic 安全组，列中的值为空或 - 符号。
4. 在 Copy to new security group（复制到新安全组）对话框中，为您的新安全组指定名称和描述。从 VPC 列表中选择您的 VPC。
5. 在 Inbound rules（入站规则）下，字段会使用您 EC2-Classic 安全组中的规则进行填充。您可以根据需要修改这些规则。在 Outbound rules（出站规则）下，已自动为您创建允许所有出站流量的规则。有关修改安全组规则的更多信息，请参阅适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)。

   Important

   您必须移除引用 EC2-Classic 中的安全组的任何规则，因为您无法从 VPC 安全组中引用 EC2-Classic 安全组。在将安全组复制到 VPC 后，您可以添加类似规则。
6. 选择Create security group（创建安全组）。

弹性 IP 地址

您可以迁移已分配的以供在 EC2-Classic 中使用的弹性 IP 地址以便与 VPC 一起使用。您不能将弹性 IP 地址迁移到另一个区域或 Amazon 账户。您不能迁移在 24 小时之前分配给您的账户弹性 IP 地址。

在迁移弹性 IP 地址时，该地址会计入 VPC 的弹性 IP 地址限制。如果某个弹性 IP 地址会导致您超出限制，则不能迁移该地址。要迁移弹性 IP 地址，则不得将该地址与实例关联。有关解除弹性 IP 地址与实例的关联的更多信息，请参阅解除弹性 IP 地址的关联 (p. 1098)。

在您执行相关命令来移动或还原弹性 IP 地址后，弹性 IP 地址的迁移过程可能需要花费几分钟时间。使用 describe-moving-addresses 命令可查看您的弹性 IP 地址是仍在移动还是已完成移动。移动完成后，您可以在 Elastic IPs（弹性 IP）页面查看弹性 IP 地址的分配 ID。如果弹性 IP 地址处于移动状态超过 5 分钟，请联系 Amazon Support。

标识已分配的以供在 EC2-Classic 中使用的弹性 IP 地址

打开 Amazon EC2 控制台。在导航窗格中选择 Elastic IPs（弹性 IP），然后选择该弹性 IP 地址对应的复选框。在 Summary（摘要）页面上，检查 Scope（范围）是 EC2-Classic 还是 VPC。

使用 Amazon EC2 控制台移动弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Elastic IPs。
3. 依次选择弹性 IP 地址、Actions 和 Move to VPC scope。
4. 在确认对话框中，选择 Move Elastic IP。

AMI 和实例

AMI 是用于启动 Amazon EC2 实例的模板。您可以基于现有 EC2-Classic 实例创建自己的 AMI，然后使用该 AMI 在 VPC 中启动实例。

目录

- 识别 EC2-Classic 实例 (p. 1213)
- 创建 AMI (p. 1213)
- （可选）共享或复制您的 AMI (p. 1214)
- （可选）在 Amazon EBS 卷上存储您的数据 (p. 1214)
- 将实例启动到 VPC 中 (p. 1215)

识别 EC2-Classic 实例

如果您有实例同时在 EC2-Classic 和 VPC 中运行，则可以识别您的 EC2-Classic 实例。

Amazon EC2 控制台

在导航窗格中选择实例。在 VPC ID 列中，每个 EC2-Classic 实例的值为空或 - 符号。如果 VPC ID 列不存在，请选择齿轮图标并将列设为可见。

Amazon CLI

使用以下 describe-instances Amazon CLI 命令。`--query` 参数只会显示 `VpcId` 的值为 `null` 的实例。

```
aws ec2 describe-instances --query 'Reservations[*].Instances[?VpcId==`null`]'
```

创建 AMI

确定您的 EC2-Classic 实例后，您可以通过该实例创建 AMI。

创建 Windows AMI

有关更多信息，请参阅创建自定义 Windows AMI。

创建 Linux AMI

用于创建 Linux AMI 的方法取决于您的实例的根设备类型，以及实例运行时所在的操作系统平台。要查明实例的根设备类型，请转到实例页面，选择您的实例，然后在存储选项卡，查看根设备类型字段中的信息。如果值为 `ebs`，则说明您的实例是由 EBS 提供支持。如果值为 `instance-store`，则说明您的实例是由实例存储提供支持。您还可以使用 describe-instances Amazon CLI 命令查明根设备类型。

下表为您提供用于基于实例的根设备类型和软件平台创建 Linux AMI 的选项。

> **Important**
>
> 一些实例类型同时支持半虚拟化 (PV) 和硬件虚拟机 (HVM) 虚拟化，而其他实例类型只支持其中之一。如果您计划使用 AMI 启动与当前实例类型不同的实例类型，请验证该实例类型是否支持 AMI 提供的虚拟化类型。如果 AMI 支持 PV 虚拟化，而您要使用支持 HVM 虚拟化的实例类型，则您可能必须在基础 HVM AMI 上重新安装软件。有关 PV 和 HVM 虚拟化的更多信息，请参阅 Linux AMI 虚拟化类型。

实例根设备类型	操作
EBS	从实例创建由 EBS 支持的 AMI。有关更多信息，请参阅创建由 Amazon EBS 提供支持的 Linux AMI。
实例存储	使用 AMI 工具从实例创建由实例存储支持的 AMI。有关更多信息，请参阅创建实例存储支持的 Linux AMI。
实例存储	将由实例存储支持的实例转换为由 EBS 支持的实例。有关更多信息，请参阅将实例存储支持的 AMI 转换为 Amazon EBS-backed AMI。

（可选）共享或复制您的 AMI

要使用 AMI 在新的 Amazon 账户中启动实例，您必须首先与新账户共享 AMI。有关更多信息，请参阅与特定 Amazon 账户共享 AMI (p. 126)。

要使用 AMI 在不同区域的 VPC 中启动实例，您必须首先将 AMI 复制到该区域。有关更多信息，请参阅复制 AMI (p. 172)。

（可选）在 Amazon EBS 卷上存储您的数据

您可以创建 Amazon EBS 卷并使用它备份和存储实例中的数据 – 如同使用物理硬盘一样。Amazon EBS 卷可以与同一可用区中的任何实例附加和分离。您可以将卷与 EC2-Classic 中实例分离，并将它附加到在同一可用区内的 VPC 中启动的新实例。

有关 Amazon EBS 卷的更多信息，请参阅以下主题：

- Amazon EBS 卷 (p. 1324)
- 创建 Amazon EBS 卷 (p. 1344)
- 将 Amazon EBS 卷挂载到实例 (p. 1347)

要备份 Amazon EBS 卷上的数据，可以拍摄卷的定期快照。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。如果您需要，可以从快照创建 Amazon EBS 卷。有关更多信息，请参阅从快照创建卷 (p. 1346)。

将实例启动到 VPC 中

创建 AMI 后，您可以使用 Amazon EC2 启动实例向导，从而在 VPC 中启动实例。实例将具有与现有 EC2-Classic 实例相同的数据和配置。

Note

您可以利用此机会升级到当前一代实例类型。但是，请验证实例类型支持 AMI 提供的虚拟化类型（PV 或 HVM）。有关半虚拟化和硬件虚拟机虚拟化的更多信息，请参阅。Linux AMI 虚拟化类型 (p. 106)

New console

在 VPC 中启动实例

1. 按照程序启动实例 (p. 576)。
2. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统映像（Amazon 机器映像）] 下，选择 My AMIs（我的 AMI），确保已选中 Owned by me（我拥有的），然后选择您创建的 AMI。或者，如果您从其他账户共享 AMI，请选中 Shared with me（与我共享的），然后选择您从 EC2-Classic 账户共享的 AMI。
3. 在 Network settings（网络设置）下，选择右侧的 Edit（编辑），然后执行以下操作：
   a. 对于 VPC，选择您的 VPC。
   b. 对于 Subnet（子网），请选择所需的子网。
   c. 对于 Security group name（安全组名称），请选择您为 VPC 创建的安全组。
4. 配置您需要的其他任何详细信息，例如实例类型和密钥对。有关启动实例向导中字段的信息，请参阅 使用定义的参数启动实例 (p. 577)。
5. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。

Old console

在 VPC 中启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制面板上，选择启动实例。
3. 在 Choose an Amazon Machine Image (选择一个Amazon 系统映像) 页面上，选择 My AMIs (我的 AMI) 类别，然后选择您创建的 AMI。或者，如果您从另一个账户共享了 AMI，请在所有权筛选列表中选择与我共享。选择您从 EC2-Classic 账户共享的 AMI。
4. 在 Choose an Instance Type 页面上，选择实例的类型，然后选择 Next: Configure Instance Details。
5. 在 Configure Instance Details (配置实例详细信息) 页面中的 Network (网络) 列表中选择您的 VPC。从 Subnet (子网) 列表中选择所需子网。配置您需要的任何其他详细信息，然后完成向导中的后续页面，直至到达配置安全组页面。
6. 选择选择现有组，然后选择您为 VPC 创建的安全组。选择 Review and Launch。
7. 查看实例详细信息，然后选择 Launch 以指定密钥对并启动实例。

有关您在向导的每个步骤中可以配置的参数的更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。

Amazon RDS 数据库实例

您可以将 EC2-Classic 数据库实例移到同一个账号、同一个区域的 VPC 中。有关更多信息，请参阅 Amazon RDS 用户指南 中的更新数据库实例的 VPC。

经典负载均衡器

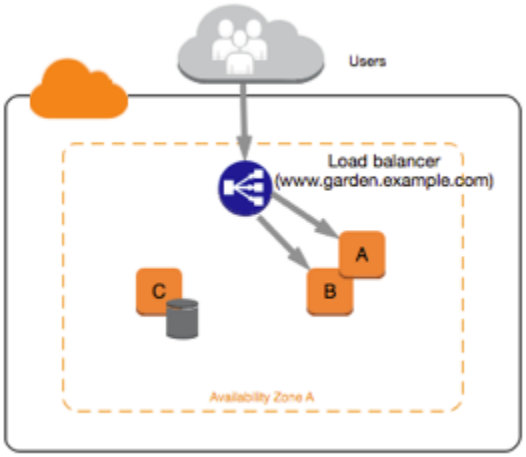
您可以将 EC2-Classic 中的经典负载均衡器迁移到 VPC 中的经典负载均衡器，或者可以将经典负载均衡器迁移到 Application Load Balancer 或 Network Load Balancer。有关更多信息，请参阅《Elastic Load Balancing 用户指南》中的 迁移经典负载均衡器。

使用 Amazon Web Services Support-MigrateEC2ClassicToVPC 运行手册

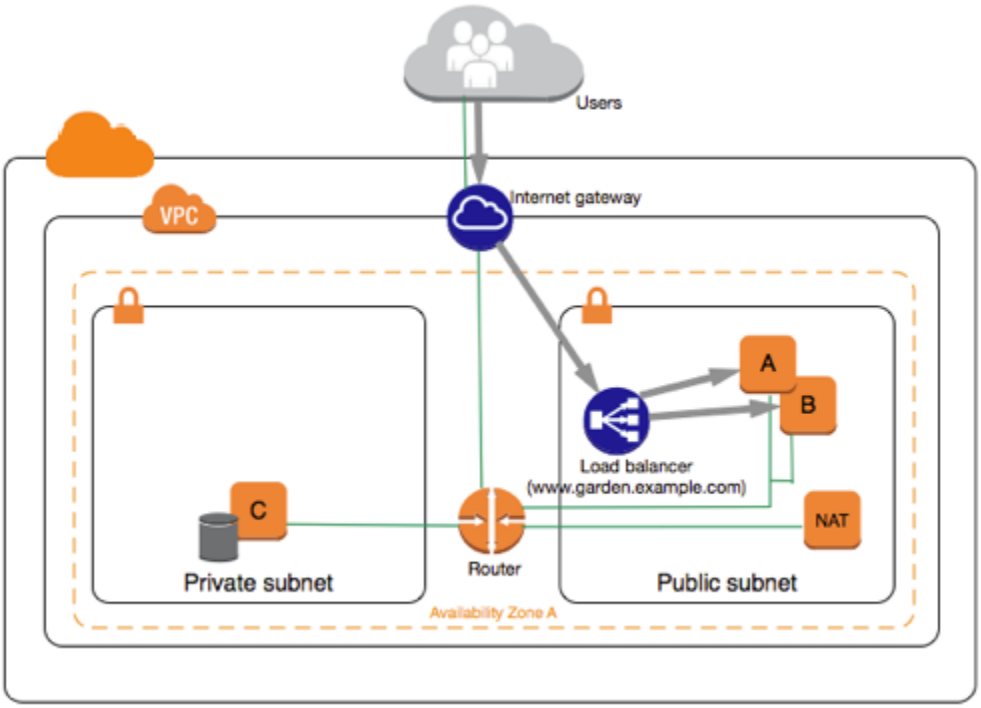
Amazon Web Services Support-MigrateEC2ClassicToVPC 运行手册将 EC2-Classic 实例迁移到 VPC。有关更多信息，请参阅如何将 EC2-Classic 实例迁移到 VPC？

示例：迁移简单的 Web 应用程序

在此示例中，您使用 Amazon 托管您的园艺网站。为了管理您的网站，您在 EC2-Classic 中有三个正在运行的实例。实例 A 和 B 托管面向公众的 Web 应用程序，Elastic Load Balancing 用于对这些实例之间的流量进行负载均衡。您向实例 A 和 B 分配了弹性 IP 地址，从而可将静态 IP 地址用于这些实例上的配置和管理任务。实例 C 存储您网站的 MySQL 数据库。您注册了域名 `www.garden.example.com`，并且使用 Route 53 创建了一个托管区域，该区域具有与负载均衡器的 DNS 名称关联的别名记录集。



第一部分往 VPC 的迁移决定了适合您需要的 VPC 架构类型。在此情况中，您做出了以下决定：将一个公有子网用于您的 Web 服务器，而将一个私有子网用于您的数据库服务器。随着您网站的发展，您可以向子网添加更多 Web 服务器和数据库服务器。默认情况下，私有子网中的实例无法访问 Internet；但是，您可以通过公有子网中的网络地址转换 (NAT) 设备启用 Internet 访问。您可能需要设置 NAT 设备，以通过 Internet 为数据库服务器提供定期更新和补丁。将弹性 IP 地址迁移到 VPC，并在公有子网中创建负载均衡器来对 Web 服务器之间的流量进行负载均衡。



要将您的 Web 应用程序迁移到 VPC，您可以执行以下步骤：

- 创建 VPC：有关更多信息，请参阅《Amazon VPC 用户指南》中的创建 VPC。有关 VPC 架构方案的信息，请参阅《Amazon VPC 用户指南》中的方案。
- 配置您的安全组：在 EC2-Classic 环境中，您将一个安全组用于 Web 服务器，并将另一个安全组用于数据库服务器。您可以使用 Amazon EC2 控制台将规则从每个安全组复制到用于您 VPC 的新安全组中。有关更多信息，请参阅安全组 (p. 1212)。

  Tip

  首先创建由其他安全组引用的安全组。
- 创建 AMI 并启动新实例：从您的一个 Web 服务器创建一个 AMI，并从数据库服务器创建第二个 AMI。然后，在公有子网中启动替换 Web 服务器，并在私有子网中启动替换数据库服务器。有关更多信息，请参阅创建 AMI (p. 1213)。
- 配置您的 NAT 设备：如果您使用的是 NAT 实例，则必须为其创建安全组，以便允许来自您的私有子网的 HTTP 和 HTTPS 流量。有关更多信息，请参阅 NAT 实例。如果您使用的是 NAT 网关，则会自动允许来自您的私有子网的流量。
- 配置您的数据库：在 EC2-Classic 中从数据库服务器创建 AMI 时，该实例中存储的所有配置信息都已复制到 AMI。您可能必须连接到新的数据库服务器并更新配置详细信息。例如，如果您将数据库配置为向 EC2-Classic 中的 Web 服务器授予完全读取、写入和修改权限，则您需要更新配置文件以改为向新 VPC Web 服务器授予相同权限。
- 配置您的 Web 服务器：您的 Web 服务器将具有与 EC2-Classic 中的实例相同的配置设置。例如，如果您将 Web 服务器配置为使用 EC2-Classic 中的数据库，请将您 Web 服务器的配置设置更新为指向您的新数据库实例。

  Note

  默认情况下，不会向在非默认子网中启动的实例分配公有 IP 地址，除非您在启动时另行指定。您的新数据库服务器可能没有公有 IP 地址。在这种情况下，您可以更新您 Web 服务器的配置文件以使用新数据库服务器的私有 DNS 名称。同一 VPC 中的实例通过私有 IP 地址互相通信。

- 迁移您的弹性 IP 地址：在 EC2-Classic 中从您的 Web 服务器取消与弹性 IP 地址的关联，然后将这些地址迁移到 VPC。迁移这些地址后，您可在 VPC 中将其与您的新 Web 服务器关联。有关更多信息，请参阅the section called “弹性 IP 地址” (p. 1213)。
- 创建新负载均衡器：要继续使用 Elastic Load Balancing 对发送到实例的流量进行负载均衡，请确保您了解在 VPC 中配置负载均衡器的各种方法。有关更多信息，请参阅 Elastic Load Balancing 用户指南。
- 更新您的 DNS 记录：在公有子网中设置了负载均衡器之后，请验证 `www.garden.example.com` 域指向您的新负载均衡器。为此，请更新 DNS 记录和 Route 53 中的别名记录集。有关使用 Route 53 的更多信息，请参阅 Route 53 入门。
- 关闭您的 EC2-Classic 资源：验证了您的 Web 应用程序是否正在 VPC 架构内运行之后，可以关闭 EC2-Classic 资源以使它们停止产生费用。

Amazon EC2 中的安全性

Amazon的云安全性的优先级最高。作为 Amazon 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为Amazon合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 Amazon EC2 的合规性计划，请参阅 Amazon 合规性计划范围内的的服务。
- 云中的安全性 – 您的责任包括以下各个方面：
  - 例如，通过配置 VPC 和安全组来控制对实例的网络访问。有关更多信息，请参阅控制网络流量 (p. 1220)。
  - 管理用于连接到您的实例的凭证。
  - 管理访客操作系统和部署到访客操作系统的软件，包括更新和安全补丁。有关更多信息，请参阅Amazon EC2 中的更新管理 (p. 1320)。
  - 配置附加到实例的 IAM 角色以及与这些角色关联的权限。有关更多信息，请参阅适用于 Amazon EC2 的 IAM 角色 (p. 1277)。

该文档帮助您了解如何在使用 Amazon EC2 时应用责任共担模式。它说明了如何配置 Amazon EC2 以实现您的安全性和合规性目标。您还会了解如何使用其他Amazon服务以帮助您监控和保护 Amazon EC2 资源。

目录

- Amazon EC2 中的基础设施安全性 (p. 1219)
- Amazon EC2 中的恢复功能 (p. 1220)
- Amazon EC2 中的数据保护 (p. 1221)
- 适用于 Amazon EC2 的 Identity and Access Management (p. 1223)
- Amazon EC2 密钥对和 Linux 实例 (p. 1289)
- 适用于 Linux 实例的 Amazon EC2 安全组 (p. 1303)
- 使用接口 VPC 终端节点访问 Amazon EC2 (p. 1319)
- Amazon EC2 中的更新管理 (p. 1320)
- Amazon EC2 的合规性验证 (p. 1320)

Amazon EC2 中的基础设施安全性

您可以使用Amazon发布的 API 调用通过网络访问 Amazon EC2。客户端必须支持传输层安全性 (TLS) 1.1 或更高版本。客户端必须在 2023 年 6 月 28 日之前支持 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用 Amazon Security Token Service（Amazon STS）生成临时安全凭证，以对请求进行签名。

有关更多信息，请参阅《安全支柱 – Amazon-Well-Architected 框架》中的 基础设施保护。

网络隔离

Virtual Private Cloud (VPC) 是 Amazon 云内您自己的逻辑隔离区域中的虚拟网络。可以使用单独的 VPC 按工作负载或组织实体隔离基础设施。

子网是 VPC 中的 IP 地址范围。在启动实例时，您可以在 VPC 上的子网中启动该实例。可以使用子网隔离单个 VPC 中的应用程序层（例如，Web、应用程序和数据库）。如果不应直接从 Internet 访问实例，请使用私有子网访问。

要使用私有 IP 地址从 VPC 调用 Amazon EC2 API，请使用 Amazon PrivateLink。有关更多信息，请参阅使用接口 VPC 终端节点访问 Amazon EC2 (p. 1319)。

物理主机上的隔离

同一物理主机上的不同 EC2 实例彼此隔离，就好像它们位于不同的物理主机上一样。管理程序隔离 CPU 和内存，并为实例提供虚拟化磁盘，而不是访问原始磁盘设备。

在停止或终止实例时，管理程序将清理分配给实例的内存（设置为零），然后再将内存分配给新实例并重置每个存储块。这会确保不会意外向另一个实例泄露数据。

网络 MAC 地址由 Amazon 网络基础设施动态分配给实例。IP 地址由 Amazon 网络基础设施动态分配给实例，或者由 EC2 管理员通过经过身份验证的 API 请求进行分配。Amazon 网络允许实例仅从分配给它们的 MAC 和 IP 地址发送流量。否则，将会丢弃流量。

默认情况下，实例无法接收未明确将其指定为目标地址的流量。如果需要在实例上运行网络地址转换 (NAT)、路由或防火墙服务，您可以为网络接口禁用源/目标检查。

控制网络流量

请考虑使用以下方法来控制到 EC2 实例的网络流量：

- 使用安全组 (p. 1303)限制实例访问。例如，您可以仅允许来自公司网络地址范围的流量。
- 如果不应直接从 Internet 访问实例，请使用私有子网访问。使用堡垒主机或 NAT 网关从私有子网中的实例进行 Internet 访问。
- 使用 Amazon Virtual Private Network 或 Amazon Direct Connect 建立从远程网络到 VPC 的私有连接。有关更多信息，请参阅网络到 Amazon VPC 的连接选项。
- 使用 VPC Flow Logs 监控到达实例的流量。
- 使用 Amazon Security Hub 检查来自实例的意外网络访问。
- 使用 EC2 Instance Connect (p. 652) 通过安全 Shell (SSH) 连接到实例，而无需共享和管理 SSH 密钥。
- 使用 Amazon Systems Manager 会话管理器远程访问实例，而不是打开入站 SSH 端口和管理 SSH 密钥。
- 使用 Amazon Systems Manager Run Command 自动执行常见的管理任务，而不是打开入站 SSH 端口和管理 SSH 密钥。

除了限制对每个 Amazon EC2 实例的网络访问之外，Amazon VPC 还支持实施额外的网络安全控制，如内联网关、代理服务器和各种网络监控选项。

Amazon EC2 中的恢复功能

Amazon全球基础设施围绕Amazon区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

如果需要跨更大的地理距离复制数据或应用程序，请使用 AmazonLocal Zones。Amazon 本地扩展区是在地理上靠近您的用户的 Amazon 区域的扩展。Local Zones 有自己的 Internet 连接并支持。Amazon Direct Connect与所有 Amazon 区域类似，Amazon Local Zones 与其他 Amazon区域完全隔离。

如果您需要在 Amazon 本地扩展区中复制数据或应用程序，Amazon 建议您使用以下区域作为故障转移区域：

- 另一个本地扩展区
- 区域中不是父区域的可用区。您可以使用 describe-availability-zones 命令查看父区域。

有关Amazon区域和可用区的更多信息，请参阅Amazon全球基础设施。

除了 Amazon 全球基础设施以外，Amazon EC2 还提供以下功能以支持数据恢复：

- 跨区域复制 AMI
- 跨区域复制 EBS 快照
- 使用 Amazon Data Lifecycle Manager 自动化 EBS 支持的 AMI
- 使用 Amazon Data Lifecycle Manager 自动处理 EBS 快照
- 使用 Amazon EC2 Auto Scaling 保持队列的运行状况和可用性
- 使用 Elastic Load Balancing 在一个或多个可用区中的多个实例之间分配传入流量

Amazon EC2 中的数据保护

Amazon 责任共担模式应用于 Amazon Elastic Compute Cloud 中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center (successor to Amazon Single Sign-On) 或 Amazon Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon Web Services 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如 Name（名称）字段）。这包括当您通过控制台、API、Amazon CLI 或 Amazon SDK 使用 Amazon EC2 或其他 Amazon Web Services 时。您在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

主题

- Amazon EBS 数据安全 (p. 1221)
- 静态加密 (p. 1222)
- 传输中加密 (p. 1222)

Amazon EBS 数据安全

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说明的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

静态加密

EBS 卷

Amazon EBS 加密是适用于 EBS 卷和快照的加密解决方案。它使用 Amazon KMS keys。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

实例存储卷

NVMe 实例存储卷上的数据是使用实例上的硬件模块中实施的 XTS-AES-256 密码加密的。用于加密写入本地连接的 NVMe 存储设备的数据的密钥是针对每个客户和每个卷的。密钥由硬件模块生成并且仅位于硬件模块内，Amazon 人员无法访问该模块。当实例停止或终止并且无法恢复时，将销毁所有加密密钥。无法禁用此加密，并且无法提供自己的加密密钥。

HDD 实例存储卷上的数据在 H1、D3 和 D3en 实例上使用 XTS-AES-256 和一次性密钥加密。

停止、休眠或终止实例时，实例存储卷中的每个存储数据块都会被重置。因此，无法通过另一实例的实例存储访问您的数据。

内存

以下实例上启用了内存加密：

- 使用 Amazon Graviton 处理器的实例。AmazonGraviton2、Amazon Graviton3 和 Amazon Graviton3E 支持始终开启的内存加密。加密密钥是在主机系统内安全生成的，不要离开主机系统，并在重新启动或关闭主机电源时销毁的。有关更多信息，请参阅 Amazon Graviton 处理器。
- 采用英特尔 Xeon 可扩展处理器 (Ice Lake) 的实例，例如 M6i 实例。这些处理器支持使用英特尔总内存加密 (TME) 的永远在线内存加密。
- 使用第三代 AMD 处理器（米兰）的实例，例如 M6a 实例。这些处理器支持使用 AMD 透明单个密钥内存加密 (TSME) 的始终在线内存加密。

传输中加密

物理层加密

所有在Amazon全球网络上跨Amazon区域流动的数据在离开Amazon保护的设施之前都会在物理层自动加密。可用区之间的所有流量均已加密。其他加密层（包括本节中列出的加密层）可能会提供额外保护。

Amazon VPC 和 Transit Gateway 跨区域对等连接提供的加密

使用 Amazon VPC 和 Transit Gateway 对等连接的所有跨区域流量在退出区域时都会自动批量加密。如本节之前所述，在物理层为所有跨区域流量自动提供一层额外加密层。

实例之间的加密

Amazon 在所有类型的 EC2 实例之间提供安全的私有连接。此外，某些实例类型使用底层 Nitro系统硬件的分载功能，使用带 256 位加密的 AEAD 算法，自动加密实例之间的传输中流量。这对网络性能没有影响。要在实例之间支持这种额外的传输中流量加密，必须满足以下要求：

- 使用以下实例类型：
  - 通用型：M5dn、M5n、M5zn、M6a、M6i、M6id、M6idn、M6in 和 M7g
  - 计算优化型：C5a、C5ad、C5n、C6a、C6gn、C6i、C6id、C6in、C7g 和 Hpc6a

  - 内存优化型：Hpc6id、R5dn、R5n、R6a、R6i、R6idn、R6in、R6id、R7g、U-3tb1、U-6tb1、U-9tb1、U-12tb1、U-18tb1、和 X2iezn
  - 存储优化型：D3、D3en、I3en、I4i、Im4gn 和 Is4gen
  - 加速计算型：DL1、G4ad、G4dn、G5、Inf1、P3dn、P4d、P4de、Trn1 和 VT1
- 这些实例位于同一区域。
- 这些实例位于相同 VPC 或对等的 VPC 中，并且流量不会通过虚拟网络设备或服务（如负载均衡器或中转网关）传输。

如本节之前所述，所有跨区域流量在离开Amazon保护的设施之前均会在物理层自动提供一层额外加密层。

使用 Amazon CLI 查看加密实例之间传输中流量的实例类型

使用以下 describe-instance-types 命令。

```
aws ec2 describe-instance-types \
--filters Name=network-info.encryption-in-transit-supported,Values=true \
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

往返于 Amazon Outposts 的加密

Outpost 会创建名为 service links（服务链接）的特殊网络连接到其 Amazon 主区域，并且可以选择创建私有连接到您指定的 VPC 子网。通过这些连接的所有流量都完全加密。有关更多信息，请参阅 。通过服务链路进行连接和传输中加密中的Amazon Outposts用户指南.

远程访问加密

SSH 直接或通过 EC2 Instance Connect 提供了用于远程访问 Linux 实例的安全通信通道。使用 Amazon Systems Manager 会话管理器或 Run Command 对实例的远程访问是使用 TLS 1.2 加密的，创建连接的请求是使用 SigV4 签名的，且由 Amazon Identity and Access Management 进行身份验证并授权。

使用传输层安全性 (TLS) 等加密协议加密在客户端和 Amazon EC2 实例之间传输的敏感数据是您的责任。

适用于 Amazon EC2 的 Identity and Access Management

您的安全凭证使 Amazon 中的服务可以识别您，并授予您对 Amazon 资源（例如您的 Amazon EC2 资源）的无限制使用权限。您可以使用 Amazon EC2 和 Amazon Identity and Access Management（IAM）的功能，在不共享您的安全证书情况下允许其他用户、服务和应用程序使用您的 Amazon EC2 资源。您可以使用 IAM 控制其他用户对您的 Amazon 账户中资源的使用方式，并且您可以使用安全组来控制对您的 Amazon EC2 实例的访问。您可以选择授予 Amazon EC2 资源的完全使用或限制使用权限。

有关使用 IAM 保护您的 Amazon 资源安全的最佳实践，请参阅 IAM 中的安全最佳实践。

目录

- 对您的实例的网络访问 (p. 1224)
- Amazon EC2 权限属性 (p. 1224)
- IAM 和 Amazon EC2 (p. 1224)
- 适用于 Amazon EC2 的 IAM policy (p. 1225)
- Amazon Amazon Elastic Compute Cloud 托管策略 (p. 1276)
- 适用于 Amazon EC2 的 IAM 角色 (p. 1277)

- 为您的 Linux 实例授权入站流量 (p. 1287)

对您的实例的网络访问

安全组起着防火墙的作用，可用于控制允许达到一个或多个实例的流量。启动实例时，您可以为其分配一个或多个安全组。您需要添加规则至每个控制实例流量的安全组。您可以随时修改安全组的规则；新规则会自动应用于该安全组所分配到的所有实例。

有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。

Amazon EC2 权限属性

您的企业可能有多个 Amazon 账户。借助 Amazon EC2，您可以指定能够使用您的 Amazon Machine Image（AMI）和 Amazon EBS 快照的其他 Amazon 账户。这些权限仅在 Amazon 账户级别有效；您不能限制指定 Amazon 账户内特定用户的权限。您指定的 Amazon 账户中的所有用户均可使用 AMI 或快照。

每个 AMI 都拥有一个 `LaunchPermission` 属性，用于控制可以访问该 AMI 的 Amazon 账户。有关更多信息，请参阅将 AMI 设为公用 (p. 124)。

每个 Amazon EBS 快照都有一个 `createVolumePermission` 属性，用于控制哪些 Amazon 账户可以使用该快照。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

IAM 和 Amazon EC2

IAM 允许您执行以下操作：

- 在 Amazon Web Services 账户 下创建用户和组
- 为 Amazon Web Services 账户 下的每个用户分配唯一的安全凭证
- 控制每个用户使用 Amazon 资源执行任务的权限
- 允许另一 Amazon Web Services 账户 中的用户共享 Amazon 资源
- 为 Amazon Web Services 账户 创建角色并定义可以担任这些角色的用户或服务
- 借助企业的现有身份，授予使用 Amazon 资源执行任务的权限

通过将 IAM 与 Amazon EC2 配合使用，您可以控制企业中的用户能否使用特定的 Amazon EC2 API 操作执行任务，以及他们能否使用特定的 Amazon 资源。

本主题有助于回答以下问题：

- 如何在 IAM 中创建组和用户？
- 如何创建策略？
- 在 Amazon EC2 中执行任务时我需要哪些 IAM policy？
- 如何授予在 Amazon EC2 中执行操作的权限？
- 如何授予在 Amazon EC2 中对特定资源执行操作的权限？

创建用户、组和角色

您可以为自己的 Amazon Web Services 账户 创建用户和组，然后为其分配所需权限。作为最佳实践，用户应通过担任 IAM 角色来获取权限。有关如何为 Amazon Web Services 账户 设置用户和组的更多信息，请参阅设置以使用 Amazon EC2。

IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色类似于 IAM 用户，因为它是一个 Amazon 身份，具有确定其在 Amazon 中可执行和不可执行的操作的权限策略。但是，角色旨在让需要它的

任何人代入，而不是唯一地与某个人员关联。此外，角色没有关联的标准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。有关如何创建 IAM 角色并向其授予权限的更多信息，请参阅 Amazon EC2 的 IAM 角色。

相关主题

有关 IAM 的更多信息，请参阅以下文档：

- 适用于 Amazon EC2 的 IAM policy (p. 1225)
- 适用于 Amazon EC2 的 IAM 角色 (p. 1277)
- Amazon Identity and Access Management (IAM)
- IAM 用户指南

适用于 Amazon EC2 的 IAM policy

默认情况下，用户没有创建或修改 Amazon EC2 资源或使用 Amazon EC2 API、Amazon EC2 控制台或 CLI 执行任务的权限。要允许用户创建或修改资源和执行任务，您必须创建 IAM policy 以允许用户使用所需的特定资源和 API 操作，然后将这些策略与需要这些权限的用户、组或 IAM 角色关联起来。

在将策略附加到一个用户、一组用户或角色时，它会授权或拒绝用户使用指定资源执行指定任务。有关 IAM policy 的更多一般信息，请参阅《IAM 用户指南》中的 IAM 中的策略与权限。有关管理和创建自定义 IAM policy 的更多信息，请参阅管理 IAM policy。

入门

IAM policy 必须授予或拒绝使用一个或多个 Amazon EC2 操作的权限。它还必须指定可以用于操作的资源(可以是所有资源，在某些情况下可以是特定资源)。策略还可以包含应用于资源的条件。

Amazon EC2 部分支持资源级权限。这意味着，对于某些 EC2 API 操作，您无法指定用户可用于该操作的资源。相反，您必须允许用户将所有资源用于该操作。

任务	主题
了解策略的基本结构	策略语法 (p. 1226)
在策略中定义操作	Amazon EC2 操作 (p. 1227)
在策略中定义特定资源	适用于 Amazon EC2 的 Amazon Resource Name (ARN) (p. 1227)
将条件应用于资源的使用	Amazon EC2 的条件键 (p. 1228)
使用可用于 Amazon EC2 的资源级权限	Amazon EC2 的操作、资源和条件键
测试策略	检查用户是否具有所需权限 (p. 1230)
生成 IAM policy	基于访问活动生成策略
针对 CLI 或软件开发工具包的策略示例	有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233)
针对 Amazon EC2 控制台的策略示例	用于 Amazon EC2 控制台的示例策略 (p. 1268)

向用户、组和角色授予权限

以下是一些 Amazon 托管式策略示例，您可以根据需求使用这些策略：

- PowerUserAccess
- ReadOnlyAccess
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess

有关可用于 Amazon EC2 的 Amazon 托管式策略的更多信息，请参阅适用于 Amazon Elastic Compute Cloud 的 Amazon 托管式策略。

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

策略结构

以下主题说明 IAM policy 的结构。

目录

- 策略语法 (p. 1226)
- Amazon EC2 操作 (p. 1227)
- Amazon EC2 API 操作支持的资源级权限 (p. 1227)
- 适用于 Amazon EC2 的 Amazon Resource Name (ARN) (p. 1227)
- Amazon EC2 的条件键 (p. 1228)
- 检查用户是否具有所需权限 (p. 1230)

策略语法

IAM policy 是包含一个或多个语句的 JSON 文档。每个语句的结构如下。

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

组成语句的各个元素如下：

- Effect：此 effect 可以是 Allow 或 Deny。默认情况下 用户没有使用资源和 API 操作的权限，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。

- Action：action 是对其授予或拒绝权限的特定 API 操作。要了解有关指定 action 的信息，请参阅 Amazon EC2 操作 (p. 1227)。
- Resource：受操作影响的资源。有些 Amazon EC2 API 操作允许您在策略中包括该操作可以创建或修改的特定资源。您可使用 Amazon Resource Name (ARN) 来指定资源，或使用通配符 (*) 以指明该语句适用于所有资源。有关更多信息，请参阅Amazon EC2 API 操作支持的资源级权限 (p. 1227)。
- Condition：条件是可选的。它们可以用于控制策略生效的时间。想要了解更多有关为 Amazon EC2 指定条件的信息，请参阅 Amazon EC2 的条件键 (p. 1228)。

有关策略要求的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素参考。有关适用于 Amazon EC2 的 IAM policy 语句示例，请参阅 有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233)。

Amazon EC2 操作

在 IAM policy 语句中，您可以从支持 IAM 的任何服务中指定任何 API 操作。对于 Amazon EC2，请使用以下前缀为 API 操作命名：`ec2:`。例如：`ec2:RunInstances` 和 `ec2:CreateImage`。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": ["ec2:action1", "ec2:action2"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名称以单词“Describe”开头的所有操作，如下所示：

```
"Action": "ec2:Describe*"
```

> **Note**
>
> 当前，Amazon EC2 描述 * API 操作都不支持资源级权限。有关 Amazon EC2 资源级权限更多信息，请参阅 适用于 Amazon EC2 的 IAM policy (p. 1225)。

要指定所有 Amazon EC2 API 操作，请使用 * 通配符，如下所示：

```
"Action": "ec2:*"
```

有关 Amazon EC2 操作的列表，请参阅 Amazon EC2 服务授权参考中定义的操作。

Amazon EC2 API 操作支持的资源级权限

资源级权限指的是能够指定允许用户对哪些资源执行操作的能力。Amazon EC2 部分支持资源级权限。这意味着对于某些 Amazon EC2 操作，您可以控制何时允许用户执行操作 (基于必须满足的条件)或是允许用户使用的特定资源。例如，您可以向用户授予启动实例的权限，但是仅限特定类型的实例，并且只能使用特定的 AMI。

要在 IAM policy 语句中指定资源，请使用其 Amazon Resource Name (ARN)。有关指定 ARN 值的详细信息，请参阅 适用于 Amazon EC2 的 Amazon Resource Name (ARN) (p. 1227)。如果 API 操作不支持单个 ARN，则必须使用通配符 (*) 来指定所有资源都可能受到操作的影响。

要查看标识哪些 Amazon EC2 API 操作支持资源级权限的表，以及您可以在策略中使用的 ARN 和条件键，请参阅 Amazon EC2 的操作、资源和条件键。

请记住，您可以在用于 Amazon EC2 API 操作的 IAM policy 中应用基于标签的资源级权限。这可让您更好地控制用户可创建、修改或使用哪些资源。有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。

适用于 Amazon EC2 的 Amazon Resource Name (ARN)

每个 IAM policy 语句适用于您使用资源的 ARN 指定的资源。

ARN 的一般语法如下：

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

service

服务 (例如，ec2)。

区域

资源所在区域（例如，us-east-1）。

account-id

Amazon 账户 ID，不包含连字符（例如，123456789012）。

resourceType

资源类型 (例如，instance)。

resourcePath

识别资源的路径。您可以在路径中使用 * 通配符。

例如，您可以使用特定实例 (i-1234567890abcdef0) 的 ARN 在语句中指定它，如下所示。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

您可以使用 * 通配符指定属于特定账户的所有实例，如下所示。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

还可以使用 * 通配符指定属于特定账户的所有 Amazon EC2 资源，如下所示。

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

要指定所有资源，或者如果特定 API 操作不支持 ARN，请在 Resource 元素中使用 * 通配符，如下所示。

```
"Resource": "*"
```

许多 Amazon EC2 API 操作涉及多种资源。例如，AttachVolume 将一个 Amazon EBS 卷附加到一个实例，从而使用户必须获得相应权限才能使用该卷和该实例。要在单个语句中指定多个资源，请使用逗号分隔其 ARN，如下所示。

```
"Resource": ["arn1", "arn2"]
```

有关 Amazon EC2 资源的 ARN 列表，请参阅 Amazon EC2 定义的资源类型。

Amazon EC2 的条件键

在策略语句中，您可以选择性指定控制策略生效时间的条件。每个条件都包含一个或多个键值对。条件键不区分大小写。我们已经定义了 Amazon 全局条件键以及其他特定于服务的条件键。

有关 Amazon EC2 的服务特定条件键的列表，请参阅 Amazon EC2 的条件键。Amazon EC2 还实施了 Amazon 全局条件键。有关更多信息，请参阅 IAM 用户指南中的在所有请求中可用的信息。

要在 IAM policy 中使用条件键，请使用 Condition 语句。例如，以下策略授予用户添加和删除任何安全组的入站和出站规则的权限。它使用 ec2:Vpc 条件键来指定只能对特定 VPC 中的安全组执行这些操作。

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
    }
  ]
}
```

如果您指定了多个条件或在单一条件中指定了多个密钥，我们将通过逻辑 AND 操作对其进行评估。如果您在单一条件中指定了一个具有多个值的密钥，我们将通过逻辑 OR 操作对其进行评估。必须满足所有条件才能授予权限。

在指定条件时，您也可使用占位符。有关更多信息，请参阅 IAM 用户指南 中的 IAM policy 元素：变量和标签。

> **Important**
>
> 许多条件键是特定于某个资源的，而某些 API 操作会使用多个资源。如果您使用条件键编写策略，请使用语句的 Resource 元素指定要应用该条件键的资源。否则，该策略可能会完全阻止用户执行操作，因为针对未应用条件键的资源的条件检查失败。如果您不想指定资源，或者如果您已将策略的 Action 元素编写为包含多个 API 操作，则必须使用 ...IfExists 条件类型以确保对不使用条件键的资源忽略条件键。有关更多信息，请参阅 IAM 用户指南 中的 ...IfExists 条件。

所有 Amazon EC2 操作都支持 aws:RequestedRegion 和 ec2:Region 条件键。有关更多信息，请参阅示例：限制对特定区域的访问权限 (p. 1234)。

ec2:SourceInstanceARN 条件键

ec2:SourceInstanceARN 条件键可用于指定作为请求源的实例的 ARN 的条件。这是一个 Amazon 全局条件键，并不特定于任何服务。有关策略示例，请参阅 Amazon EC2：附加或分离卷至 EC2 实例和 示例：允许特定实例查看其他 Amazon 服务中的资源 (p. 1264)。ec2:SourceInstanceARN 键不能用作变量来填充语句中 Resource 元素的 ARN。

有关适用于 Amazon EC2 的策略语句示例，请参阅 有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233)。

ec2:Attribute 条件键

ec2:Attribute 条件键可用于按资源的属性筛选访问权限的条件。条件键仅支持原始数据类型的属性，例如字符串或整数，或者只有 Value 属性的复杂对象，例如 ModifyImageAttribute API 操作的 Description（描述）对象。

例如，以下策略使用 ec2:Attribute/Description 条件键按 ModifyImageAttribute API 操作的复杂 Description（描述）对象筛选访问权限。条件键仅允许将图像描述修改为 Production 或 Development 的请求。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

以下示例策略使用 `ec2:Attribute` 条件键按 ModifyImageAttribute API 操作的主要 Attribute（属性）属性筛选访问权限。条件键拒绝尝试修改图像描述的所有请求。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

检查用户是否具有所需权限

在您创建 IAM policy 后，建议您检查它是否允许用户使用策略生效前所需的特定 API 操作和资源。

首先，创建一个用于测试目的的用户，然后将您创建的 IAM policy 与该测试用户关联起来。然后，以测试用户身份提出请求。

如果您测试的 Amazon EC2 操作创建或修改了一种资源，您在提交请求时应该使用 `DryRun` 参数（或运行带有 `--dry-run` 选项的 Amazon CLI 命令）。在这种情况下，调用会完成身份验证检查，但是不会完成该操作。例如，您可以检查用户能否终止特定实例，但不会真的终止它。如果测试用户具有所需的权限，请求会返回 `DryRunOperation`；否则，它会返回 `UnauthorizedOperation`。

如果策略未授予用户您所期望的权限，您可以根据需要调节策略并重新测试，直到您获得预期的结果。

> **Important**
>
> 在其生效之前，它需要几分钟时间将策略更改为适合状态。因此，我们建议您在测试策略更新前，等候五分钟的时间。

如果身份验证检查失败，该请求将返回一个带有诊断信息的代码消息。您可以使用 `DecodeAuthorizationMessage` 操作对消息进行解码。有关更多信息，请参阅 Amazon Security Token Service API Reference 中的 DecodeAuthorizationMessage，以及 Amazon CLI Command Reference 中的 decode-authorization-message。

在创建过程中授予标记资源的权限

某些资源创建 Amazon EC2 API 操作允许您在创建资源时指定标签。您可以使用资源标签来实现基于属性的控制 (ABAC)。有关更多信息，请参阅标记 资源 (p. 1665)和使用资源标签控制对 EC2 资源的访问 (p. 1233)。

为使用户能够在创建时为资源添加标签，他们必须具有使用创建该资源的操作（如 `ec2:RunInstances` 或 `ec2:CreateVolume`）的权限。如果在资源创建操作中指定了标签，则 Amazon 会对 `ec2:CreateTags` 操作执行额外的授权，以验证用户是否具备创建标签的权限。因此，用户还必须具有使用 `ec2:CreateTags` 操作的显式权限。

在 `ec2:CreateTags` 操作的 IAM policy 定义中，使用带有 `Condition` 条件键的 `ec2:CreateAction` 元素，为创建资源的操作授予添加标签的权限。

例如，下面的策略允许用户启动实例并在启动期间向实例和卷应用任何标签。用户无权标记任何现有资源 (他们无法直接调用 `ec2:CreateTags` 操作)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

同样，下面的策略允许用户创建卷并在创建卷期间向卷应用任何标签。用户无权标记任何现有资源 (他们无法直接调用 `ec2:CreateTags` 操作)。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
```

```
            "ec2:CreateAction" : "CreateVolume"
         }
      }
   }
  ]
}
```

仅当用户在资源创建操作中应用了标签时，系统才会评估 ec2:CreateTags 操作。因此，如果未在此请求中指定任何标签，则拥有创建资源权限 (假定没有标记条件) 的用户无需具备使用 ec2:CreateTags 操作的权限。但是，如果用户不具备使用 ec2:CreateTags 操作的权限而又试图创建带标签的资源，则请求将失败。

如果在启动模板中提供了标签，也会对 ec2:CreateTags 操作进行评估。有关策略示例，请参阅启动模板中的标签 (p. 1253)。

控制对特定标签的访问

您可以在 IAM policy 的 Condition 元素中使用其他条件来控制可应用到资源的标签键和值。

以下条件键可用于上一节中的示例：

- aws:RequestTag：指示请求中必须存在特定的标签键或标签键和值。也可在此请求中指定其他标签。
  - 与 StringEquals 条件运算符配合使用，以强制实施特定的标签键和值组合，例如强制实施标签 cost-center=cc123：

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - 与 StringLike 条件运算符配合使用，以在请求中强制实施特定的标签键；如强制实施标签键 purpose：

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- aws:TagKeys：强制实施在请求中使用的标签键。
  - 与 ForAllValues 修饰符配合使用，以只强制实施请求中提供的特定标签键 (如果在请求中指定了标签，则只允许特定的标签键；不允许任何其他标签)。例如，允许标签键 environment 或 cost-center：

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

  - 与 ForAnyValue 修饰符配合使用，以强制请求中至少存在一个指定的标签键。例如，强制请求中至少存在标签键 environment 或 webserver 中的一个：

    ```
    "ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
    ```

上述条件键可应用于支持标记的资源创建操作，以及 ec2:CreateTags 和 ec2:DeleteTags 操作。要了解 Amazon EC2 API 操作是否支持添加标签，请参阅 Amazon EC2 的操作、资源和条件建。

为强制用户指定标签，在创建资源时，您必须使用 aws:RequestTag 条件键或 aws:TagKeys 条件键，并在资源创建操作中使用修饰符 ForAnyValue。如果用户没有为资源创建操作指定标签，则不会对 ec2:CreateTags 操作进行评估。

对于条件，条件键不区分大小写，条件值区分大小写。因此，要强制标签键区分大小写，请使用 aws:TagKeys 条件键，其中标签键指定为条件中的值。

有关示例 IAM policies，请参阅 有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233)。有关多值条件的更多信息，请参阅IAM 用户指南中的创建测试多个键值的条件。

使用资源标签控制对 EC2 资源的访问

在创建向用户授予使用 EC2 资源的权限的 IAM policy 时，可以在该策略的 Condition 元素中包含标签信息，以根据标签控制访问权限。这称为基于属性的访问控制 (ABAC)。ABAC 可以让您更好地控制用户可以修改、使用或删除哪些 EC2 资源。有关更多信息，请参阅什么是适用于 Amazon 的 ABAC？

例如，您可以创建一个策略，允许用户终止实例，但在实例具有 environment=production 标签时拒绝此操作。为此，您可以使用 aws:ResourceTag 条件键来基于附加到资源的标签允许或拒绝对资源的访问。

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

要了解 Amazon EC2 API 操作是否支持使用 aws:ResourceTag 条件键控制访问，请参阅 Amazon EC2 的操作、资源和条件建。请注意，Describe 操作不支持资源级权限，因此，您必须在不带条件的单独语句中指定它们。

有关示例 IAM policies，请参阅 有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233)。

如果您基于标签允许或拒绝用户访问资源，则必须考虑显式拒绝用户对相同资源添加或删除这些标签的能力。否则，用户可能通过修改资源标签来绕过您的限制并获得资源访问权限。

有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略

您必须通过 IAM policy 为用户授予使用 Amazon EC2 所需的权限。以下示例显示了可用于控制用户对 Amazon EC2 拥有的权限的策略语句。这些策略设计用于采用 Amazon CLI 或 Amazon 开发工具包发出的请求。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy。有关用于 Amazon EC2 控制台的策略示例，请参阅 用于 Amazon EC2 控制台的示例策略 (p. 1268)。有关特定于 Amazon VPC 的 IAM policy 示例，请参阅 Identity and Access Management for Amazon VPC。

在以下示例中，将每个 *user input placeholder* 替换为您自己的信息。

示例

- 示例：只读访问权限 (p. 1233)
- 示例：限制对特定区域的访问权限 (p. 1234)
- 使用实例 (p. 1234)
- 使用卷 (p. 1236)
- 使用快照 (p. 1238)
- 启动实例 (RunInstances) (p. 1245)
- 使用竞价型实例 (p. 1256)
- 示例：使用预留实例 (p. 1261)
- 示例：标记资源 (p. 1261)
- 示例：使用 IAM 角色 (p. 1263)
- 示例：使用路由表 (p. 1264)
- 示例：允许特定实例查看其他 Amazon 服务中的资源 (p. 1264)
- 示例：使用启动模板 (p. 1265)
- 使用实例元数据 (p. 1266)

示例：只读访问权限

以下策略为用户授予使用名称以 Describe 开头的所有 Amazon EC2 API 操作的权限。Resource 元素使用通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 *

通配符。有关哪些 ARN 可用于哪些 Amazon EC2 API 操作的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

用户无权对资源执行任何操作 (除非其他语句为用户授予执行此操作的权限)，因为在默认情况下会对用户拒绝使用 API 操作的权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

示例：限制对特定区域的访问权限

以下策略拒绝用户使用所有 Amazon EC2 API 操作的权限，除非区域为欧洲（法兰克福）。该区域使用全局条件键 `aws:RequestedRegion`，所有 Amazon EC2 API 操作均支持此条件键。

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
}
```

或者，您也可以使用条件键 `ec2:Region`，此条件键是 Amazon EC2 特定的，所有 Amazon EC2 API 操作均支持它。

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

使用实例

示例

- 示例：描述、启动、停止和终止所有实例 (p. 1235)
- 示例：描述所有实例，以及仅停止、启动和终止特定实例 (p. 1235)

示例：描述、启动、停止和终止所有实例

以下策略为用户授予使用 Action 元素中指定的 API 操作的权限。Resource 元素使用 * 通配符表示用户可以通过这些 API 操作指定所有资源。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。有关哪些 ARN 可用于哪些 Amazon EC2 API 操作的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

用户无权使用任何其他 API 操作 (除非其他语句允许用户执行此操作)，因为用户在默认情况下没有使用 API 操作的权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

示例：描述所有实例，以及仅停止、启动和终止特定实例

以下策略允许用户描述所有实例，但只能启动和停止实例 i-1234567890abcdef0 和 i-0598c7d356eba48d7，且只能终止在 美国东部（弗吉尼亚北部）地区 (us-east-1) 中具有“purpose=test”资源标签的实例。

第一条语句为 Resource 元素使用 * 通配符以指示用户可以在操作中指定所有资源；在本例中，用户可以列出所有实例。在 API 操作不支持资源级权限的情况下 (在此情况下，为 ec2:DescribeInstances)，也需要 * 通配符。有关哪些 ARN 可用于哪些 Amazon EC2 API 操作的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

第二条语句为 StopInstances 和 StartInstances 操作使用资源级权限。特定实例在 Resource 元素中通过其 ARN 进行指示。

第三条语句允许用户终止在美国东部（弗吉尼亚北部）区域（us-east-1）中属于指定 Amazon 账户的所有实例（但仅在实例具有 "purpose=test" 标签的情况下）。当策略语句生效时，Condition 元素具备资格。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
```

```
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

使用卷

示例

- 示例：附加和分离卷 (p. 1236)
- 示例：创建卷 (p. 1237)
- 示例：创建带有标签的卷 (p. 1237)

示例：附加和分离卷

在 API 操作需要发起人指定多种资源时，您必须创建一个策略语句，允许用户访问所需的所有资源。如果使用 Condition 元素时需要其中一种或多种资源，则必须创建多个语句，如本示例所示。

以下策略允许用户将带有 “volume_user=iam-user-name” 标签的卷与带有 “department=dev” 标签的实例关联起来，以及将这些卷与这些实例取消关联。如果您将此策略添加到 IAM 组，aws:username 策略变量将授权组中的每位用户向具有 volume_user 标签（将用户的用户名作为值）的实例挂载卷，或从那些实例分离这些卷。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
    }
  ]
}
```

示例：创建卷

以下策略允许用户使用 CreateVolume API 操作。系统只允许用户创建加密且大小不足 20 GiB 的卷。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition":{
         "NumericLessThan": {
             "ec2:VolumeSize" : "20"
          },
          "Bool":{
              "ec2:Encrypted" : "true"
          }
       }
    }
  ]
}
```

示例：创建带有标签的卷

下面的策略包含 aws:RequestTag 条件键，该条件键要求用户标记其使用标签 costcenter=115 和 stack=prod 创建的任何卷。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，用户还必须具有使用 CreateTags 操作的权限。第二个语句使用 ec2:CreateAction 条件键使用户只能在 CreateVolume 上下文中创建标签。用户无法标记现有卷或任何其他资源。有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "CreateVolume"
        }
      }
    }
  ]
}
```

下面的策略允许用户创建卷而无需指定标签。仅当用户在 CreateTags 请求中指定了标签时，系统才会评估 CreateVolume 操作。如果用户指定了标签，则标签必须为 purpose=test。请求中不允许使用任何其他标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "CreateVolume"
         },
         "ForAllValues:StringEquals": {
             "aws:TagKeys": "purpose"
         }
      }
    }
  ]
}
```

使用快照

以下是 CreateSnapshot（EBS 卷的时间点快照）和 CreateSnapshots（多卷快照）的示例策略。

示例

- 示例：创建快照 (p. 1238)
- 示例：创建快照 (p. 1239)
- 示例：创建具有标签的快照 (p. 1239)
- 示例：创建带有标签的多卷快照 (p. 1240)
- 示例：复制快照 (p. 1244)
- 示例：修改快照的权限设置 (p. 1245)

示例：创建快照

以下策略允许客户使用 CreateSnapshot API 操作。仅当卷已加密并且卷大小不超过 20 GiB 时，客户才能创建快照。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "NumericLessThan":{
               "ec2:VolumeSize":"20"
            },
            "Bool":{
               "ec2:Encrypted":"true"
            }
         }
      }
   ]
}
```

示例：创建快照

以下策略允许客户使用 CreateSnapshots API 操作。仅当实例上的所有卷均为类型 GP2 时，客户才能创建快照。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
             }
     }

      }
   ]
}
```

示例：创建具有标签的快照

下面的策略包含 aws:RequestTag 条件键，该条件键要求客户将标签 costcenter=115 和 stack=prod 应用于任何新快照。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，客户还必须具有使用 CreateTags 操作的权限。第三个语句使用 ec2:CreateAction 条件键使客户只能在 CreateSnapshot 上下文中创建标签。客户无法标记现有卷或任何其他资源。有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*"
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshot"
            }
         }
      }
   ]
}
```

示例：创建带有标签的多卷快照

下面的策略包含 aws:RequestTag 条件键，该条件键要求客户在创建多卷快照集时应用标签 costcenter=115 和 stack=prod。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"

   ]
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
```

```
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

下面的策略允许客户创建快照而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshot"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

下面的策略允许客户创建多卷快照集而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
```

```
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。客户可向快照添加其他标签。

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

CreateSnapshots 的以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:instance/*",
 },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
```

```
        }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

以下策略仅允许在以下情况下删除快照：快照已使用客户的 User:username 进行标记。

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
```

```
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

以下策略允许您将多个操作整合到单个策略中。您只能在快照在区域 us-east-1 中创建时创建快照（在 CreateSnapshots 的上下文稿中）。您只能在快照正在区域 CreateSnapshots 中创建时且实例类型为 us-east-1 时创建快照（在 t2* 的上下文中）。

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
         "Condition":{
            "StringEqualsIgnoreCase": {
              "ec2:Region": "us-east-1"
            },
            "StringLikeIfExists": {
              "ec2:InstanceType": ["t2.*"]
            }
         }
      }
   ]
}
```

示例：复制快照

为 CopySnapshot 操作指定的资源级权限仅适用于新快照。无法为源快照指定资源级权限。

只有在使用标签键 purpose 和标签值 production (purpose=production) 创建新快照时，以下示例策略才允许委托人复制快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

示例：修改快照的权限设置

以下策略仅允许在以下情况下修改快照：快照已使用 User:*username* 标记，其中 *username* 是客户的 Amazon 账户用户名。如果未满足此条件，则请求将失败。

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
         }
      }
   ]
}
```

启动实例 (RunInstances)

RunInstances API 操作可启动一个或多个按需实例或一个或多个 Spot 实例。RunInstances 需要 AMI 并创建实例。用户可以在请求中指定键对和安全组。启动到 VPC 中需要子网，会创建网络接口。从 Amazon EBS-backed AMI 启动将创建卷。因此，用户必须具有使用这些 Amazon EC2 资源的权限。您可以创建要求用户对 RunInstances 指定可选参数或限制用户针对某个参数使用特定值的策略语句。

有关启动实例所需的资源级权限的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

默认情况下，用户没有描述、启动、停止或终止生成的实例的权限。授予用户管理所生成实例的权限的一种方法是：为每个实例创建一个特定标签，然后创建一个允许用户使用该标签管理实例的语句。有关更多信息，请参阅使用实例 (p. 1234)。

资源

- AMI (p. 1246)
- 实例类型 (p. 1247)
- 子网 (p. 1248)
- EBS 卷 (p. 1249)

- 标签 (p. 1249)
- 启动模板中的标签 (p. 1253)
- Elastic GPUs (p. 1254)
- 启动模板 (p. 1254)

AMI

以下策略仅允许用户使用指定的 AMI、ami-9e1670f7 和 ami-45cf5c3c 启动实例。用户无法使用其他 AMI 启动实例（除非其他语句允许用户执行此操作）。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

另外，以下策略允许用户从 Amazon 或某些受信任和经过验证的合作伙伴拥有的所有 AMI 启动实例。第一个语句的 Condition 元素测试 ec2:Owner 是不是 amazon。用户无法使用其他 AMI 启动实例（除非其他语句允许用户执行此操作）。

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
```

```
   ]
}
```

实例类型

以下策略仅允许用户使用 t2.micro 或 t2.small 实例类型启动实例，您也可以通过此操作控制成本。用户无法启动更大的实例，因为第一条语句的 Condition 元素会测试 ec2:InstanceType 是否是 t2.micro 或 t2.small。

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

或者，您也可以创建一个策略，以拒绝用户启动 t2.micro 和 t2.small 实例类型之外的任何实例的权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
```

```
            "arn:aws:ec2:region:account-id:instance/*",
            "arn:aws:ec2:region:account-id:subnet/*",
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:key-pair/*",
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}
```

子网

以下策略仅允许用户使用指定子网 subnet-*12345678* 启动实例。组无法将实例启动到任何其他子网中 (除非其他语句授予执行此操作的用户权限)。

```
{
    "Version": "2012-10-17",
    "Statement": [
     {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
         "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
       ]
     }
    ]
}
```

或者，您也可以创建一个策略，以拒绝用户将实例启动到任何其他子网的权限。该语句通过拒绝创建网络接口的权限来执行此操作，除非指定了子网 subnet-*12345678*。此拒绝会覆盖创建的任何其他策略以允许将实例启动到其他子网中。

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
       "Effect": "Deny",
       "Action": "ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:region:account-id:network-interface/*"
       ],
       "Condition": {
          "ArnNotEquals": {
             "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
          }
       }
    },
    {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:region::image/ami-*",
          "arn:aws:ec2:region:account-id:network-interface/*",
          "arn:aws:ec2:region:account-id:instance/*",
          "arn:aws:ec2:region:account-id:subnet/*",
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:key-pair/*",
```

```
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}
```

EBS 卷

仅当实例的 EBS 卷为加密卷时，下面的策略才允许用户启动实例。用户必须从使用加密快照创建的 AMI 启动实例，以确保根卷是加密的。此外，用户在启动期间附加到此实例的任何其他卷也必须是加密的。

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

标签

在创建时标记实例

下面的策略允许用户启动实例并在创建期间标记实例。对于应用标签的资源创建操作，用户必须具有使用 CreateTags 操作的权限。第二个语句使用 ec2:CreateAction 条件键使用户只能在 RunInstances 上下文中且只能为实例创建标签。用户无法标记现有资源，并且用户无法使用 RunInstances 请求标记卷。

有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

在创建时使用特定标签标记实例和卷

下面的策略包含 aws:RequestTag 条件键，该条件键要求用户标记使用标签 RunInstances 和 environment=production 通过 purpose=webserver 创建的任何卷。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/environment": "production" ,
             "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
```

```
}
```

在创建时使用至少一个特定标记标记实例和卷

下面的策略对 ForAnyValue 条件使用了 aws:TagKeys 修饰符，以指示必须在请求中指定至少一个标签，并且其必须包含键 environment 或 webserver。标签必须应用于实例及卷。可以在请求中指定任何标签值。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
          "ForAnyValue:StringEquals": {
              "aws:TagKeys": ["environment","webserver"]
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
          "StringEquals": {
              "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

如果在创建时标记实例，则必须使用特定标签标记它们

在下面的策略中，用户不必在请求中指定标签，但如果用户指定标签，则标签必须为 purpose=test。不允许使用任何其他标签。用户可以在 RunInstances 请求中向任何可标记资源应用标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

禁止任何人在创建时为 RunInstances 调用标签

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

仅允许为 spot-instances-request 使用特定标签。第二个意外的不一致之处在这里发挥了作用。在正常情况下，不指定标签将导致 Unauthenticated 错误。对于 spot-instances-request，如果没有 spot-instances-request 标签，则不会评估此策略，因此无标签的 Spot on Run 请求将成功。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

启动模板中的标签

在以下示例中，用户可以启动实例，但前提是他们使用特定的启动模板 (lt-09477bcd97b0d310e)。ec2:IsLaunchTemplateResource 条件键禁止用户覆盖在启动模板中指定的任何资源。语句的第二部分允许用户在创建时标记实例 — 如果在启动模板中为实例指定了标签，则该语句部分是必需的。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
         "StringEquals": {
```

```
            "ec2:CreateAction" : "RunInstances"
         }
      }
   }
  ]
}
```

Elastic GPUs

在以下策略中，用户可以启动实例并指定要附加到实例的 Elastic GPU。用户可以在任何区域中启动实例，但他们只能在 us-east-2 区域中启动期间附加 Elastic GPU。

ec2:ElasticGpuType 条件键使用 ForAnyValue 修饰符指示只允许在请求中使用 Elastic GPU 类型 eg1.medium 和 eg1.large。

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2"
                },
                "ForAnyValue:StringLike": {
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

启动模板

在以下示例中，用户可以启动实例，但前提是他们使用特定的启动模板 (lt-09477bcd97b0d310e)。用户可以在 RunInstances 操作中指定参数以覆盖启动模板中的任何参数。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

在该示例中，只有在用户使用启动模板时，他们才能启动实例。该策略使用 ec2:IsLaunchTemplateResource 条件键防止用户覆盖启动模板中任何预先存在的 ARN。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

以下示例策略允许用户启动实例，但前提是他们使用启动模板。用户无法覆盖请求中的子网和网络接口参数；只能在启动模板中指定这些参数。语句的第一部分使用 NotResource 元素允许子网和网络接口以外的所有其他资源。语句的第二部分允许子网和网络接口资源，但前提是它们来自于启动模板。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
```

```
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

以下示例允许用户启动实例，但前提是他们使用启动模板，并且启动模板具有标签 `Purpose=Webservers`。用户无法覆盖 `RunInstances` 操作中的任何启动模板参数。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
       }
     }
  ]
}
```

使用竞价型实例

您可以使用 RunInstances 操作创建竞价型实例请求，并在创建时标记竞价型实例请求。要为 RunInstances 指定的资源为 `spot-instances-request`。

在 IAM policy 中评估 `spot-instances-request` 资源，如下所示：

- 如果您在创建时未标记竞价型实例请求，则 Amazon EC2 不会在 RunInstances 语句中评估 `spot-instances-request` 资源。
- 如果您在创建时标记竞价型实例请求，则 Amazon EC2 会在 RunInstances 语句中评估 `spot-instances-request` 资源。

因此，对于 `spot-instances-request` 资源，以下规则适用于 IAM policy：

- 如果您使用 RunInstances 创建竞价型实例请求，并且您不打算在创建时标记竞价型实例请求，则无需明确允许 `spot-instances-request` 资源；调用将成功。
- 如果您使用 RunInstances 创建竞价型实例请求并打算在创建时标记竞价型实例请求，则必须在 RunInstances 允许语句中包含 `spot-instances-request` 资源，否则调用将失败。
- 如果您使用 RunInstances 创建竞价型实例请求并打算在创建时标记竞价型实例请求，则必须在 CreateTags 允许语句中指定 `spot-instances-request` 资源或 * 通配符，否则调用将失败。

您可以使用 RunInstances 或 RequestSpotInstances 请求竞价型实例。以下示例 IAM policy 仅在使用 RunInstances 请求竞价型实例时适用。

示例：使用 RunInstances 请求竞价型实例

以下策略允许用户使用 RunInstances 操作请求竞价型实例。由 RunInstances 创建的 `spot-instances-request` 资源将请求 Spot 实例。

Note

要使用 RunInstances 创建竞价型实例请求，您可以从 `spot-instances-request` 列表中省略 `Resource`（如果您不打算在创建时标记竞价型实例请求）。这是因为，如果在创建时未标记竞价型实例请求，则 Amazon EC2 不会在 RunInstances 语句中评估 `spot-instances-request` 资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

Warning

不支持 – 示例：拒绝用户使用 RunInstances 请求竞价型实例的权限
`spot-instances-request` 资源不支持以下策略。
以下策略旨在向用户授予启动按需型实例的权限，但拒绝用户请求竞价型实例的权限。由 RunInstances 创建的 `spot-instances-request` 资源是请求 Spot 实例的资源。第二个语句旨在拒绝针对 `spot-instances-request` 资源的 RunInstances 操作。但不支持此条件，这是因为，如果在创建时未标记竞价型实例请求，则 Amazon EC2 不会在 RunInstances 语句中评估 `spot-instances-request` 资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
```

```
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

示例：在创建时标记竞价型实例请求

以下策略允许用户标记在实例启动期间创建的所有资源。第一个语句允许 RunInstances 创建列出的资源。由 RunInstances 创建的 spot-instances-request 资源是请求 Spot 实例的资源。第二个语句提供了一个 * 通配符，以允许在实例启动时创建所有资源时对其进行标记。

Note

如果您在创建时标记竞价型实例请求，则 Amazon EC2 会在 RunInstances 语句中评估 spot-instances-request 资源。因此，您必须明确允许 RunInstances 操作的 spot-instances-request 资源，否则调用将失败。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

示例：拒绝在创建时标记竞价型实例请求

以下策略拒绝用户标记在实例启动期间创建的资源的权限。

第一个语句允许 RunInstances 创建列出的资源。由 RunInstances 创建的 spot-instances-request 资源是请求 Spot 实例的资源。第二个语句提供了一个 * 通配符，以拒绝在实例启动时创建所有资源时对其进行标记。如果在创建时标记 spot-instances-request 或任何其他资源，则 RunInstances 调用将失败。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Warning

不支持 – 示例：仅在为竞价型实例请求分配了特定标签时允许创建该请求 `spot-instances-request` 资源不支持以下策略。
以下策略旨在向 RunInstances 授予权限以仅在使用特定标签标记竞价型实例请求时创建该请求。
第一个语句允许 RunInstances 创建列出的资源。
第二个语句旨在向用户授予权限以仅在竞价型实例请求具有标签 `environment=production` 时创建该请求。如果将此条件应用于由 RunInstances 创建的其他资源，则不指定标签会导致 `Unauthenticated` 错误。但是，如果没有为竞价型实例请求指定标签，则 Amazon EC2 不会在 RunInstances 语句中评估 `spot-instances-request` 资源，这会导致 RunInstances 创建未标记的竞价型实例请求。
请注意，请指定 `environment=production` 之外的其他标签会导致错误 `Unauthenticated`，这是因为，如果用户标记竞价型实例请求，则 Amazon EC2 会在 RunInstances 语句中评估 `spot-instances-request` 资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
```

```
        },
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

示例：在为竞价型实例请求分配了特定标签的情况下拒绝创建该请求

如果使用 environment=production 标记了竞价型实例请求，则以下策略将拒绝 RunInstances 创建该请求的权限。

第一个语句允许 RunInstances 创建列出的资源。

第二个语句在竞价型实例请求具有标签 environment=production 时拒绝用户创建该请求的权限。指定 environment=production 作为标签会导致 Unauthenticated 错误。指定其他标签或不指定标签将导致创建竞价型实例请求。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
```

```
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

示例：使用预留实例

下面的策略向用户授予在账户中查看、修改和购买预留实例的权限。

无法为个别的预留实例设置资源级别的许可。此策略表示用户可以访问账户中的所有预留实例。

Resource 元素使用 * 通配符指示用户可以在操作中指定所有资源；在本例中，他们可以列出并修改账户中的所有 预留实例。他们还可以使用账户凭证购买预留实例。在 API 操作不支持资源级权限的情况下，也需要 * 通配符。

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

要允许用户查看和修改账户中的 预留实例，但不允许购买新的 预留实例，请使用以下命令：

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
}
```

示例：标记资源

仅当标签包含键 CreateTags 和值 environment 时，下面的策略才允许用户使用 production 操作向实例应用标签。不允许使用其他标签，并且用户无法为任何其他资源类型添加标签。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

以下策略允许用户标记已具有键为 owner、值为用户名的标签的任何可标记资源。此外，用户还必须在请求中指定键为 anycompany:environment-type、值为 test 或 prod 的标签。用户可以在请求中指定其他的标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

您可以创建允许用户删除资源的特定标签的 IAM policy。例如，当在请求中指定的标签键为 environment 或 cost-center 时，下面的策略允许用户删除卷的标签。可以为此标签指定任何值，但标签键必须匹配某个指定键。

Note

如果删除资源，则所有与资源相关的标签都将被删除。用户不需要使用 ec2:DeleteTags 操作删除具有标签的资源的权限，他们仅需要执行删除操作的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
```

```
}
```

该策略仅允许用户删除任何资源上的 environment=prod 标签，但前提是已使用键为 owner、值为用户名的标签标记该资源。用户无法删除资源的任何其他标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

示例：使用 IAM 角色

以下策略允许用户将 IAM 角色附加、替换到具有标签 department=test 的实例或与之分离。替换或分离 IAM 角色需要一个关联 ID，因此该策略还授予用户使用 ec2:DescribeIamInstanceProfileAssociations 操作的权限。

用户必须具有使用 iam:PassRole 操作的权限，才能将角色传递到实例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
```

```
}
```

以下策略允许用户为所有实例附加或替换 IAM 角色。用户只能附加或替换名称以 TestRole- 开头的 IAM 角色。对于 iam:PassRole 操作，请确保您指定的是 IAM 角色的名称而不是实例配置文件的名称（如果名称不同）。有关更多信息，请参阅实例配置文件 (p. 1278)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

示例：使用路由表

以下策略允许用户添加、删除和替换仅与 VPC vpc-ec43eb89 关联的路由表的路由。要为 ec2:Vpc 条件键指定 VPC，必须指定 VPC 的完整 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

示例：允许特定实例查看其他 Amazon 服务中的资源

下面是您可能附加到 IAM 角色的策略的示例。该策略允许实例查看不同 Amazon 服务中的资源。它使用 ec2:SourceInstanceARN 条件键指定从中发出请求的实例必须是实例 i-093452212644b0dd6。如果同一个 IAM 角色还与另一个实例关联，则另一个实例无法执行任何这些操作。

ec2:SourceInstanceARN 键是一个 Amazon 全局条件键，因此可用于其他服务操作，而不局限于 Amazon EC2。

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

示例：使用启动模板

以下策略允许用户创建启动模板版本和修改启动模板，但仅适用于特定的启动模板 (lt-*09477bcd97b0d3abc*)。用户无法使用其他启动模板。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

以下策略允许用户删除任何启动模板和启动模板版本，但前提是启动模板具有标签 Purpose=Testing。

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
```

```
      }
    }
  ]
}
```

使用实例元数据

以下策略确保用户只能使用 实例元数据服务版本 2 (IMDSv2) 检索实例元数据 (p. 754)。您可以将以下四个策略合并为一个具有四个语句的策略。当合并为一个策略时，您可以将该策略用作服务控制策略 (SCP)。它可以很好地用作应用于现有 IAM policy 的拒绝 策略（取消和限制现有权限），也可以很好地用作在账户、组织单位 (OU) 或整个组织间全局应用的 SCP。

> **Note**
>
> 以下 RunInstances 元数据选项策略必须与授予委托人使用 RunInstances 启动实例的权限的策略结合使用。如果委托人没有同时具有 RunInstances 权限，则无法启动实例。有关更多信息，请参阅使用实例 (p. 1234)和启动实例 (RunInstances) (p. 1245) 中的策略。

> **Important**
>
> 如果您使用 Auto Scaling 组且需要要求对所有新实例使用 IMDSv2，您的 Auto Scaling 组必须使用启动模板。
> 当 Auto Scaling 组使用启动模板时，会在创建新 Auto Scaling 组时检查 IAM 委托人的 `ec2:RunInstances` 权限。当更新现有 Auto Scaling 组以使用新启动模板或新版本的启动模板时，也会检查这些内容。
> 只有在创建或更新正在使用启动模板的 Auto Scaling 组时，才会检查对 `RunInstances` 的 IAM 委托人使用 IMDSv1 的限制。对于配置为使用 `Latest` 或 `Default` 启动模板的 Auto Scaling 组，在创建启动模板的新版本时不会检查权限。要检查权限，您必须将 Auto Scaling 组配置为使用特定版本 的启动模板。
>
> 要在 Auto Scaling 组启动的实例上强制使用 IMDSv2，需要执行以下附加步骤：
>
> 1. 通过对创建的新委托人使用服务控制策略 (SCP) 或 IAM 权限边界，请对组织中的所有账户禁用启动配置。对于具有 Auto Scaling 组权限的现有 IAM 委托人，请使用此条件键更新其关联策略。要禁用启动配置，请使用值指定为 `"autoscaling:LaunchConfigurationName"` 的 `null` 条件键创建或修改相关 SCP、权限边界或 IAM policy。
> 2. 对于新启动模板，请在启动模板中配置实例元数据选项。对于现有启动模板，创建启动模板的新版本，并在新版本中配置实例元数据选项。
> 3. 在向任何委托人授予使用启动模板的权限的策略中，通过指定 `$latest` 来限制 `$default` 和 `"autoscaling:LaunchTemplateVersionSpecified": "true"` 的关联。通过限制只使用特定版本的启动模板，您可以确保使用在其中配置实例元数据选项的版本启动新实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling API 参考 中的 LaunchTemplateSpecification，特别是 `Version` 参数。
> 4. 对于使用启动配置的 Auto Scaling 组，请将启动配置替换为启动模板。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的使用启动模板替换启动配置。
> 5. 对于使用启动模板的 Auto Scaling 组，请确保它使用配置了实例元数据选项的新启动模板，或使用配置了实例元数据选项的新版本的当前启动模板。有关更多信息，请参阅 Amazon CLI Command Reference 中的 update-auto-scaling-group。

示例

- 要求使用 IMDSv2 (p. 1267)
- 指定最大跃点数限制 (p. 1267)
- 限制可以修改实例元数据选项的用户 (p. 1267)
- 要求从 IMDSv2 检索角色凭证 (p. 1268)

要求使用 IMDSv2

以下策略指定您不能调用 RunInstances API，除非该实例也选择需要使用 IMDSv2（由 "ec2:MetadataHttpTokens": "required" 指示）。如果您未指定实例需要 IMDSv2，则在调用 RunInstances API 时会收到 UnauthorizedOperation 错误。

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

指定最大跃点数限制

以下策略指定您不能调用 RunInstances API，除非您还指定了跃点限制，且跃点限制不能超过 3。如果您无法执行此操作，则在调用 RunInstances API 时会收到 UnauthorizedOperation 错误。

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

限制可以修改实例元数据选项的用户

以下策略仅允许具有 ec2-imds-admins 角色的用户对实例元数据选项进行更改。如果除 ec2-imds-admins 角色以外的任何委托人尝试调用 ModifyInstanceMetadataOptions API，则会收到 UnauthorizedOperation 错误。此语句可用于控制 ModifyInstanceMetadataOptions API 的使用；目前对于 ModifyInstanceMetadataOptions API 没有精细访问控制（条件）。

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
```

```
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

要求从 IMDSv2 检索角色凭证

以下策略指定如果将此策略应用于某个角色，并且该角色由 EC2 服务代入且生成的凭证用于对请求进行签名，则必须由从 IMDSv2 中检索的 EC2 角色凭证对该请求进行签名。否则，它的所有 API 调用都会收到 `UnauthorizedOperation` 错误。此语句/策略可广泛应用，因为如果请求未由 EC2 角色证书签名，则其为无效。

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

用于 Amazon EC2 控制台的示例策略

您必须通过 IAM policy 为用户授予使用 Amazon EC2 所需的权限。您可以使用 IAM policy 向用户授予在 Amazon EC2 控制台中查看和使用特定资源的权限。您可以使用上一部分中的策略；但是，这些策略设计用于使用 Amazon CLI 或 Amazon 开发工具包发出的请求。有关更多信息，请参阅《IAM 用户指南》中的 有关使用 Amazon CLI 或 Amazon 开发工具包的示例策略 (p. 1233) 和 创建 IAM policy。

控制台使用其他 API 操作实现其功能，因此这些策略可能不会按预期方式起作用。例如，只拥有 `DescribeVolumes` API 操作使用权限的用户在控制台中查看卷时会遇到错误。此部分演示使用户可以使用控制台的特定部分的策略。有关创建 Amazon EC2 控制台的策略的更多信息，请参阅发布的以下Amazon安全博客：授予用户在 Amazon EC2 控制台中工作的权限。

> **Tip**
>
> 为帮助您了解在控制台中执行任务所需的相应 API 操作，您可以使用 Amazon CloudTrail 等服务。有关更多信息，请参阅 Amazon CloudTrail 用户指南。如果您的策略不授予创建或修改特定资源的权限，则控制台显示一个包含诊断信息的编码消息。您可以使用适用于 Amazon STS 的 DecodeAuthorizationMessage API 操作或 Amazon CLI 中的 decode-authorization-message 命令对该消息解码。

示例

- 示例：只读访问权限 (p. 1269)
- 示例：使用 EC2 启动实例向导 (p. 1269)
- 示例：使用卷 (p. 1272)
- 示例：使用安全组 (p. 1273)
- 示例：使用弹性 IP 地址 (p. 1275)

- 示例：使用预留实例 (p. 1276)

示例：只读访问权限

要允许用户在 Amazon EC2 控制台中查看所有资源，您可以使用与以下示例相同的策略：示例：只读访问权限 (p. 1233)用户无法对这些资源执行任何操作或创建新资源 (除非其他语句为用户授予执行此操作的权限)。

查看实例、AMI 和快照

或者，您可以提供对资源子集的只读访问权限。为此，请对每个资源将 `ec2:Describe` API 操作中的 * 通配符替换为特定 `ec2:Describe` 操作。以下策略允许用户在 Amazon EC2 控制台中查看所有实例、AMI 和快照。`ec2:DescribeTags` 操作允许用户查看公用 AMI。控制台需要标记信息来显示公用 AMI；但是，您可以删除此操作以允许用户只查看私有 AMI。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Amazon EC2 `ec2:Describe*` API 操作不支持资源级权限，因此您无法控制用户可以在控制台中查看哪些单个资源。因此，在以上语句的 `Resource` 元素中需要 * 通配符。有关哪些 ARN 可用于哪些 Amazon EC2 API 操作的更多信息，请参阅 Amazon EC2 的操作、资源和条件键。

查看实例和 CloudWatch 指标

以下策略允许用户在 Amazon EC2 控制台中查看实例，以及在 Instances 页面的 Monitoring 选项卡中查看 CloudWatch 警报和指标。Amazon EC2 控制台使用 CloudWatch API 显示警报和指标，因此您必须向用户授予对 `cloudwatch:DescribeAlarms` 和 `cloudwatch:GetMetricStatistics` 操作的使用权。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
   }
   ]
}
```

示例：使用 EC2 启动实例向导

Amazon EC2 启动实例向导是一个屏幕，其中包含用于配置和启动实例的选项。您的策略必须包含允许用户使用向导选项的 API 操作使用权限。如果您的策略不包含使用这些操作的权限，则向导中的一些项目无法正确加载，用户无法完成启动。

启动实例向导基本访问权限

要成功完成启动，必须为用户授予使用 ec2:RunInstances API 操作以及至少以下 API 操作的权限：

- ec2:DescribeImages：查看并选择 AMI。
- ec2:DescribeInstanceTypes：查看并选择一种实例类型。
- ec2:DescribeVpcs：查看可用网络选项。
- ec2:DescribeSubnets：查看所选 VPC 的所有可用子网。
- ec2:DescribeSecurityGroups 或 ec2:CreateSecurityGroup：查看并选择现有安全组，或者创建新的安全组。
- ec2:DescribeKeyPairs 或 ec2:CreateKeyPair：选择现有密钥对，或者创建新密钥对。
- ec2:AuthorizeSecurityGroupIngress：添加入站规则。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

您可以向策略添加 API 操作以便为用户提供更多选项，例如：

- ec2:DescribeAvailabilityZones：查看并选择特定可用区。
- ec2:DescribeNetworkInterfaces：查看并选择所选子网的现有网络接口。
- 要向 VPC 安全组添加出站规则，必须为用户授予使用 ec2:AuthorizeSecurityGroupEgress API 操作的权限。要修改或删除现有规则，必须为用户授予使用相关 ec2:RevokeSecurityGroup* API 操作的权限。
- ec2:CreateTags：标记通过 RunInstances 创建的资源。有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。如果用户没有使用此操作的权限而又尝试在启动实例向导的标记页上应用标签，则启动失败。

  Important

  启动实例时指定 Name（名称）会创建一个标签并需要 ec2:CreateTags 操作。向用户授予使用 ec2:CreateTags 操作的权限时请谨慎，因为这样做会限制您使用 aws:ResourceTag 条件键限制用户使用其他资源的功能。如果您授予用户使用 ec2:CreateTags 操作的权限，则他们可以更改资源的标签以绕过这些限制。有关更多信息，请参阅使用资源标签控制对 EC2 资源的访问 (p. 1233)。

- 要在选择 AMI 时使用 Systems Manager 参数，您必须将 `ssm:DescribeParameters` 和 `ssm:GetParameters` 添加到 IAM policy 中。`ssm:DescribeParameters` 会授予用户查看和选择 Systems Manager 参数的权限。`ssm:GetParameters` 则会授予用户获取 Systems Manager 参数值的权限。您还可以限制对特定 Systems Manager 参数的访问权限。有关更多信息，请参阅本节后文中的限制对特定 Systems Manager 参数的访问。

当前，Amazon EC2 `Describe*` API 操作不支持资源级权限，因此您无法限制用户可以在启动实例向导中查看的单个资源。但是，您可以对 `ec2:RunInstances` API 操作应用资源级权限，以限制用户可以用于启动实例的资源。如果用户选择未授权他们使用的选项，则启动会失败。

限制对特定实例类型、子网和区域的访问

以下策略允许用户使用 Amazon 拥有的 AMI 启动 `t2.micro` 实例，并且仅在特定子网 (`subnet-1a2b3c4d`) 中启动。用户只能在 `sa-east-1` 区域中启动。如果用户在启动实例向导中选择不同区域或选择不同实例类型、AMI 或子网，则启动会失败。

第一条语句为用户授予权限以查看启动实例向导中的选项或创建新选项，如上例所示。第二条语句为用户授予将网络接口、卷、密钥对、安全组和子网资源 (在 VPC 中启动实例需要这些资源) 用于 `ec2:RunInstances` 操作的权限。有关使用 `ec2:RunInstances` 操作的更多信息，请参阅 启动实例 (RunInstances) (p. 1245)。第三和第四条语句分别为用户授予权限以使用实例（仅当实例是 `t2.micro` 实例时）和 AMI 资源（仅当 AMI 由 Amazon 或某些受信任或经过验证的合作伙伴所有时）。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
   ],
   "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action":"ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
         "arn:aws:ec2:sa-east-1:111122223333:volume/*",
         "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
         "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
         "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
      ]
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:sa-east-1:111122223333:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": "t2.micro"
         }
      }
```

```
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
            "arn:aws:ec2:sa-east-1::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   }
   ]
}
```

限制对特定 Systems Manager 参数的访问

以下策略授予访问权限以使用具有特定名称的 Systems Manager 参数。

第一条语句授予用户权限，可在启动实例向导中选择 AMI 时查看 Systems Manager 参数。第二条语句授予用户仅使用名为 `prod-*` 的参数的权限。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
   }
   ]
}
```

示例：使用卷

以下策略为用户授予查看和创建卷以及将卷与特定实例附加和分离的权限。

用户可以将任何卷附加到具有标签“`purpose=test`”的实例，也可以从这些实例分离卷。要使用 Amazon EC2 控制台连接卷，用户有权使用 `ec2:DescribeInstances` 操作会很有帮助，因为这可以让他们从 Attach Volume (连接卷) 对话框的预填充列表中选择实例。但是，这也会允许用户在控制台的 Instances 页面上查看所有实例，因此，您可以省略此操作。

在第一条语句中，需要 `ec2:DescribeAvailabilityZones` 操作以确保用户可以在创建卷时选择可用区。

用户无法标记其创建的卷 (卷创建期间或之后)。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
```

```
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateVolume",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose": "test"
        }
     }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:volume/*"
   }
   ]
}
```

示例：使用安全组

查看安全组以及添加和删除规则

以下策略为用户授予相应的权限，以便在 Amazon EC2 控制台中查看安全组、添加和删除入站和出站规则，以及为具有标签 `Department=Test` 的现有安全组列出并修改规则描述。

在第一条语句中，`ec2:DescribeTags` 操作允许用户在控制台中查看标签，这样，用户更易于识别自己可修改的安全组。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
```

```
            "arn:aws:ec2:region:111122223333:security-group/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Department": "Test"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySecurityGroupRules"
        ],
        "Resource": [
            "arn:aws:ec2:region:111122223333:security-group-rule/*"
        ]
    }
]}
```

使用 Create Security Group（创建安全组）对话框

您可以创建一个策略，以允许用户使用 Amazon EC2 控制台中的 Create Security Group (创建安全组) 对话框。要使用此对话框，必须为用户授予使用至少以下 API 操作的权限：

- ec2:CreateSecurityGroup: 创建新安全组。
- ec2:DescribeVpcs查看 VPC 列表中的现有 VPC 列表。

借助这些权限，用户可以成功创建新安全组，但是他们不能向其中添加任何规则。要在 Create Security Group (创建安全组) 对话框中使用规则，您可以向策略添加以下 API 操作：

- ec2:AuthorizeSecurityGroupIngress：添加入站规则。
- ec2:AuthorizeSecurityGroupEgress：向 VPC 安全组添加出站规则。
- ec2:RevokeSecurityGroupIngress：修改或删除现有入站规则。如果要允许用户使用控制台中的 Copy to new 功能，这十分有用。此功能会打开 Create Security Group (创建安全组) 对话框，并使用所选安全组的规则进行填充。
- ec2:RevokeSecurityGroupEgress：修改或删除适用于 VPC 安全组的出站规则。若要允许用户修改或删除允许所有出站流量的默认出站规则，这十分有用。
- ec2:DeleteSecurityGroup：适用于无效规则无法保存的情况。控制台首先创建安全组，然后添加指定的规则。如果规则无效，则操作会失败，而控制台会尝试删除安全组。用户仍会停留在“Create Security Group”对话框中，这样就能更正无效规则和尝试重新创建安全组。此 API 操作不是必需的，但是如果用户在无权使用它的情况下尝试创建具有无效规则的安全组，则会创建不包含任何规则的安全组，用户必须在之后添加规则。
- ec2:UpdateSecurityGroupRuleDescriptionsIngress：添加或更新入口（入站）安全组规则的描述。
- ec2:UpdateSecurityGroupRuleDescriptionsEgress：添加或更新出口（出站）安全组规则的描述。
- ec2:ModifySecurityGroupRules：修改安全组规则。
- ec2:DescribeSecurityGroupRules：列出安全组规则。

以下策略向用户授予使用 Create Security Group (创建安全组) 对话框，以及为与特定 VPC (vpc-1a2b3c4d) 关联的安全组创建入站和出站规则的权限。用户可以为 EC2-Classic 或其他 VPC 创建安全组，但是无法向它们添加任何规则。同样，用户无法向不与 VPC vpc-1a2b3c4d 关联的任何现有安全组添加任何规则。还向用户授予了在控制台中查看所有安全组的权限。这样，用户更易于识别自己可添加入站规则的安全组。此策略还为用户授予删除与 VPC vpc-1a2b3c4d 关联的安全组的权限。

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
    }
   ]
}
```

示例：使用弹性 IP 地址

为了让用户能够查看 Amazon EC2 控制台中的弹性 IP 地址，您必须授予用户使用 `ec2:DescribeAddresses` 操作的权限。

要允许用户使用弹性 IP 地址，可将以下操作添加到您策略中。

- `ec2:AllocateAddress`：分配弹性 IP 地址。
- `ec2:ReleaseAddress`: 解除弹性 IP 地址。
- `ec2:AssociateAddress`：将弹性 IP 地址与实例或网络接口关联。
- `ec2:DescribeNetworkInterfaces` 和 `ec2:DescribeInstances`：使用 Associate Address (关联地址) 屏幕。屏幕显示了您可以将弹性 IP 地址关联到的可用实例或网络接口。
- `ec2:DisassociateAddress`：取消弹性 IP 地址与实例或网络接口的关联。

以下策略允许用户查看弹性 IP 地址并将其分配给实例和与实例相关联。用户不可以将弹性 IP 地址与网络接口关联、取消弹性 IP 地址的关联或释放弹性 IP 地址。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

示例：使用预留实例

以下策略允许用户查看和修改账户中的预留实例，同时也能在 Amazon Web Services Management Console 内购买新的预留实例。

此策略允许用户查看账户中的所有预留实例和按需型实例。无法为单个预留实例设置资源级别的权限。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

必须执行 ec2:DescribeAvailabilityZones 操作才能确保 Amazon EC2 控制台可以显示有关您能够购买预留实例的可用区的信息。ec2:DescribeInstances 操作不是必须的，但是请确保用户可查看账户内的实例并且能够购买预留实例，以匹配正确的规格。

您可以调整 API 操作，以限制用户访问，例如删除ec2:DescribeInstances，而ec2:DescribeAvailabilityZones表示用户有只读形式的访问权。

Amazon Amazon Elastic Compute Cloud 托管策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管策略。这些策略涵盖常见使用案例，可在您的 Amazon 账户中使用。有关 Amazon 托管策略的更多信息，请参阅 IAM 用户指南中的 Amazon 托管策略。

Amazon 服务负责维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管策略。例如，ReadOnlyAccess Amazon 托管策略提供对所有 Amazon 服务和资源的只读访问权限。当服务启动新功能时，Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管策略。

Amazon 托管策略：AmazonEC2FullAccess

您可以将 AmazonEC2FullAccess 策略附加得到 IAM 身份。此策略授予允许完全访问 Amazon EC2 的权限。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AmazonEC2FullAccess。

Amazon 托管策略：AmazonEC2ReadOnlyAccess

您可以将 AmazonEC2ReadOnlyAccess 策略附加得到 IAM 身份。此策略授予允许对 Amazon EC2 进行只读访问的权限。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AmazonEC2ReadOnlyAccess。

Amazon托管策略：AWSEC2CapacityReservationFleetRolePolicy

此策略将附加到名为 AWSServiceRoleForEC2CapacityReservationFleet 的服务相关角色，以允许容量预留代表您创建、修改和取消容量预留。有关更多信息，请参阅容量预留实例集的服务相关角色 (p. 567)。

Amazon托管策略：AWSEC2FleetServiceRolePolicy

此策略将附加到名为 AWSServiceRoleForEC2Fleet 的服务相关角色，以允许 EC2 机群代表您请求、启动、终止和标记实例。有关更多信息，请参阅EC2 队列的服务相关角色 (p. 855)。

Amazon 托管策略：AWSEC2SpotFleetServiceRolePolicy

此策略将附加到名为 AWSServiceRoleForEC2SpotFleet 的服务相关角色，以允许竞价型实例集代表您启动和管理实例。有关更多信息，请参阅Spot 队列的服务相关角色 (p. 896)。

Amazon 托管策略：AWSEC2SpotServiceRolePolicy

此策略将附加到名为 AWSServiceRoleForEC2Spot 的服务相关角色，以允许 Amazon EC2 代表您启动和管理 Spot 实例。有关更多信息，请参阅竞价型实例请求的服务相关角色 (p. 458)。

Amazon 托管策略的 Amazon EC2 更新

查看有关 Amazon EC2 的 Amazon 托管策略的更新的详细信息（此服务开始跟踪这些更改）。

更改	说明	日期
Amazon EC2 开始跟踪更改	Amazon EC2 已开始跟踪 Amazon 托管式策略的更改	2021 年 3 月 1 日

适用于 Amazon EC2 的 IAM 角色

应用程序必须通过 Amazon 凭证签署其 API 请求。因此，如果您是应用程序开发人员，您需要一个策略来为 EC2 实例上运行的应用程序管理凭证。例如，您可以安全地将您的 Amazon 凭证分配至实例，从而允许这些实例上的应用程序使用您的凭证签署请求，并保护您的凭证不被其他用户使用。但是，要将凭证安全地分配至每个实例是有难度的，尤其是 Amazon 以您的名义创建的实例，例如竞价型实例或 Auto Scaling 组中的实例。当您轮换 Amazon 凭证时，您还必须能够更新每项实例上的凭证。

> **Note**
>
> 对于您的 Amazon EC2 工作负载，我们建议您使用下述方法检索会话凭证。借助这些凭证，您的工作负载能够发出 Amazon API 请求，而无需使用 `sts:AssumeRole` 来代入已与实例关联的相同角色。除非您需要为基于属性的访问权限控制 (ABAC) 传递会话标签或传递会话策略以进一步限制角色的权限，否则您无需调用角色代入，因为此操作会创建一组新的相同临时角色会话凭证。
> 如果您的工作负载使用某个角色代入自己，则必须创建明确允许该角色代入自己的信任策略。如果您没有创建信任策略，您会收到 `AccessDenied` 错误消息。有关更多信息，请参阅《IAM 用户指南》中修改角色信任策略。

我们设计了 IAM 角色，以便您的应用程序能够安全地从实例发出 API 请求，而无需管理应用程序使用的安全凭证。您可以使用 IAM 角色委托授权以发出 API 请求，而不用创建并分配您的 Amazon 凭证，如下所示：

1. 创建一个 IAM 角色。
2. 定义能够担任此角色的账户或 Amazon 服务。

3. 定义担任角色后应用程序可以使用的 API 操作和资源。
4. 在您启动实例时指定角色，或者将角色附加到现有实例。
5. 让应用程序检索一组临时证书并使用它们。

例如，您可以使用 IAM 角色为在实例上运行的应用程序授予使用 Amazon S3 中的存储桶所需的权限。您可以通过创建 JSON 格式的策略为 IAM 角色指定权限。这些类似于您为 用户创建的策略。如果您更改了某个角色，系统会将此更改传播到所有实例。

在创建 IAM 角色时，请关联最小权限 IAM policies，这些策略将限制对应用程序所需的特定 API 调用的访问权限。

您只能将一个 IAM 角色附加到实例，但可以将同一角色附加到多个实例。有关创建和使用 IAM 角色的更多信息，请参阅 IAM 用户指南 中的角色。

您可以将资源级权限应用到您的 IAM policy，以便控制用户为一个实例附加、替换或分离 IAM 角色的能力。有关更多信息，请参阅 Amazon EC2 API 操作支持的资源级权限 (p. 1227) 以及以下示例：示例：使用 IAM 角色 (p. 1263)。

目录

- 实例配置文件 (p. 1278)
- 从实例元数据中检索安全凭证 (p. 1278)
- 向用户授予将 IAM 角色传递给实例的权限 (p. 1279)
- 使用 IAM 角色 (p. 1280)

实例配置文件

Amazon EC2 使用实例配置文件 作为 IAM 角色的容器。使用 IAM 控制台创建 IAM 角色时，控制台自动创建实例配置文件，按相应的角色为文件命名。如果您使用 Amazon EC2 控制台启动一个带 IAM 角色的实例或将一个 IAM 角色附加到实例，则请根据实例配置文件名称列表选择角色。

如果您使用 Amazon CLI、API 或 Amazon 开发工具包创建角色，则是以单独操作的形式创建角色和实例配置文件，可以为它们提供不同的名称。如果您使用 Amazon CLI、API 或 Amazon 开发工具包启动带有 IAM 角色的实例，或将 IAM 角色附加到实例，请指定实例配置文件名称。

一个实例配置文件只能包含一个 IAM 角色。不能提高此限制。

有关更多信息，请参阅 IAM 用户指南 中的实例配置文件。

从实例元数据中检索安全凭证

实例上的应用程序通过实例元数据条目 `iam/security-credentials/role-name` 检索角色提供的安全证书。该应用程序具有使用您通过与角色关联的安全凭证为其定义的操作和资源的权限。这些安全凭证是临时的，我们会自动更换它们。我们会在旧凭证过期前至少五分钟提供可用的新凭证。

> **Warning**
>
> 如果您使用的服务采用了带有 IAM 角色的实例元数据，请确保服务代表您进行 HTTP 调用时不会泄露您的凭证。可能泄露您的凭证的服务类型包括 HTTP 代理、HTML/CSS 验证程序服务和支持 XML 包含的 XML 处理程序。

以下命令检索名为 `s3access` 的 IAM 角色的安全证书。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

下面是示例输出。

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

对于实例上运行的应用程序、Amazon CLI 和 Tools for Windows PowerShell 命令，您无需显式获取临时安全凭证 – Amazon开发工具包、Amazon CLI 和 Windows PowerShell 工具会自动从 EC2 实例元数据服务中获取凭证并使用这些凭证。要使用临时安全凭证在实例外部发出调用 (例如，为了测试 IAM policy)，您必须提供访问密钥、私有密钥和会话令牌。有关更多信息，请参阅 IAM 用户指南中的使用临时安全凭证以请求对 Amazon 资源的访问权限。

有关实例元数据的更多信息，请参阅 实例元数据和用户数据 (p. 754)。有关实例元数据 IP 地址的信息，请参阅检索实例元数据 (p. 766)。

向用户授予将 IAM 角色传递给实例的权限

要支持用户启动带有 IAM 角色的实例或为现有实例替换 IAM 角色，您必须授予用户使用以下 API 操作的权限：

- iam:PassRole
- ec2:AssociateIamInstanceProfile
- ec2:ReplaceIamInstanceProfileAssociation

例如，以下 IAM policy 将授权用户启动带有 IAM 角色的实例，或者使用 Amazon CLI 为现有实例附加或替换 IAM 角色。

> **Note**
>
> 如果您希望策略授予用户对所有角色的访问权限，请将资源指定为策略中的 *。但是，请考虑最低权限原则作为最佳实践。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
```

```
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
  ]
}
```

要授予用户启动带有 IAM 角色的实例的权限，或使用 Amazon EC2 控制台为现有实例附加或替换 IAM 角色，您必须授予用户使用 `iam:ListInstanceProfiles`、`iam:PassRole`、`ec2:AssociateIamInstanceProfile` 和 `ec2:ReplaceIamInstanceProfileAssociation` 以及他们可能需要的任何其他权限。有关示例策略，请参阅 用于 Amazon EC2 控制台的示例策略 (p. 1268)。

使用 IAM 角色

在启动过程中或启动之后，您可以创建一个 IAM 角色并将其附加到实例。您也可以为实例替换或分离 IAM 角色。

目录

- 创建 IAM 角色 (p. 1280)
- 启动带有 IAM 角色的实例 (p. 1282)
- 将 IAM 角色附加到实例 (p. 1284)
- 替换 IAM 角色 (p. 1285)
- 分离 IAM 角色 (p. 1286)
- 根据访问活动为您的 IAM 角色生成策略 (p. 1287)

创建 IAM 角色

您必须先创建 IAM 角色，然后才能启动带有该角色的实例或将其附加到该实例。

Console

使用 IAM 控制台创建 IAM 角色

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 在选择可信实体页面上，选择 Amazon Web Service，然后选择 EC2 使用案例。选择 Next（下一步）。
4. 在添加权限页面上，选择向实例授予对所需资源的访问权限的策略。选择 Next（下一步）。
5. 在命名、查看和创建页面上，输入角色的名称和描述。您也可以为角色添加标签。选择 Create role（创建角色）。

Command line

以下示例创建了一个 IAM 角色，并指定允许其使用 Amazon S3 桶的策略。

创建 IAM 角色和实例配置文件（Amazon CLI）

1. 创建以下信任策略并将其保存在名为 `ec2-role-trust-policy.json` 的文本文件中。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 创建 s3access 角色并指定使用创建 create-role 命令创建的信任策略。

```
aws iam create-role \
    --role-name s3access \
    --assume-role-policy-document file://ec2-role-trust-policy.json
```

响应示例

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2013-12-12T23:46:37.247Z",
        "RoleName": "s3access",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/s3access"
    }
}
```

3. 创建访问策略并将其保存在名为 ec2-role-access-policy.json 的文本文件中。例如，此策略向在实例上运行的应用程序授予针对 Amazon S3 管理员权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:*"],
      "Resource": ["*"]
    }
  ]
}
```

4. 使用 put-role-policy 命令将该访问策略附加到角色。

```
aws iam put-role-policy \
    --role-name s3access \
    --policy-name S3-Permissions \
    --policy-document file://ec2-role-access-policy.json
```

5. 使用 create-instance-profile 命令创建名为 s3access-profile 的实例配置文件。

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

响应示例

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. 将 s3access 角色添加到 s3access-profile 实例配置文件。

```
aws iam add-role-to-instance-profile \
    --instance-profile-name s3access-profile \
    --role-name s3access
```

或者，您可以使用以下 Amazon Tools for Windows PowerShell 命令：

- New-IAMRole
- Register-IAMRolePolicy
- New-IAMInstanceProfile

启动带有 IAM 角色的实例

创建一个 IAM 角色之后，您可以启动实例，并在启动过程中将该角色与实例关联。

> **Important**
>
> 创建 IAM 角色后，可能需要几秒钟时间来让权限传播。若您第一次尝试启动带角色的实例失败，请等待几秒然后重试。有关更多信息，请参阅《IAM 用户指南》中的IAM 角色故障排除。

New console

启动带有 IAM 角色的实例（控制台）

1. 按照程序启动实例 (p. 576)。
2. 展开 Advanced details（高级详细信息），对于 IAM instance profile（IAM 实例配置文件），选择您创建的 IAM 角色。

   > **Note**
   >
   > IAM instance profile（IAM 实例配置文件）列表显示您在创建 IAM 角色时创建的实例配置文件的名称。如果您是使用控制台创建的 IAM 角色，则为您创建了实例配置文件，并提供了与角色相同的名称。如果使用 Amazon CLI、API 或 Amazon 开发工具包创建了 IAM 角色，则可能对实例配置文件指定了不同名称。
3. 为实例配置您需要的其他任何详细信息或接受默认设置，然后选择一个密钥对。有关启动实例向导中字段的信息，请参阅 使用定义的参数启动实例 (p. 577)。
4. 在 Summary（摘要）面板中查看实例配置，然后选择 Launch instance（启动实例）。
5. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 Amazon 安全凭证，并使用它们签署请求。Amazon 开发工具包将为您执行此操作。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
meta-data/iam/security-credentials/role_name
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Old console

启动带有 IAM 角色的实例（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在控制面板上，选择启动实例。
3. 选择 AMI 和实例类型，然后选择 Next: Configure Instance Details。
4. 在 Configure Instance Details (配置实例详细信息) 页面上，为 IAM role (IAM 角色) 选择您创建的 IAM 角色。

   Note

   IAM role (IAM 角色) 列表显示您在创建 IAM 角色时创建的实例配置文件的名称。如果您是使用控制台创建的 IAM 角色，则为您创建了实例配置文件，并提供了与角色相同的名称。如果使用 Amazon CLI、API 或 Amazon 开发工具包创建了 IAM 角色，则可能对实例配置文件指定了不同名称。
5. 配置其他详细信息，然后按照向导的其余说明操作，或选择 Review and Launch 接受默认设置并直接转到 Review Instance Launch 页面。
6. 检查设置，然后选择 Launch 以选择密钥对并启动实例。
7. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 Amazon 安全凭证，并使用它们签署请求。Amazon 开发工具包将为您执行此操作。

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
   credentials/role_name
   ```

Command line

您可以在启动过程中使用 Amazon CLI 将角色关联到实例。您必须在命令中指定实例配置文件。

启动带有 IAM 角色的实例（Amazon CLI）

1. 使用 run-instances 命令启动使用实例配置文件的实例。以下示例演示如何使用实例配置启动实例。

```
aws ec2 run-instances \
    --image-id ami-11aa22bb \
    --iam-instance-profile Name="s3access-profile" \
    --key-name my-key-pair \
    --security-groups my-security-group \
    --subnet-id subnet-1a2b3c4d
```

或者，使用 New-EC2Instance Tools for Windows PowerShell 命令。

2. 如果您的应用程序使用的是 Amazon EC2 API 操作，请检索实例中可用的 Amazon 安全凭证，并使用它们签署请求。Amazon 开发工具包将为您执行此操作。

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

将 IAM 角色附加到实例

要将 IAM 角色附加到没有角色的实例，该实例可以处于 `stopped` 或 `running` 状态。

Console

将 IAM 角色附加到实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions (操作)、Security (安全)、Modify IAM role (修改 IAM 角色)。
4. 选择要附加到您的实例的 IAM 角色，然后选择 Save (保存)。

Command line

要将 IAM 角色附加到实例（Amazon CLI）

1. 如果需要，请描述您的实例以获取要附加角色的实例的 ID。

```
aws ec2 describe-instances
```

2. 使用 associate-iam-instance-profile 并通过指定实例配置文件，将 IAM 角色附加到实例。您可以使用实例配置文件的 Amazon Resource Name (ARN)，或者使用实例的名称。

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

响应示例

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
```

```
}
```

或者，使用以下 Tools for Windows PowerShell 命令：

- Get-EC2Instance
- Register-EC2IamInstanceProfile

替换 IAM 角色

要替换已附加了 IAM 角色的实例上的 IAM 角色，实例必须处于 `running` 状态。如果要更改实例的 IAM 角色而先不分离现有角色，则您可以执行此操作。例如，您可以执行此操作，以确保正在实例上运行的应用程序所执行的 API 操作不会被中断。

Console

替换实例的 IAM 角色

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions (操作)、Security (安全)、Modify IAM role (修改 IAM 角色)。
4. 选择要附加到您的实例的 IAM 角色，然后选择 Save (保存)。

Command line

要替换实例的 IAM 角色（Amazon CLI）

1. 如果需要，请描述您的 IAM 实例配置文件关联情况，以获取要替换的 IAM 实例配置文件的关联 ID。

```
aws ec2 describe-iam-instance-profile-associations
```

2. 使用 replace-iam-instance-profile-association 命令并通过为现有实例配置文件或 ARN 指定关联 ID 或指定替换实例配置文件的名称，替换 IAM 实例配置文件。

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

响应示例

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

或者，使用以下 Tools for Windows PowerShell 命令：

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

分离 IAM 角色

您可以将 IAM 角色从正在运行或已停止的实例上分离。

Console

从实例中分离 IAM 角色

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions (操作)、Security (安全)、Modify IAM role (修改 IAM 角色)。
4. 对于 IAM 角色，请选择无 IAM 角色。选择 Save (保存)。
5. 在确认对话框中，输入分离，然后选择分离。

Command line

从实例中分离 IAM 角色（Amazon CLI）

1. 如果需要，使用 describe-iam-instance-profile-associations 描述您的 IAM 实例配置文件关联，并获取要分离的 IAM 实例配置文件的关联 ID。

```
aws ec2 describe-iam-instance-profile-associations
```

响应示例

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. 使用 disassociate-iam-instance-profile 命令分离使用其关联 ID 的 IAM 实例配置文件。

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

响应示例

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
```

```
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

或者，使用以下 Tools for Windows PowerShell 命令：

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

根据访问活动为您的 IAM 角色生成策略

首次为应用程序创建 IAM 角色时，有时授予的权限可能超出所需权限。在生产环境中启动应用程序之前，您可以根据 IAM 角色的访问活动生成 IAM policy。IAM 访问分析器会查看您的 Amazon CloudTrail 日志并生成一个策略模板，其中包含角色在指定日期范围内使用的权限。您可以使用模板创建具有精细权限的托管策略，然后将其附加到 IAM 角色。这样，您仅需授予角色与特定使用案例中的 Amazon 资源进行交互所需的权限。这可帮助您遵循授予最低权限的最佳实践。要了解更多信息，请参阅 IAM 用户指南中的基于访问活动生成策略。

为您的 Linux 实例授权入站流量

您可以采用安全组控制实例的流量，包括可到达您的实例的流量类型。例如，您可以只允许来自您家庭网络的计算机使用 SSH 访问您的实例。如果您的实例为 Web 服务器，那么您可以允许所有 IP 地址通过 HTTP 或 HTTPS 访问您的实例，以便外部用户能够浏览您的 Web 服务器上的内容。

您的默认安全组和新创建的安全组包含不支持您从 Internet 访问实例的默认规则。有关更多信息，请参阅默认安全组 (p. 1308)和自定义安全组 (p. 1308)。若要启用对实例的网络访问，您必须允许该实例的入站流量。要为入站流量打开端口，您需要在启动实例时向与实例关联的安全组添加规则。

要连接到您的实例，您必须设置规则以向来自您计算机的公有 IPv4 地址的 SSH 流量授权。要允许来自其他 IP 地址范围的 SSH 流量，请为需要授权的每个范围另外添加规则。

如果您已启用了支持 IPv6 的 VPC 并使用 IPv6 地址启动您的实例，则可以使用其 IPv6 地址而非公有 IPv4 地址连接到您的实例。您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。

如果您需要启用对 Windows 实例的网络访问，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的为 Windows 实例授权入站流量。

在您开始之前

确定谁需要访问您的实例；例如，您信任的单个主机或特定网络 (例如，本地计算机的公有 IPv4 地址)。Amazon EC2 控制台的安全组编辑器可自动为您检测本地计算机的公有 IPv4 地址。此外，您可以在 Internet 浏览器中使用搜索短语“什么是我的 IP 地址”，或使用以下服务：检查 IP。如果您正通过 ISP 或从防火墙后面连接，没有静态 IP 地址，您需要找出客户端计算机使用的 IP 地址范围。

Warning

如果使用 `0.0.0.0/0`，则允许所有 IPv4 地址使用 SSH 访问您的实例。如果您使用 `::/0`，则所有 IPv6 地址都可以访问您的实例。您应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。

决定您是否支持使用 EC2 Instance Connect 对实例进行 SSH 访问。如果您将不使用 EC2 Instance Connect，则考虑卸载它或在 IAM policy 中拒绝以下操作：`ec2-instance-connect:SendSSHPublicKey`。有关更多信息，请参阅 卸载 EC2 Instance Connect (p. 661)和为 EC2 Instance Connect 配置 IAM 权限 (p. 656)。

添加 Linux 实例的入站 SSH 流量规则

安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。您必须向安全组添加可让您使用 SSH 从 IP 地址连接到 Linux 实例的规则。

在安全组中为通过 IPv4 的入站 SSH 流量添加规则（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从顶部的导航栏中选择安全组的区域。安全组特定于区域，因此您应选择您创建实例的区域。
3. 在导航窗格中，选择实例。
4. 选择您的实例，然后在屏幕下半部分选择 Security (安全) 选项卡。Security groups (安全组) 列出了与实例关联的安全组。Inbound rules (入站规则) 显示对实例生效的入站规则列表。
5. 对于要添加新规则的安全组，请选择安全组 ID 链接以打开安全组。
6. 在 Inbound Rules (入站规则) 选项卡上，选择 Edit inbound rules (编辑入站规则)。
7. 在 Edit inbound rules (编辑入站规则) 页面上，执行以下操作：

   a. 选择 Add rule (添加规则)。
   b. 对于 Type (类型)，请选择 SSH。
   c. 对于 Source（源），选择 My IP（我的 IP）以便使用本地计算机的公有 IPv4 地址自动填充该字段。

      或者，对于 Source（源），选择 Custom（自定义）并使用 CIDR 表示法输入计算机的公有 IPv4 地址或网络。例如，如果您的 IPv4 地址为 `203.0.113.25`，请输入 `203.0.113.25/32`，以使用 CIDR 表示法列出此单个 IPv4 地址。如果您的公司要分配同一范围内的地址，请输入整个范围，例如 `203.0.113.0/24`。

      有关查找 IP 地址的信息，请参阅在您开始之前 (p. 1287)。
   d. 选择 Save rules（保存规则）。

如果您已启动带有 IPv6 地址的实例并希望使用其 IPv6 地址连接到您的实例，则必须添加允许通过 SSH 的入站 IPv6 流量的规则。

在安全组中为通过 IPv6 的入站 SSH 流量添加规则（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从顶部的导航栏中选择安全组的区域。安全组特定于区域，因此您应选择您创建实例的区域。
3. 在导航窗格中，选择实例。
4. 选择您的实例，然后在屏幕下半部分选择 Security (安全) 选项卡。Security groups (安全组) 列出了与实例关联的安全组。Inbound rules (入站规则) 显示对实例生效的入站规则列表。
5. 对于要添加新规则的安全组，请选择安全组 ID 链接以打开安全组。
6. 在 Inbound Rules (入站规则) 选项卡上，选择 Edit inbound rules (编辑入站规则)。
7. 在 Edit inbound rules (编辑入站规则) 页面上，执行以下操作：

   a. 选择 Add rule (添加规则)。
   b. 对于 Type (类型)，选择 SSH。
   c. 对于 Source（源），选择 Custom（自定义），并使用 CIDR 表示法为您的计算机输入 IPv6 地址。例如，如果您的 IPv6 地址为 `2001:db8:1234:1a00:9691:9503:25ad:1761`，请输入 `2001:db8:1234:1a00:9691:9503:25ad:1761/128`，以使用 CIDR 表示法列出单个 IP 地址。如果您的公司要分配同一范围内的地址，请输入整个范围，例如 `2001:db8:1234:1a00::/64`。
   d. 选择 Save rules（保存规则）。

Note

请确保以下命令在您的本地系统中运行，而不是针对实例本身。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

使用命令行向安全组添加规则

1. 使用以下命令之一找到与您的实例关联的安全组：

   - describe-instance-attribute (Amazon CLI)

   ```
   aws ec2 describe-instance-attribute --region region --instance-id instance_id --
   attribute groupSet
   ```

   - Get-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

   ```
   PS C:\> (Get-EC2InstanceAttribute -Region region -InstanceId instance_id -Attribute
    groupSet).Groups
   ```

   两个命令均返回一个安全组 ID，您将在下一步中使用该 ID。

2. 使用以下命令之一向安全组添加规则：

   - authorize-security-group-ingress (Amazon CLI)

   ```
   aws ec2 authorize-security-group-ingress --region region --group-id security_group_id
    --protocol tcp --port 22 --cidr cidr_ip_range
   ```

   - Grant-EC2SecurityGroupIngress (Amazon Tools for Windows PowerShell)

   `Grant-EC2SecurityGroupIngress` 命令需要 `IpPermission` 参数，该参数描述要用于安全组规则的协议、端口范围和 IP 地址范围。以下命令创建 `IpPermission` 参数：

   ```
   PS C:\> $ip1 = @{ IpProtocol="tcp"; FromPort="22"; ToPort="22";
    IpRanges="cidr_ip_range" }
   ```

   ```
   PS C:\> Grant-EC2SecurityGroupIngress -Region region -GroupId security_group_id -
   IpPermission @($ip1)
   ```

向实例分配安全组

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。

启动实例后，您可以更改其安全组。想要了解更多有关信息，请参阅 Amazon VPC 用户指南中的更改实例的安全组主题。

Amazon EC2 密钥对和 Linux 实例

密钥对（由公有密钥和私有密钥组成）是一组安全凭证，可在连接到 Amazon EC2 实例时用来证明您的身份。Amazon EC2 在您的实例上存储公有密钥，您需要存储私有密钥。对于 Linux 实例，私有密钥允许您安全地 SSH 进入您的实例。作为密钥对的替代，您可以使用 Amazon Systems Manager Session Manager，通过基于浏览器的交互式、一键式 Shell 或 Amazon Command Line Interface（Amazon CLI）连接到您的实例。

拥有您的私有密钥的任何人都可以连接到您的实例，因此将您的私有密钥存储在一个安全位置非常重要。

启动实例时，您可以指定密钥对 (p. 579)。如果您计划使用 SSH 连接到实例，则必须指定密钥对。您可以选择现有密钥对或创建新的密钥对。当您的实例首次启动时，您在启动时指定的公有密钥将放置在 Linux 实例中的 `~/.ssh/authorized_keys` 的条目中。在使用 SSH 连接到 Linux 实例时，要进行登录，您必须指定与公有密钥对应的私有密钥。有关连接到实例的更多信息，请参阅连接到您的 Linux 实例 (p. 644)。有关密钥对和 Windows 实例的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 Amazon EC2 密钥对和 Windows 实例。

由于 Amazon EC2 不保存私有密钥的副本，因此，如果您丢失私有密钥，则无法恢复它。但是，仍可通过一种方法连接到丢失了密钥对的实例。有关更多信息，请参阅 我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)

您可以使用 Amazon EC2 创建密钥对。您还可以使用第三方工具创建密钥对，然后将公有密钥导入 Amazon EC2。

Amazon EC2 支持适用于 Linux 实例的 ED25519 和 2048 位 SSH-2 RSA 密钥。

每个地区最多可拥有 5,000 个密钥对。

目录

- 创建密钥对 (p. 1290)
- 标记公有密钥 (p. 1294)
- 描述公有密钥 (p. 1296)
- 在 Amazon EC2 上删除您的公有密钥 (p. 1300)
- 在实例上添加或删除公有密钥 (p. 1301)
- 验证密钥 (p. 1302)

创建密钥对

您可以使用 Amazon EC2 创建 RSA 或 ED25519 密钥对，或者可以使用第三方工具创建密钥对并将公有密钥导入 Amazon EC2。

有关在创建密钥对后使用 SSH 连接到您的 Linux 实例的步骤，请参阅连接到您的 Linux 实例。

目录

- 使用 Amazon EC2 创建密钥对 (p. 1290)
- 使用 Amazon CloudFormation 创建密钥对 (p. 1292)
- 使用第三方工具创建密钥对，并将公有密钥导入 Amazon EC2 (p. 1293)

使用 Amazon EC2 创建密钥对

当您使用 Amazon EC2 创建密钥对时，公有密钥将存储在 Amazon EC2 中，您需要存储私有密钥。

您可以使用 Amazon EC2 通过以下方法之一创建密钥对。

Console

要使用 Amazon EC2 创建密钥对

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 Network & Security 下，选择 Key Pairs。

3. 选择 Create key pair (创建密钥对)。
4. 对于 Name (名称)，为模板输入一个描述性名称。Amazon EC2 将公有密钥与您指定的密钥名称相关联。密钥名称最多可包含 255 个 ASCII 字符。它不能包含前导空格或尾随空格。
5. 对于 Key pair type（密钥对类型），选择 RSA 或者 ED25519。
6. 对于 Private key file format（私有密钥文件格式），选择要保存私有密钥的格式。要以可与 OpenSSH 一起使用的格式保存私有密钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私有密钥，请选择 ppk。
7. 要添加标签到公有密钥，请选择 Add tag（添加标签），然后输入标签的键和值。对每个标签重复此操作。
8. 选择 Create key pair (创建密钥对)。
9. 您的浏览器会自动下载私有密钥文件。基本文件名是指定为密钥对名称的名称，文件扩展名由您选择的文件格式确定。将私有密钥文件保存在安全位置。

   Important

   这是您保存私有密钥文件的唯一机会。
10. 如果您计划在 macOS 或 Linux 计算机上使用 SSH 客户端连接到 Linux 实例，请使用以下命令设置私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 key-pair-name.pem
```

如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅错误：未保护的私有密钥文件 (p. 1692)。

Amazon CLI

要使用 Amazon EC2 创建密钥对

1. 按如下方式使用 create-key-pair 命令生成密钥对，并将私有密钥保存到 .pem 文件中。

   对于 --key-name，为公有密钥指定一个名称。该名称最多为 255 个 ASCII 字符。

   对于 --key-type，请指定 rsa 或 ed25519。如果您不包括 --key-type 参数，原定设置创建一个 rsa 密钥。请注意，Windows 实例不支持 ED25519 密钥。

   对于 --key-format，请指定 pem 或 ppk。如果您不包括 --key-format 参数，原定设置将创建一个 pem 文件。

   --query "KeyMaterial" 将私有密钥材料打印到输出中。

   --output text > *my-key-pair.pem* 会将私有密钥材料保存在一个具有指定扩展名的文件中。该扩展名可以是 .pem 或 .ppk。私有密钥的名称可以与公有密钥的名称不同，但为了便于使用，请使用相同的名称。

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. 如果您计划在 macOS 或 Linux 计算机上使用 SSH 客户端连接到 Linux 实例，请使用以下命令设置私有密钥文件的权限，以确保只有您可以读取该文件。

```
chmod 400 key-pair-name.pem
```

如果不设置这些权限，则无法使用此密钥对连接到实例。有关更多信息，请参阅错误：未保护的私有密钥文件 (p. 1692)。

PowerShell

要使用 Amazon EC2 创建密钥对

按如下方式使用 New-EC2KeyPair Amazon Tools for Windows PowerShell 命令生成密钥，并将其保存到 .pem 或 .ppk 文件中。

对于 -KeyName，为公有密钥指定一个名称。该名称最多为 255 个 ASCII 字符。

对于 -KeyType，请指定 rsa 或 ed25519。如果您不包括 -KeyType 参数，原定设置创建一个 rsa 密钥。请注意，Windows 实例不支持 ED25519 密钥。

对于 -KeyFormat，请指定 pem 或 ppk。如果您不包括 -KeyFormat 参数，原定设置将创建一个 pem 文件。

KeyMaterial 将私有密钥材料打印到输出中。

Out-File -Encoding ascii -FilePath *C:\path\my-key-pair*.pem 会将私有密钥材料保存在一个具有指定扩展名的文件中。该扩展名可以是 .pem 或 .ppk。私有密钥的名称可以与公有密钥的名称不同，但为了便于使用，请使用相同的名称。

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

使用 Amazon CloudFormation 创建密钥对

当您使用 Amazon CloudFormation 创建新的密钥对时，私有密钥会保存到 Amazon Systems Manager Parameter Store。参数名称有以下形式：

```
/ec2/keypair/key_pair_id
```

有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的 Amazon Systems Manager Parameter Store。

使用 Amazon CloudFormation 创建密钥对

1. 在您的模板中指定 AWS::EC2::KeyPair 资源。

```
Resources:
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

2. 按如下方式使用 describe-key-pairs 命令获取密钥对的 ID。

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

下面是示例输出。

```
key-05abb699beEXAMPLE
```

3. 按如下方式使用 get-parameter 命令获取密钥的参数，并将密钥材料保存在 .pem 文件中。

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption --
query Parameter.Value --output text > new-key-pair.pem
```

所需的 IAM 权限

要启用 Amazon CloudFormation 以代表您管理 Parameter Store 参数，由 Amazon CloudFormation 或您用户担任的 IAM 角色必须拥有以下权限：

- `ssm:PutParameter` – 授予权限以创建私有密钥材料的参数。
- `ssm:DeleteParameter` – 授予权限以删除存储私有密钥材料的参数。无论密钥对是由 Amazon CloudFormation 导入还是创建的，都需要此权限。

当 Amazon CloudFormation 删除由堆栈创建或导入的密钥对时，它会执行权限检查，以确定您是否有权删除参数，即使 Amazon CloudFormation 仅在创建密钥对而非导入密钥对时才创建参数。Amazon CloudFormation 使用与您账户中的任何参数都不匹配的虚构参数名称测试所需的权限。因此，您可能会在 `AccessDeniedException` 错误消息中看到虚构的参数名称。

使用第三方工具创建密钥对，并将公有密钥导入 Amazon EC2

如果不使用 Amazon EC2 创建密钥对，您可以使用第三方工具创建一个 RSA 或 ED25519 密钥对，然后将公有密钥导入 Amazon EC2。

密钥对的要求

- 支持的类型：RSA 和 ED25519。Amazon EC2 不接受 DSA 密钥。

  Note

  Windows 实例不支持 ED25519 密钥。
- 支持的格式：
  - OpenSSH 公有密钥格式（格式为 `~/.ssh/authorized_keys`）。如果您在使用 EC2 Instance Connect API 时使用 SSH 进行连接，则也支持 SSH2 公司。
  - SSH 私有密钥文件格式必须为 PEM 或 PPK
  - （仅 RSA）Base64 编码的 DER 格式
  - （仅 RSA）SSH 公有密钥文件格式如 RFC 4716 所指定
- 支持的长度：1024、2048 和 4096。如果您在使用 EC2 Instance Connect API 时使用 SSH 进行连接，则支持的长度为 2048 和 4096。

要使用第三方工具创建密钥对

1. 使用您选择的第三方工具生成密钥对。例如，您可以使用 ssh-keygen（通过标准 OpenSSH 安装提供的工具）。或者，您可以使用 Java、Ruby、Python 和很多其他提供标准库的编程语言来创建 RSA 或 ED25519 密钥对。

   Important

   私有密钥必须采用 PEM 或 PPK 格式。例如，使用 `ssh-keygen -m PEM` 生成 PEM 格式的 OpenSSH 密钥。
2. 将公有密钥保存至本地文件。例如：`~/.ssh/my-key-pair.pub`。此文件的文件扩展名并不重要。

3. 将私有密钥保存至扩展名为 .pem 或 .ppk 的本地文件。例如，~/.ssh/my-key-pair.pem 或 ~/.ssh/my-key-pair.ppk。

   Important

   将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供公有密钥的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

创建密钥对后，使用以下方法之一将公有密钥导入到 Amazon EC2。

Console

要将公有密钥导入至 Amazon EC2

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Key Pairs (密钥对)。
3. 选择 Import key pair (导入密钥对)。
4. 对于 Name（名称），为公有密钥输入一个描述性名称。该名称最多可包含 255 个 ASCII 字符。它不能包含前导空格或尾随空格。

   Note

   当您从 EC2 控制台连接到实例时，控制台会建议使用此名称作为私有密钥文件的名称。
5. 选择 Browse (浏览) 以导航到您的公有密钥并选择它，或者将公有密钥的内容粘贴到 Public key contents (公有密钥内容) 字段中。
6. 选择 Import key pair (导入密钥对)。
7. 验证您导入的公有密钥是否显示在密钥对列表中。

Amazon CLI

要将公有密钥导入至 Amazon EC2

使用 import-key-pairAmazon CLI 命令。

验证密钥对是否已成功导入

使用 describe-key-pairsAmazon CLI 命令。

PowerShell

要将公有密钥导入至 Amazon EC2

使用 Import-EC2KeyPairAmazon Tools for Windows PowerShell 命令。

验证密钥对是否已成功导入

使用 Get-EC2KeyPairAmazon Tools for Windows PowerShell 命令。

标记公有密钥

要对您使用 Amazon EC2 创建或导入 Amazon EC2 的公有密钥进行分类和管理，您可使用自定义元数据对其进行标记。有关标签的工作原理的更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

您可以使用以下方法之一查看、添加和删除标签。

Console

要查看、添加或删除公有密钥的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Key Pairs (密钥对)。
3. 选择一个公有密钥，然后依次选择 Actions (操作)、Manage tags (管理标签)。
4. Manage tags (管理标签) 显示分配给公有密钥的所有标签。
   - 要添加标签，请选择 Add tag (添加标签)，然后输入标签键和值。您最多可以为每个密钥添加 50 个标签。有关更多信息，请参阅标签限制 (p. 1668)。
   - 要删除标签，请选择要删除的标签旁的 Remove (删除)。
5. 选择 Save。

Amazon CLI

查看公有密钥标签

使用 describe-tagsAmazon CLI 命令。在以下示例中，您将描述所有公有密钥的标签。

```
$ aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

描述特定公有密钥的标签

使用 describe-key-pairsAmazon CLI 命令。

```
$ aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
```

```
}
```

要标记公有密钥

使用 create-tagsAmazon CLI 命令。在以下示例中，使用 Key=Cost-Center 和 Value=CC-123 标记公有密钥。

```
$ aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

从公有密钥中删除标签

使用 delete-tagsAmazon CLI 命令。有关示例，请参阅 Amazon CLI Command Reference 中的示例。

PowerShell

查看公有密钥标签

使用 Get-EC2Tag 命令。

描述特定公有密钥的标签

使用 Get-EC2KeyPair 命令。

要标记公有密钥

使用 New-EC2Tag 命令。

从公有密钥中删除标签

使用 Remove-EC2Tag 命令。

描述公有密钥

您可以描述存储在 Amazon EC2 中的公有密钥。您还可以检索公有密钥材料并识别启动时指定的公有密钥。

主题

- 描述公有密钥 (p. 1296)
- 检索公有密钥材料 (p. 1298)
- 确定启动时指定的公有密钥 (p. 1300)

描述公有密钥

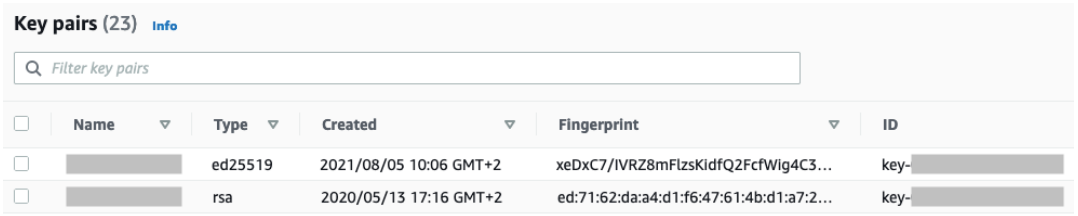
您可以查看有关存储在 Amazon EC2 中的公有密钥的以下信息：公有密钥名称、ID、密钥类型、指纹、公有密钥材料、Amazon EC2 创建密钥的日期和时间（采用 UTC 时区）（如果密钥是由第三方工具创建的，则是将该密钥导入 Amazon EC2 的日期和时间），以及与该公有密钥相关联的所有标签。

您可以使用 Amazon EC2 控制台或 Amazon CLI 以查看有关您的公有密钥的信息。

Console

要查看有关您的公有密钥的信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航器中，选择 Key Pairs（密钥对）。
3. 您可以在Key pairs（密钥对）表中查看每个公有密钥的相关信息。



4. 要查看公有密钥的标签，请选中密钥旁边的复选框，然后选择 Actions（操作）、Manage tags（管理标签）。

Amazon CLI

要描述公有密钥

使用 describe-key-pairs 命令指定 `--key-names` 参数。

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

输出示例

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

或者，您可以指定 `--key-pair-ids` 参数，而不是 `--key-names`，以识别公有密钥。

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

要查看输出中的公有密钥材料，必须指定 `--include-public-key` 参数。

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

示例输出 - 在输出中，PublicKey 字段包含公有密钥材料。

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
```

```
    ]
}
```

检索公有密钥材料

您可以使用多种方法获取对公有密钥材料的访问权限。您可以从本地电脑上匹配的私有密钥中检索公有密钥材料，或从使用公有密钥启动的实例上的实例元数据或 `authorized_keys` 文件中检索公有密钥材料，或者使用 `describe-key-pairs` Amazon CLI 命令来检索公有密钥材料。

使用以下方法之一检索公有密钥材料。

From the private key

要从私有密钥中检索公有密钥材料

在本地 Linux 或 macOS 计算机上，可使用 ssh-keygen 命令检索密钥对的公有密钥。指定您已在其中下载私有密钥的路径（`.pem` 文件）。

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

该命令返回公有密钥，如以下示例所示。

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

如果该命令失败，请运行以下命令以确保更改对您的私有密钥对文件的权限，以便只有您才能查看该文件。

```
chmod 400 key-pair-name.pem
```

From the instance metadata

您可以使用实例元数据服务版本 2 或实例元数据服务版本 1 从实例元数据中检索公有密钥。

> **Note**
>
> 如果您更改用于连接到实例的密钥对，Amazon EC2 不会更新实例元数据以显示新的公有密钥。实例元数据将继续显示您在启动实例时指定的密钥对的公有密钥。

要从实例元数据中检索公有密钥材料

使用实例中的以下命令之一。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

输出示例

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

有关实例元数据的更多信息，请参阅 检索实例元数据 (p. 766)。

From the instance

如果您在启动 Linux 实例时指定密钥对，当您的实例首次启动时，公有密钥的内容将放置 ~/.ssh/authorized_keys 内的一个条目中的实例上。

要从实例中检索公有密钥材料

1. 连接到您的实例。 (p. 644)
2. 在终端窗口中，使用您常用的文本编辑器（如 authorized_keys 或 vim）打开 nano 文件。

   ```
   [ec2-user ~]$ nano ~/.ssh/authorized_keys
   ```

   authorized_keys 文件打开，显示公有密钥，后面是密钥对的名称。以下是名为 *key-pair-name* 的密钥对的示例条目。

   ```
   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
   hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
   lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
   qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
   BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
   ```

From describe-key-pairs

通过 **describe-key-pairs**Amazon CLI 命令检索公有密钥材料

使用 describe-key-pairs 命令指定 --key-names 参数，以识别公有密钥。要将公有密钥材料包含在输出中，请指定 --include-public-key 参数。

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

示例输出 - 在输出中，PublicKey 字段包含公有密钥材料。

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

或者，您可以指定 `--key-pair-ids` 参数，而不是 `--key-names`，以识别公有密钥。

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

确定启动时指定的公有密钥

如果您在启动实例时指定公有密钥，则该实例将记录公有密钥名称。

要确定启动时指定的公有密钥

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在详细信息选项卡的实例详细信息下，启动时分配的密钥对字段会显示您在启动实例时指定的公有密钥名称。

Note

即使您更改实例上的公有密钥或添加公有密钥，启动时分配的密钥对字段的值也不会更改。

在 Amazon EC2 上删除您的公有密钥

您可以删除存储在 Amazon EC2 中的公有密钥。删除一个公有密钥不会删除匹配的私有密钥。

使用以下方法删除公有密钥时，您仅删除了创建 (p. 1290)或导入 (p. 1293)密钥对时在 Amazon EC2 中存储的公有密钥。删除公有密钥并不会从您添加公有密钥的任何实例中删除公有密钥，无论是在启动实例时还是启动后。也不会删除本地计算机上的私有密钥。您可以继续连接到使用已从 Amazon EC2 删除的公有密钥启动的实例，只要您仍然拥有私有密钥（`.pem`）文件。

Note

要从实例中删除公有密钥，请参阅 在实例上添加或删除公有密钥 (p. 1301)。

Important

如果您使用的是 Auto Scaling 组（例如，在 Elastic Beanstalk 环境中），请确保您要删除的公有密钥未在关联的启动模板或启动配置中指定。如果 Amazon EC2 Auto Scaling 检测到运行不正常的实例，它将启动替代实例。但是，如果找不到公有密钥，则实例启动失败。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的启动模板。

您可以使用以下方法删除 Amazon EC2 上的公有密钥。

Console

要在 Amazon EC2 上删除您的公有密钥

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Key Pairs (密钥对)。
3. 选择要删除的密钥对，然后依次选择 Actions（操作）、Delete（删除）。
4. 在确认字段中，输入 `Delete`，然后选择 Delete (删除)。

Amazon CLI

要在 Amazon EC2 上删除您的公有密钥

使用 delete-key-pairAmazon CLI 命令。

PowerShell

要在 Amazon EC2 上删除您的公有密钥

使用 Remove-EC2KeyPairAmazon Tools for Windows PowerShell 命令。

在实例上添加或删除公有密钥

启动实例时，您可以指定密钥对 (p. 579)。如果您在启动时指定密钥对，当您的实例首次启动时，公有密钥将放置在 ~/.ssh/authorized_keys 内的一个条目中的 Linux 实例中。

您可以更改用于访问实例默认系统账户的密钥对，方法是在实例上添加新的公有密钥，或者替换实例上的公有密钥（删除现有公有密钥并添加新的公有密钥）。您还可以从实例中删除所有公有密钥。您可能出于以下原因需要执行这些操作：

- 如果组织中有用户需要使用单独的密钥访问系统用户，您可以将此公有密钥添加到实例。
- 如果某人有私有密钥的副本（.pem 文件），而您想要防止他们连接到实例（例如在他们已离开企业的情况下），您可以删除实例上的公有密钥，并将其替换为新的密钥。
- 如果您从实例创建 Linux AMI，则公有密钥材料将从实例复制到 AMI。如果您从 AMI 启动实例，则新实例将包含来自原始实例的公有密钥。要防止拥有私有密钥的用户连接到新实例，您可以在创建 AMI 之前从原始实例中删除公有密钥。

公有密钥位于实例上的 .ssh/authorized_keys 文件中。

要添加或替换密钥对，您必须能够连接到实例。如果您丢失了现有的私有密钥，或者在没有密钥对的情况下启动了实例，则您将无法连接到实例，因此无法添加或替换密钥对。如果您丢失了私有密钥，则可以检索它。有关更多信息，请参阅 我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)。如果启动实例而没有密钥对，则将无法连接到此实例，除非您选择配置为允许用户以其他方式登录的 AMI。

Note

这些程序用于修改默认用户的密钥对，例如 ec2-user。有关向实例添加用户的信息，请参阅 管理 Linux 实例上的用户 (p. 705)。

添加或替换密钥对

1. 使用 Amazon EC2 控制台 (p. 1290)或第三方工具 (p. 1293)创建新的密钥对。
2. 从新密钥对检索公有密钥。有关更多信息，请参阅检索公有密钥材料 (p. 1298)。
3. 使用现有私有密钥连接到实例 (p. 644)。
4. 使用您选择的文本编辑器，在实例上打开 .ssh/authorized_keys 文件。将新密钥对的公有密钥信息粘贴到现有公有密钥信息下。保存文件。
5. 从实例分离，并测试能否使用新的私有密钥文件连接到实例。
6. (可选) 如果您要替换现有密钥对，请连接到实例并从 .ssh/authorized_keys 文件中删除原始密钥对的公有密钥信息。

Important

如果您使用的是 Auto Scaling 组，请确保您要替换的密钥对未在启动模板或启动配置中指定。如果 Amazon EC2 Auto Scaling 检测到运行不正常的实例，它将启动替代实例。但是，如果找不到密钥对，则实例启动失败。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南中的启动模板。

要从实例中删除公有密钥

1. 连接到您的实例 (p. 644)。

2. 使用您选择的文本编辑器，在实例上打开 `.ssh/authorized_keys` 文件。删除公有密钥信息，然后保存该文件。

   Warning

   从实例中删除所有公有密钥并断开与实例的连接后，您将无法再次连接到该实例，除非 AMI 提供了其他登录方式。

验证密钥

验证您的密钥对的指纹

在 Amazon EC2 控制台的 Key Pairs（密钥对）页面，Fingerprint（指纹）列显示从您的密钥对生成的指纹。

您可以使用 Key Pairs（密钥对）页面上显示的指纹验证您本地机器上的私有密钥是否与 Amazon EC2 中存储的公有密钥匹配。在您已下载私有密钥文件的电脑上，从私有密钥文件生成指纹。输出应与控制台中显示的指纹匹配。当 Amazon EC2 计算指纹时，Amazon EC2 可能会用 = 字符在指纹上添加填充。ssh-keygen 等其他工具可能会省略此填充。

指纹如何计算

Amazon EC2 使用不同的哈希函数来计算 RSA 和 ED25519 密钥对的指纹。此外，对于 RSA 密钥对，Amazon EC2 使用不同的哈希函数以不同方式计算指纹，具体取决于密钥对是由 Amazon EC2 创建还是导入到 Amazon EC2 的。

下表所列的哈希函数用于计算由 Amazon EC2 创建以及导入到 Amazon EC2 的 RSA 和 ED25519 密钥对的指纹。

用于计算指纹的哈希函数

密钥对来源	RSA 密钥对	ED25519 密钥对
由 Amazon EC2 创建	SHA-1	SHA-256
导入到 Amazon EC2	MD5[1]	SHA-256

[1] 如果您将公有的 RSA 密钥导入到 Amazon EC2，系统会使用 MD5 哈希函数计算指纹。无论您如何创建密钥对（例如，通过使用第三方工具或者从使用 Amazon EC2 创建的现有私有密钥生成新的公有密钥），都是如此。

在不同区域使用相同的密钥对时

如果您计划使用相同的密钥对连接到不同 Amazon Web Services 区域 中的实例，必须将公有密钥导入到将在其中使用公有密钥的所有区域。如果使用 Amazon EC2 创建密钥对，您可以 检索公有密钥材料 (p. 1298) 以便将公有密钥导入到其他区域。

Note

如果您使用 Amazon EC2 创建 RSA 密钥对，然后从 Amazon EC2 私有密钥生成公有密钥，则导入的公有密钥的指纹将与原始公有密钥不同。这是因为使用 Amazon EC2 创建的原始 RSA 密钥的指纹是使用 SHA-1 哈希函数计算的，而导入的 RSA 密钥的指纹则使用 MD5 哈希函数计算。

对于 ED25519 密钥对，无论它们是由 Amazon EC2 创建还是导入到 Amazon EC2 的，指纹都将相同，因为两种情况下都使用相同的 SHA-256 哈希函数来计算指纹。

从私有密钥生成指纹

使用以下命令之一可从本地机器上的私有密钥生成指纹。

如果您使用的是 Windows 本地计算机，您可以使用 Windows Subsystem for Linux (WSL) 运行以下命令。按照 Windows 10 安装指南中的说明执行操作来安装 WSL 和 Linux 发行版。说明中的示例安装的是 Linux 的 Ubuntu 发行版，但您可以安装任意发行版。系统会提示您重新启动电脑以使更改生效。

- 如果您使用 Amazon EC2 创建密钥对

  如以下示例中所示，使用 OpenSSL 工具生成指纹。

  对于 RSA 密钥对：

  ```
  openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt | openssl
   sha1 -c
  ```

  对于 ED25519 密钥对：

  ```
  ssh-keygen -l -f path_to_private_key
  ```

- （仅限 RSA 密钥对）如果您将公有密钥导入 Amazon EC2

  无论密钥对的创建方式如何（例如，使用第三方工具或者从使用 Amazon EC2 创建的现有私有密钥生成新的公有密钥），都可以遵循此过程。

  如以下示例中所示，使用 OpenSSL 工具生成指纹。

  ```
  openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
  ```

- 如果您使用 OpenSSH 7.8 或更高版本创建 OpenSSH 密钥对，并将公有密钥导入到 Amazon EC2

  如以下示例中所示，使用 ssh-keygen 生成指纹。

  对于 RSA 密钥对：

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER |
   openssl md5 -c
  ```

  对于 ED25519 密钥对：

  ```
  ssh-keygen -l -f path_to_private_key
  ```

适用于 Linux 实例的 Amazon EC2 安全组

安全组 充当 EC2 实例的虚拟防火墙，用于控制传入和传出流量。入站规则控制传入到实例的流量，出站规则控制从实例传出的流量。启动实例时，您可以指定一个或多个安全组。如果您未指定安全组，则 Amazon EC2 将使用默认安全组。您可以为每个安全组添加规则，规定流入或流出其关联实例的流量。您可以随时修改安全组的规则。新规则和修改后的规则将自动应用到与安全组相关联的所有实例。在 Amazon EC2 确定是否允许流量到达实例时，它评估与实例关联的所有安全组中的所有规则。

在 VPC 中启动实例时，您必须指定一个为该 VPC 创建的安全组。启动实例后，您可以更改其安全组。安全组与网络接口关联。更改实例的安全组也会更改与主网络接口 (eth0) 关联的安全组。有关更多信息，请参阅更改实例的安全组 (p. 1315)。您还可以更改与任何其他网络接口关联的安全组。有关更多信息，请参阅修改网络接口属性 (p. 1134)。

安全性是 Amazon 和您的共同责任。有关更多信息，请参阅 Amazon EC2 中的安全性 (p. 1219)。Amazon 提供安全组作为一项工具用于保护您的实例，您需要对其进行配置以满足您的安全需求。如果安全组无法满足您的要求，除了使用安全组外，您还可以在任何一个实例上保持自己的防火墙。

要允许流量进入 Windows 实例，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的适用于 Windows 实例的 Amazon EC2 安全组。

使用安全组不收取任何额外费用。

目录

- 安全组规则 (p. 1304)
- 安全组连接跟踪 (p. 1306)
  - 未跟踪的连接 (p. 1306)
  - 自动跟踪的连接 (p. 1306)
  - 限制 (p. 1307)
  - 示例 (p. 1307)
- 默认和自定义安全组 (p. 1308)
  - 默认安全组 (p. 1308)
  - 自定义安全组 (p. 1308)
- 使用安全组 (p. 1309)
  - 创建安全组 (p. 1309)
  - 复制安全组 (p. 1310)
  - 查看安全组 (p. 1310)
  - 向安全组添加规则 (p. 1311)
  - 更新安全组规则 (p. 1312)
  - 从安全组中删除规则 (p. 1313)
  - 删除安全组 (p. 1314)
  - 向实例分配安全组 (p. 1314)
  - 更改实例的安全组 (p. 1315)
- 针对不同使用案例的安全组规则 (p. 1315)
  - Web 服务器规则 (p. 1316)
  - 数据库服务器规则 (p. 1316)
  - 用于从您的计算机连接到实例的规则 (p. 1317)
  - 用于在具有相同安全组的实例之间进行连接的规则 (p. 1317)
  - 用于 ping/ICMP 的规则 (p. 1317)
  - DNS 服务器规则 (p. 1318)
  - Amazon EFS 规则 (p. 1318)
  - Elastic Load Balancing 规则 (p. 1319)
  - VPC 对等规则 (p. 1319)

安全组规则

安全组的规则控制允许达到与该安全组相关联实例的入站流量。这些规则还控制允许离开实例的出站流量。

以下是您的安全组规则的特征：

- 默认情况下，安全组包含允许所有出站流量的出站规则。您可以删除这些规则。请注意，默认情况下 Amazon EC2 会阻止端口 25 上的流量。有关更多信息，请参阅对使用端口 25 发送的电子邮件的限制 (p. 1680)。

- 安全组规则始终是宽松的；您无法创建拒绝访问的规则。
- 安全组规则允许您根据协议和端口号筛选流量。
- 安全组是有状态的 — 如果您从实例发送一个请求，则无论入站安全组规则如何，都将允许该请求的响应流量流入。对于 VPC 安全组，这还意味着，无论出站规则如何，都允许对允许的入站流量的响应流出。有关更多信息，请参阅安全组连接跟踪 (p. 1306)。
- 您可以随时添加和删除规则。您所做的更改将会自动应用到与安全组关联的实例中。

  某些规则变更产生的影响可能会取决于跟踪流量的方式。有关更多信息，请参阅安全组连接跟踪 (p. 1306)。
- 当您将多个安全组与一个实例相关联时，将有效汇总每个安全组的规则，以创建一组规则。Amazon EC2 使用这组规则确定是否允许访问。

  您可以为一个实例分配多个安全组。因此，一个实例可以有数百条适用的规则。访问该实例时，这可能会导致问题。因此，我们建议您尽可能使规则简洁。

  Note

  安全组无法阻止发送至或来自 Route 53 Resolver 的 DNS 请求，Route 53 Resolver 有时称为“VPC+2 IP 地址”（请参阅《Amazon Route 53 开发者指南》中的什么是 Amazon Route 53 Resolver？）或“AmazonProvidedDNS”（请参阅《Amazon Virtual Private Cloud 用户指南》中的使用 DHCP 选项集）。如果希望通过 Route 53 Resolver 筛选 DNS 请求，则可以启用 Route 53 Resolver DNS Firewall（请参阅《Amazon Route 53 开发人员指南》中的 Route 53 Resolver DNS Firewall）。

对于每个规则，您可以指定以下内容：

- 名称：安全组的名称（例如，"my-security-group"）。

  名称最长可达 255 个字符。允许的字符包括 a-z、A-Z、0-9、空格和 ._-:/()#,@[]+=;{}!$*。如果名称后面带有空格，我们在保存名称时会删除这些空格。例如，如果您输入“Test Security Group ”作为名称，我们会将其存储为“Test Security Group”。
- 协议：允许的协议。最常见的协议为 6 (TCP)、17 (UDP) 和 1 (ICMP)。
- 端口范围：对于 TCP、UDP 或自定义协议，允许的端口范围。您可以指定单个端口号（例如 22）或端口号范围（例如`7000-8000`）。
- ICMP 类型和代码：对于 ICMP，ICMP 类型和代码。例如，对于 ICMP 回应请求使用类型 8，对 ICMPv6 回显请求使用键入 128。
- 源或目标：允许的流量的源（入站规则）或目标（出站规则）。指定下列项之一：
  - 一个 IPv4 地址。您必须使用 `/32` 前缀长度。例如，`203.0.113.1/32`。
  - 一个 IPv6 地址。您必须使用 `/128` 前缀长度。例如，`2001:db8:1234:1a00::123/128`。
  - 采用 CIDR 块表示法的 IPv4 地址范围。例如，`203.0.113.0/24`。
  - 采用 CIDR 块表示法的 IPv6 地址范围。例如，`2001:db8:1234:1a00::/64`。
  - 前缀列表的 ID。例如，`pl-1234abc1234abc123`。有关更多信息，请参阅 Amazon VPC 用户指南 中的前缀列表。
  - 安全组的 ID（此处称为指定的安全组）。例如，当前安全组、来自同一 VPC 的安全组或对等 VPC 的安全组。这允许基于与指定安全组关联的资源的私有 IP 地址的流量。这并不会将指定安全组的规则添加到当前安全组。
- （可选）描述：您可以添加规则的说明；这可帮助您在以后识别它。描述的长度最多为 255 个字符。允许的字符包括 a-z、A-Z、0-9、空格和 ._-:/()#,@[]+=;{}!$*。

当您创建安全组规则时，Amazon 会将唯一 ID 分配给规则。当您使用 API 或 CLI 修改或删除某规则时，您可以使用该规则的 ID。

当您指定一个安全组作为规则的源或目标时，规则会影响与该安全组关联的所有实例。允许的传入流量基于与源安全组相关联的实例的私有 IP 地址 (而不是公有 IP 或弹性 IP 地址)。有关 IP 地址的更多信息，请参阅 Amazon EC2 实例 IP 寻址 (p. 1053)。如果您的安全组规则引用相同 VPC 或对等 VPC 中的已删除安全组，或引用 VPC 对等连接已删除的对等 VPC 中的安全组，该规则将被标记为过时。有关更多信息，请参阅Amazon VPC Peering Guide中的使用过时的安全组规则。

如果特定端口具有多个规则，Amazon EC2 将应用最宽松的规则。例如，如果有一条规则允许从 IP 地址 203.0.113.1 访问 TCP 端口 22 (SSH)，而另一条规则允许所有人访问 TCP 端口 22，那么所有人都可以访问 TCP 端口 22。

当您添加、更新或删除规则时，相关修改会自动应用到所有与该安全组相关的实例。

安全组连接跟踪

您的安全组使用连接跟踪来跟踪有关进出实例的流量的信息。将基于流量的连接状态应用规则以确定允许还是拒绝流量。有了这种方法，安全组就具有状态。这意味着无论出站安全组规则如何都允许对入站流量的响应流出实例，反之亦然。

例如，假设您从家中的计算机对您的实例启动 netcat 或与您的实例类似的命令，并且您的入站安全组规则允许 ICMP 流量。跟踪有关连接的信息（包括端口信息）。来自 命令的实例的响应流量不会作为新请求来跟踪，而是作为已建立的连接来跟踪，并且可以流出实例，即使您的出站安全组规则限制出站 ICMP 流量也是如此。

对于除 TCP、UDP 或 ICMP 以外的协议，仅跟踪 IP 地址和协议编号。如果您的实例将流量发送到另一个主机，且该主机在 600 秒内将同一类型的流量发送到您的实例，则无论入站安全组规则如何，您的实例的安全组都将接受该请求。安全组接受它，因为它被视为原始流量的响应流量。

更改安全组规则时，其跟踪的连接不会立即中断。在现有连接超时之前，安全组将继续允许数据包。要确保该流量立即中断，或确保所有流量无论跟踪状态如何，均遵循防火墙规则，您可以使用子网的网络 ACL。网络 ACL 是无状态的，因此不会自动允许响应流量。添加阻止任一方向的流量的网络 ACL 会破坏现有连接。有关更多信息，请参阅 Amazon VPC 用户指南中的网络 ACL。

> Note
>
> 安全组对传入或传出 Route 53 Resolver 的 DNS 流量没有影响，Route 53 Resolver 有时称为“VPC+2 IP 地址”（请参阅《Amazon Route 53 开发者指南》中的什么是 Amazon Route 53 Resolver？）或“AmazonProvidedDNS”（请参阅《Amazon Virtual Private Cloud 用户指南》中的使用 DHCP 选项集）。如果希望通过 Route 53 Resolver 筛选 DNS 请求，则可以启用 Route 53 Resolver DNS Firewall（请参阅《Amazon Route 53 开发人员指南》中的 Route 53 Resolver DNS Firewall）。

未跟踪的连接

并非所有通信流都会被跟踪。如果有一个安全组规则允许所有通信（0.0.0.0/0 或 ::/0）的 TCP 或 UDP 流，而另一个方向上存在一个对应的规则允许所有端口（0-65535）的所有响应通信（0.0.0.0/0 或 ::/0），则不会跟踪该通信流，除非它属于自动跟踪连接 (p. 1306)的一部分。基于允许响应流量的入站或出站规则允许未跟踪流的响应流量，而不是基于跟踪信息。

如果删除或修改了支持该流的规则，则会立即中断未被跟踪的通信流。例如，如果您有一个开放 (0.0.0.0/0) 出站规则，并且删除了允许所有 (0.0.0.0/0) 入站 SSH（TCP 端口 22）流量传输到实例的规则（或修改它以使不再允许连接），则您与实例的现有 SSH 连接将立即删除。该连接以前未跟踪，因此更改将断开连接。另一方面，如果您有一个较细化的入站规则，最初允许 SSH 连接（意味着已跟踪该连接），但将该规则更改为不再允许来自当前 SSH 客户端地址的新连接，则由于现有的 SSH 连接被跟踪，它不会中断。

自动跟踪的连接

即使安全组配置无需跟踪，也会自动跟踪通过以下各项建立的连接。必须跟踪这些连接以确保对称路由，因为可能有多个有效的回复路径。

- 仅出口互联网网关
- Gateway Load Balancer
- Global Accelerator 加速器
- NAT 网关
- Network Firewall 防火墙端点
- Network Load Balancer
- Amazon PrivateLink（接口 VPC 终端节点）
- 中转网关挂载

限制

Amazon EC2 定义每个实例可以跟踪的最大连接数量。达到最大值后，由于无法建立新连接，所有发送或接收的数据包都将丢失。发生这种情况时，发送和接收数据包的应用程序无法正常通信。使用 `conntrack_allowance_available` 网络性能指标来确定该实例类型仍然可用的跟踪连接数。

要确定数据包是否因为您实例的网络流量超过了可跟踪的最大连接数量而丢弃，请使用 `conntrack_allowance_exceeded` 网络性能指标。有关更多信息，请参阅监控 EC2 实例的网络性能 (p. 1164)。

如果您超过了每个实例可跟踪的最大连接数量，建议您借助 Elastic Load Balancing 扩展负载均衡器注册的实例数或实例大小。

示例

在以下示例中，安全组具有允许 TCP 和 ICMP 流量的入站规则，并具有允许所有出站流量的出站规则。

入站规则		
协议类型	端口号	源 IP
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	All	0.0.0.0/0
出站规则		
协议类型	端口号	目的地 IP
All	All	0.0.0.0/0
All	All	::/0

通过与实例或网络接口的直接网络连接，跟踪行为如下：

- 将会跟踪端口 22（SSH）上的入站和出站 TCP 流量，因为入站规则只允许来自 203.0.113.1/32 的流量，而不是所有 IP 地址（0.0.0.0/0）。
- 不会跟踪端口 80（HTTP）上的入站和出站 TCP 流量，因为入站和出站规则允许来自所有 IP 地址的流量。
- 始终跟踪 ICMP 流量。

如果您删除 IPv4 流量的出站规则，则将跟踪所有入站和出站 IPv4 流量，包括端口 80（HTTP）上的流量。如果您删除 IPv6 流量的出站规则，这同样适用于 IPv6 流量。

默认和自定义安全组

您的 Amazon 账户在每个区域的默认 VPC 中都自动拥有一个默认安全组。如果您在启动实例时没有指定安全组，实例会自动与 VPC 的默认安全组关联。如果您不希望您的实例使用默认安全组，则可创建自己的自定义安全组，并在启动实例时指定它们。

主题

- 默认安全组 (p. 1308)
- 自定义安全组 (p. 1308)

默认安全组

您的 Amazon 账户在每个区域的默认 VPC 中都自动拥有一个默认安全组。如果您在启动实例时没有指定安全组，实例会自动与 VPC 的默认安全组关联。

原定设置安全组名称为 "default"，而且拥有一个由 Amazon 分配的 ID。下表介绍默认安全组的默认规则。

入站规则			
源	协议	端口范围	描述
安全组 ID（其自己的资源 ID）	All	All	允许来自分配给相同安全组的网络接口和实例的入站流量。
出站规则			
目的地	协议	端口范围	描述
0.0.0.0/0	All	All	允许所有的出站 IPv4 流量。
::/0	All	All	允许所有的出站 IPv6 流量。仅当 VPC 具有关联的 IPv6 CIDR 块时才添加此规则。

您可以添加或删除任何默认安全组的入站和出站规则。

您无法删除默认安全组。如果您尝试删除默认安全组，会显示以下错误：`Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user`。

自定义安全组

如果您不希望您的实例使用默认安全组，则可创建自己的安全组，并在启动实例时指定它们。您可以创建多个安全组以反映实例扮演的不同角色；例如，Web 服务器或数据库服务器。

创建安全组时，您必须为其提供名称和描述。安全组的名称和描述最多 255 个字符，而且仅限于以下字符：

a-z、A-Z、0-9、空格和 ._-:/()#,@[]+=&;{}!$*

安全组名称不能以 sg- 开头。安全组名称在 VPC 中必须是唯一的。

以下是您创建的安全组的默认规则：

- 不允许入站流量
- 允许所有出站流量

创建安全组后，您可以更改其入站规则，以反映您希望到达关联实例的入站流量的类型。您也可以更改其出站规则。

有关您可以添加到安全组的规则的更多信息，请参阅针对不同使用案例的安全组规则 (p. 1315)。

使用安全组

在启动实例时，您可以向实例分配安全组。在添加或删除规则时，所做的更改将自动应用于已分配安全组的所有实例。有关更多信息，请参阅向实例分配安全组 (p. 1314)。

启动实例后，您可以更改其安全组。有关更多信息，请参阅更改实例的安全组 (p. 1315)。

您可以使用 Amazon EC2 控制台和命令行工具创建、查看、更新和删除安全组及安全组规则。

任务

- 创建安全组 (p. 1309)
- 复制安全组 (p. 1310)
- 查看安全组 (p. 1310)
- 向安全组添加规则 (p. 1311)
- 更新安全组规则 (p. 1312)
- 从安全组中删除规则 (p. 1313)
- 删除安全组 (p. 1314)
- 向实例分配安全组 (p. 1314)
- 更改实例的安全组 (p. 1315)

创建安全组

尽管您可以为实例指定默认安全组，您可能仍希望创建自己的安全组，以反映实例在您的系统中扮演的不同角色。

在默认情况下，新安全组起初只有一条出站规则，即允许所有通信离开实例。您必须添加规则，以便允许任何入站数据流或限制出站数据流。

安全组只能在为其创建该组的 VPC 中使用。

Console

创建安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择Create security group（创建安全组）。
4. 在 Basic details (基本详细信息) 部分中，执行以下操作。
   a. 输入安全组的描述性名称和简要说明。创建安全组后，无法对其进行编辑。名称和描述的长度最多为 255 个字符。允许的字符包括 a-z、A-Z、0-9、空格和 ._-:/()#,@[]+=&;{}!$*。
   b. 对于 VPC，请选择 VPC。

5. 您可以现在添加安全组规则，也可以稍后再添加。有关更多信息，请参阅向安全组添加规则 (p. 1311)。
6. 您可以现在添加标签，也可以稍后再添加。要添加标签，请选择 Add new tag（添加新标签），然后输入标签键和值。
7. 选择Create security group（创建安全组）。

Command line

创建安全组

使用以下命令之一：

- create-security-group (Amazon CLI)
- New-EC2SecurityGroup (Amazon Tools for Windows PowerShell)

复制安全组

您可以通过创建现有安全组的副本来创建新安全组。复制安全组时，将使用与原始安全组相同的入站和出站规则创建副本。如果原始安全组位于 VPC 中，则除非您指定不同的安全组，否则将在相同 VPC 中创建副本。

副本会收到一个新的唯一安全组 ID，您必须为其指定名称。您还可以添加描述。

您无法将安全组从一个区域复制到另一区域。

您可以使用 Amazon EC2 控制台创建安全组副本。

复制安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择要复制的安全组，然后选择 Actions (操作)、Copy to new security group (复制到新安全组)。
4. 指定名称和可选描述，并根据需要更改 VPC 和安全组规则。
5. 选择 Create (创建)。

查看安全组

您可以使用以下方法之一查看有关安全组的信息。

Console

查看安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 此时将列出您的安全组。要查看特定安全组的详细信息，包括其入站和出站规则，请在安全组 ID 列中选择其 ID。

Command line

查看安全组

使用以下命令之一。

- describe-security-groups (Amazon CLI)
- 描述安全组规则 (Amazon CLI)
- Get-EC2SecurityGroup (Amazon Tools for Windows PowerShell)

Amazon EC2 Global View

您可以使用 Amazon EC2 全局视图查看启用 Amazon 账户的所有区域中的安全组。有关更多信息，请参阅使用 Amazon EC2 全局视图列出和筛选跨区域的资源 (p. 1663)。

向安全组添加规则

当您向安全组添加规则时，这一新规则会自动应用于与该安全组关联的任何实例。应用规则可能会有短暂的延迟。有关更多信息，请参阅针对不同使用案例的安全组规则 (p. 1315)和安全组规则 (p. 1304)。

Console

在安全组中添加入站规则

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择安全组，选择 Actions (操作)，然后选择 Edit inbound rules (编辑入站规则)。
4. 对于每一条规则，选择 Add rule（添加规则），然后执行以下操作：
   a. 对于Type（类型），选择要允许的协议类型。
      - 对于自定义 TCP 或 UDP，您必须输入允许的端口范围。
      - 对于自定义 ICMP，您必须从 Protocol (协议) 中选择 ICMP 类型，并从 Port range (端口范围) 中选择代码（如果适用）。例如，要允许ping命令中，从协议选择Echo 请求。
      - 对于任何其他类型，则会为您配置协议和端口范围。
   b. 对于 Source (源)，请执行以下操作之一以允许流量通信。
      - 选择 Custom（自定义），然后以 CIDR 表示法输入 IP 地址、CIDR 块、其他安全组或前缀列表。
      - 选择 Anywhere (任何位置) 以允许指定协议的所有流量到达您的实例。此选项将自动添加 0.0.0.0/0 IPv4 CIDR 块作为源。如果您的安全组位于启用 IPv6 的 VPC 中，则此选项会自动为 ::/0 IPv6 CIDR 块添加规则。

        Warning

        如果您选择 Anywhere（任意位置），则允许所有 IPv4 和 IPv6 地址使用指定协议访问您的实例。如果您要为端口 22（SSH）或 3389（RDP）添加规则，则应该仅授权特定 IP 地址或特定范围内的 IP 地址访问您的实例。
      - 选择我的 IP 以仅允许来自本地计算机的公有 IPv4 地址的入站流量。
   c. 对于 Description (描述)，您可以选择指定规则的简单描述。
5. 选择 Preview changes (预览更改)，然后选择 Save rules (保存规则)。

在安全组中添加出站规则

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择安全组，然后选择 Actions (操作)、Edit outboud rules (编辑出站规则)。
4. 对于每一条规则，选择 Add rule（添加规则），然后执行以下操作：

a. 对于Type（类型），选择要允许的协议类型。

   - 对于自定义 TCP 或 UDP，您必须输入允许的端口范围。
   - 对于自定义 ICMP，您必须从 Protocol (协议) 中选择 ICMP 类型，并从 Port range (端口范围) 中选择代码（如果适用）。
   - 对于任何其他类型，则会自动配置协议和端口范围。

b. 对于目标，执行以下操作之一。

   - 选择自定义，然后以 CIDR 表示法输入 IP 地址、CIDR 块、其他安全组或允许出站流量的前缀列表。
   - 选择任意位置以允许传送到所有 IP 地址的出站流量。此选项将自动添加 0.0.0.0/0 IPv4 CIDR 块作为目标。

     如果您的安全组位于启用 IPv6 的 VPC 中，则此选项会自动为 ::/0 IPv6 CIDR 块添加规则。
   - 选择我的 IP 以仅允许流向本地计算机的公有 IPv4 地址的出站流量。

c. （可选）对于 Description (描述)，请指定规则的简单描述。

5. 选择 Preview changes (预览更改)、Confirm (确认)。

Command line

向安全组添加规则

使用以下命令之一。

- authorize-security-group-ingress (Amazon CLI)
- Grant-EC2SecurityGroupIngress (Amazon Tools for Windows PowerShell)

向安全组添加一个或多个传出规则

使用以下命令之一。

- authorize-security-group-egress (Amazon CLI)
- Grant-EC2SecurityGroupEgress (Amazon Tools for Windows PowerShell)

更新安全组规则

您可以使用以下方法之一更新安全组规则。更新的规则将自动应用于与安全组关联的任何实例。

Console

使用控制台修改现有安全组规则的协议、端口范围或者源或目标时，控制台会删除现有规则并为您添加新规则。

更新安全组规则

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择安全组。
4. 选择 Actions（操作）、Edit inbound rules（编辑入站规则）以更新入站流量的规则，或选择 Actions（操作）、Edit outbound rules（编辑出站规则）以更新出站流量的规则。
5. 根据需要更新规则。
6. 选择 Preview changes (预览更改)、Confirm (确认)。

为安全组规则添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择安全组。
4. 在 Inbound rules（入站规则）或 Outbound rules（出站规则）选项卡上，选中规则的复选框，然后选择 Manage tags（管理标签）。
5. Manage tags（管理标签）页面显示分配给规则的所有标签。要添加标签，请选择 Add tag（添加标签），然后输入标签键和值。要删除标签，请选择要删除的标签旁边的 Remove（删除）。
6. 选择 Save changes（保存更改）。

Command line

您无法使用 Amazon EC2 API 或命令行工具更新现有规则的协议、端口范围或者源或目标。相反，您必须删除该现有规则并添加新规则。不过，您可以更新现有规则的描述。

更新规则

使用以下命令之一。

- 修改安全组规则 (Amazon CLI)

更新现有入站规则的描述

使用以下命令之一。

- update-security-group-rule-descriptions-ingress (Amazon CLI)
- Update-EC2SecurityGroupRuleIngressDescription (Amazon Tools for Windows PowerShell)

更新现有出站规则的描述

使用以下命令之一。

- update-security-group-rule-descriptions-egress (Amazon CLI)
- Update-EC2SecurityGroupRuleEgressDescription (Amazon Tools for Windows PowerShell)

为安全组规则添加标签

使用以下命令之一。

- create-tags（Amazon CLI）
- New-EC2Tag（Amazon Tools for Windows PowerShell）

从安全组中删除规则

当您从安全组中删除规则时，此更改会自动应用于与该安全组关联的任何实例。

您可以使用以下方法之一从安全组中删除规则。

Console

删除安全组规则

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择要更新的安全组，选择 Actionis (操作)，然后选择 Edit inbound rules (编辑入站规则) 以删除入站规则，或选择 Edit outbound rules (编辑出站规则) 以删除出站规则。
4. 选择要删除的规则右侧的 Delete（删除）按钮。
5. 选择 Preview changes (预览更改)、Confirm (确认)。

Command line

从安全组中删除一个或多个传入规则

使用以下命令之一。

- revoke-security-group-ingress (Amazon CLI)
- Revoke-EC2SecurityGroupIngress (Amazon Tools for Windows PowerShell)

从安全组中删除一个或多个传出规则

使用以下命令之一。

- revoke-security-group-egress(Amazon CLI)
- Revoke-EC2SecurityGroupEgress (Amazon Tools for Windows PowerShell)

删除安全组

您不能删除与实例关联的安全组。您不能删除默认安全组。您不能删除由同一 VPC 中其他安全组中的规则引用的安全组。如果您的安全组由自己的一个规则引用，则必须先删除该规则，然后才能删除安全组。

Console

删除安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups (安全组)。
3. 选择要删除的安全组，然后选择操作、删除安全组、删除。

Command line

删除安全组

使用以下命令之一。

- delete-security-group (Amazon CLI)
- Remove-EC2SecurityGroup (Amazon Tools for Windows PowerShell)

向实例分配安全组

启动实例时，您可以将一个或多个安全组分配给实例。您还可以在启动模板中指定一个或多个安全组。安全组将分配给使用启动模板启动的所有实例。

- 要在启动实例时向实例分配安全组，请参阅 使用定义的参数启动实例 (p. 577) 的 Network settings (网络设置) (p. 579)（新控制台）或 步骤 6：配置安全组 (p. 588)（旧控制台）。

- 要在启动模板中指定安全组，请参阅 使用您定义的参数创建新启动模板 (p. 590) 的 Network settings (网络设置) (p. 593)。

更改实例的安全组

启动实例后，您可以通过添加或删除安全组来更改其安全组。

要求

- 实例必须处于 `running` 或 `stopped` 状态。
- 安全组特定于 VPC。您可以将一个安全组分配给在您为其创建安全组的 VPC 中启动的一个或多个实例。

Console

更改实例的安全组

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择您的实例，依次选择 Actions（操作）、Security（安全）和 Change security groups（更改安全组）。
4. 对于 Associated security groups (关联的安全组)，从列表中选择一个安全组，然后选择 Add security group (添加安全组)。

   要删除已关联的安全组，请为该安全组选择 Remove (删除)。
5. 选择 Save（保存）。

Command line

更改实例的安全组

使用以下命令之一。

- modify-instance-attribute (Amazon CLI)
- Edit-EC2InstanceAttribute (Amazon Tools for Windows PowerShell)

针对不同使用案例的安全组规则

您可以创建安全组，并添加可反映与安全组关联的实例角色的规则。例如，配置作为 Web 服务器的实例需要允许入站 HTTP 和 HTTPS 访问的安全组规则。同样，数据库实例需要允许数据库类型访问的规则，例如，对 MySQL 允许通过端口 3306 进行访问。

以下是您可以添加到允许特定类型访问的安全组的规则类型示例。

示例

- Web 服务器规则 (p. 1316)
- 数据库服务器规则 (p. 1316)
- 用于从您的计算机连接到实例的规则 (p. 1317)
- 用于在具有相同安全组的实例之间进行连接的规则 (p. 1317)
- 用于 ping/ICMP 的规则 (p. 1317)
- DNS 服务器规则 (p. 1318)

- Amazon EFS 规则 (p. 1318)
- Elastic Load Balancing 规则 (p. 1319)
- VPC 对等规则 (p. 1319)

Web 服务器规则

以下入站规则允许来自任何 IP 地址的 HTTP 和 HTTPS 访问。如果您为 VPC 启用了 IPv6，则可添加规则以控制来自 IPv6 地址的入站 HTTP 和 HTTPS 流量。

协议类型	协议编号	端口	源 IP	备注
TCP	6	80 (HTTP)	0.0.0.0/0	允许来自任何 IPv4 地址的入站 HTTP 访问。
TCP	6	443 (HTTPS)	0.0.0.0/0	允许来自任何 IPv4 地址的入站 HTTPS 访问
TCP	6	80 (HTTP)	::/0	允许来自任何 IPv6 地址的入站 HTTP 访问
TCP	6	443 (HTTPS)	::/0	允许来自任何 IPv6 地址的入站 HTTPS 访问

数据库服务器规则

以下入站规则是您可以为数据库访问添加的规则示例，具体取决于您在实例运行的数据库类型。有关 Amazon RDS 实例的更多信息，请参阅 Amazon RDS 用户指南。

对于源 IP，请指定以下其中一项：

- 本地网络中的特定 IP 地址或 IP 地址范围（采用 CIDR 块表示法）
- 访问数据库的一组实例的安全组 ID

协议类型	协议编号	端口	备注
TCP	6	1433 (MS SQL)	访问 Microsoft SQL Server 数据库的默认端口，例如，在 Amazon RDS 实例上
TCP	6	3306 (MYSQL/Aurora)	访问 MySQL 或 Aurora 数据库的默认端口，例如，在 Amazon RDS 实例上
TCP	6	5439 (Redshift)	访问 Amazon Redshift 集群数据库的默认端口。
TCP	6	5432 (PostgreSQL)	访问 PostgreSQL 数据库的默认端口，例如，在 Amazon RDS 实例上
TCP	6	1521 (Oracle)	访问 Oracle 数据库的默认端口，例如，在 Amazon RDS 实例上

您可以选择限制来自数据库服务器的出站流量。例如，您可能希望允许访问 Internet 进行软件更新，但限制所有其他类型的流量。您必须先删除允许所有出站流量的默认出站规则。

协议类型	协议编号	端口	目的地 IP	备注
TCP	6	80 (HTTP)	0.0.0.0/0	允许对任何 IPv4 地址进行出站 HTTP 访问
TCP	6	443 (HTTPS)	0.0.0.0/0	允许对任何 IPv4 地址进行出站 HTTPS 访问
TCP	6	80 (HTTP)	::/0	(仅限已启用 IPv6 的 VPC) 允许对任何 IPv6 地址进行出站 HTTP 访问
TCP	6	443 (HTTPS)	::/0	(仅限已启用 IPv6 的 VPC) 允许对任何 IPv6 地址进行出站 HTTPS 访问

用于从您的计算机连接到实例的规则

要连接到您的实例，您的安全组必须拥有允许 SSH 访问 (适用于 Linux 实例) 或 RDP 访问 (适用于 Windows 实例) 的入站规则。

协议类型	协议编号	端口	源 IP
TCP	6	22 (SSH)	您电脑的公有 IPv4 地址或您的本地网络中的 IP 地址范围。如果您为 VPC 启用了 IPv6，并且您的实例有一个 IPv6 地址，则可以输入一个 IPv6 地址或范围。
TCP	6	3389 (RDP)	您电脑的公有 IPv4 地址或您的本地网络中的 IP 地址范围。如果您为 VPC 启用了 IPv6，并且您的实例有一个 IPv6 地址，则可以输入一个 IPv6 地址或范围。

用于在具有相同安全组的实例之间进行连接的规则

要允许与同一安全组关联的实例之间相互通信，您必须明确添加实现此目的的规则。

> **Note**
>
> 如果您将路由配置为通过中间设备在不同子网中的两个实例之间转发流量，则必须确保这两个实例的安全组允许流量在实例之间流动。每个实例的安全组必须引用另一个实例的私有 IP 地址或包含另一个实例的子网的 CIDR 范围作为源。如果您引用另一个实例的安全组作为源，则安全组不允许流量在实例之间流动。

下表描述了允许关联的实例相互通信的安全组的入站规则。该规则允许所有类型的流量。

协议类型	协议编号	端口	源 IP
-1 (All)	-1 (All)	-1 (All)	安全组的 ID 或包含另一个实例的子网的 CIDR 范围（请参阅注释）。

用于 ping/ICMP 的规则

ping 命令是一种 ICMP 流量。要对实例执行 ping 操作，您必须添加以下入站 ICMP 规则。

协议类型	协议编号	ICMP 类型	ICMP 代码	源 IP
ICMP	1	8 (Echo 请求)	不适用	您的计算机的公有 IPv4 地址或您的本地网络中的 IPv4 地址范围

要使用 ping6 命令对您的实例的 IPv6 地址执行 ping 操作，您必须添加以下入站 ICMPv6 规则。

协议类型	协议编号	ICMP 类型	ICMP 代码	源 IP
ICMPv6	58	128 (Echo 请求)	0	您的计算机的 IPv6 地址或您的本地网络中的 IPv6 地址范围

DNS 服务器规则

如果您已将 EC2 实例设置为 DNS 服务器，则必须确保 TCP 和 UDP 流量可通过端口 53 访问您的 DNS 服务器。

对于源 IP，请指定以下其中一项：

- 网络中的 IP 地址或 IP 地址范围（采用 CIDR 块表示法）
- 您网络中需要访问 DNS 服务器的实例组的安全组 ID。

协议类型	协议编号	端口
TCP	6	53
UDP	17	53

Amazon EFS 规则

如果您将 Amazon EFS 文件系统与 Amazon EC2 实例结合使用，与 Amazon EFS 挂载目标关联的安全组必须允许使用 NFS 协议传输的流量。

协议类型	协议编号	端口	源 IP	备注
TCP	6	2049 (NFS)	安全组 ID	允许从与该安全组关联的资源 (包括挂载目标) 进行入站 NFS 访问。

要在 Amazon EC2 实例上挂载 Amazon EFS 文件系统，您必须连接到您的实例。因此，与您的实例关联的安全组必须拥有允许来自本地计算机或本地网络的入站 SSH 的规则。

协议类型	协议编号	端口	源 IP	备注
TCP	6	22 (SSH)	本地计算机的 IP 地址范围或网络的 IP 地址范围（采用 CIDR 块表示法）。	允许从您的本地计算机进行入站 SSH 访问。

Elastic Load Balancing 规则

如果您正在使用负载均衡器，则与您的负载均衡器关联的安全组必须具有允许与您的实例或目标进行通信的规则。有关更多信息，请参阅《经典负载均衡器用户指南》中的 为经典负载均衡器配置安全组以及《应用程序负载均衡器用户指南》中的 应用程序负载均衡器的安全组。

VPC 对等规则

您可以更新 VPC 安全组的入站或出站规则以引用对等的 VPC 中的安全组。此操作将允许流量流入和流出与对等的 VPC 中的已引用安全组关联的实例。有关如何为 VPC 对等配置安全组的更多信息，请参阅更新安全组以引用对等 VPC 组。

使用接口 VPC 终端节点访问 Amazon EC2

您可以通过在 VPC 和 Amazon EC2 之间创建私有连接，以改善 VPC 的安保状况。您可以像在 VPC 中一样访问 Amazon EC2，而无需使用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。VPC 中的实例不需要公有 IP 地址即可访问 Amazon EC2。

有关更多信息，请参阅 Amazon PrivateLink 指南中的通过 Amazon PrivateLink 访问 Amazon Web Services。

目录

- 创建接口 VPC 终端节点 (p. 1319)
- 创建端点策略 (p. 1319)

创建接口 VPC 终端节点

使用以下服务名称为 Amazon EC2 创建接口终端节点：

- com.amazonaws.*region*.ec2 - 为 Amazon EC2 API 操作创建终端节点。

有关更多信息，请参阅 Amazon PrivateLink 指南中的使用接口 VPC 终端节点访问 Amazon Web Service。

创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口终端节点。默认端点策略允许通过接口终端节点访问 Amazon EC2 API 的完全权限。要控制允许从 VPC 访问 Amazon EC2 API 的权限，请将自定义端点策略附加到接口终端节点。

端点策略指定以下信息：

- 可以执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

> **Important**
>
> 当将非默认策略应用于 Amazon EC2 的接口 VPC 终端节点时，某些失败的 API 请求（例如 `RequestLimitExceeded` 中失败的请求）可能不会记录到 Amazon CloudTrail 或 Amazon CloudWatch。

有关更多信息，请参阅 Amazon PrivateLink 指南中的使用端点策略控制对服务的访问权限。

以下示例显示一个 VPC 终端节点策略，该策略拒绝创建未加密的卷或启动具有未加密卷的实例的权限。示例策略还授予执行所有其他 Amazon EC2 操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
}
```

Amazon EC2 中的更新管理

我们建议您定期修补、更新和保护 EC2 实例上的操作系统和应用程序。您可以使用 Amazon Systems Manager Patch Manager 自动执行为操作系统和应用程序安装安全相关更新的过程。

对于自动扩缩组中的 EC2 实例，您可以使用 AWS-PatchAsgInstance 运行手册以避免正在修补的实例被替换。或者，您也可以使用任何自动更新服务或建议的过程安装应用程序供应商提供的更新。

有关运行 Windows Server 的最新 Amazon EC2 AMI 的列表，请参阅有关 Amazon Windows AMI 版本的详细信息。

Amazon EC2 的合规性验证

要了解某个 Amazon Web Service 是否在特定合规性计划范围内，请参阅 合规性计划范围内的 Amazon Web Services，然后选择您感兴趣的合规性计划。有关常规信息，请参阅Amazon Web Services合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

您使用 Amazon Web Services 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。Amazon 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 Amazon 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub – 此 Amazon Web Service 向您提供 Amazon 中安全状态的全面视图。Security Hub 通过安全控件评估您的 Amazon 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。

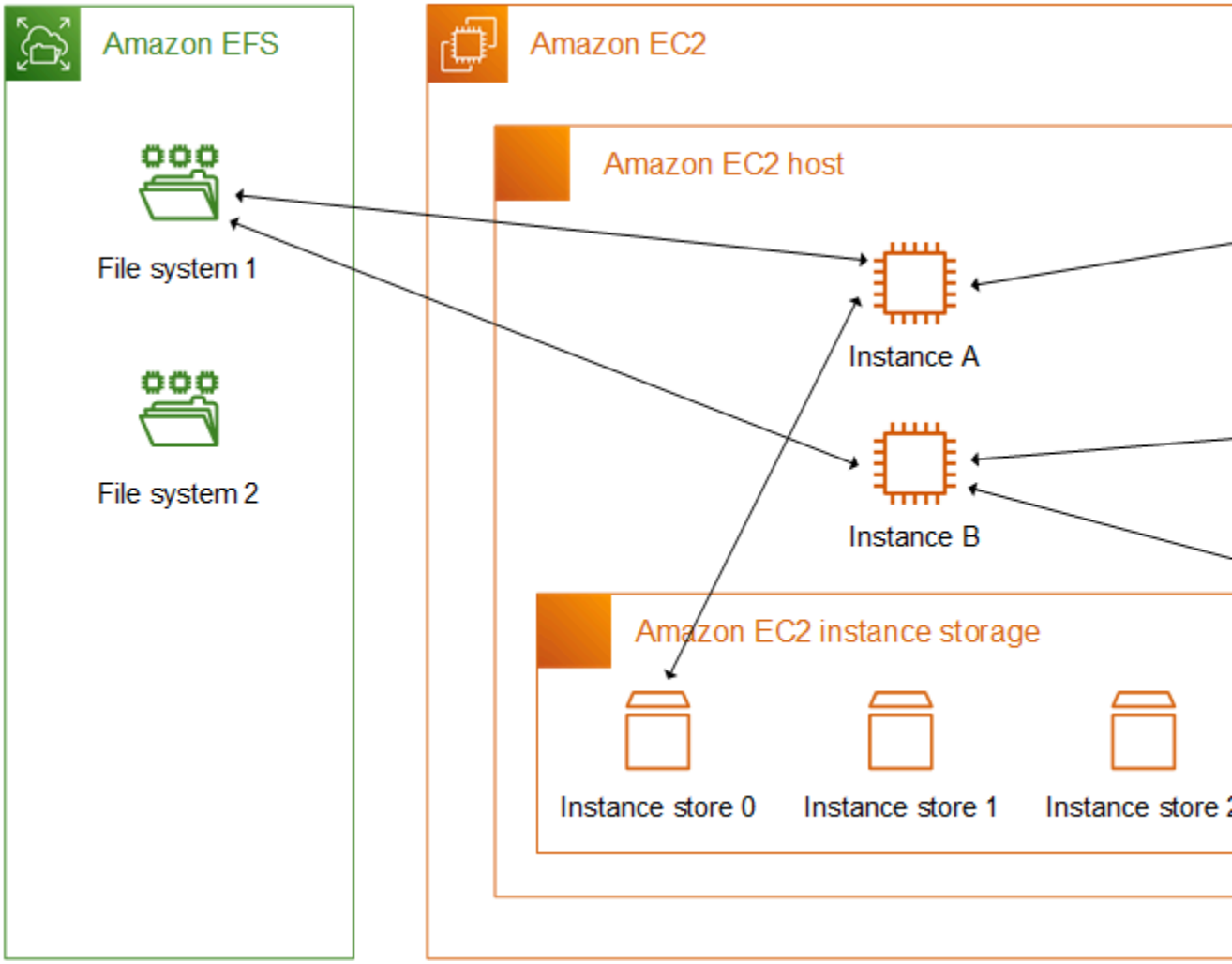
存储

Amazon EC2 为您的实例提供了灵活、经济且易于使用的数据存储选项。各选项都具有独特的性能和耐久性。这些存储选项既可以单独使用，也可以组合使用，以便满足您的需求。

阅读本部分后，您应该会对如何使用 Amazon EC2 支持的数据存储选项来满足特定要求有很好的了解。这些存储选项包含以下产品：

- Amazon Elastic Block Store (p. 1323)
- Amazon EC2 实例存储 (p. 1579)
- 将 Amazon EFS 与 Amazon EC2 结合使用 (p. 1602)
- 将 Amazon S3 与 Amazon EC2 结合使用 (p. 1600)

下图显示了这些存储选项和您的实例之间的关系。



Amazon EBS

Amazon EBS 提供块级别的持久存储卷，您可将这些卷附加到正在运行的实例。可以使用 Amazon EBS 作为主要存储设备，以获取需要频繁更新和精细更新的数据。例如，如果在实例上运行数据库，则建议选用 Amazon EBS 作为存储设备。

EBS 卷就像原始未经格式化的外部数据块储存设备，可附加到单个实例。卷始终不受实例运行时间的影响。将 EBS 卷附加到实例后，您可以像使用其他物理硬盘一样使用它。如上图所示，可以将多个卷附加到一个实例。您也可以将 EBS 卷从实例中分离，并将其附加到另一个实例。您可以动态更改附加到实例的卷的配置。还可以使用 Amazon EBS 加密功能以加密卷的形式创建 EBS 卷。有关更多信息，请参阅 Amazon EBS 加密 (p. 1504)。

为保留您的数据的备份副本，您可以创建 EBS 卷的快照，该快照存储在 Amazon S3 中。您可以从快照创建 EBS 卷，并将其附加到另一个实例。有关更多信息，请参阅 Amazon Elastic Block Store (p. 1323)。

Amazon EC2 实例存储

很多实例可以访问物理附加到主机的磁盘中的存储。此磁盘存储称为实例存储。实例存储可为实例提供临时性块级存储。实例存储卷上的数据仅在关联实例的生命周期内保留；如果您停止、休眠或终止实例，则实例存储卷上的所有数据都会丢失。有关更多信息，请参阅 Amazon EC2 实例存储 (p. 1579)。

Amazon EFS 文件系统

Amazon EFS 提供可扩展文件存储以供和 Amazon EC2 一起使用。您可以创建 EFS 文件系统并配置实例来装载文件系统。您可以使用 EFS 文件系统作为在多个实例上运行的工作负载和应用程序的通用数据源。有关更多信息，请参阅 将 Amazon EFS 与 Amazon EC2 结合使用 (p. 1602)。

Amazon S3

Amazon S3 为您提供了可靠的廉价数据存储基础设施。它的设计理念是通过支持您随时从 Amazon EC2 内部或从网络上的任何地方存储和检索任何数量的数据，从而简化整个网络计算。例如，您可以使用 Amazon S3 存储数据和应用程序的备份副本。Amazon EC2 使用 Amazon S3 存储 EBS 快照以及由实例存储支持的 AMI。有关更多信息，请参阅 将 Amazon S3 与 Amazon EC2 结合使用 (p. 1600)。

添加存储

您每次从 AMI 启动实例时，系统都会为该实例创建一个根存储设备。根存储设备中包含启动实例所需的全部信息。当您创建 AMI 或使用块储存设备映射启动实例时，除了根设备外，您还可以指定存储卷。有关更多信息，请参阅 块设备映射 (p. 1615)。

您还可以将 EBS 卷附加到运行中的实例。有关更多信息，请参阅 将 Amazon EBS 卷挂载到实例 (p. 1347)。

存储定价

有关存储定价的信息，请打开 Amazon 定价，向下滚动至 Services Pricing（服务定价），选择 Storage（存储），然后选择存储选项以打开该存储选项的定价页面。有关估算存储成本的信息，请参阅 Amazon 定价计算器。

Amazon Elastic Block Store (Amazon EBS)

Amazon Elastic Block Store (Amazon EBS) 提供了块级存储卷以用于 EC2 实例。EBS 卷的行为类似于原始、未格式化的块储存设备。您可以将这些卷作为设备挂载在实例上。附加到 EBS 实例的卷公开为独立于实例生命周期而持续存在的存储卷。您可以在这些卷上创建文件系统，或者以使用块储存设备（如硬盘）的任何方式使用这些卷。您可以动态更改附加到实例的卷的配置。

建议为必须能够快速访问且需要长期保存的数据使用 Amazon EBS。EBS 卷特别适用于文件系统和数据库的主存储，还适用于任何需要细粒度更新及访问原始的、未格式化的块级存储的应用程序。Amazon EBS 非常适合依赖随机读写操作的数据库式应用程序以及执行长期持续读写操作的吞吐量密集型应用程序。

使用 Amazon EBS，您可以按实际用量付费。有关 Amazon EBS 定价的更多信息，请参阅 Amazon Elastic Block Store 页面的“预计费用”部分。

目录

- Amazon EBS 的功能 (p. 1324)
- Amazon EBS 卷 (p. 1324)
- Amazon EBS 快照 (p. 1368)
- Amazon Data Lifecycle Manager (p. 1448)
- Amazon EBS 数据服务 (p. 1493)
- Linux 实例上的 Amazon EBS 和 NVMe (p. 1518)
- Amazon EBS 优化的实例 (p. 1522)
- Linux 实例上的 Amazon EBS 卷性能 (p. 1550)
- Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)
- 适用于 Amazon EBS 的 EventBridge (p. 1569)

Amazon EBS 的功能

- 您可以在特定可用区中创建 EBS 卷，然后将其附加到同一可用区中的实例。若要在可用区外部提供某个卷，您可以创建一个快照并将该快照还原到该区域中任意位置处的新卷。您可以将快照复制到其他区域，再将它们还原到该区域中的新卷，从而更轻松地利用多个 Amazon 区域来实现地理扩展、数据中心迁移和灾难恢复。
- Amazon EBS 提供以下卷类型：通用型 SSD、预置 IOPS SSD、吞吐量优化型 HDD 和 Cold HDD。有关更多信息，请参阅 EBS 卷类型 (p. 1327)。

  以下是每种卷类型的性能和使用案例摘要。

  - 通用型 SDD 卷（gp2 和 gp3）在各种事务性工作负载的价格和性能之间实现平衡。这些卷非常适合启动卷、中型单实例数据库以及开发和测试环境等使用案例。
  - 预置 IOPS SSD 卷（io1 和 io2）旨在满足 I/O 密集型工作负载的需要，这些工作负载对存储性能和一致性非常敏感。它们提供您在创建卷时指定的一致 IOPS 速率。因此，您可预见性地将每个实例扩展到数万 IOPS。此外，io2 卷可提供最高级别的卷耐用性。
  - 吞吐量优化型 HDD 卷 (st1) 提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。这些卷非常适合大型顺序工作负载，例如，Amazon EMR、ETL、数据仓库和日志处理。
  - Cold HDD 卷 (sc1) 提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。这些卷非常适合大型顺序冷数据工作负载。如果您不需要经常访问数据并希望节约成本，这些卷提供价格低廉的块存储。
- 您可以创建 EBS 卷以作为加密卷，以便满足监管/审核的数据和应用程序的各种静态数据加密要求。创建加密 EBS 卷并将它附加到支持的实例类型时，该卷上静态存储的数据、磁盘 I/O 和通过该卷创建的快照都会进行加密。加密在托管 EC2 实例的服务器上进行，对从 EC2 实例传输到 EBS 存储的数据进行加密。有关更多信息，请参阅 Amazon EBS 加密 (p. 1504)。
- 您可以创建持久保存到 Amazon S3 的 EBS 卷的时间点快照。快照可为数据提供保护以获得长期持久性，可用作新 EBS 卷的起点。同一快照可根据需要创建任意数量的卷。可以跨多个 Amazon 区域复制这些快照。有关更多信息，请参阅 Amazon EBS 快照 (p. 1368)。
- 带宽、吞吐量、延迟和平均队列长度等性能指标是通过 Amazon Web Services Management Console提供的。通过 Amazon CloudWatch 提供的这些指标，您可以监视卷的性能，确保为应用程序提供足够性能，又不会为不需要的资源付费。有关更多信息，请参阅 Linux 实例上的 Amazon EBS 卷性能 (p. 1550)。

Amazon EBS 卷

Amazon EBS 卷是一种耐用的数据块级存储设备，您可以将其附加到您的实例。将卷附加到实例后，您可以像使用其他物理硬盘一样使用它。EBS 卷非常灵活。对于附加到当前一代实例类型的当前一代卷，您可以动态增加大小、修改预配置 IOPS 容量以及更改实际生产卷上的卷类型。

可以将 EBS 卷用作需要频繁更新的数据的主存储 (如实例的系统驱动器或数据库应用程序的存储)。还可以将其用于执行连续磁盘扫描的吞吐量密集型应用程序。EBS 卷始终不受 EC2 实例运行时间的影响。

您可以将多个 EBS 卷附加到单个实例。该卷与实例必须位于同一可用区。。

Amazon EBS 提供以下卷类型：通用型 SSD（gp2 和 gp3）、预置 IOPS SSD（io1 和 io2）、吞吐量优化型 HDD (st1)、Cold HDD (sc1) 以及磁介质卷 (standard)。它们的性能特点和价格不同，您可根据应用程序要求定制您所需的存储性能和相应费用。有关更多信息，请参阅 Amazon EBS 卷类型 (p. 1327)。

您的账户对您可以使用的 EBS 卷数量和总存储量有相应的限制。有关这些限制以及如何请求提高限制的更多信息，请参阅 Amazon EC2 Service Quotas (p. 1678)。

有关定价的更多信息，请参阅 Amazon EBS 定价。

目录

- 使用 EBS 卷的优势 (p. 1325)
- Amazon EBS 卷类型 (p. 1327)
- 针对 EBS 卷的大小和配置的限制 (p. 1342)
- 创建 Amazon EBS 卷 (p. 1344)
- 将 Amazon EBS 卷挂载到实例 (p. 1347)
- 使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)
- 查看关于 Amazon EBS 卷的信息 (p. 1351)
- 使用以前的快照替换卷 (p. 1353)
- 替换根卷 (p. 1354)
- 监控您的卷状态 (p. 1359)
- 从 Linux 实例分离 Amazon EBS 卷 (p. 1364)
- 删除 Amazon EBS 卷 (p. 1366)
- 在 Amazon EBS 上进行故障测试 (p. 1367)

使用 EBS 卷的优势

EBS 卷具有实例存储卷不具备的优势。

主题

- 数据可用性 (p. 1325)
- 数据持久性 (p. 1326)
- 数据加密 (p. 1326)
- 数据安全性 (p. 1326)
- 快照 (p. 1326)
- 弹性 (p. 1327)

数据可用性

当您创建 EBS 卷时，系统会在其可用区内自动复制该卷，以防止因任何一个硬件组件出现故障而导致数据丢失。您可以将 EBS 卷附加到同一可用区中的任何 EC2 实例。附加后，该卷显示为类似于硬盘或其他物理设备的本机块储存设备。这时，实例就像与本地驱动器交互一样与该卷交互。您可以连接到实例并使用文件系统（例如 ext3）格式化 EBS 卷，然后安装应用程序。

如果您将多个卷附加到您指定的一个设备，则可以在卷内将数据条带化，以增强 I/O 性能和吞吐量。

您可以获取针对 EBS 卷 (包括 EBS 支持的实例的根设备卷) 的监控数据，而无需额外付费。有关监控指标的更多信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)。有关跟踪卷状态的信息，请参阅适用于 Amazon EBS 的 EventBridge (p. 1569)。

数据持久性

EBS 卷是一种实例外存储，其数据的保存期限不受实例使用寿命的影响。只要数据存在，您就要继续支付卷的使用费用。

如果您在 EC2 控制台中为您的实例配置 EBS 卷时取消选中了终止时删除复选框，则在运行的实例终止时，附加到该实例的 EBS 卷会自动从该实例分离，并保持数据完整。然后，可将卷重新附加到新的实例，从而快速恢复数据。如果选中终止时删除复选框，则在 EC2 实例终止时删除卷。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其附加的卷中保存储的数据。在从停止到启动的整个周期中，该卷均为已附加状态。这使您能够无限期地在卷上处理和存储数据，并只在需要时使用处理和存储资源。数据将一直保存在该卷上，直至将其显式删除。对于已删除的 EBS 卷使用的物理块存储，将首先用零覆盖，然后分配给新卷。如果要处理敏感数据，应考虑手动加密数据或将数据存储在由 Amazon EBS 加密 保护的卷上。有关更多信息，请参阅 Amazon EBS 加密 (p. 1504)。

默认情况下，当一个实例终止时，将删除在启动时创建并附加到该实例的根 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `false`。修改值后，即使实例终止，也可将该卷保留下来并附加到其他实例。

默认情况下，当一个实例终止时，不会删除在启动时创建并附加到该实例的额外 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `true`。此修改的值会导致在实例终止时删除卷。

数据加密

为简化数据加密，您可以使用 Amazon EBS 加密功能创建加密 EBS 卷。所有 EBS 卷类型都支持加密。您可以使用加密 EBS 卷，为监管/审核的数据和应用程序实现各种静态数据加密要求。Amazon EBS 加密使用 256 位高级加密标准算法 (AES-256) 和 Amazon 托管密钥基础设施。加密在托管 EC2 实例的服务器上进行，从而为从 EC2 实例传输到 Amazon EBS 存储的数据提供加密。有关更多信息，请参阅 Amazon EBS 加密 (p. 1504)。

Amazon EBS 加密在创建加密卷以及通过加密卷创建任何快照时，使用 Amazon Key Management Service (Amazon KMS) 主密钥。首次在区域中创建加密的 EBS 卷时，将自动为您创建一个默认主密钥。此密钥用于 Amazon EBS 加密，除非您选择采用 Amazon KMS 单独创建的客户主密钥 (CMK)。创建您自己的 CMK 可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥的能力。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南。

数据安全性

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说明的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

快照

Amazon EBS 提供为任何 EBS 卷创建快照（备份）并将卷中数据的副本写入 Amazon S3（其中数据以冗余方式存储在多个可用区中）的功能。不必将该卷附加到运行中的实例，也可以制作快照。因为您不断向卷写入数据，则可定期创建该卷的快照，以用作创建新卷的基准。也可利用这些快照创建多个新的 EBS 卷或在可用区间移动卷的位置。加密 EBS 卷的快照会自动加密。

从快照创建新卷时，新卷是制作快照时的原始卷的精确副本。通过加密快照创建的 EBS 卷会自动加密。通过指定不同的可用区 (可选)，您可以使用此功能在该区域中创建重复的卷。可与特定的 Amazon 账户共享这些快照或使其公开可用。当您创建快照时，您需根据卷的总大小支付 Amazon S3 费用。对于连续的卷快照，您只需支付任何超过卷原始大小的附加数据的费用。

快照是增量备份，这意味着仅保存卷上在最新快照之后更改的数据块。如果您的卷中有 100 GiB 的数据，但自上次快照以来只更改了 5 GiB 的数据，则只有这 5 GiB 经过修改的数据会写入 Amazon S3。尽管快照是以增量方式保存的，但快照删除过程仅要求保留最新的快照。

为了便于对卷和快照进行分类和管理，您可以使用选择的元数据对它们加以标记。有关更多信息，请参阅 标记 Amazon EC2 资源 (p. 1664)。

要自动备份卷，您可以使用 Amazon Data Lifecycle Manager (p. 1448) 或 Amazon Backup。

弹性

EBS 卷支持生产期间的实时配置更改。您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。有关更多信息，请参阅 Amazon EBS 弹性卷 (p. 1493)。

Amazon EBS 卷类型

Amazon EBS 提供以下卷类型，各种类型性能特点和价格不同，因此您可根据应用程序要求定制您所需的存储性能和相应成本。

> **Important**
>
> 有多种因素会影响 EBS 卷的性能，如实例配置、I/O 特性和工作负载需求。为了充分利用 EBS 卷上预置的 IOPS，请使用 EBS 优化实例 (p. 1522)。有关充分利用 EBS 卷的更多信息，请参阅 Linux 实例上的 Amazon EBS 卷性能 (p. 1550)。

有关定价的更多信息，请参阅 Amazon EBS 定价。

卷类型

- 固态硬盘（SSD）卷 (p. 1327)
- 硬盘驱动器（HDD）卷 (p. 1328)
- 上一代卷 (p. 1329)

固态硬盘（SSD）卷

支持 SSD 的卷针对涉及小型 I/O 的频繁读/写操作的事务性工作负载进行了优化，其中管理性能属性为 IOPS。由 SSD 支持的卷类型包括通用型 SSD 和预调配 IOPS SSD。下面是 SSD 支持的卷的使用案例和特征摘要。

	通用型 SSD 卷 (p. 1329)		预置 IOPS SSD 卷 (p. 1332)		
卷类型	gp3	gp2	io2 Block Express ‡	io2	io1
持久性	99.8% - 99.9% 耐用性 （0.1% - 0.2% 的年故障率）		99.999% 的耐用性 （0.001% 的年故障率）		99.8% - 99.9% 耐用性（0.1% - 0.2% 的年故障率）
使用案例	• 事务性工作负载 • 虚拟桌面 • 中型单实例数据库 • 低延迟交互式应用程序 • 引导卷 • 开发和测试环境		需要以下工作负载： • 亚毫秒级延迟 • 持续 IOPS 绩效 • 超过 64,000 IOPS 或 1,000 MiB/s 吞吐量	• 需要持续 IOPS 性能或超过 16,000 IOPS 性能的工作负载 • I/O 密集型数据库工作负载	

	通用型 SSD 卷 (p. 1329)		预置 IOPS SSD 卷 (p. 1332)	
卷大小	1 GiB - 16 TiB		4 GiB - 64 TiB	4 GiB - 16 TiB
每个卷的最大 IOPS (16 KiB I/O)	16,000		256,000	64,000 †
每个卷的最大吞吐量	1,000 MiB/s	250 MiB/s *	4,000 MiB/s	1,000 MiB/s †
Amazon EBS 多重挂载	不支持		支持	
引导卷	支持			

* 吞吐量限制介于 128 MiB/s 和 250 MiB/s 之间，具体取决于卷大小。有关更多信息，请参阅gp2 卷性能 (p. 1331)。除非您修改卷 (p. 1493)，否则在 2018 年 12 月 3 日之前创建并且自创建以来未经修改的卷可能无法实现完全性能。

† 要实现 1000MiB/s 的最大吞吐量，必须为卷配置 64000 IOPS，并且必须将卷连接到基于 Nitro 系统构建的实例 (p. 246)。除非您修改卷 (p. 1493)，否则在 2017 年 12 月 6 日之前创建并且自创建以来未经修改的 `io1` 卷可能无法实现完全性能。

‡ `io2` Block Express 卷仅支持
C6a、C6in、C7g、M6a、M6in、M6idn、M7g、R5b、R6in、R6idn、R7g、Trn1、X2idn 和 X2iedn 实例。在启动过程中或启动之后，附加到这些实例的 `io2` 卷会在 Block Express 上自动运行。有关更多信息，请参阅io2 Block Express 卷 (p. 1334)。

有关 SSD 支持的卷类型的更多信息，请参阅以下文件：

- 通用型 SSD 卷 (p. 1329)
- 预置 IOPS SSD 卷 (p. 1332)

硬盘驱动器（HDD）卷

HDD 支持的卷针对大型流式处理工作负载进行了优化，其中主要的性能属性是吞吐量。HDD 容量类型包括吞吐量优化型 HDD 和冷 HDD。下面是 HDD 支持的卷的使用案例和特征摘要。

	吞吐量优化型 HDD 卷 (p. 1336)	Cold HDD 卷 (p. 1338)
卷类型	`st1`	`sc1`
持久性	99.8% - 99.9% 耐用性（0.1% - 0.2% 的年故障率）	
使用案例	• 大数据 • 数据仓库 • 日志处理	• 适用于访问频率较低的数据的高吞吐量存储 • 最低存储成本至关重要的情形
卷大小	125 GiB - 16 TiB	
每个卷的最大 IOPS (1 MiB I/O)	500	250

	吞吐量优化型 HDD 卷 (p. 1336)	Cold HDD 卷 (p. 1338)
每个卷的最大吞吐量	500 MiB/s	250 MiB/s
Amazon EBS 多重挂载	不支持	
引导卷	不支持	

有关硬盘驱动器（HDD）卷的更多信息，请参阅 吞吐量优化型 HDD 和 Cold HDD 卷 (p. 1335)。

上一代卷

磁性 (standard) 卷是上一代卷，由磁性驱动器支持。它们适用于具有较小数据集的工作负载，在这些工作负载中，数据访问不频繁，性能不是最重要的。这些卷平均提供大约 100 IOPS，突增能力最大可达数百 IOPS，大小范围是 1 GiB 到 1 TiB。

> **Tip**
>
> 磁介质卷是上一代卷类型。如果您需要比上一代卷更高的性能或性能一致性，建议您考虑使用一种更新的卷类型。

下表列出了上一代 EBS 卷类型。

	磁介质
卷类型	standard
使用案例	数据不常访问的工作负载
卷大小	1 GiB - 1 TiB
每个卷的最大 IOPS	40–200
每个卷的最大吞吐量	40–90 MiB/s
引导卷	支持

有关更多信息，请参阅上一代卷。

通用型 SSD 卷

固态硬盘（SSD）支持通用型 SSD （gp2 和 gp3）卷。通用型 SSD 卷在各种事务性工作负载的价格和性能之间实现平衡。其中包括虚拟桌面、中型单实例数据库、延迟敏感型交互式应用程序、开发和测试环境以及启动卷。建议为大多数工作负载使用这种卷。

Amazon EBS 提供两种类型的通用型 SSD 卷：

- 通用型 SSD (gp3) 卷 – 最新一代通用型 SSD 卷
- 通用型 SSD (gp2) 卷

主题

- 通用型 SSD（gp3）卷 (p. 1330)
- 通用型 SSD (gp2) 卷 (p. 1330)

通用型 SSD（gp3）卷

通用型 SSD（gp3）卷是最新一代通用型 SSD 卷，也是 Amazon EBS 提供的成本最低的 SSD 卷。这种卷类型有助于为大多数应用程序提供合理得当的价格和性能。其还可以帮助您独立于卷大小扩展卷的性能。这意味着您可以预置所需性能，而无需预置额外的块存储容量。此外，gp3 卷每 GiB 价格比通用型 SSD（gp2）卷低了 20%。

gp3 卷提供不超过十毫秒的延迟以及 99.8% 到 99.9% 的卷耐用性，年故障率（AFR）不高于 0.2%，这意味着在一年期间内，每 1000 个运行的卷最多发生两个卷故障。Amazon 设计 gp3 卷在 99% 的时间内提供其预置性能。

主题

- gp3 卷性能 (p. 1330)
- gp3 卷大小 (p. 1330)
- 从 gp2 迁移到 gp3 (p. 1330)

gp3 卷性能

> Tip
>
> gp3 卷不使用突增性能。其可以无限期地维持其完全预调配 IOPS 和吞吐量性能。

IOPS 性能

gp3 卷提供 3000 IOPS 的一致基准 IOPS 性能，这包含在存储价格中。您可以按每 GiB 卷大小 500 IOPS 的比例预置额外的 IOPS（最大 16000 IOPS），但需支付额外费用。可为 32 GiB 或更大的卷预置最大 IOPS（每 GiB 500 IOPS × 32 GiB = 16000 IOPS）。

吞吐量性能

gp3 卷提供 125 MiB/s 的一致基准吞吐量性能，这包含在存储价格中。您可以按每个预调配 IOPS 0.25 MiB/s 的比例预置额外的吞吐量（最高 1000 MiB/s），但需支付额外费用。最大吞吐量可预置为 4000 IOPS 或更高以及 8 GiB 或更大（4000 IOPS × 每 IOPS 0.25 MiB/s = 1000 MiB/s）。

gp3 卷大小

gp3 卷的大小范围为 1 GiB 到 16 TiB。

从 gp2 迁移到 gp3

如果您当前正在使用 gp2 卷，则可以使用 Amazon EBS 弹性卷 (p. 1493) 操作将卷迁移到 gp3。您可以使用 Amazon EBS 弹性卷操作修改现有卷的卷类型、IOPS 和吞吐量，而不中断 Amazon EC2 实例。此外，创建新卷、启动新实例或创建 AMI 时，您可以在此时选择 gp3 作为卷类型，而不是使用默认的 gp2 卷类型。

若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 Amazon EBS gp2 至 gp3 迁移成本节省计算器。

通用型 SSD (gp2) 卷

通用型 SSD (gp2) 卷是 Amazon EC2 实例的默认 Amazon EBS 卷类型。这种卷类型可提供经济实惠的存储，是广泛事务性工作负载的理想选择。使用 gp2 卷，性能随卷大小而扩展。

> Tip
>
> gp3 卷是最新一代通用型 SSD 卷。其提供更加可预测的性能扩展，而且价格比 gp2 卷低 20%。有关更多信息，请参阅通用型 SSD（gp3）卷 (p. 1330)。
> 若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 Amazon EBS gp2 至 gp3 迁移成本节省计算器。

gp2 卷提供不超过十毫秒的延迟以及 99.8% 到 99.9% 的卷耐用性，年故障率 (AFR) 不高于 0.2%，也就是说，在一年内，每 1000 个运行的卷最多有两个故障卷。Amazon 设计 gp2 卷在 99% 的时间内交付其预置性能。

主题

- gp2 卷性能 (p. 1331)
- gp2 卷大小 (p. 1332)

gp2 卷性能

IOPS 性能

基准 IOPS 性能以每 GiB 卷大小 3 IOPS 的速度，在最小 100 IOPS 和最大 16000 IOPS 之间进行线性扩缩。IOPS 性能预置如下：

- 33.33 GiB 及更小的卷预置至少 100 IOPS。
- 大于 33.33 GiB 的卷预置每 GiB 卷大小 3 IOPS，最高可达 16000 IOPS，达到 5334 GiB (3 X 5334)。
- 5334 GiB 及更大的卷预置 16000 IOPS。

小于 1 TiB 的 gp2 卷（且预置的 IOPS 低于 3000）可在需要较长时间时突增至 3000 IOPS。卷的突增能力受 I/O 积分的控制。I/O 需求大于基准性能时，卷花费 I/O 积分以突增至所需的性能级别（最多 3000 IOPS）。突增时，I/O 积分不会累积，而是按照高于基准 IOPS 的 IOPS 速率进行消费（费用率 = 突增 IOPS - 基准 IOPS）。卷累积的 I/O 积分越多，其维持突增性能的时间就越长。您可以按如下方式计算突增持续时间：

```
                      (I/O credit balance)
Burst duration  =  -----------------------------
                  (Burst IOPS) - (Baseline IOPS)
```

I/O 需求降至基准性能水平或更低时，卷开始以每 GiB 卷大小每秒 3 个 I/O 积分的速率获得 I/O 积分。每个卷都有 540 万 I/O 积分的 I/O 积分累积限制，这足以在至少 30 分钟内维持 3000 IOPS 的最大突增性能。

> **Note**
>
> 每个卷都有 540 万 I/O 积分的初始 I/O 积分余额，这为启动卷提供了快速初始启动循环，并为其他应用程序提供良好的引导过程。

下表列出了示例卷大小和卷的相关基准性能、突增持续时间（从 540 万 I/O 积分开始时）以及重填空 I/O 积分余额所需的时间。

卷大小 (GiB)	基准性能 (IOPS)	3000 IOPS 时的最大突增持续时间（秒）	重填空 I/O 积分余额所需的时间（秒）
1 至 33.33	100	1862	54000
100	300	2000	18000
334（最大吞吐量的最小大小）	1,002	2,703	5,389
750	2250	7200	2400
1000	3000	不适用*	不适用*
5334（最大 IOPS 的最小大小）及更大	16000	不适用*	不适用*

*卷的基准性能超过了最大突发性能。

您可以使用 Amazon CloudWatch 中的 Amazon EBS `BurstBalance` 指标监控卷的 I/O 积分余额。此指标显示 gp2 剩余的 I/O 积分百分比。有关更多信息，请参阅I/O 特性和监控 (p. 1552)。您可以设置警报，以便在 `BurstBalance` 值降到特定水平时获取通知。有关更多信息，请参阅 Creating CloudWatch Alarms（创建 CloudWatch 警报）。

吞吐量性能

gp2 提供介于 128 MiB/s 和 250 MiB/s 之间的吞吐量，具体取决于卷大小。吞吐量性能预置如下：

- 170 GiB 或更小的卷提供最大 128 MiB/s 的吞吐量。
- 大于 170 GiB 但小于 334 GiB 的卷可以突增至 250 MiB/s 的最大吞吐量。
- 334 GiB 及更大的卷提供 250 MiB/s 的吞吐量。

gp2 卷的吞吐量可以使用以下公式计算，吞吐量上限为 250 MiB/s：

```
Throughput in MiB/s = IOPS performance × I/O size in KiB
```

gp2 卷大小

gp2 卷的大小范围为 1 GiB 到 16 TiB。请记住，卷性能随卷大小呈线性扩缩。

预置 IOPS SSD 卷

固态硬盘（SSD）支持预调配 IOPS SSD 卷。这种卷是性能最高的 Amazon EBS 存储卷，专为需要低延迟的 IOPS 密集型和吞吐量密集型关键工作负载而设计。

Amazon EBS 提供三种类型的预调配 IOPS SSD 卷：

- 预调配 IOPS SSD (`io2`) 卷
- 预调配 IOPS SSD (`io2`) Block Express 卷
- 预调配 IOPS SSD (`io1`) 卷

主题

- 预调配 IOPS SSD（io1 和 io2）卷 (p. 1332)
- io2 Block Express 卷 (p. 1334)

预调配 IOPS SSD（io1 和 io2）卷

预置 IOPS SSD（`io1` 和 `io2`）卷旨在满足 I/O 密集型工作负载（尤其是数据库工作负载）的需要，这些工作负载对存储性能和一致性非常敏感。预置 IOPS SSD 卷使用一致的 IOPS 速率（在创建卷时指定），而 Amazon EBS 在 99.9% 的时间里可提供预置性能。

`io1` 卷旨在提供 99.8% 到 99.9% 的卷耐用性且年故障率 (AFR) 不高于 0.2%，这意味着在一年期间内，每 1000 个正在运行的卷最多发生两个卷故障。`io2` 卷旨在提供 99.999% 的卷耐用性且 AFR 不高于 0.001%，这意味着在一年期间内，每 10 万个正在运行的卷出现仅出现一个卷故障。

预置 IOPS SSD `io1` 和 `io2` 卷可用于所有 Amazon EC2 实例类型。附加到 C6a、C6in、C7g、M6a、M6in、M6idn、M7g、R5b、R6in、R6idn、R7g、Trn1、X2idn 和 X2iedn 实例的预调配 IOPS SSD `io2` 卷会在 EBS Block Express 上运行。有关更多信息，请参阅`io2` Block Express 卷 (p. 1334)。

io2 卷的注意事项

- io2 卷目前可用于以下区域：美国东部（俄亥俄州）、美国东部（弗吉尼亚州北部）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）、亚太地区（香港）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）、加拿大（中部）、欧洲地区（法兰克福）、欧洲地区（爱尔兰）、欧洲地区（伦敦）、欧洲地区（斯德哥尔摩）和中东（巴林）。
- 通过 **io2** 卷启动实例时请牢记以下事项：
  - 如果您启动了具有 io2 卷的实例，并且使用支持 Block Express 的实例类型，则该卷将自动在 Block Express 上运行，无论卷的大小和 IOPS 如何。
  - 如果 io2 卷的大小大于 16TiB 或 IOPS 大于 64,000，则无法启动不支持 Block Express (p. 1334) 的实例类型。
  - 您无法从支持 Block Express 的未加密 AMI 或共享加密 AMI 启动具有大小超过 16TiB 或 IOPS 超过 64,000 的加密 io2 卷的实例。在这种情况下，您必须首先在您的账户中创建加密 AMI，然后使用该 AMI 启动实例。
- 创建 **io2** 卷时请牢记以下事项：
  - 如果您在一个支持 Block Express (p. 1334) 的区域创建一个大于 16TiB 或 IOPS 大于 64,000 的 io2 卷，该卷将自动运行于 Block Express。
  - 您无法在一个不支持 Block Express (p. 1334) 的区域创建一个大于 16TiB 或 IOPS 大于 64,000 的 io2 卷，该卷将自动运行于 Block Express。
  - 如果您在一个支持 Block Express (p. 1334) 的区域创建一个 16TiB 或更小或 IOPS 为 64,000 或以下的 io2 卷，该卷不会运行于 Block Express。
  - 您无法从未加密的快照或共享的加密快照创建一个大于 16TiB 或 IOPS 大于 64,000 的加密io2卷。在这种情况下，您必须首先在您的账户中创建加密快照，然后使用该快照创建卷。
- 将 **io2** 卷挂载至实例时请牢记以下事项：
  - 如果您将 io2 卷挂载到支持 Block Express 的实例，则该卷会自动在 Block Express 上运行。优化 Block Express 卷可能需要长达 48 小时。在此期间，卷提供 io2 延迟。卷优化后，可提供 Block Express 支持的亚毫秒级延迟。
  - 如果 io2 卷的大小大于 16TiB 或 IOPS 大于 64,000，则无法挂载至不支持 Block Express (p. 1334) 的实例类型。
  - 如果从支持 Block Express 的实例分离大小为 16TiB 或以下、IOPS 为 64000 或以下的 io2 卷，并将该卷挂载到不支持 Block Express (p. 1334) 的实例类型，则该卷将不再在 Block Express 上运行并且将提供 io2 延迟。
- 修改 **io2** 卷时请牢记以下事项：
  - 如果 io2 卷挂载至不支持 Block Express (p. 1334) 的实例类型，则您无法对其进行修改或将其大小增加超过 16TiB 或 IOPS 超过 64000。

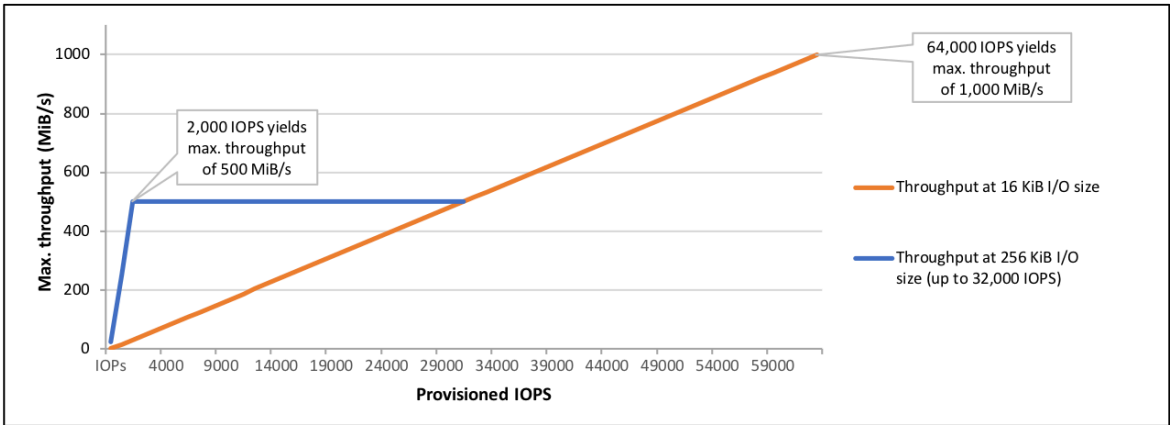
性能

预置 IOPS SSD 卷的大小范围为 4 GiB 到 16 TiB，您可以预置为每卷 100 IOPS 到最高 64,000 IOPS。您只能在 基于 Nitro 系统构建的实例 (p. 246) 上达到最高 64,000 IOPS。在其他实例系列中，您可以实现最高 32,000 IOPS 的性能。预置 IOPS 与请求的卷大小（单位 GiB）的最大比率：io1 卷为 50:1，io2 卷为 500:1。例如，一个 100 GiB io1 卷可以配置高达 5,000 IOPS，而一个 100 GiB io2 卷可以配置高达 50,000 IOPS。在受支持的实例类型上，以下卷大小允许预置高达 64,000 IOPS 最大值：

- io1 卷，大小为 1,280 GiB 或更高（50 × 1,280 GiB = 64,000 IOPS）
- io2 卷，大小为 128 GiB 或更高（500 × 128 GiB = 64,000 IOPS）

预置了最高 32000 IOPS 的 Provisioned IOPS SSD 卷支持 256 KiB 的最大 I/O 大小，可以达到最高 500 MiB/s 的吞吐量。当 I/O 大小达到最大时，吞吐量也将达到峰值 2000 IOPS。预置超过 32,000 IOPS（最高可达 64,000 IOPS）的卷以每预置 IOPS 16 KiB 的速率线性增加吞吐量。例如，预置了 48,000 IOPS 的卷可以支持高达 750 MiB/s 的吞吐量（每个预置 IOPS 16 KiB x 48,000 个预置 IOPS = 750 Mib/s）。要实现

1,000 MiB/s 的最大吞吐量，必须为卷预置 64,000 IOPS（每个预置 IOPS 16 KiB x 64,000 个预置 IOPS = 1,000 Mib/s）。下图说明了这些性能特性：



您的每 I/O 延迟体验取决于预置 IOPS 以及您的工作负载模式。要获得最佳 I/O 延迟体验，请确保您预配置 IOPS 以满足工作负载的 I/O 配置文件。

io2 Block Express 卷

Note

io2 Block Express 卷支持 C6a、C6in、C7g、M6a、M6in、M6idn、M7g、R5b、R6in、R6idn、R7g、Trn1、X2idn 和 X2iedn 实例。

io2 Block Express 卷是下一代 Amazon EBS 存储服务器架构。它旨在满足基于 Nitroon 的 Amazon EC2 实例上运行的最苛刻 I/O 密集型应用程序的性能要求。

Block Express 架构提高了性能和规模。Block Express 服务器使用可扩展的可靠数据报 (SRD) 网络协议与基于 Nitrol 的实例通信。此接口在专用于实例主机硬件上 Amazon EBS I/O 功能的 Nitro Card 中实现。它最大限度地减少 I/O 延迟和延迟变化（网络抖动），从而为应用程序提供更快、更一致的性能。有关更多信息，请参阅 io2 Block Express 卷。

io2 Block Express 卷适合可从达到亚毫秒级延迟的单个卷受益的工作负载，并支持比 io2 卷更高的 IOPS、更高的吞吐量和更大容量。

io2 Block Express 卷支持与 io2 卷一样的功能，包括多重挂载和加密。

主题

- 注意事项 (p. 1334)
- 性能 (p. 1335)
- 配额 (p. 1335)
- 定价和计费 (p. 1335)

注意事项

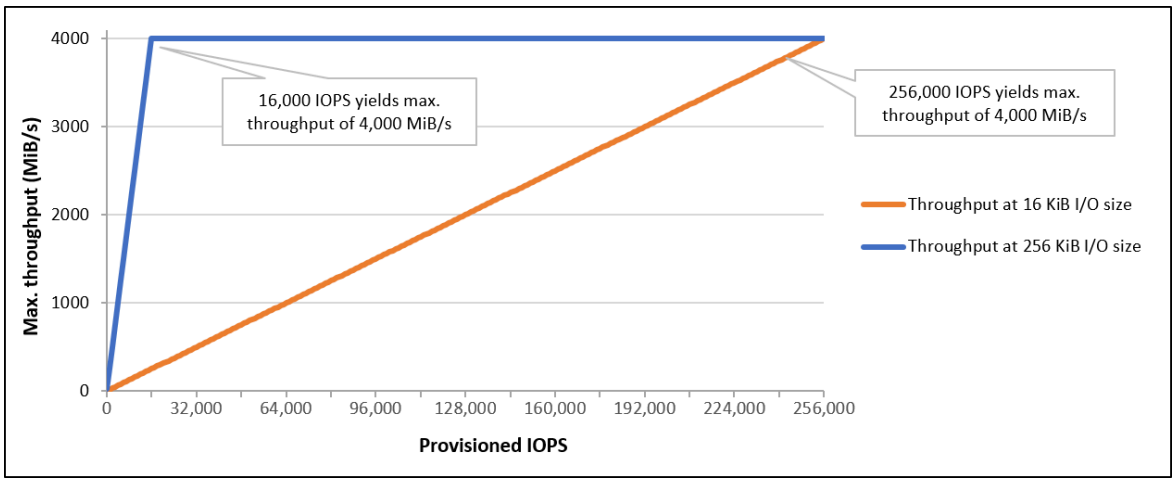
- io2 Block Express 卷目前支持 C6a、C6in、C7g、M6a、M6in、M6idn、M7g、R5b、R6in、R6idn、R7g、Trn1、X2idn 和 X2iedn 实例。
- io2 Block Express 卷目前可用于支持实例可用的所有区域，包括美国东部（俄亥俄州）、美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）、加拿大（中部）、欧洲（法兰克福）、欧洲（爱尔兰）、

欧洲（伦敦）和欧洲（斯德哥尔摩）。实例的可用性可能因可用区而异。有关更多信息，请参阅查找 Amazon EC2 实例类型。

性能

借助 io2 Block Express 卷，您可以通过以下方式预置卷：

- 亚毫秒级平均延迟
- 存储容量高达 64 TiB (65,536 GiB)
- 预置 IOPS 高达 256,000，IOPS:GiB 比率为 1,000:1。最大 IOPS 可通过大小为 256 GiB 或更大的卷 (1,000 IOPS x 256 GiB = 256,000 IOPS) 进行预置。
- 卷吞吐量高达 4,000 MiB/s。吞吐量按比例扩展至每个预置 IOPS 0.256 Mib/s。最大吞吐量可在 16,000 IOPS 或更高的情况下实现。



配额

io2 Block Express 卷遵守与 io2 卷相同的服务配额。有关更多信息，请参阅 Amazon EBS 配额。

定价和计费

io2 卷和 io2 Block Express 卷按同样的费率计费。有关更多信息，请参阅 Amazon EBS 定价。

使用情况报告不区分 io2 Block Express 卷和 io2 卷。我们建议您使用标签来帮助识别与 io2 Block Express 卷相关的成本。

吞吐量优化型 HDD 和 Cold HDD 卷

Amazon EBS 提供的 HDD 卷分为以下几个类别：

- 吞吐量优化型 HDD – 适用于访问频率较高的吞吐量密集型工作负载的低成本 HDD。
- Cold HDD – 适用于访问频率较低的工作负载的最低成本 HDD。

主题

- 每实例吞吐量限制 (p. 1336)
- 吞吐量优化型 HDD 卷 (p. 1336)
- Cold HDD 卷 (p. 1338)
- 使用 HDD 卷时的性能注意事项 (p. 1340)

- 监控卷的突发存储桶余额 (p. 1342)

每实例吞吐量限制

st1 和 sc1 卷的吞吐量始终由以下限制中较小的决定：

- 卷的吞吐量限制
- 实例的吞吐量限制

对于所有 Amazon EBS 卷，我们建议选择适当的 EBS 优化型 EC2 实例来避免网络瓶颈。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

吞吐量优化型 HDD 卷

吞吐量优化型 HDD（st1）卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。该卷类型是大型顺序工作负载 (如 Amazon EMR、ETL、数据仓库和日志处理) 的理想之选。不支持可启动的 st1 卷。

吞吐量优化型 HDD (st1) 卷虽然与 Cold HDD (sc1) 卷类似，但其旨在支持频繁访问的数据。

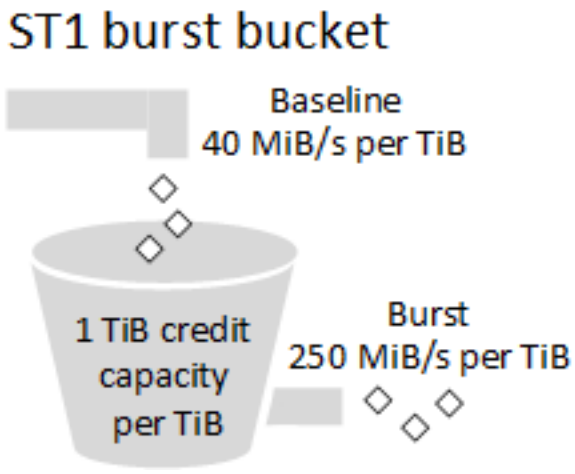
该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅HDD 上的小型读/写效率低下问题 (p. 1342)。

附加到 EBS 优化型实例的吞吐量优化型 HDD (st1) 卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

吞吐量积分和突增性能

与 gp2 类似，st1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。

下图显示 st1 的突增存储桶行为。



st1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

对于 1 TiB st1 卷，突增吞吐量限制为 250 MiB/s，存储桶以 40 MiB/s 的速度填充，最多可容纳 1 TiB 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 500 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 40 MiB/s。

在从 0.125 TiB 到 16 TiB 的卷大小范围内，基准吞吐量从 5 MiB/s 到上限 500 MiB/s 变化，12.5 TiB 时达到上限，如下所示：

```
            40 MiB/s
12.5 TiB × ---------- = 500 MiB/s
             1 TiB
```

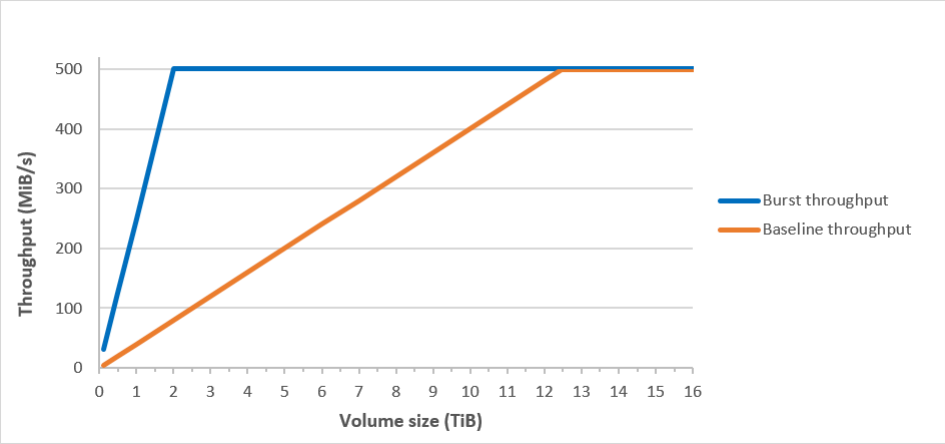
突增吞吐量从 31 MiB/s 到上限 500 MiB/s 变化，2 TiB 时达到上限，如下所示：

```
         250 MiB/s
2 TiB × ---------- = 500 MiB/s
          1 TiB
```

下表列出了 st1 基准和突增吞吐量值的完整范围。

卷大小 (TiB)	ST1 基准吞吐量 (MiB/s)	ST1 突增吞吐量 (MiB/s)
0.125	5	31
0.5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12.5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

下图绘制了表值：



Note

如果创建吞吐量优化型 HDD（st1）卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅监控卷的突发存储桶余额 (p. 1342)。

Cold HDD 卷

Cold HDD（sc1）卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。st1 的吞吐量限制比 sc1 更低，是大型顺序冷数据工作负载的绝佳选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的块存储。不支持可启动的 sc1 卷。

Cold HDD (sc1) 卷虽然与吞吐量优化型 HDD (st1) 卷类似，但其旨在支持不频繁访问的数据。

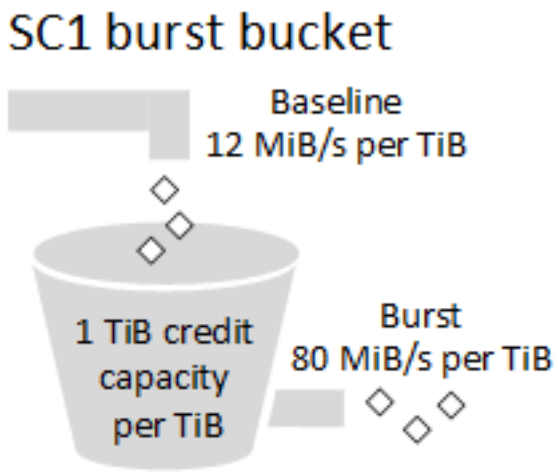
Note

该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 gp2。有关更多信息，请参阅HDD 上的小型读/写效率低下问题 (p. 1342)。

附加到 EBS 优化型实例的 Cold HDD (sc1) 卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

吞吐量积分和突增性能

与 gp2 类似，sc1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。



sc1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

对于 1 TiB sc1 卷，突增吞吐量限制为 80 MiB/s，存储桶以 12 MiB/s 的速度填充，最多可容纳 1 TiB 积分。

较大的卷会线性扩展这些限制，吞吐量上限为最大 250 MiB/s。在存储桶耗尽时，吞吐量会限制为基准速率，即每 TiB 12 MiB/s。

在从 0.125 TiB 到 16 TiB 的卷大小范围内，基准吞吐量从 1.5 MiB/s 到最大 192 MiB/s 变化，16 TiB 时达到上限，如下所示：

```
           12 MiB/s
16 TiB × ---------- = 192 MiB/s
            1 TiB
```

突增吞吐量从 10 MiB/s 到上限 250 MiB/s 变化，3.125 TiB 时达到上限，如下所示：

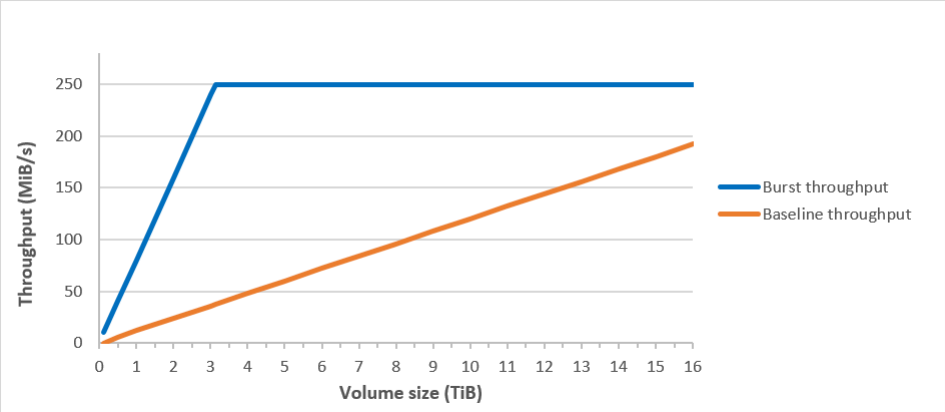
```
             80 MiB/s
3.125 TiB × ----------- = 250 MiB/s
              1 TiB
```

下表列出了 sc1 基准和突增吞吐量值的完整范围：

卷大小 (TiB)	SC1 基准吞吐量 (MiB/s)	SC1 突增吞吐量 (MiB/s)
0.125	1.5	10
0.5	6	40
1	12	80
2	24	160
3	36	240
3.125	37.5	250
4	48	250

卷大小 (TiB)	SC1 基准吞吐量 (MiB/s)	SC1 突增吞吐量 (MiB/s)
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

下图绘制了表值：



Note

如果创建 Cold HDD（sc1）卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报来监控突增存储桶余额的信息，请参阅监控卷的突发存储桶余额 (p. 1342)。

使用 HDD 卷时的性能注意事项

为了使用 HDD 卷获得最优的吞吐量结果，请根据以下注意事项计划您的工作负载。

比较吞吐量优化型 HDD 和 Cold HDD

st1 和 sc1 存储桶大小因卷大小而异，满的存储桶包含充足的令牌用于完整卷扫描。不过，因为每实例和每卷的吞吐量限制，更大的 st1 和 sc1 卷需要更长的时间完成卷扫描。附加到较小实例的卷被限制在每实例吞吐量上，而不是 st1 或 sc1 吞吐量限制。

st1 和 sc1 专为在 99% 的时间内实现 90% 的突增吞吐量性能一致性而设计。不合规时间段大致均匀分布，目标是达到 99% 的每小时预计总吞吐量。

一般来说，扫描时间可由此公式表示：

```
 Volume size
------------ = Scan time
 Throughput
```

例如，考虑到性能一致性保证和其他优化，拥有 5 TiB 卷的 st1 客户预计在 2.91 到 3.27 小时内完成整卷扫描。

- 最佳扫描时间

```
   5 TiB            5 TiB
----------- = ------------------ = 10,486 seconds = 2.91 hours
 500 MiB/s     0.00047684 TiB/s
```

- 最长扫描时间

```
  2.91 hours
-------------- = 3.27 hours
 (0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time
```

同样，拥有 5 TiB 卷的 sc1 客户预计在 5.83 到 6.54 小时内完成整卷扫描。

- 最佳扫描时间

```
   5 TiB             5 TiB
----------- = ------------------- = 20972 seconds = 5.83 hours
 250 MiB/s     0.000238418 TiB/s
```

- 最长扫描时间

```
  5.83 hours
-------------- = 6.54 hours
 (0.90)(0.99)
```

下表列出了不同大小卷的理想扫描时间，假设存储桶是满的并且有充足的实例吞吐量。

卷大小 (TiB)	带突增的 ST1 扫描时间（小时）*	带突增的 SC1 扫描时间（小时）*
1	1.17	3.64
2	1.17	3.64
3	1.75	3.64
4	2.33	4.66
5	2.91	5.83
6	3.50	6.99
7	4.08	8.16

卷大小 (TiB)	带突增的 ST1 扫描时间（小时）*	带突增的 SC1 扫描时间（小时）*
8	4.66	9.32
9	5.24	10.49
10	5.83	11.65
11	6.41	12.82
12	6.99	13.98
13	7.57	15.15
14	8.16	16.31
15	8.74	17.48
16	9.32	18.64

* 这些扫描时间在执行 1 MiB 顺序 I/O 时采取平均队列深度 (四舍五入到最近的整数) 四或更多。

因此，如果您有面向吞吐量的工作负载需要快速完成扫描 (最快 500 MiB/s) 或一天查询几个整卷，请使用 `st1`。如果您针对成本进行了优化，数据访问相对不频繁，而且不需要超过 250 MiB/s 的扫描性能，请使用 `sc1`。

HDD 上的小型读/写效率低下问题

`st1` 和 `sc1` 卷的性能模型针对顺序 I/O 进行了优化，支持高吞吐量工作负载，对具有混合 IOPS 和吞吐量的工作负载提供可接受的性能，不建议使用具有小型随机 I/O 的工作负载。

例如，1 MiB 或更小的 I/O 请求计为 1 MiB I/O 积分。但是，如果是顺序 I/O，则会合并为 1 MiB I/O 数据块，并且只计为 1 MiB I/O 积分。

监控卷的突发存储桶余额

您可以使用 Amazon CloudWatch 中提供的 Amazon EBS `BurstBalance` 指标来监控 `st1` 和 `sc1` 卷的突增存储桶水平。此指标显示 `st1` 和 `sc1` 在突增存储桶中剩余的吞吐量积分。有关 `BurstBalance` 指标以及与 I/O 相关的其他指标的更多信息，请参阅 I/O 特性和监控 (p. 1552)。CloudWatch 还允许您设置警报，以便在 `BurstBalance` 值降到特定水平时通知您。有关更多信息，请参阅 Creating CloudWatch Alarms（创建 CloudWatch 警报）。

针对 EBS 卷的大小和配置的限制

Amazon EBS 卷的大小受制于块数据存储的物理和算术特性，以及操作系统（OS）和文件系统设计者的实现决策。Amazon 对卷大小施加了额外的限制，以保证其服务的可靠性。

以下部分介绍了限制 EBS 卷的可用大小并提供配置 EBS 卷的建议的最重要因素。

目录

- 存储容量 (p. 1342)
- 服务限制 (p. 1343)
- 分区方案 (p. 1343)
- 数据块大小 (p. 1344)

存储容量

下表总结了 Amazon EBS 上的最常用文件系统的理论和实现存储容量（假定 4096 字节块大小）。

分区方案	最大可寻址块数	理论最大大小（块数 x 块大小）	Ext4 实现的最大大小*	XFS 实现的最大大小**	NTFS 实现的最大大小	EBS 支持的最大大小
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB	1 EiB = 242 [1]0TiB (在 RHEL7 上认证的 50 TiB)	500 TiB (在 RHEL7 上认证)	256 TiB	64 TiB †

、https://ext4.wiki.kernel.org/index.php/Ext4_Howto 和 https://access.redhat.com/solutions/1532

** https://access.redhat.com/solutions/1532

† io2 Block Express 卷最高支持 64TiB 的 GPT 分区。有关更多信息，请参阅io2 Block Express 卷 (p. 1334)。

服务限制

Amazon EBS 将数据中心的大规模分布式存储提取到虚拟硬盘中。对安装在 EC2 实例上的操作系统而言，附加的 EBS 卷似乎是包含 512 字节磁盘扇区的物理硬盘驱动器。操作系统通过其存储管理实用程序对数据块 (或集群) 分配到这些虚拟扇区进行管理。分配与卷分区方案 (如主启动记录 (MBR) 或 GUID 分区表 (GPT)) 一致，并且属于已安装文件系统 (ext4、NTFS 等) 的功能。

EBS 不知道其虚拟磁盘扇区中包含的数据；它只会确保扇区的完整性。这意味着 Amazon 操作和操作系统操作是彼此独立的。在您选择卷大小时，请注意二者的功能和限制，如以下情况中所示：

- EBS 当前支持最大卷大小 64 TiB。这意味着您可以创建一个大小为 64 TiB 的 EBS 卷，但操作系统是否能够识别该容量的全部取决于其自身的设计特征以及该卷的分区方式。
- Linux 引导卷可以使用 MBR 或 GPT 分区方案。您从中启动实例的 AMI 决定了启动模式参数以及随后可用于启动卷的分区方案。MBR 支持最大为 2047 GiB (2 TiB - 1 GiB) 的引导卷。带 GRUB 2 的 GPT 支持 2TiB 或更大的引导卷。如果您的 Linux AMI 使用 MBR，则引导卷限制为 2047GiB，但非引导卷没有此限制。有关更多信息，请参阅 使 Amazon EBS 卷可在 Linux 上使用 (p. 1348) 和 设置 AMI 的启动模式。

分区方案

除其他影响之外，分区方案还确定了可以在单个卷中唯一寻址的逻辑数据块的数量。有关更多信息，请参阅数据块大小 (p. 1344)。正在使用的常见分区方案是主启动记录（MBR）和 GUID 分区表（GPT）。这两个方案之间的重要差别可归纳如下。

MBR

MBR 使用 32 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{32} 个可能整数之一。卷的最大可寻址大小由以下公式给出：

```
2^32 × Block size
```

MBR 卷的块大小通常限制为 512 字节。因此：

```
2^32 × 512 bytes = 2 TiB
```

工程解决办法是提高 MBR 卷的这个 2 TiB 限制，但还没有被行业广泛采用。因此，即使 Amazon 显示 MBR 卷的大小大于 2 TiB，Linux 和 Windows 也绝不会检测到它。

GPT

GPT 使用 64 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{64} 个可能整数之一。卷的最大可寻址大小由以下公式给出：

$$2^{64} \times \text{Block size}$$

GPT 卷的块大小通常限制为 4,096 字节。因此：

$$\begin{aligned} & 2^{64} \times 4{,}096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{70} \times 2^{6} \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

现实世界中的计算机系统不支持任何接近这个理论最大值的值。实施的文件系统大小目前上限为 50TiB（对于 ext4）和 256TiB（对于 NTFS）。

数据块大小

现代硬盘驱动器上的数据存储是通过逻辑块寻址 来管理的，逻辑块寻址是一个抽象层，它允许操作系统在逻辑块中读取和写入数据，而无需详细了解底层硬件。操作系统依赖存储设备将块映射到其物理扇区。EBS 将 512 字节的扇区通告给操作系统，操作系统使用数据块 (是扇区大小的数倍) 将数据读写到磁盘。

逻辑数据块的行业默认大小当前为 4096 字节 (4 KiB)。由于某些工作负载受益于较小或较大的块大小，因此文件系统支持可在格式化期间指定的非默认块大小。应使用非默认块大小的情况不在本主题的范围之内，但块大小的选择会对卷的存储容量产生影响。下表显示了存储容量随不同块大小的变化：

块大小	最大卷大小
4 KiB (默认)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (最大)	256 TiB

EBS 实施的卷大小限制（64TiB）目前等于 16KiB 数据块支持的最大大小。

创建 Amazon EBS 卷

您可以创建一个 Amazon EBS 卷，然后将它附加到同一可用区内的任何 EC2 实例。如果您创建加密的 EBS 卷，则只能将其附加到支持的实例类型。有关更多信息，请参阅支持的实例类型 (p. 1505)。

如果您要针对一种高性能存储情形来创建卷，应确保使用预置 IOPS SSD 卷（`io1` 或 `io2`）并将它挂载到一个具有足够带宽支持您的应用程序的实例，如 EBS 优化实例。此建议同样适用于吞吐量优化型 HDD（`st1`）和 Cold HDD（`sc1`）卷。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

空的 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。但是，从快照创建的卷上的存储块必须先进行初始化 (从 Amazon S3 提取并写入到卷)，然后您才能访问该块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。对于大部分应用程序，可将此成本分摊到卷的整个使用期限。为了避免最初在生产环境中出现这种性能下降，您可以强制立即初始化整个卷或启用快速快照还原。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。

Important

如果您在一个支持 EBS Block Express 的区域创建一个大于 16TiB 或 IOPS 大于 64,000 的 io2 卷，该卷将自动运行于 Block Express。io2Block Express 卷仅能挂载到受支持的实例。有关更多信息，请参阅 io2 Block Express 卷。

创建卷的方法

- 在指定块储存设备映射以启动实例时，创建并附加 EBS 卷。有关更多信息，请参阅 使用新启动实例向导启动实例 (p. 575) 和 块设备映射 (p. 1615)：
- 创建空 EBS 卷并将其附加到运行的实例。有关更多信息，请参阅下面的 创建空卷 (p. 1345)。
- 从以前创建的快照中创建 EBS 卷，并将其附加到运行的实例。有关更多信息，请参阅下面的 从快照创建卷 (p. 1346)。

创建空卷

空卷一旦可用便能实现其最高性能，而不需要初始化。

您可以使用以下方法之一创建空的 EBS 卷。

Console

使用控制台创建空 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择 Create volume (创建卷)。
4. 对于 Volume Type（卷类型），选择需要创建的卷类型。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。
5. 对于 Size (大小)，以 GiB 为单位输入卷的大小。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
6. （仅限于 io1、io2 及 gp3）对于 IOPS，输入该卷应提供的每秒进行读写操作的次数 (IOPS) 的最大值。
7. （仅限于 gp3）对于 Throughput（吞吐量），以 MiB/s 为单位输入卷应提供的吞吐量。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。一个卷只能够附加到同一可用区中的实例。
9. 对于 Snapshot ID（快照 ID），保留默认值，即 Don't create volume from a snapshot（不要从快照中创建卷）。
10. 设置卷的加密状态。

    如果您的账户已启用 encryption by default (p. 1507)（默认加密），那么加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

    如果默认情况下您的账户未启用加密，则加密是可选的。要加密卷，请为 Encryption（加密）选择 Encrypt this volume（加密此卷），然后选择要用于加密卷的 KMS 密钥。

    Note

    加密卷只能附加到支持 Amazon EBS 加密的实例。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。
11. （可选）要为卷分配自定义标签，请在 Tags（标签）部分，选择 Add tag（添加标签），然后输入标签键和值对。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。
12. 选择 Create volume (创建卷)。

    Note

    Volume state（卷状态）为 available（可用）时，卷即可供使用。

13. 要使用卷，请将其附加到实例。有关更多信息，请参阅将 Amazon EBS 卷挂载到实例 (p. 1347)。

Amazon CLI

使用命令行创建空 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-volumeAmazon CLI
- New-EC2VolumeAmazon Tools for Windows PowerShell

`state` 状态为 `available` 时，卷即可供使用。

从快照创建卷

从快照创建的新卷在后台延时加载。这意味着在实例开始访问附加的卷及其所有数据之前，无需等待所有数据从 Amazon S3 传输到 EBS 卷。如果您的实例访问尚未加载的数据，卷会立即从 Amazon S3 下载请求的数据，然后在后台继续加载卷数据的剩余部分。在下载所有块并将其写入到卷后，才会实现卷性能。为避免在生产环境中影响初始性能，请参阅 初始化 Amazon EBS 卷 (p. 1554)。

从加密快照创建的新 EBS 卷会自动加密。您还可以在从未加密的快照还原卷的同时对卷进行动态加密。加密的卷只能附加到支持 EBS 加密的实例类型。有关更多信息，请参阅支持的实例类型 (p. 1505)。

您可以使用以下方法之一从快照创建卷。

Console

使用控制台从快照中创建 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择 Create volume (创建卷)。
4. 对于 Volume Type（卷类型），选择需要创建的卷类型。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。
5. 对于 Size (大小)，以 GiB 为单位输入卷的大小。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
6. （仅限于 `io1`、`io2` 及 `gp3`）对于 IOPS，输入该卷应提供的每秒进行读写操作的次数 (IOPS) 的最大值。
7. （仅限于 `gp3`）对于 Throughput（吞吐量），以 MiB/s 为单位输入卷应提供的吞吐量。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。一个卷只能附加到位于相同可用区中的实例。
9. 对于 Snapshot ID（快照 ID），选择快照并从中创建卷。
10. 设置卷的加密状态。

    如果选定的快照已加密，或者您的账户已启用默认加密 (p. 1507)，则加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

    如果选定的快照未加密，且默认情况下账户未启用加密，则加密是可选的。要加密卷，请为 Encryption（加密）选择 Encrypt this volume（加密此卷），然后选择要用于加密卷的 KMS 密钥。

    Note

    加密卷只能附加到支持 Amazon EBS 加密的实例。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

11. （可选）要为卷分配自定义标签，请在 Tags（标签）部分，选择 Add tag（添加标签），然后输入标签键和值对。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。
12. 选择 Create Volume。

    Note

    Volume state（卷状态）为 available（可用）时，卷即可供使用。
13. 要使用卷，请将其附加到实例。有关更多信息，请参阅将 Amazon EBS 卷挂载到实例 (p. 1347)。

Amazon CLI

使用命令行从快照中创建 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-volumeAmazon CLI
- New-EC2VolumeAmazon Tools for Windows PowerShell

`state` 状态为 `available` 时，卷即可供使用。

将 Amazon EBS 卷挂载到实例

您可以将可用的 EBS 卷附加到与该卷处于同一可用区中的一个或多个实例。

有关在启动时向实例添加 EBS 卷的信息，请参阅实例块储存设备映射 (p. 1620)。

先决条件

- 确定您可以将多少个卷附加到您的实例。有关更多信息，请参阅实例卷限制 (p. 1607)。
- 如果卷已加密，只能将它附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅支持的实例类型 (p. 1505)。
- 如果卷有 Amazon Web Services Marketplace 产品代码：
  - 卷只能附加到已停止的实例。
  - 您必须订阅卷上的 Amazon Web Services Marketplace 代码。
  - 实例的配置（实例类型、操作系统）必须支持这一特定的 Amazon Web Services Marketplace 代码。例如，您不能从 Windows 实例取用卷，然后将其附加到 Linux 实例。
  - Amazon Web Services Marketplace 产品代码从卷复制到实例。

  Important

  如果您将 `io2` 卷挂载到支持 Block Express 的实例，则该卷会始终在 Block Express 上运行。有关更多信息，请参阅 `io2` Block Express 卷。

您可以使用以下方法之一将卷挂载到实例。

Console

使用控制台将 EBS 卷附加到实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择需要附加的卷，然后选择 Actions（操作）、Attach volume（附加卷）。

Note

您只能附加处于 `Available` 状态中的卷。

4. 对于 Instance（实例），输入实例的 ID 或从选项列表中选择实例。

   Note

   - 卷必须附加到位于同一可用区的实例上。
   - 如果卷已加密，只能将它附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

5. 对于 Device name（设备名称），输入卷支持的设备名称。该设备名称由 Amazon EC2 使用。在挂载卷时，实例的块储存设备驱动程序将分配不同的卷名称。有关更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。
6. 选择附加卷。
7. 连接到实例并挂载卷。有关更多信息，请参阅使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)。

Amazon CLI

使用命令行将 EBS 卷附加到实例

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- attach-volume (Amazon CLI)
- Add-EC2Volume (Amazon Tools for Windows PowerShell)

Note

在某些情况下，您可能会发现某个并非附加到 `/dev/xvda` 或 `/dev/sda` 的卷成为了您的实例的根卷。当您将另一个实例的根卷或从某个根卷的快照中创建的卷附加到带有现有根卷的实例时，可能会发生这种情况。有关详细信息，请参阅从错误的卷启动。

使 Amazon EBS 卷可在 Linux 上使用

将某个 Amazon EBS 卷附加到实例后，该卷将显示为块储存设备您可以使用任何文件系统将卷格式化，然后进行挂载。在使 EBS 卷可供使用后，您可以像访问其他所有卷一样访问该卷。任何写入此文件系统的数据均写入 EBS 卷，并且对使用该设备的应用程序是透明的。

您可以制作 EBS 卷的快照以进行备份或在您创建其他卷时作为基准。有关更多信息，请参阅Amazon EBS 快照 (p. 1368)。

如果您准备使用的 EBS 卷大于 2TiB，则必须使用 GPT 分区方案才能访问整个卷。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。

您可以从Amazon EC2 用户指南（适用于 Windows 实例）中的使卷可在 Windows 上使用获得有关 Windows 实例上的卷的指示。

格式化并挂载附加的卷

假设您的根设备 `/dev/xvda` 拥有一个具有 EBS 卷的 EC2 实例，并且您已使用 `/dev/sdf` 将一个空的 EBS 卷添加到了该实例。按照以下过程使新附加的卷可用。

在 Linux 上格式化并挂载 EBS 卷

1. 使用 SSH 连接到您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。

2. 设备可附加到设备名称与您在块储存设备映射中指定的设备名称不同的实例。有关更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。使用 lsblk 命令可查看可用磁盘设备及其挂载点（如果适用），以帮助您确定要使用的正确设备名称。lsblk 的输出从完整的设备路径中去掉了 /dev/ 前缀。

   以下是基于 Nitro 系统 (p. 246)构建的实例的示例输出，该实例将 EBS 卷公开为 NVMe 块存储设备。根设备为 /dev/nvme0n1，它有两个名为 nvme0n1p1 和 nvme0n1p128。如果没有分区且尚未附加，则附加卷为 /dev/nvme1n1。

   ```
   [ec2-user ~]$ lsblk
   NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme1n1       259:0    0  10G  0 disk
   nvme0n1       259:1    0   8G  0 disk
   -nvme0n1p1    259:2    0   8G  0 part /
   -nvme0n1p128  259:3    0   1M  0 part
   ```

   以下是 T2 实例的示例输出。根设备为 /dev/xvda，它有名为 xvda1 的一个分区。如果没有分区且尚未附加，则附加卷为 /dev/xvdf。

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   -xvda1  202:1    0    8G  0 part /
   xvdf    202:80   0   10G  0 disk
   ```

3. 确定卷上是否存在文件系统。新卷为原始的块储存设备，您必须先在这种设备上创建文件系统，然后才能够挂载并使用它们。从快照创建的卷可能已经含有文件系统；如果您在现有的文件系统上创建新的文件系统，则该操作将覆盖您的数据。

   使用以下一种或两种方法来确定卷上是否有文件系统：

   - 使用 file -s 命令获取有关特定设备的信息，例如其文件系统类型。如果输出仅显示 data（如以下示例输出所示），则说明设备上没有文件系统。

     ```
     [ec2-user ~]$ sudo file -s /dev/xvdf
     /dev/xvdf: data
     ```

     如果设备有文件系统，该命令会显示有关文件系统类型的信息。例如，以下示例输出显示具有 XFS 文件系统的根设备。

     ```
     [ec2-user ~]$ sudo file -s /dev/xvda1
     /dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
     ```

   - 使用 lsblk -f 命令获取有关连接到实例的所有设备的信息。

     ```
     [ec2-user ~]$ sudo lsblk -f
     ```

     例如，以下输出显示有三个设备连接到实例 —nvme1n1、nvme0n1 和 nvme2n1。第一列列出了设备及其分区。FSTYPE 列显示每个设备的文件系统类型。如果该列对于特定设备为空，则表示该设备没有文件系统。在这种情况下，设备 nvme1n1 和设备 nvme0n1 上的分区 nvme0n1p1 都使用 XFS 文件系统进行格式化，而设备 nvme2n1 和设备 nvme0n1 上的分区 nvme0n1p128 没有文件系统。

     ```
     NAME  FSTYPE LABEL UUID      MOUNTPOINT
     nvme1n1         xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
     nvme0n1
     ##nvme0n1p1 xfs     / 90e29211-2de8-4967-b0fb-16f51a6e464c         /
     ##nvme0n1p128
     nvme2n1
     ```

如果这些命令的输出显示设备上没有文件系统，则必须创建一个文件系统。

4. （有条件）如果您在上一步中发现设备上存在文件系统，请跳过此步骤。如果您有一个空卷，请使用 mkfs -t 命令在该卷上创建一个文件系统。

   Warning

   如果要挂载已具有数据的卷（例如，从快照创建的卷），请勿使用此命令。否则，您会格式化卷并删除现有数据。

   ```
   [ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
   ```

   如果出现“找不到 mkfs.xfs”错误，请使用以下命令安装 XFS 工具，然后重复上一命令：

   ```
   [ec2-user ~]$ sudo yum install xfsprogs
   ```

5. 使用 mkdir 命令创建卷的挂载点目录。挂载点是卷在文件系统树中的位置，以及您在安装卷之后读写文件的位置。下面的示例创建一个名为 /data 的目录。

   ```
   [ec2-user ~]$ sudo mkdir /data
   ```

6. 使用以下命令在您在上一步中创建的目录挂载卷。

   ```
   [ec2-user ~]$ sudo mount /dev/xvdf /data
   ```

7. 检查新卷挂载的文件权限，确保您的用户和应用程序可以向该卷写入数据。有关文件权限的更多信息，请参阅 Linux 文档项目 文件安全性。
8. 重启实例后，挂载点不会自动保留。要在重启后自动挂载此 EBS 卷，请使用重启后自动挂载附加的卷 (p. 1350)。

重启后自动挂载附加的卷

要在每次系统重启时附加附加的 EBS 卷，可在 /etc/fstab 文件中为该设备添加一个条目。

您可以在 /dev/xvdf 中使用设备名称（如 /etc/fstab），但建议改为使用设备的 128 位通用唯一标识符 (UUID)。设备名称可以更改，但 UUID 会在整个分区的使用寿命期间保留。通过使用 UUID，您可以减少系统在硬件重新配置后无法启动的机会。有关更多信息，请参阅识别 EBS 设备 (p. 1520)。

重启后自动附加附加卷

1. （可选）创建 /etc/fstab 文件的备份，以便在编辑时误损坏或删除此文件时使用。

   ```
   [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
   ```

2. 使用 blkid 命令查找设备的 UUID。记下要在重新启动后挂载的设备的 UUID。在下一步中您将需要用到它。

   例如，以下命令显示有两个设备挂载到实例上，并显示了两个设备的 UUID。

   ```
   [ec2-user ~]$ sudo blkid
   /dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
    PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
   /dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
   ```

   对于 Ubuntu 18.04，请使用 lsblk 命令。

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. 使用任何文本编辑器（如 /etc/fstab 和 nano）打开 vim 文件。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. 将以下条目添加到 /etc/fstab 以在指定的挂载点挂载设备。这些字段是 blkid（或用于 Ubuntu 18.04 的 lsblk）返回的 UUID 值、挂载点、文件系统以及建议的文件系统挂载选项。有关必填字段的更多信息，请运行 man fstab 以打开 fstab 手册。

   在以下示例中，我们将 UUID 为 aebf131c-6957-451e-8d34-ec978d9581ae 的设备挂载到挂载点 /data，然后我们使用 xfs 文件系统。我们还使用 defaults 和 nofail 标志。我们指定 0 以防止文件系统被转储，并且我们指定 2 以指示它是非根设备。

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae  /data  xfs  defaults,nofail  0  2
```

   Note

   如果您要在未附加此卷的情况下启动实例（例如，将卷移动到另一个实例之后），nofail 附加选项允许该实例即使在卷附加过程中出现错误时也可启动。Debian 衍生物 (包括早于 16.04 的 Ubuntu 版本) 还必须添加 nobootwait 挂载选项。

5. 要检查条目是否有效，请在 /etc/fstab 中运行以下命令以卸载设备，然后挂载所有文件系统。如果未产生错误，则说明 /etc/fstab 文件正常，您的文件系统会在重启后自动挂载。

```
[ec2-user ~]$ sudo umount /data
[ec2-user ~]$ sudo mount -a
```

   如果收到错误消息，请解决文件中的错误。

   Warning

   /etc/fstab 文件中的错误可能显示系统无法启动。请勿关闭 /etc/fstab 文件中有错误的系统。

   如果您无法确定如何更正 /etc/fstab 中的错误并且您在此过程的第一步中创建了一个备份文件，则可以使用以下命令从您的备份文件还原。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

查看关于 Amazon EBS 卷的信息

您可以查看有关您的 EBS 卷的描述信息。例如，您可以查看有关特定区域中所有卷的信息，或者查看有关单个卷的详细信息，包括其大小、卷类型、卷是否加密、加密卷所用的主密钥以及卷附加到的特定实例。

您可以获得有关您的 EBS 卷的其他信息，例如该实例的操作系统上有多少空间磁盘可用。

查看卷信息

您可以使用以下方法之一查看有关卷的信息。

Console

使用控制台查看有关卷的信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Volumes。
3. 要减少列表，您可以使用标签和卷属性来筛选卷。选择筛选条件字段，选择标签或卷属性，然后选择筛选条件值。
4. 要查看有关卷的更多信息，请选择其 ID。

使用控制台查看已附加到实例的 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择实例。
4. 在 Storage（存储）选项卡上，Block devices（块储存设备）部分列出了已附加到实例的卷。要查看有关特定卷的信息，请在 Volume ID（卷 ID）列中选择卷 ID。

Amazon CLI

使用命令行查看有关 EBS 卷的信息

您可以使用以下命令之一查看卷属性。有关更多信息，请参阅访问 Amazon EC2 (p. 3)。

- describe-volumes (Amazon CLI)
- Get-EC2Volume (Amazon Tools for Windows PowerShell)

Amazon EC2 Global View

您可以使用 Amazon EC2 全局视图查看启用 Amazon 账户的所有区域中的卷。有关更多信息，请参阅使用 Amazon EC2 全局视图列出和筛选跨区域的资源 (p. 1663)。

卷状态

卷状态描述 Amazon EBS 卷的可用性。您可以在控制台的 Volumes（卷）页面上的 State（状态）列中查看卷状态，也可以使用 describe-volumes Amazon CLI 命令查看卷状态。

可能的卷状态包括：

`creating`

正在创建卷。

`available`

卷未连接到实例。

`in-use`

卷已连接到实例。

`deleting`

正在删除卷。

`deleted`

卷被删除。

`error`

与 EBS 卷有关的底层硬件出现故障，与卷关联的数据不可恢复。有关如何还原卷或恢复卷上的数据的信息，请参阅我的 EBS 卷的状态为“错误”。

查看卷指标

您可以从 Amazon CloudWatch 中获取有关 EBS 卷的附加信息。有关更多信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)。

查看可用磁盘空间

您可以获得有关您的 EBS 卷的其他信息，例如该实例的 Linux 操作系统上有多少空间磁盘可用。例如，使用以下命令：

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

Tip

您还可以使用 CloudWatch 代理从 Amazon EC2 实例采集磁盘空间使用情况指标，但无需连接到该实例。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的创建 CloudWatch 代理配置文件和安装 CloudWatch 代理。如果需要监控多个实例的磁盘空间使用情况，则可以使用 Systems Manager 在这些实例上安装和配置 CloudWatch 代理。有关更多信息，请参阅使用 Systems Manager 安装 CloudWatch 代理。

有关在 Windows 实例上查看可用磁盘空间的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的查看可用磁盘空间。

使用以前的快照替换卷

由于速度、便利性和成本，Amazon EBS 快照是 Amazon EC2 上的首选备份工具。当从快照中创建卷时，您重新创建了它在过去特定时间点的状态，并且所有数据完整无缺。通过将从快照中创建的卷附加到实例，您可以在不同的区域之间复制数据，创建测试环境，完全替换受损或损坏的生产卷，或检索特定文件和目录并将其传输到另一个附加的卷。有关更多信息，请参阅Amazon EBS 快照 (p. 1368)。

您可以使用以下过程之一将 Amazon EBS 卷替换为从该卷的早期快照创建的另一个卷。您必须分离当前卷，然后附加新的卷。

Note

Amazon EBS 卷只能附加到位于相同可用区中的实例。

Console

替换卷

1. 从快照中创建一个卷，并记下新卷的 ID。有关更多信息，请参阅从快照创建卷 (p. 1346)。
2. 在 Instances（实例）页面上，选择要替换卷的实例，然后记下实例 ID。

   在实例处于选中状态时，选择 Storage（存储）选项卡。在 Block devices（块储存设备）部分中，找到要替换的卷并记下该卷的设备名称，例如 /dev/sda1。

   选择卷 ID。
3. 在 Volumes（卷）屏幕上，选择该卷并选择 Actions（操作）、Detach volume（分离卷）、Detach（分离）。
4. 选择在步骤 1 中创建的新卷，然后选择 Actions（操作）、Attach volume（附加卷）。

   对于 Instance（实例）和 Device name（设备名称），输入您在步骤 2 中记下的实例 ID 和设备名称，然后选择 Attach volume（附加卷）。

5. 连接到您的实例并安装卷。有关更多信息，请参阅使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)。

替换根卷

Amazon EC2 使您能够替换正在运行的实例的根 Amazon EBS 卷，同时保留以下内容：

- 存储在实例存储卷上的数据 — 还原根卷后，实例存储卷仍附加到实例。
- 存储在数据（非根）Amazon EBS 卷上的数据 — 在还原根卷后，非根 Amazon EBS 卷仍附加到实例。
- 网络配置 — 所有网络接口均仍附加到实例，并保留其 IP 地址、标识符和附件 ID。当实例变为可用时，将刷新所有待处理的网络流量。此外，实例保留在同一个物理主机上，因此它会保留其公有和私有 IP 地址以及 DNS 名称。
- IAM policy — 将保留和强制实施与实例相关联的 IAM 配置文件和策略（例如基于标签的策略）。

主题

- 如何工作？ (p. 1354)
- 替换根卷 (p. 1356)
- 查看根卷替换任务 (p. 1357)

如何工作？

在您替换实例的根卷时，将通过以下方法之一还原新的（替换）根卷：

- 到初始启动状态 — 该卷将在实例启动时还原到其初始状态。有关更多信息，请参阅将根卷还原到其启动状态 (p. 1355)。
- 从来自与当前根卷相同世系的快照 — 这将允许您修复问题，如根卷损坏或客户机操作系统网络配置错误。有关更多信息，请参阅使用快照替换卷 (p. 1355)。
- 从与实例具有相同关键属性的 AMI — 这将允许您执行操作系统和应用程序修补或升级。有关更多信息，请参阅使用 AMI 替换根卷 (p. 1355)。

原始根卷与实例分离，新根卷将在其位置附加到实例。将更新实例的块设备映射，以反映替换根卷的 ID。您可以选择在根卷替换过程完成后是否保留原始根卷。如果您在替换过程完成后选择删除原始根卷，则原始根卷将被自动删除，并变得不可恢复。如果您选择在该过程完成后保留原始根卷，则该卷仍会在您的账户中预调配；当您不再需要它时，必须手动删除它。

如果根卷替换任务失败，则实例将重新启动，原始根卷仍附加到该实例。

根卷更换的注意事项

- 该实例必须处于 `running` 状态。
- 在此过程中，实例将自动重新启动。在重启过程中，将清空内存 (RAM) 的内容。无需手动重启。
- 如果根卷是实例存储卷，则无法替换它。仅支持具有 Amazon EBS 根卷的实例。
- 您可以替换所有虚拟化实例类型和 EC2 Mac 裸机实例的根卷。不支持所有其他裸机实例类型。
- Amazon EC2 Mac 裸机实例支持将根卷恢复到其启动状态并使用快照替换根卷。Amazon EC2 Mac 裸机实例目前不支持使用 AMI 替换根卷。
- 您可以使用与实例先前根卷属同谱系的任何快照。

主题

- 将根卷还原到其启动状态 (p. 1355)

- 使用快照替换卷 (p. 1355)
- 使用 AMI 替换根卷 (p. 1355)

将根卷还原到其启动状态

您可以执行根卷替换，将实例的根卷替换为还原到原始根卷启动状态的替换根卷。替换卷将自动从实例启动期间用于创建原始卷的快照中还原。

替换根卷的类型、大小和终止时删除属性与原始根卷相同。

使用快照替换卷

您可以执行根卷替换，将实例的根卷替换为还原到特定快照的替换卷。这使您可以将实例的根卷还原到您之前从该根卷创建的特定快照。

替换根卷的类型、大小和终止时删除属性与原始根卷相同。

使用快照的注意事项

- 您只能使用与实例当前根卷属同谱系的快照。
- 您不能使用从根卷拍摄的快照创建的快照副本。
- 在成功替换根卷后，从原始根卷拍摄的快照仍可用于替换新的（替换）根卷。

使用 AMI 替换根卷

您可以使用自己拥有的 AMI、与您共享的 AMI 或 Amazon Web Services Marketplace AMI 来执行根卷替换。AMI 必须具有与实例相同的产品代码、账单信息、架构类型和虚拟化类型。

如果实例启用了 NitroTPM、ENA 或 sriov-net，则必须使用支持这些功能的 AMI。如果实例未启用 NitroTPM、ENA 或 sriov-net，则您可以选择不支持这些功能的 AMI；也可以选择支持这些功能的 AMI，在这种情况下，将向该实例添加支持。

您可以选择与实例的启动模式不同的 AMI，前提是该实例支持 AMI 的启动模式。如果实例不支持启动模式，则该请求将失败。如果实例支持启动模式，则新的启动模式将传播到该实例，并相应更新其 UEFI 数据。如果您手动修改了启动顺序或添加了私有 UEFI 安全启动密钥来加载私有内核模块，则在根卷替换期间，更改将丢失。

替换根卷获得与原始根卷相同的卷类型和终止时删除属性，并获取 AMI 根卷块设备映射的大小。

> **Note**
>
> AMI 根卷块设备映射的大小必须等于或大于原始根卷的大小。如果 AMI 根卷块设备映射的大小小于原始根卷的大小，则请求失败。

在根卷替换任务完成后，当您使用控制台 Amazon CLI 或 Amazon SDK 描述实例时，将反映以下新的和经过更新的信息：

- 新 AMI ID
- 根卷的新卷 ID
- 经过更新的启动模式配置（如果由 AMI 更改）
- 经过更新的 NitroTPM 配置（如果由 AMI 启用）
- 经过更新的 ENA 配置（如果由 AMI 启用）
- 经过更新的 sriov-net 配置（如果由 AMI 启用）

新 AMI ID 也反映在实例元数据中。

使用 AMI 的注意事项：

- 如果您使用拥有多个块设备映射的 AMI，则仅使用该 AMI 的根卷。其他（非根）卷将被忽略。
- 您只能使用您的账户拥有启动权限的 AMI。
- 仅当实例没有产品代码时，您才能使用没有产品代码的 AMI。
- 您无法指定替换根卷的加密状态。下表汇总了可能的加密结果。

原始根卷	AMI 块储存设备映射	替换根卷
已加密	未加密	请求失败
已加密	已加密	已加密
未加密	未加密	未加密
未加密	已加密	已加密

- AMI 根卷块设备映射的大小必须等于或大于原始根卷的大小。如果 AMI 根卷块设备映射的大小小于原始根卷的大小，则请求失败。
- 将自动更新实例的实例身份文档。
- 如果实例支持 NitroTPM，则将重置该实例的 NitroTPM 数据，并将生成新密钥。

替换根卷

当您替换实例的根卷时，将创建根卷替换任务。您可以使用根卷更换任务来监控替换过程的进度和结果。有关更多信息，请参阅查看根卷替换任务 (p. 1357)。

您可以使用以下方法之一替换实例的根卷。

Note

如果使用 Amazon EC2 控制台，此功能仅在新控制台中可用。

New console

替换根卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择要替换其根卷的实例，然后选择 Actions（操作）、Monitor and troubleshoot（监控和故障排除）、Replace root volume（替换根卷）。

   Note

   如果选定的实例不在 `running` 状态，替换根卷操作将被禁用。
4. 在 Replace root volume（替换根卷）屏幕中，执行以下操作之一：
   - 若要将替换根卷还原到其初始启动状态，请在不选择快照的情况下选择 Create replacement task（创建替换任务）。
   - 若要将替换根卷还原到特定快照，对于 Snapshot（快照），请选择要使用的快照，然后选择 Create replacement task（创建替换任务）。
   - 若要使用 AMI 还原替换根卷，对于 AMI，请选择要使用的 AMI，然后选择 Create replacement task（创建替换任务）。
5. 若要在替换任务完成后删除原始根卷，请选择 Delete replaced root volume（删除替换的根卷）。

Amazon CLI

将替换根卷还原到启动状态

使用 create-replace-root-volume-task 命令。对于 --instance-id，指定要为其替换根卷的实例的 ID。省略 --snapshot-id --image-id 参数。若要在替换原始根卷后将其删除，请包括 --delete-replaced-root-volume 并指定 true。

```
$ aws ec2 create-replace-root-volume-task --instance-id instance_id --delete-replaced-root-volume true
```

例如：

```
$ aws ec2 create-replace-root-volume-task --instance-id i-1234567890abcdef0 --delete-replaced-root-volume true
```

将替换根卷还原到特定快照

使用 create-replace-root-volume-task 命令。对于 --instance-id，指定要为其替换根卷的实例的 ID。对于 --snapshot-id，请定要使用的快照的 ID。若要在替换原始根卷后将其删除，请包括 --delete-replaced-root-volume 并指定 true。

```
$ aws ec2 create-replace-root-volume-task --instance-id instance_id --snapshot-id snapshot_id --delete-replaced-root-volume true
```

例如：

```
$ aws ec2 create-replace-root-volume-task --instance-id i-1234567890abcdef0 --snapshot-id snap-9876543210abcdef0 --delete-replaced-root-volume true
```

使用 AMI 还原替换根卷

使用 create-replace-root-volume-task 命令。对于 --instance-id，指定要为其替换根卷的实例的 ID。对于 --image-id，指定要使用的 AMI 的 ID。若要在替换原始根卷后将其删除，请包括 --delete-replaced-root-volume 并指定 true。

```
$ aws ec2 create-replace-root-volume-task --instance-id instance_id --image-id ami_id
 --delete-replaced-root-volume true
```

例如：

```
$ aws ec2 create-replace-root-volume-task --instance-id i-01234567890abcdef --image-id
 ami-09876543210abcdef --delete-replaced-root-volume true
```

查看根卷替换任务

当您替换实例的根卷时，将创建根卷替换任务。在此过程中，根卷更换任务将转换为以下状态：

- pending — 正在创建替换卷。
- in-progress — 正在分离原始卷，正在附加替换卷。
- succeeded — 已将替换卷成功附加到实例并且实例可用。
- failing — 替换任务即将失败。

- `failed` — 替换任务已失败，但原始根卷仍然处于附加状态。
- `failing-detached` — 替换任务即将失败，并且实例可能未附加根卷。
- `failed-detached` — 替换任务已失败，并且实例未附加根卷。

您可以使用以下方法之一查看实例的根卷替换任务。

Note

如果使用 Amazon EC2 控制台，此功能仅在新控制台中可用。

Console

查看根卷替换任务

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择要查看其根卷替换任务的实例，然后选择 Storage（存储）选项卡。
4. 在 Storage（存储）选项卡中，展开 Recent root volume replacement tasks（最近的根卷替换任务）。

Amazon CLI

查看根卷替换任务的状态

使用 describe-replace-root-volume-tasks 命令并指定要查看的根卷替换任务的 ID。

```
$ aws ec2 describe-replace-root-volume-tasks --replace-root-volume-task-
ids task_id_1 task_id_2
```

例如：

```
$ aws ec2 describe-replace-root-volume-tasks --replace-root-volume-task-ids
 replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

或者，请指定 `instance-id` 筛选条件以按实例筛选结果。

```
$ aws ec2 describe-replace-root-volume-tasks --filters Name=instance-
id,Values=instance_id
```

例如：

```
$ aws ec2 describe-replace-root-volume-tasks --filters Name=instance-
id,Values=i-1234567890abcdef0
```

监控您的卷状态

Amazon Web Services（Amazon）自动提供可用于监控 Amazon Elastic Block Store（Amazon EBS）卷的数据。

目录

- EBS 卷状态检查 (p. 1359)
- EBS 卷事件 (p. 1360)
- 使用受损的卷 (p. 1362)
- 使用自动启用 IO 卷属性 (p. 1363)

有关其他监控信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)和适用于 Amazon EBS 的 EventBridge (p. 1569)。

EBS 卷状态检查

通过卷状态检查，您可以更好地了解、追踪和管理 Amazon EBS 卷上数据的潜在不一致性。它们的作用是在您需要确定 Amazon EBS 卷是否损坏的时候为您提供信息，帮助您控制处理潜在不一致卷的方式。

卷状态检查为自动执行的测试，该测试每隔 5 分钟运行一次并返回通过或故障状态。如果所有的检查都通过，则卷的状态为ok。如果一个检查返回故障，则卷的状态为impaired。如果状态为insufficient-data，那么该检查将在该卷上继续进行。您可以查看卷状态检查的结果来识别任意受损卷并进行所需操作。

当 Amazon EBS 判定一个卷中的数据具有潜在不一致性时，默认禁用从任何附加的 EC2 实例到该卷的 I/O，以此来防止数据损坏。禁用 I/O 后，下一个卷状态检查故障，并且卷状态为impaired。此外，您还会看到一个通知您 I/O 被禁用的事件，并且您可以通过使能到该卷的 I/O 来解决卷的损坏状态。我们将等待您启用 I/O，在此期间您有机会决定是继续让您的实例使用该卷，还是在使用该卷之前先使用命令（如 fsck）运行一致性检查。

> **Note**
>
> 卷状况以卷状况检查为依据，并不反映卷状态。因此，卷状态并不表示卷处于 error 状态（例如，卷无法接受 I/O 时）。有关卷状态的信息，请参阅 卷状态 (p. 1352)。

如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是“受损”，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用 Auto-Enable IO (自动启用 IO) 卷属性（API 中的 autoEnableIO），则卷状态检查会继续通过。此外，您将会看到一个通知您该卷具有潜在不一致性的事件，但它的 I/O 不会自动启用。这使您能够检查卷的一致性或随后替换它。

I/O 性能状态检查将实际卷性能与卷的预期性能进行比较。如果卷的表现低于预期，它会提醒您。此状态检查仅适用于挂载到实例的预置 IOPS SSD（io1 和 io2）和通用型 SSD (gp3) 卷。状态检查对于通用型 SSD (gp2)、吞吐量优化型 HDD (st1)、Cold HDD (sc1) 或磁介质 (standard) 卷无效。I/O 性能状态检查每分钟执行一次，CloudWatch 每 5 分钟收集一次这些数据。从您将 io1 或 io2 卷挂载到实例的那一刻起，可能需要 5 分钟来进行状态检查，以报告 I/O 性能状态。

> **Important**
>
> 在初始化已从快照还原的 Provisioned IOPS SSD 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O 性能状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 Provisioned IOPS SSD 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。

下表列出了 Amazon EBS 卷的状态。

卷状态	I/O 使能状态	I/O 性能状态（仅限 **io1**、**io2** 和 **gp3** 卷）
ok	使能 (I/O 使能或 I/O 自动使能)	正常 (卷的期望性能)
warning	使能 (I/O 使能或 I/O 自动使能)	降级 (卷的性能低于期望性能) 严重降级 (卷的性能大大低于期望性能)
impaired	使能 (I/O 使能或 I/O 自动使能) 禁用 (卷脱机和挂起恢复，或等待用户使能 I/O)	停滞 (卷性能受到严重影响) 不可用 (由于 I/O 被禁用，所以不能确定 I/O 性能)
insufficient-data	使能 (I/O 使能或 I/O 自动使能) 数据不足	数据不足

您可以使用以下方法查看和处理状态检查。

Console

查看状态检查，需要进行以下操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。

   卷状态列显示每个卷的运行状态。
3. 要查看特定卷的详细状态信息，请在网格中选择该卷，然后选择 Status checks（状态检查）选项卡。
4. 如果您的卷状态检查返回故障（状态是 `impaired`），请参阅 使用受损的卷 (p. 1362)。

另外，您还可以在导航器中选择事件来查看实例和卷所有的事件。有关更多信息，请参阅EBS 卷事件 (p. 1360)。

Amazon CLI

查看卷状态信息

使用以下命令之一。

- describe-volume-status (Amazon CLI)
- Get-EC2VolumeStatus（Amazon Tools for Windows PowerShell）

有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

EBS 卷事件

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何附加的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。

想要自动使能具有潜在不一致性卷上的 I/O，您可以改变自动启用 IO 卷属性（在 API 中为 `autoEnableIO`）的设置。更多关于改变这些属性的信息，请参阅使用受损的卷 (p. 1362)。

每一个事件都包括一个开始时间，该时间指明事件发生的时间，和一个持续时间，该时间会指明该卷 I/O 会被禁用多久。当该卷的 I/O 被使能时，将会为该事件添加结束时间。

卷状态事件包括下列描述中的一个：

`Awaiting Action: Enable IO`

卷数据具有潜在一致性。在您明确的使能它之前，将一直禁用 I/O。当您明确启用 I/O 后，事件描述变为 IO Enabled。

`IO Enabled`

明确地使能这些卷的 I/O 操作。

`IO Auto-Enabled`

事件发生后，自动使能这些卷上的 I/O 操作。我们建议您在继续使用数据前，先检查数据的不一致性。

`Normal`

仅适用于 io1、io2 和 gp3 卷。卷执行其期望性能。

`Degraded`

仅适用于 io1、io2 和 gp3 卷。卷性能低于期望性能。

`Severely Degraded`

仅适用于 io1、io2 和 gp3 卷。卷性能大大地低于期望性能。

`Stalled`

仅适用于 io1、io2 和 gp3 卷。卷的性能受到严重影响。

您可以使用以下方法查看卷的事件。

Console

想要查看您的卷事件，需要执行以下操作

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。列出具有事件的所有实例和卷。
3. 可以按卷进行筛选以便仅查看卷状态。您也可以筛选指定的状态类型。
4. 选择一个卷以查看其特定事件。

Amazon CLI

想要查看您的卷事件，需要执行以下操作

使用以下命令之一。

- describe-volume-status (Amazon CLI)
- Get-EC2VolumeStatus（Amazon Tools for Windows PowerShell）

有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

如果您的卷 I/O 被禁用，请参阅使用受损的卷 (p. 1362)。如果您的卷 I/O 性能低于正常值，这可能是因为您之前的操作（例如，在使用高峰期间创建卷快照、在无法支持所需 I/O 带宽的实例上运行卷、第一次访问卷上的数据，等等）而造成的暂时状况。

使用受损的卷

如果卷受损，请使用以下选项，因为卷的数据可能不一致。

选项

- 选项 1：对附加到其实例的卷执行一致性检查 (p. 1362)
- 选项 2：使用其他实例对该卷执行一致性检查 (p. 1362)
- 选项 3：如果您不再需要卷，请将其删除 (p. 1363)

选项 1：对附加到其实例的卷执行一致性检查

最简单的选择是使能 I/O，然后在卷上进行一次数据一致性检查，但该卷仍附加到它的 Amazon EC2 实例。

想要在一个附加的卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 在该卷上使能 I/O。使用以下方法之一。

   Console

   1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   2. 在导航窗格中，选择 Events。
   3. 选择要使能 I/O 操作的卷。
   4. 选择 Actions（操作）、Enable I/O（启用输入/输出）。

   Amazon CLI

   使用命令行启用卷的 I/O

   您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

   - enable-volume-io (Amazon CLI)
   - Enable-EC2VolumeIO (Amazon Tools for Windows PowerShell)
3. 检查卷上数据。

   a. 运行 fsck 命令。
   b. （可选）查看所有适用的应用程序或系统日志以了解相关错误消息。
   c. 如果卷受损时间超过 20 分钟，您可以联系 Amazon 支持中心。选择问题排查，然后在状态检查故障排除对话框上选择联系客户服务提交一个支持案例。

选项 2：使用其他实例对该卷执行一致性检查

按照以下程序在您的产品环境外检查该卷。

Important

当卷 I/O 被禁用时，这些程序可能会导致挂起的写入 I/O 丢失。

想要在一个隔离环境中在一个卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 将该卷从实例中分离。有关更多信息，请参阅从 Linux 实例分离 Amazon EBS 卷 (p. 1364)。

3. 在该卷上使能 I/O。使用以下方法之一。

   Console

   1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   2. 在导航窗格中，选择 Events。
   3. 选择您在之前的步骤中分离的卷。
   4. 选择 Actions（操作）、Enable I/O（启用输入/输出）。

   Amazon CLI

   使用命令行启用卷的 I/O

   您可以使用以下命令之一查看卷 Amazon EBS 的事件信息。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

   - enable-volume-io (Amazon CLI)
   - Enable-EC2VolumeIO (Amazon Tools for Windows PowerShell)

4. 将该卷附加到另一个实例。有关更多信息，请参阅启动实例 (p. 574)和将 Amazon EBS 卷挂载到实例 (p. 1347)。
5. 检查卷上数据。

   a. 运行 fsck 命令。
   b. （可选）查看所有适用的应用程序或系统日志以了解相关错误消息。
   c. 如果卷受损时间超过 20 分钟，您可以联系 Amazon 支持中心。选择 Troubleshoot，然后在故障排除对话框中选择 Contact Support 以提交支持案例。

选项 3：如果您不再需要卷，请将其删除

如果您想将该卷从您的环境中去除，只需删除它即可。关于删除一个卷的信息，请查阅删除 Amazon EBS 卷 (p. 1366)。

如果您有在该卷上备份的近期快照，那么您可以从快照中创建一个新卷。有关更多信息，请参阅从快照创建卷 (p. 1346)。

使用自动启用 IO 卷属性

默认情况下，当 Amazon EBS 判定一个卷数据具有潜在不一致性时，它将会禁用从任何附加的 EC2 实例到该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是受损，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用 Auto-Enabled IO (自动启用 IO) 卷属性（API 中的 `autoEnableIO`），卷和实例之间的 I/O 会自动重新启用，并且卷将通过状态检查。此外，您将会看到一个通知您该卷具有潜在不一致状态的事件，但它的 I/O 不会自动启用。如果发生此事件，您应该检查该卷的一致性，如有必要，可对其进行更换。有关更多信息，请参阅EBS 卷事件 (p. 1360)。

您可以使用以下方法查看和修改卷的 Auto-Enabled IO（自动启用输入/输出）属性。

New console

查看卷的“自动启用 IO”属性

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择卷，然后选择 Status checks（状态检查）选项卡。

Auto-enabled I/O（自动启用输入/输出）字段为所选择的卷显示当前设置：Enabled（已启用）或 Disabled（已禁用）。

修改卷的“自动启用 IO”属性

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions（操作）、Manage auto-enabled I/O（管理自动启用的输入/输出）。
4. 选中 Auto-enable I/O for impaired volumes（为受损卷自动启用输入/输出）复选框，以便为受损卷自动启用输入/输出。想要禁用该功能，请清除复选框。
5. 选择更新。

Amazon CLI

查看卷的 autoEnableIO 属性

使用以下命令之一。

- describe-volume-attribute (Amazon CLI)
- Get-EC2VolumeAttribute（Amazon Tools for Windows PowerShell）

修改卷的 **autoEnableIO** 属性

使用以下命令之一。

- modify-volume-attribute (Amazon CLI)
- Edit-EC2VolumeAttribute（Amazon Tools for Windows PowerShell）

有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)

从 Linux 实例分离 Amazon EBS 卷

您需要将 Amazon Elastic Block Store (Amazon EBS) 卷与实例分离，然后才能将其挂载到其他实例或删除该卷。分离卷不会影响卷上的数据。

有关从 Windows 实例分离卷的信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的从 Windows 实例分离卷。

主题

- 注意事项 (p. 399)
- 卸载并分离卷 (p. 1365)
- 问题排查 (p. 1365)

注意事项

- 您可以明确地将 Amazon EBS 卷与实例分离，或终止实例。但是，如果实例正在运行，您首先必须从实例卸载卷。
- 如果 EBS 卷是实例的根设备，则在分离卷之前必须停止该实例。

- 您可以重新附加分离的卷（无需卸载），但可能不能获得相同挂载点。如果分离时正在写入卷，那么卷上的数据可能不同步。
- 分离卷之后，只要存储量超出了 AmazonFree Tier（免费套餐）的限额，您仍需为卷存储付费。您必须删除卷以避免产生更多费用。有关更多信息，请参阅删除 Amazon EBS 卷 (p. 1366)。

卸载并分离卷

使用以下程序从实例卸载并分离卷。当您需要将卷挂载到不同实例时或当您需要删除卷时，此操作非常有用。

步骤

- 第 1 步：卸载卷 (p. 1365)
- 第 2 步：从实例分离卷 (p. 1365)

第 1 步：卸载卷

从 Linux 实例中，使用以下命令卸载 /dev/sdh 设备。

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

第 2 步：从实例分离卷

要将卷与实例分离，请使用以下方法之一：

Console

使用控制台将 EBS 卷分离

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择需要分离的卷，然后选择 Actions（操作）、Detach Volume（分离卷）。
4. 当系统提示进行确认时，选择分离。

Command line

使用命令行将 EBS 卷从实例分离

卸载卷后，您可以使用下列命令之一来分离卷。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- detach-volume (Amazon CLI)
- Dismount-EC2Volume (Amazon Tools for Windows PowerShell)

问题排查

以下内容介绍在分离卷时遇到的常见问题并以及如何解决这些问题。

Note

要防止出现数据丢失的可能性，请在尝试卸载之前为您的卷制作快照。强制分离一个状态卡住的卷可能对文件系统或其中包含的数据造成破坏，或者除非重启实例，否则无法使用同样的设备名称附加新卷。

- 如果在通过 Amazon EC2 控制台分离卷时遇到问题，您可使用 describe-volumes CLI 命令来诊断问题。有关更多信息，请参阅 describe-volumes。
- 如果您的卷处于 `detaching` 状态，您可以通过选择 Force Detach 强制执行分离操作。请将该选项仅用作在不得已的情况下从故障实例分离卷的方法，或是在要删除卷的情况下分离卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用该选项，则必须执行文件系统检查和修复流程。
- 如果在几分钟内多次尝试强制分离卷，并且该卷处于 `detaching` 状态，则可以向 Amazon EC2 论坛发布帮助请求。为了帮助加快解决问题，请提供卷 ID 并描述已采取的步骤。
- 如果尝试分离仍挂载的卷，该卷可能在尝试分离时卡在 `busy` 状态。describe-volumes 的以下输出说明了这种情况：

```
"Volumes": [
    {
        "AvailabilityZone": "us-west-2b",
        "Attachments": [
            {
                "AttachTime": "2016-07-21T23:44:52.000Z",
                "InstanceId": "i-fedc9876",
                "VolumeId": "vol-1234abcd",
                "State": "busy",
                "DeleteOnTermination": false,
                "Device": "/dev/sdf"
            }
        ...
    }
]
```

如果遇到这种状态，可能无限期延迟分离，直到您卸载卷，强制分离，重启实例，或者执行前述全部三项操作。

删除 Amazon EBS 卷

如果您不再需要某个 Amazon EBS 卷，可以将其删除。删除后，卷上的数据都不复存在，并且再也不能附加到任何实例。然而，您可在删除之前保存卷的快照，以便以后可以使用该快照重新创建卷。

> **Note**
>
> 无法删除连接到实例的卷。要删除卷，必须先将其与实例分离。有关更多信息，请参阅从 Linux 实例分离 Amazon EBS 卷 (p. 1364)。
> 您可以检查卷是否已连接到实例。在控制台的卷页面上，可以查看卷的状态。
>
> - 如果卷已连接到实例，则会处于`in-use`状态。
> - 如果卷已与实例分离，则会处于`available`状态。您可以删除此卷。

您可以使用以下方法之一删除 EBS 卷。

Console

使用控制台删除 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择需要删除的卷，然后选择 Actions（操作）、Delete Volume（删除卷）。

   > **Note**
   >
   > 如果 Delete volume（删除卷）显示为灰色，则表示该卷已连接到实例。您必须先将卷与实例分离，然后才能将其删除。

4. 在确认对话框中，选择 Delete (删除)。

Amazon CLI

使用命令行删除 EBS 卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- delete-volume (Amazon CLI)
- Remove-EC2Volume (Amazon Tools for Windows PowerShell)

在 Amazon EBS 上进行故障测试

使用 Amazon Fault Injection Simulator 和“暂停 I/O”操作暂时停止 Amazon EBS 卷与其附加实例之间的 I/O，以测试工作负载如何处理 I/O 中断。借助 Amazon FIS，您可以使用受控实验来测试架构和监控，例如 Amazon CloudWatch 告警和操作系统超时配置，并提高应对存储故障的弹性。

有关 Amazon FIS 的更多信息，请参阅 Amazon Fault Injection Simulator 用户指南。

注意事项

暂停卷 I/O 时请注意以下事项：

- 可以为附加到在 Nitro System 上构建的实例 (p. 246)的所有 Amazon EBS 卷类型暂停 I/O。
- 可以为根卷暂停 I/O。
- 可以为启用多重挂载的卷暂停 I/O。如果为已启用多重挂载的卷暂停 I/O，则该卷及其所有附加实例之间将暂停 I/O。
- 要测试操作系统超时配置，请将实验持续时间设置为等于或大于为 `nvme_core.io_timeout` 指定的值。有关更多信息，请参阅I/O 操作超时 (p. 1522)。
- 如果提升对已暂停 I/O 卷的 I/O，会发生以下情况：
  - 卷的状态将在 120 秒内转换为 `impaired`。有关更多信息，请参阅监控您的卷状态 (p. 1359)。
  - 队列长度 (`VolumeQueueLength`) 的 CloudWatch 指标将为非零。任何告警或监控都应监控非零队列深度。有关更多信息，请参阅挂载到所有实例类型的卷的卷指标 (p. 1564)。
  - `VolumeReadOps` 或 `VolumeWriteOps` 的 CloudWatch 指标将为 `0`，这表明该卷不再处理 I/O。

限制

暂停卷 I/O 时请注意以下限制：

- 不支持实例存储卷。
- 不支持基于 Xen 的实例类型。
- 您无法为 Amazon Outposts、Amazon Wavelength 区域或 Local Zone 中 Outpost 上创建的卷暂停 I/O。
- “暂停 I/O”操作在 Amazon GovCloud (US) Regions 中不可用。

您可以从 Amazon EC2 控制台执行基础实验，也可以使用 Amazon FIS 控制台执行更高级的实验。有关使用 Amazon FIS 控制台执行高级实验的更多信息，请参阅《Amazon Fault Injection Simulator 用户指南》中的 Amazon FIS 教程。

使用 Amazon EC2 控制台执行基础实验

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Volumes。
3. 选择要为其暂停 I/O 的卷，然后选择操作、错误注入、暂停卷 I/O。
4. 对于持续时间，输入要在卷和实例之间暂停 I/O 的持续时间。“持续时间”下拉列表旁边的字段将以 ISO 8601 格式显示持续时间。
5. 在服务访问权限部分中，选择 Amazon FIS 执行实验所担任的 IAM 服务角色。您可以使用默认角色，也可以使用您创建的现有角色。有关更多信息，请参阅为 Amazon FIS 创建 IAM 角色。
6. 选择暂停卷 I/O。系统提示时，在确认字段中输入 `start` 并选择开始实验。
7. 监控实验的进度和影响。有关更多信息，请参阅《Amazon FIS 用户指南》中的监控 Amazon FIS。

Amazon EBS 快照

您可以通过拍摄时间点快照将 Amazon EBS 卷上的数据备份到 Amazon S3。快照属于增量 备份，这意味着仅保存设备上在最新快照之后更改的数据块。由于无需复制数据，这将最大限度缩短创建快照所需的时间和增加存储成本节省。每个快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。

当您基于快照创建新 EBS 卷时，新卷将开始作为用于创建快照的原始卷的精确副本。复制的卷将在后台加载数据，让您可以立即开始使用数据。如果您访问尚未加载的数据，则卷将立即从 Amazon S3 下载请求的数据，然后继续在后台加载卷的剩余数据。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。

删除快照时，仅会删除该快照特有的数据。有关更多信息，请参阅删除 Amazon EBS 快照 (p. 1375)。

快照事件

您可以通过 CloudWatch Events 跟踪 EBS 快照的状态。有关更多信息，请参阅EBS 快照事件 (p. 1572)。

多卷快照

快照可用于创建关键工作负载的备份，如跨多个 EBS 卷的大型数据库或文件系统。利用多卷快照，您可以跨附加到 EC2 实例的多个 EBS 卷拍摄准确的时间点、数据协调和崩溃一致性快照。您不再需要停止实例或在多个卷之间协调来确保崩溃一致性，因为快照将跨多个 EBS 卷自动进行拍摄。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)下创建多卷 EBS 快照的步骤。

快照定价

快照的费用取决于存储的数据量。由于快照是增量的，因此删除快照可能不会降低您的数据存储成本。删除快照时，专由某个快照引用的数据将被删除，但保留其他快照引用的数据。有关更多信息，请参阅 Amazon Billing 用户指南中的 Amazon Elastic Block Store 卷和快照。

目录

- 快照的工作原理 (p. 1369)
- 复制和共享快照 (p. 1371)
- 快照的加密支持 (p. 1371)
- 创建 Amazon EBS 快照 (p. 1372)
- 删除 Amazon EBS 快照 (p. 1375)
- 复制 Amazon EBS 快照 (p. 1377)
- 归档 Amazon EBS 快照 (p. 1381)
- 查看 Amazon EBS 快照信息 (p. 1402)
- 共享 Amazon EBS 快照 (p. 1403)
- 从回收站中还原快照 (p. 1407)
- Amazon EBS local snapshots on Outposts (p. 1409)

- 使用 EBS direct API 访问 EBS 快照的内容 (p. 1418)
- 自动化快照生命周期 (p. 1448)

快照的工作原理

您从卷创建的第一个快照始终是完整快照。它包括创建快照时写入卷的所有数据块。同一卷的后续快照为增量快照。这些快照仅包括自上次创建快照以来写入卷的已更改数据块和新数据块

完整快照的大小取决于备份数据的大小，而非源卷的大小。同样地，与完整快照相关的存储成本取决于快照的大小，而非源卷的大小。例如，您创建了仅包含 50 GiB 数据的 200 GiB Amazon EBS 卷的第一个快照。这会生成大小为 50 GiB 的完整快照，并且您需要为 50 GiB 快照存储付费。

同样，增量快照的大小和存储成本取决于自上次快照创建以来写入卷的任何数据的大小。继续此示例，如果您在更改 20 GiB 数据和添加 10 GiB 数据后创建 200 GiB 卷的第二个快照，则增量快照的大小为 30 GiB。然后，您需要为额外的 30 GiB 快照存储付费。

有关快照定价的更多信息，请参阅 Amazon EBS 定价。

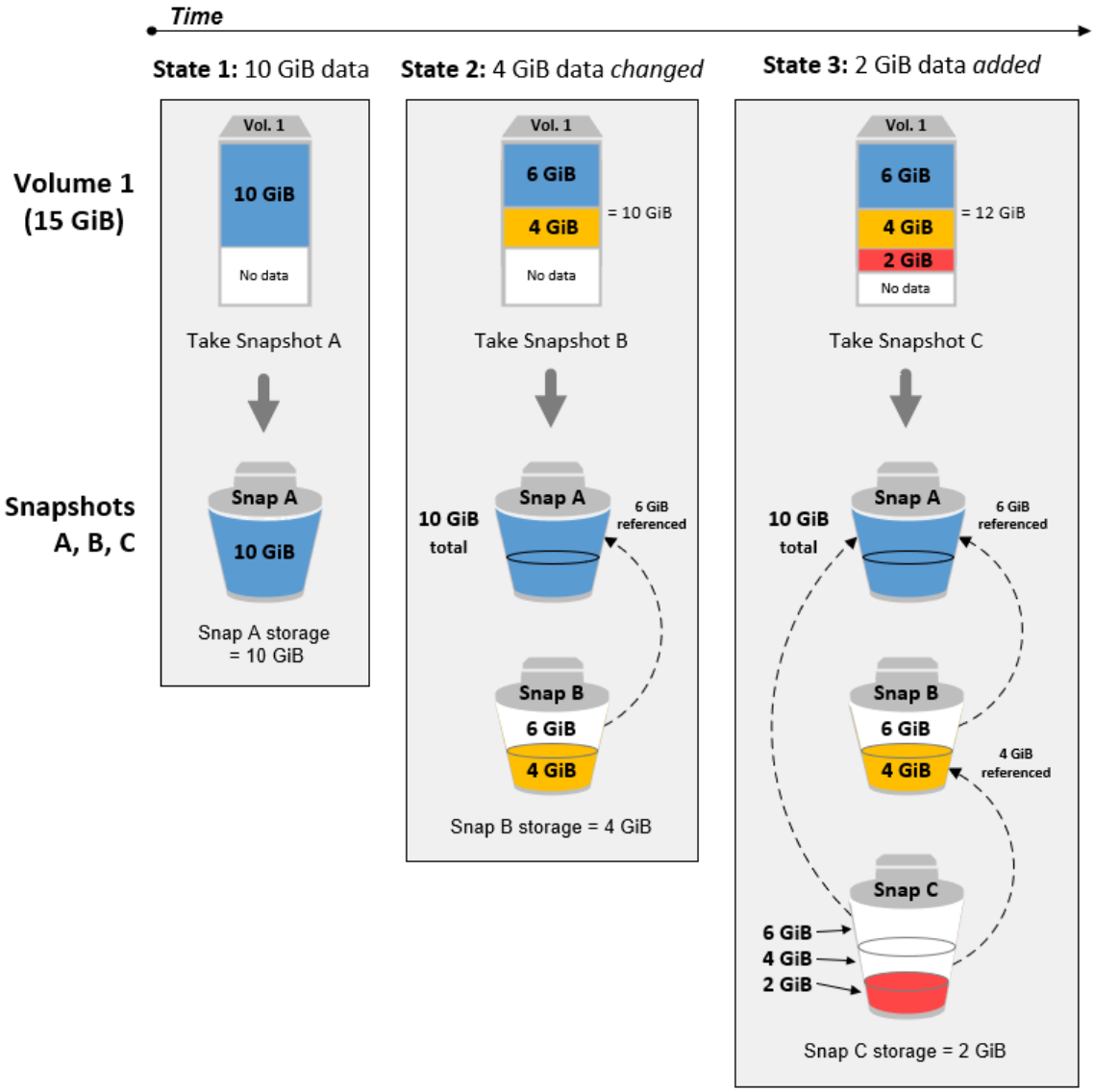
> **Important**
>
> 归档增量快照时，增量快照将转换为完整快照，其中包括创建快照时写入卷的所有块。然后，快照将移动到 Amazon EBS 快照归档层。归档层中的快照费率与标准层中的快照费率不同。有关更多信息，请参阅定价和计费 (p. 1382)。

以下部分阐述了 EBS 快照如何捕获卷在某一时间点的状态，以及正在更改的卷的后续快照如何创建这些更改的历史记录。

同一卷的多个快照

在本部分的图表中，大小为 15 GiB 的卷 1 在 3 个时间点上显示。为这三个卷状态分别制作快照。该图表明确显示以下内容：

- 在状态 1 中，该卷具有 10 GiB 数据。快照 A 是为该卷制作的第一个快照。快照 A 是完整快照，所有 10 GiB 数据均已备份。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，捕获快照 A 后仅 4 GiB 数据发生更改。快照 B 是增量快照。只需要备份已更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已在快照 A 中备份）将由快照 B 引用，而不会再次备份。这通过虚线箭头指示。
- 在状态 3 中，捕获快照 B 后，2 GiB 数据已添加到该卷中，共计 12 GiB 数据。快照 C 是增量快照。只需要对捕获快照 B 之后添加的 2 GiB 数据进行备份。如虚线箭头所示，快照 C 还引用了存储在快照 B 中的 4 GiB 数据和存储在快照 A 中的 6 GiB 数据。
- 三个快照共需 16 GiB 存储空间。这相当于快照 A 需要 10 GiB，快照 B 需要 4 GiB，快照 C 需要 2 GiB。



不同卷的增量快照

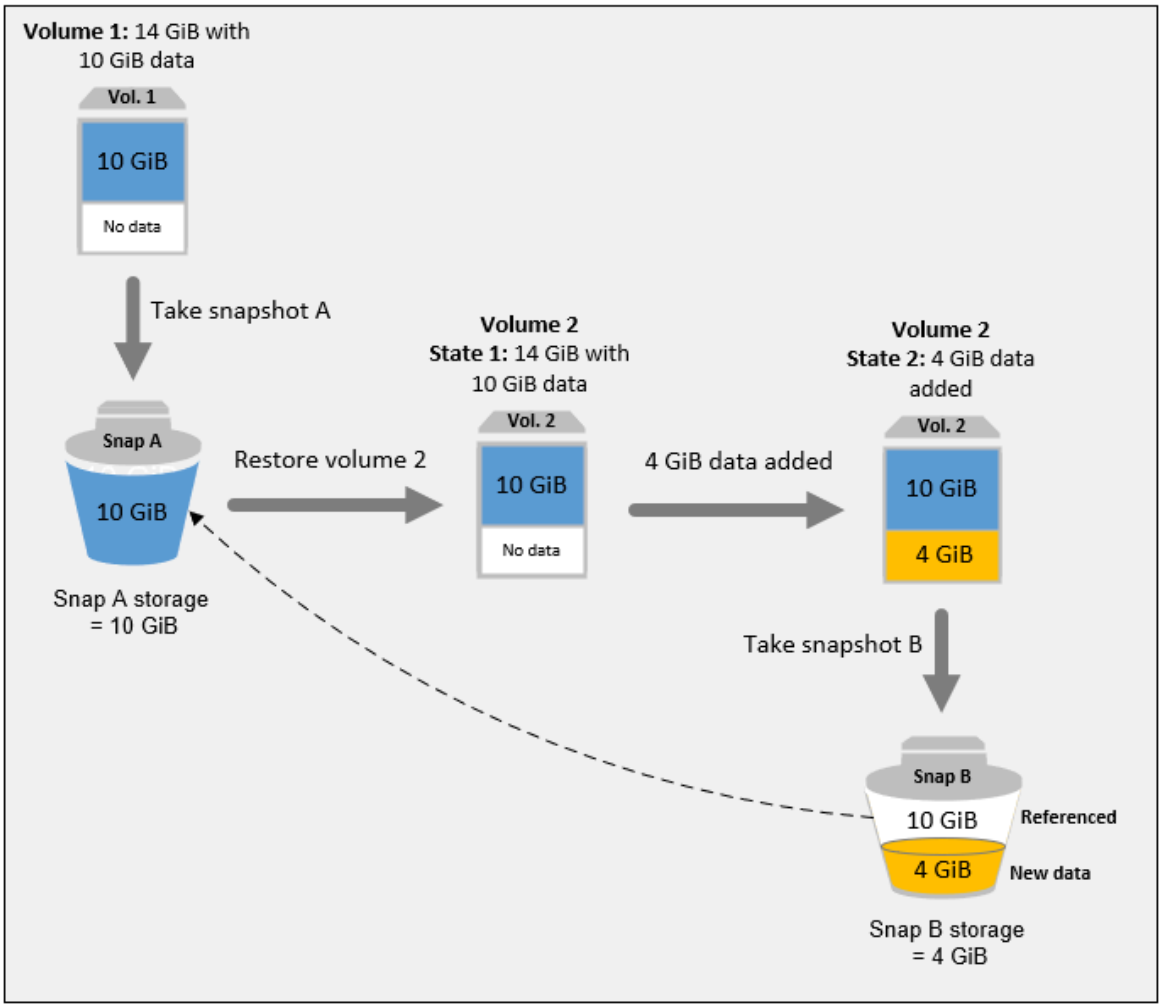
本节中的图表显示了如何从不同卷获取增量快照。

1. 大小为 14 GiB 的卷 1 包含 10 GiB 数据。因为快照 A 是为该卷捕获的首个快照，是完整快照，因此会备份所有 10 GiB 数据。
2. 卷 2 是从快照 A 创建的，所以它是卷 1 在拍摄快照时的精准副本。
3. 随着时间的推移，4 GiB 的数据将添加到卷 2，并且其数据总大小为 14 GiB。
4. 快照 B 是基于卷 2 制作的。对于快照 B，仅备份从快照 A 创建卷后添加的 4 GiB 数据。未更改的其他 10 GiB 数据（已存储在快照 A 中）将由快照 B 引用，而不会再次备份。

   快照 B 是快照 A 的增量快照，即使它是从不同的卷创建的。

Important

该图表假定您拥有卷 1 和快照 A，并且卷 2 使用与卷 1 相同的 KMS 密钥进行加密。如果卷 1 归另一个 Amazon 账户所有，并且该账户捕获了快照 A 并将其与您共享，则快照 B 将是完整快照。或者，如果卷 2 使用与卷 1 不同的 KMS 密钥进行加密，则快照 B 将是完整快照。



有关删除快照后如何管理数据的更多信息，请参阅删除 Amazon EBS 快照 (p. 1375)。

复制和共享快照

您可通过修改快照的访问权限来跨 Amazon 账户共享快照。您可以复制您拥有的快照以及与您共享的快照。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

快照受限于创建它的 Amazon 区域。在您创建 EBS 卷的快照之后，可在同一个区域中使用它来创建新卷。有关更多信息，请参阅从快照创建卷 (p. 1346)。您还可以跨区域复制快照，从而能够使用多个区域进行地理扩展、数据中心迁移和灾难恢复。您可以复制具有 `completed` 状态的任何可访问快照。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。

快照的加密支持

EBS 快照完全支持 EBS 加密。

- 加密卷的快照会自动加密。

- 通过加密快照创建的卷会自动加密。
- 您从已拥有或有权访问的未加密快照创建的卷可进行动态加密。
- 在复制您拥有的未加密快照时，您可以在复制过程中对其加密。
- 在复制您拥有或有权访问的加密快照时，可在复制过程中使用其他密钥对其重新加密。
- 对于从未加密的快照中创建的加密卷，拍摄的第一个快照始终是完整快照。
- 为重新加密的卷拍摄的第一个快照（具有与源快照不同的 CMK）始终是完整快照。

创建 Amazon EBS 快照 (p. 1372) 和 复制 Amazon EBS 快照 (p. 1377) 中提供了可能的快照加密方案的完整文档。

有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

创建 Amazon EBS 快照

您可以创建 EBS 卷的时间点快照，并将其用作新卷的基准或用于数据备份。如果您定期为卷拍摄快照，则快照为增量快照，新快照上仅保存自上次快照后已更改的块。

快照是异步制作的；时间点快照是立即创建的，但在快照完成（当所有已修改数据块都已转移到 Amazon S3 时）之前，其状态为 `pending`，很多大型初始快照或后续快照（其中的数据块已更改）可能需要几个小时才能完成。执行期间，正在进行的快照不会受到同时发生的卷读写操作的影响。

您可以制作正在使用的已附加卷的快照。但是，快照只能捕获发出快照命令时已经写入您的 Amazon EBS 卷的数据。其中可能不包括已由任何应用程序或操作系统缓存的任何数据。如果您可以将该卷的所有文件写入暂停足够长的时间以制作快照，则快照应该是完整的。但是，如果您无法暂停该卷的所有文件写入，则应该从实例中卸载该卷、发出快照命令，然后重新安装该卷，以确保获得一致且完整的快照。当快照状态为 `pending` 时，您可以重新挂载并使用卷。

要简化快照的管理，您可以在创建期间为快照添加标签，也可在创建后添加。例如，您可以应用标记，描述该快照对应的原始卷，或描述用于将原始卷附加到实例上的设备名称。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

快照加密

从加密卷制作的快照会自动加密。通过加密快照创建的卷也会自动加密。加密卷及所有关联快照中的数据在静态或传输过程中均受到保护。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。

默认情况下，只有您可以从您拥有的快照创建卷。但是，您可以将未加密的快照将共享给特定 Amazon 账户，还可通过将其设为公开来与整个 Amazon 社区共享。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

您仅可以将加密快照共享给特定 Amazon 账户。要让其他账户使用您共享的加密快照，您还必须与其共享用于加密该快照的 CMK 密钥。获取了您的加密快照访问权限的用户必须先自行创建该快照的副本，然后使用该副本。还可以使用其他密钥重新加密您的共享加密快照的副本。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

多卷快照

您可以创建多卷快照，这些快照是附加到实例的所有或某些卷的时间点快照。

默认情况下，您从实例创建多卷快照时，Amazon EBS 会创建附加到该实例的所有卷 [根和数据（非根）] 的快照。不过，您可以选择创建附加到实例的卷子集的快照。

您可以标记多卷快照，就像您使用单个卷快照执行的操作一样。我们建议您标记多个卷快照以在还原、复制或保留操作期间集中管理它们。还可以选择自动将标签从源卷复制到相应的快照。这将帮助您设置快照元数据（如访问策略、附件信息和成本分配）以匹配源卷。

创建快照后，每个快照将视为单个快照。您可以执行所有快照操作，如还原、删除和跨区域或账户复制，就像您使用单个卷快照执行的操作一样。

多卷、崩溃一致性快照通常以集的形式进行还原。这有助于通过使用实例 ID、名称或其他相关详细信息标记您的集，以标识位于崩溃一致性快照集中的快照。

创建快照后，它们会在确切的时间点创建时显示在您的 EC2 控制台中。

如果多卷快照集的任何一个快照失败，所有其他快照将显示错误状态，并将 `createSnapshots` CloudWatch 事件的 `failed` 结果发送到您的 Amazon 账户。有关更多信息，请参阅创建多个快照 (createSnapshots) (p. 1573)。

Amazon Data Lifecycle Manager

您可以创建快照生命周期策略来自动创建和保留单个卷快照和实例的多卷快照。有关更多信息，请参阅Amazon Data Lifecycle Manager (p. 1448)。

注意事项

创建快照时需考虑以下事项：

- 当您为充当根设备的 EBS 卷创建快照时，建议您在拍摄快照之前停止实例。
- 您不能从启用了休眠的实例或从已休眠实例创建快照。如果您从已休眠或已启用休眠的实例创建快照或 AMI，则可能无法连接到从该 AMI 启动的新实例，或者通过从快照创建的 AMI 启动的新实例。
- 尽管您可以在某个卷的前一个快照处于 `pending` 状态时拍摄该卷的快照，但一个卷有多个 `pending` 快照可能会导致该卷的性能降低，直至这些快照完成。
- 单个 `pending` 或 `st1` 卷限制为一个 `sc1` 快照，其他卷类型的单个卷限制为五个 `pending` 快照。如果您在尝试给同一个卷创建多个并发快照时收到 `ConcurrentSnapshotLimitExceeded` 错误，请等待一个或多个 `pending` 快照完成，然后再为该卷创建另一个快照。
- 如果快照从具有 Amazon Web Services Marketplace 产品代码的卷创建，产品代码将传播到快照。
- 从实例创建多卷快照集时，最多可以指定 40 个要排除的数据（非根）卷。

创建快照

要从指定的卷中创建快照，请使用以下方法之一。

Console

使用控制台创建快照

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots（快照）、Create snapshot（创建快照）。
3. 对于 Resource type (资源类型)，选择 Volume (卷)。
4. 对于 Volume ID（卷 ID），选择需要从其创建快照的卷。

   Encryption（加密）字段指示所选卷的加密状态。如果选定的卷已加密，则使用相同的 KMS 密钥自动加密快照。如果选定的卷未加密，则不会对快照进行加密。
5. （可选）对于 Description (描述)，输入对快照的简短描述。
6. （可选）要为快照分配自定义标签，请在 Tags（标签）部分选择 Add tag（添加标签），然后输入标签键和值对。您最多可以添加 50 个标签。
7. 选择 Create snapshot (创建快照)。

Amazon CLI

使用命令行创建快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-snapshot (Amazon CLI)
- New-EC2Snapshot(Amazon Tools for Windows PowerShell)

创建多卷快照

从实例创建多卷快照集时，您可以选择是否从源卷将标签复制到相应的快照。您可以指定是否创建根卷的快照。您还可以指定是为附加到实例的所有数据（非根）卷创建快照，还是为这些卷的子集创建快照。

注意事项

- 多卷快照为每个实例支持多达 40 个 EBS 卷。

要从实例的卷中创建快照，请使用以下方法之一。

Console

使用控制台创建多卷快照

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots（快照）、Create snapshot（创建快照）。
3. 对于 Resource type (资源类型)，选择 Instance (实例)。
4. 对于 Description （描述），输入快照的简短描述。此描述适用于所有快照。
5. （可选）默认情况下，Amazon EBS 会创建实例根卷的快照。如果您不想创建实例根卷的快照，请选择 Exclude root volume（排除根卷）。
6. （可选）默认情况下，Amazon EBS 会创建附加到实例的所有数据（非根）卷的快照。如果您想创建附加到实例的数据（非根）卷子集的快照，请选择 Exclude specific data volumes（排除特定数据卷）。Attached data volumes（附加的数据卷）部分列出了当前附加到所选实例的所有数据卷。

   在 Attached data volumes（附加的数据卷）部分，选择您不想为其创建快照的数据卷。只有未选中的卷才会包含在多卷快照集中。最多可以排除 40 个卷。
7. （可选）若要自动将标签从源卷复制到相应快照，请为 Copy tags from source volume（从源卷复制标签）选择 Copy tags（复制标签）。这将设置快照元数据（如访问策略、附件信息和成本分配）以匹配源卷。
8. （可选）若要为快照分配自定义标签，请在 Tags（标签）部分选择 Add tag（添加标签），然后输入键值对。您最多可以添加 50 个标签。
9. 选择 Create snapshot (创建快照)。

   快照创建期间，将一起管理快照。如果卷集中的其中一个快照失败，则其他快照将移至卷集的错误状态。您可以使用 CloudWatch Events 监控快照的进度。在快照创建过程完成后，CloudWatch 将生成一个事件，其中包含受影响实例的状态及所有相关的快照详细信息。

Command line

Amazon CLI

若要使用 Amazon CLI 创建多卷快照，请使用 create-snapshots 命令。

如果您不想创建根卷的快照，请为 `--instance-specification ExcludeBootVolume` 指定 `true`。如果您不想创建附加到实例的所有数据（非根）卷的快照，对于 `--instance-specification ExcludeDataVolumes`，请指定不想为其创建快照的数据卷 ID。您最多可以指定 40 个要排除的卷。

Amazon Tools for Windows PowerShell

若要使用 Tools for Windows PowerShell 创建多卷快照，请使用 New-EC2SnapshotBatch 命令。

如果您不想创建根卷的快照，请为 `-InstanceSpecification_ExcludeBootVolume` 指定 1。如果您不想创建附加到实例的所有数据（非根）卷的快照，对于 `-InstanceSpecification_ExcludeDataVolumes`，请指定不想为其创建快照的数据卷 ID。您最多可以指定 40 个要排除的卷。

如果所有快照都成功完成，`createSnapshots` CloudWatch 事件的 `succeeded` 结果将发送到您的 Amazon 账户。如果多卷快照集的任何一个快照失败，所有其他快照将显示错误状态，并将 `createSnapshots` CloudWatch 事件的 `failed` 结果发送到您的 Amazon 账户。有关更多信息，请参阅创建多个快照 (createSnapshots) (p. 1573)。

使用 EBS 快照

您可以复制快照、共享快照和从快照创建卷。有关更多信息，请参阅下列内容：

- 复制 Amazon EBS 快照 (p. 1377)
- 共享 Amazon EBS 快照 (p. 1403)
- 从快照创建卷 (p. 1346)

删除 Amazon EBS 快照

当您不再需要卷的 Amazon EBS 快照后，可以将其删除。删除快照对卷没有影响。删除卷对从它生成的快照无任何影响。

增量快照删除

如果定期拍摄卷快照，则这些快照为增量快照。这意味着该设备上在您的最新快照之后更改的数据块将保存在新快照中。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以创建卷。

如果数据存在于早期的单个快照或一系列快照中保存的卷上，并且该数据随后从卷中删除，则该数据仍被视为早期快照的唯一数据。只有引用唯一数据的所有快照都被删除，该唯一数据才会从快照序列中删除。

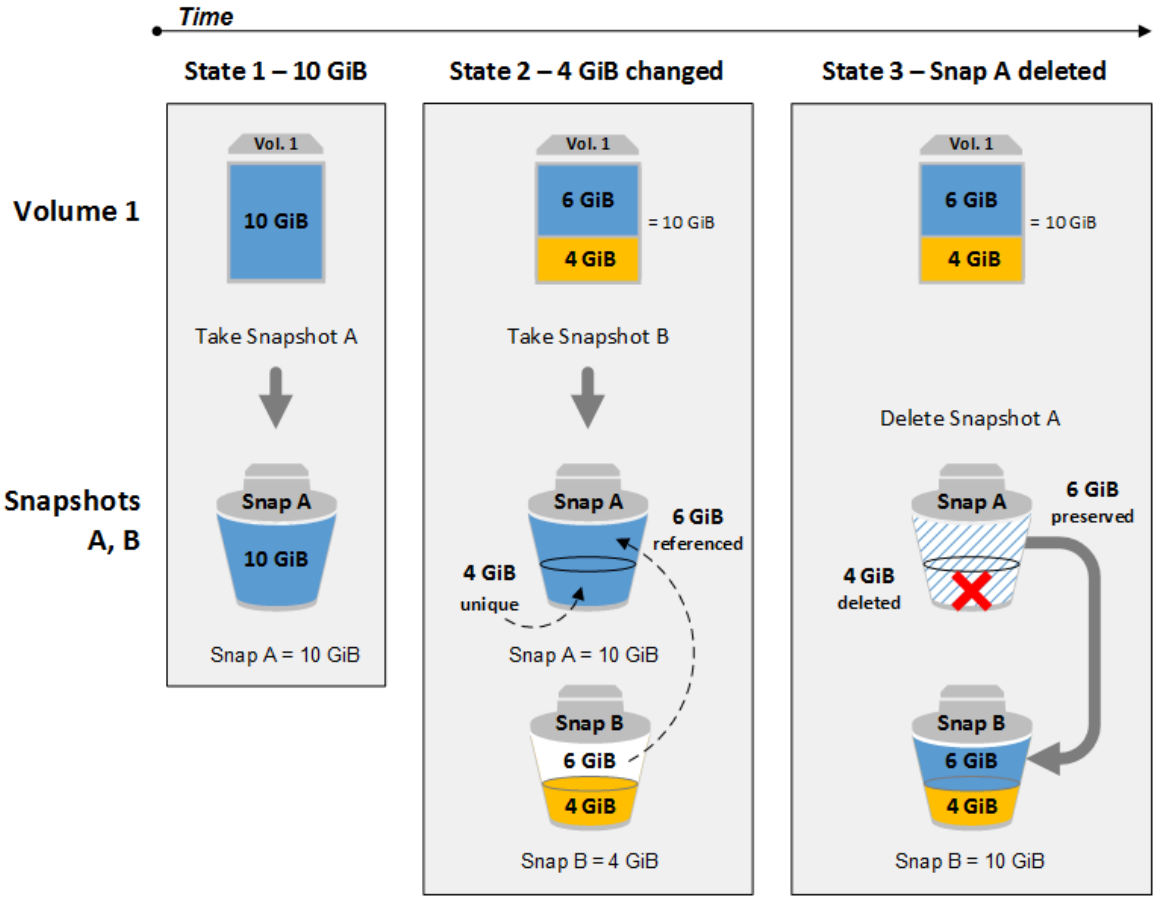
删除快照时，仅删除该快照专门引用的数据。只有在删除引用唯一数据的所有快照时，才会删除该唯一数据。删除卷的之前快照不会影响您使用该卷的之后快照创建卷的能力。

删除快照可能不会降低组织的数据存储成本。其他快照可引用已删除快照的数据，已引用的数据总是会被保留。如果您删除了一个快照，而该快照包含以后的快照使用的数据，那么与所引用数据关联的成本将分配到后来的快照。有关快照如何存储数据的更多信息，请参阅快照的工作原理 (p. 1369)和下面的示例。

在下图中，卷 1 在三个时间点上显示。某个快照已捕获前两种状态，在第三种状态中，某个快照已被删除。

- 在状态 1 中，该卷具有 10 GiB 数据。因为快照 A 是为该卷制作的首个快照，因此必须复制所有 10 GiB 数据。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，4 GiB 数据已更改。快照 B 只需复制并存储制作快照 A 后更改的 4 GiB 数据。未更改的其他 6 GiB 数据 (已复制并存储在快照 A 中) 将由快照 B 引用 而不是再次复制。这通过虚线箭头指示。
- 在状态 3 中，卷自状态 2 以来未更改，但快照 A 已被删除。快照 B 引用的存储在快照 A 中的 6 GiB 数据现已移至快照 B，如粗箭头所示。因此，您仍需支付存储 10 GiB 数据的费用；快照 A 中保留的 6 GiB 未更改数据和快照 B 中的 4 GiB 已更改数据。

删除快照及其由其他快照引用的部分数据



注意事项

删除快照时需考虑以下事项：

- 您不能删除注册 AMI 使用的 EBS 卷的根设备快照。您必须先注销 AMI，然后才能删除快照。有关更多信息，请参阅注销您的 AMI (p. 188)。
- 您无法删除由 Amazon Backup 服务使用 Amazon EC2 管理的快照。而是应该使用 Amazon Backup 删除备份文件库中相应的恢复点。有关更多信息，请参阅 Amazon Backup 开发人员指南中的删除备份。
- 您可以手动创建、保留和删除快照，也可以使用 Amazon Data Lifecycle Manager 来管理快照。有关更多信息，请参阅Amazon Data Lifecycle Manager (p. 1448)。
- 尽管您可以删除仍在制作的快照，但该快照必须先完成，删除才能生效。这可能需要较长时间。如果您还具有并发快照限制，而您尝试再制作一个快照，可能会遇到 `ConcurrentSnapshotLimitExceeded` 错误。有关更多信息，请参阅 Amazon Web Services General Reference 中的适用于 Amazon EBS 的 Service Quotas。
- 如果您删除符合回收站保留规则的快照，快照将保留在回收站中，而不是立即删除。有关更多信息，请参阅回收站 (p. 1627)。

删除快照

要删除快照，请使用以下方法之一。

Console

如需使用控制台删除快照

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择要删除的快照，然后选择 Actions（操作）、Delete snapshot（删除快照）。
4. 选择 Delete (删除)。

Amazon CLI

使用命令行删除快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- delete-snapshot (Amazon CLI)
- Remove-EC2Snapshot（Amazon Tools for Windows PowerShell）

删除多卷快照

要删除多卷快照，请使用您在创建快照时应用于多卷快照集的标签检索集的所有快照。然后，分别删除这些快照。

系统不会阻止您删除多卷快照集中的各个快照。如果在 `pending state` 中删除快照，则只删除该快照。多卷快照集中的其他快照仍成功保留。

复制 Amazon EBS 快照

利用 Amazon EBS，您可以创建卷的时间点快照，我们为您将其存储在 Amazon S3 中。创建快照并且已完成到 Amazon S3 的复制（快照状态为 `completed` 时）后，您可将快照从一个 Amazon 区域复制到另一个区域，也可在相同区域内复制。Amazon S3 服务器端加密（256 位 AES）可在复制操作期间保护传输中的快照数据。快照副本将获得与原始快照 ID 不同的 ID。

要将多卷快照复制到另一个 Amazon 区域，请使用您在创建快照时应用于多卷快照集的标签检索快照。然后分别将快照复制到另一个区域。

如果希望另一账户能够复制您的快照，您必须修改快照权限以允许访问该账户，或使快照公开可用，以便所有 Amazon 账户均可复制它。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

有关复制 Amazon RDS 快照的信息，请参阅 Amazon RDS 用户指南 中的复制数据库快照。

使用案例

- 地理扩展：在新 Amazon 区域中启动您的应用程序。
- 迁移：将应用程序迁移到新区域，以实现更好的可用性以及最大限度地降低成本。
- 灾难恢复：在不同的地理位置定期备份您的数据和日志。出现灾难情况时，您可以使用辅助区域存储的时间点备份恢复您的应用程序。该操作能够让数据丢失和恢复时间降至最低。
- 加密：对之前未加密的快照进行加密、更改用于加密快照的密钥，或创建您拥有的副本以从中创建卷（用于与您共享的加密快照）。
- 数据保留和审计要求：将您的加密 EBS 快照从一个 Amazon 账户复制到另一个账户，以保留数据日志或其他文件，便于进行审计或数据保留。使用不同的账户有助于防止意外删除快照，并在您的主要 Amazon 账户遭到泄露时为您提供保护。

先决条件

- 您可以复制任何状态为 `completed` 的可访问快照，包括共享快照和您创建的快照。
- 您可以复制 Amazon Web Services Marketplace、VM Import/Export 和 Storage Gateway 快照，但必须确认目标区域支持该快照。

注意事项

- 每个目标区域限制并发快照复制请求不得超过 `20` 个。如果您超出此配额，会收到 `ResourceLimitExceeded` 错误。如果收到此错误，请等待一个或多个复制请求完成，然后再发出新的快照复制请求。
- 用户定义的标签不会从源快照复制到新快照。您可以在复制操作期间或之后添加用户定义的标签。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。
- 由快照复制操作创建的快照具有一个不应用于任何用途的任意卷 ID。
- 为快照复制操作指定的资源级权限仅适用于新快照。您不能为源快照指定资源级权限。有关示例，请参阅示例：复制快照 (p. 1244)。

定价

- 有关跨 Amazon 区域和账户复制快照的定价信息，请参阅 Amazon EBS 定价。
- 只要快照副本的加密状态不更改，单个账户和区域内的快照复制操作就完全不会复制任何实际数据，因此是免费的。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 如果将快照复制到新区域，则会创建完整（非增量）副本。这会产生额外的存储成本。同一快照的后续副本是增量副本。

增量快照复制

快照副本是否为增量副本是由最近完成的快照复制决定的。在跨区域或账户复制快照时，如果满足以下条件，则副本为增量副本：

- 快照以前已复制到目标区域或账户。
- 最新的快照副本仍位于目标区域或账户中。
- 目标区域或账户中的所有快照副本均未加密，或者是使用同一 KMS 密钥加密的。

如果删除了最新的快照副本，则下一个副本是完整副本，而不是增量副本。如果某个副本在您启动另一个副本时仍处于挂起状态，则第二个副本仅在第一个副本完成后才开始。

增量快照复制会缩短复制快照所需的时间，并且不会复制数据，从而节省数据传输和存储成本。

我们建议您使用卷 ID 和创建时间来标记快照，以便在目标区域或账户中跟踪卷的最新快照副本。

要确定快照副本是否为增量副本，请检查 copySnapshot (p. 1574) CloudWatch 事件。

加密和快照复制

在复制快照时，您可以加密副本，也可以指定一个与原始快照不同的 KMS 密钥，这样，生成的快照副本将使用新 KMS 密钥。但是，在复制操作过程中更改快照的加密状态可能会生成完整（非增量）副本，这可能产生更多的数据传输和存储费用。有关更多信息，请参阅增量快照复制 (p. 1378)。

要复制从其他 Amazon 账户共享的加密快照，您必须拥有使用该快照以及用于加密快照的客户主密钥 (CMK) 的权限。使用与您共享的加密快照时，我们建议您使用您拥有的 KMS 密钥复制快照以对其进行重新加密。这样，即使原始 KMS 密钥泄露或拥有者将其撤销，您也不会失去对使用快照创建的任何加密卷的访问权限。有关更多信息，请参阅共享 Amazon EBS 快照 (p. 1403)。

您可以将 Encrypted 参数设置为 true，以将加密应用到 EBS 快照副本。（如果启用了默认加密 (p. 1507)，Encrypted 参数是可选的）。

或者，您可以使用 KmsKeyId 指定要用于加密快照副本的自定义密钥。（即使启用了默认加密，也必须将 Encrypted 参数设置为 true。）如果未指定 KmsKeyId，则用于加密的密钥取决于源快照的加密状态及其所有权。

下表描述了每种可能的设置组合的加密结果。

主题

- 加密结果：复制您拥有的快照 (p. 1379)
- 加密结果：复制与您共享的快照 (p. 1379)

加密结果：复制您拥有的快照

默认加密	是否设置了 **Encrypted** 参数？	源快照加密状态	默认值（未指定 KMS 密钥）	自定义（已指定 KMS 密钥）
已禁用	否	未加密	未加密	不适用
		已加密	由 Amazon 托管式密钥 加密	
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	
已启用	否	未加密	由默认 KMS 密钥加密	不适用
		已加密	由默认 KMS 密钥加密	
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	

** 这是为复制操作指定的客户托管密钥。将为 Amazon 账户和区域使用此客户托管密钥，而不是使用默认的客户托管密钥。

加密结果：复制与您共享的快照

默认加密	是否设置了 **Encrypted** 参数？	源快照加密状态	默认值（未指定 KmsKeyId）	自定义（已指定 KmsKeyId）
已禁用	否	未加密	未加密	不适用
		已加密	由 Amazon 托管式密钥 加密	

默认加密	是否设置了 **Encrypted** 参数？	源快照加密状态	默认值（未指定 KmsKeyId）	自定义（已指定 KmsKeyId）
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	
已启用	否	未加密	由默认 KMS 密钥加密	不适用
		已加密	由默认 KMS 密钥加密	
	是	未加密	由默认 KMS 密钥加密	由指定的 KMS 密钥加密**
		已加密	由默认 KMS 密钥加密	

** 这是为复制操作指定的客户托管密钥。将为 Amazon 账户和区域使用此客户托管密钥，而不是使用默认的客户托管密钥。

复制快照

要复制快照，请使用以下方法之一。

Console

使用控制台复制快照

1. 打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择要复制的快照，然后选择 Actions（操作）、Copy snapshot（复制快照）。
4. （可选）在 Description（描述）中，输入快照副本的简短描述。

   在默认情况下，描述包括源快照的相关信息，以便您能区别副本和原始内容。您可以按需更改此描述。
5. 对于 Destination Region（目标区域），选择要在其中创建快照副本的区域。
6. 指定快照副本的加密状态。

   如果源快照已加密，或者您的账户已启用默认加密 (p. 1507)，快照副本会自动加密，您无法更改其加密状态。

   如果源快照未加密，并且在默认情况下未为您的账户启用加密，则您可以选择启用或禁用加密。要加密快照副本，请在 Encryption（加密）中选择 Encrypt this snapshot（加密快照）。然后，在 KMS key（KMS 密钥）中，选择要用于对目标区域中的快照进行加密的 KMS 密钥。
7. 选择 Copy snapshot (复制快照)。

Amazon CLI

使用命令行复制快照

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- copy-snapshot (Amazon CLI)
- Copy-EC2Snapshot（Amazon Tools for Windows PowerShell）

检查是否失败

如果您在未获得加密密钥使用权限的情况下试图复制加密快照，则操作将失败，且系统不会提示。您刷新页面后，控制台才会显示错误状态。您还可以通过命令行检查快照的状态，如以下示例所示。

```
aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

如果复制因密钥权限不足而失败，您将看到以下消息："StateMessage": "Given key ID is not accessible"。

在复制加密的快照时，您必须对默认 CMK 具有 `DescribeKey` 权限。显式拒绝这些权限将导致复制失败。有关管理 CMK 密钥的信息，请参阅控制对客户主密钥的访问权限。

归档 Amazon EBS 快照

Amazon EBS 快照归档是一个新存储层，可用于长期低成本地存储很少访问且不需要频繁或快速检索的快照。

默认情况下，快照在创建时将存储在 Amazon EBS 快照标准层中（标准层）。存储在标准层中的快照可递增。这意味着只在卷上保存在最新快照之后发生更改的数据块。

归档快照时，增量快照将转换为完整快照，然后从标准层移动到 Amazon EBS 快照归档层（归档层)。完整快照包括创建快照时写入卷的所有数据块。

当您需要访问归档的快照时，可以将其从归档层还原到标准层，然后像使用账户中任何其它快照一样使用它。

Amazon EBS 快照归档为您存储极少需要访问的快照达 90 天或更长时间，同时存储成本降低 75%。

一些典型的使用案例包括：

- 归档卷的唯一快照，例如项目结束快照
- 出于合规性考虑，请将完整的时间点增量快照归档。
- 归档月度、季度或每年的增量快照。

主题

- 注意事项和限制 (p. 1381)
- 定价和计费 (p. 1382)
- 配额 (p. 1383)
- 归档快照的准则和最佳做法 (p. 1384)
- 所需的 IAM 权限 (p. 1391)
- 使用快照归档 (p. 1392)
- 监控快照归档 (p. 1399)

注意事项和限制

注意事项

- 最短归档期为 90 天。如果您在最短 90 天的归档期限到来之前删除或永久还原已归档的快照，则需要为归档层的剩余天数付费（四舍五入到最接近的小时数）。有关更多信息，请参阅定价和计费 (p. 1382)。

- 将归档快照从归档层还原到标准层最长可能需要 72 小时，具体时间取决于快照的大小。
- 归档的快照始终是完整的快照。完整快照包含创建快照时写入卷的所有块。完整快照可能会大于它赖以创建的增量快照。但是，如果您在标准层上只有一个卷的增量快照，则归档层中的完整快照的大小将与标准层中的快照大小相同。这是因为卷的第一个快照始终是完整快照。
- 在归档快照时，快照谱系中其它快照引用的快照数据将保留在标准层中。与保留在标准层中的引用数据相关的数据和存储成本将分配给谱系中的下一个快照。这可以确保谱系中的后续快照不会受到归档的影响。
- 如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。要使用快照，您必须首先从回收站中恢复快照，然后从归档层中还原它。有关更多信息，请参阅 回收站 (p. 1627) 和 定价和计费 (p. 1382)。

限制

- 您只能归档状态为 `completed` 状态的快照。
- 您只能归档您在账户中拥有的快照。要归档与您共享的快照，首先将快照复制到您的账户，然后将快照副本归档。
- 您不能归档注册 AMI 的 EBS 根设备卷的快照。
- 您无法归档与 Amazon EBS-backed AMI 关联的快照。
- 在快照归档或快照还原过程启动后，您无法取消它。
- 您不能共享已归档的快照。如果归档了与其它账户共享的快照，则在归档快照后，与之共享快照的账户将失去访问权限。
- 您不能复制已归档的快照。如果需要复制归档的快照，则必须首先将其还原。
- 您不能为归档快照启用快速快照还原。快照归档后，快速快照还原会自动禁用。如果您需要使用快速快照还原，则必须在还原快照后手动启用该选项。
- 您无法存档由 Amazon Backup 创建的快照。

定价和计费

归档的快照按每 GB 每月 0.0125 美元的费率计费。例如，如果您归档 100GiB 快照，则每月需支付 1.25 美元（100GiB x 0.0125 美元）的费用。

快照还原的费率为每 GB 还原数据收费 0.03 美元。例如，如果您从归档层还原 100GiB 快照，则需要一次向您收取费用 3 美元（100GiB x 0.03 美元）。

快照还原到标准层后，快照按每 GB 每月 0.05 美元的标准费率计费。

有关更多信息，请参阅 Amazon EBS 定价。

按最短归档期收费

最短归档期为 90 天。如果您在最短 90 天的归档期限之前删除或永久还原归档的快照，则按比例收取的费用等于剩余天数的归档层存储费用（四舍五入到最接近的小时数）。例如，如果在 40 天之后删除或永久恢复归档快照，则将收取剩余 50 归天的最小存档期的费用。

> **Note**
>
> 在最短 90 天的归档期限之前暂时还原已归档的快照，不会产生此费用。

临时还原

当您临时还原快照时，快照将从归档层还原到标准层，并且快照的副本将保留在归档层中。在临时还原期间，您需要为标准层中的快照和归档层中的快照副本付费。从标准层中删除临时还原的快照时，您不再需要为其付费，而只需为归档层中的快照付费。

永久还原

当您永久还原快照时，快照将从归档层还原到标准层，并且快照将从归档层删除。您仅需为标准层中的快照付费。

删除快照

如果在归档快照时删除快照，则需要为已移动到归档层的快照数据付费。数据最短归档期限为 90 天，并要在删除时支付相应的费用。例如，如果您归档了 100GiB 快照，并且在仅归档 40GiB 之后删除快照，则对于已归档的 40GiB 而言，您需要支付最少 90 天的归档期费用 1.50 美元（每 GB 每月费率 0.0125 美元 * 40GB *（90 天 * 24 小时）/（24 小时/天 * 每月 30 天））。

如果在从归档层还原快照时删除快照，您需要为快照的完整大小（快照大小 x 0.03 美元）支付快照还原费用。例如，如果您从归档层还原 100GiB 快照，并且在快照还原完成之前的任何时候删除快照，则需支付 3 美元（100GiB 快照大小 x 0.03 美元）的费用。

回收站

归档的快照在回收站中时，按归档快照的费率计费。回收站中的归档快照的最短归档期限为 90 天，如果在最短归档期限到来之前被回收站删除，则会产生相应费用。换句话说，如果按照某保留规则，在最短期限 90 天之前从回收站中删除了归档的快照，则需要为剩余天数付费。

如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。它会按归档快照的费率计费。

如果在还原快照时删除与保留规则匹配的快照，则还原的快照将在保留期剩余时间内保留在回收站中，并按标准快照费率计费。要使用快照，您必须首先从回收站中恢复快照。

有关更多信息，请参阅回收站 (p. 1627)。

成本跟踪

归档的快照在 Amazon Cost and Usage Report 显示相同的资源 ID 和 Amazon Resource Name (ARN)。有关更多信息，请参阅 Amazon Cost and Usage Report 用户指南。

您可以使用以下使用类型来确定相关成本：

- `SnapshotArchiveStorage` – 月度数据存储费
- `SnapshotArchiveRetrieval` – 快照还原的一次性费用
- `SnapshotArchiveEarlyDelete` – 在最短归档期限（90 天）之前删除或永久还原快照的费用

配额

本部分介绍了归档快照和正在进行的快照的默认配额。

配额	默认配额			
每卷的已归档快照	25			
每个账户的正在并发进行的快照归档	25			
每个账户的正在并发进行的快照还原	5			

如果您需要的容量超出目标容量的默认限制，请填写 Amazon Web Services Support 中心创建案例表格请求增加限制。

归档快照的准则和最佳做法

本部分提供了归档快照的准则和最佳做法。

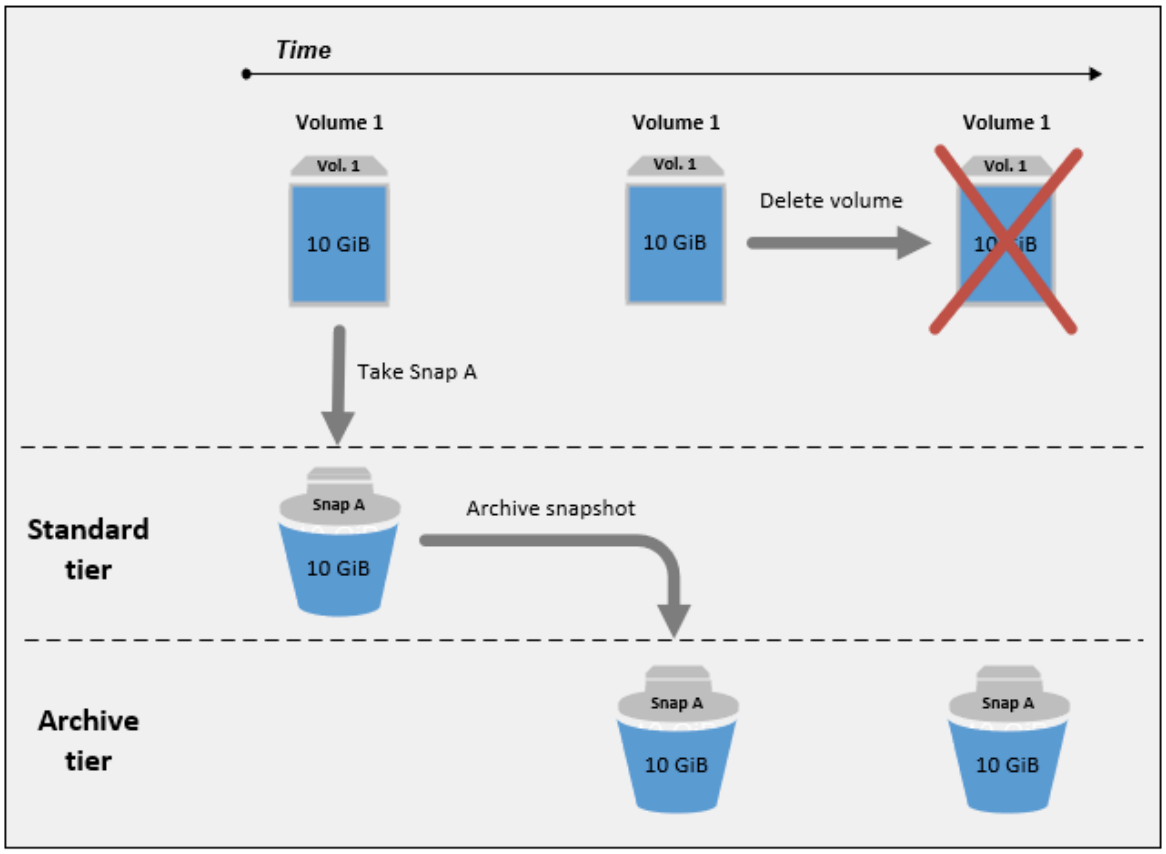
主题

- 归档卷的唯一快照 (p. 1384)
- 归档单个卷的增量快照 (p. 1384)
- 出于合规性原因归档完整快照 (p. 1385)
- 确定标准层存储成本的减少程度 (p. 1386)

归档卷的唯一快照

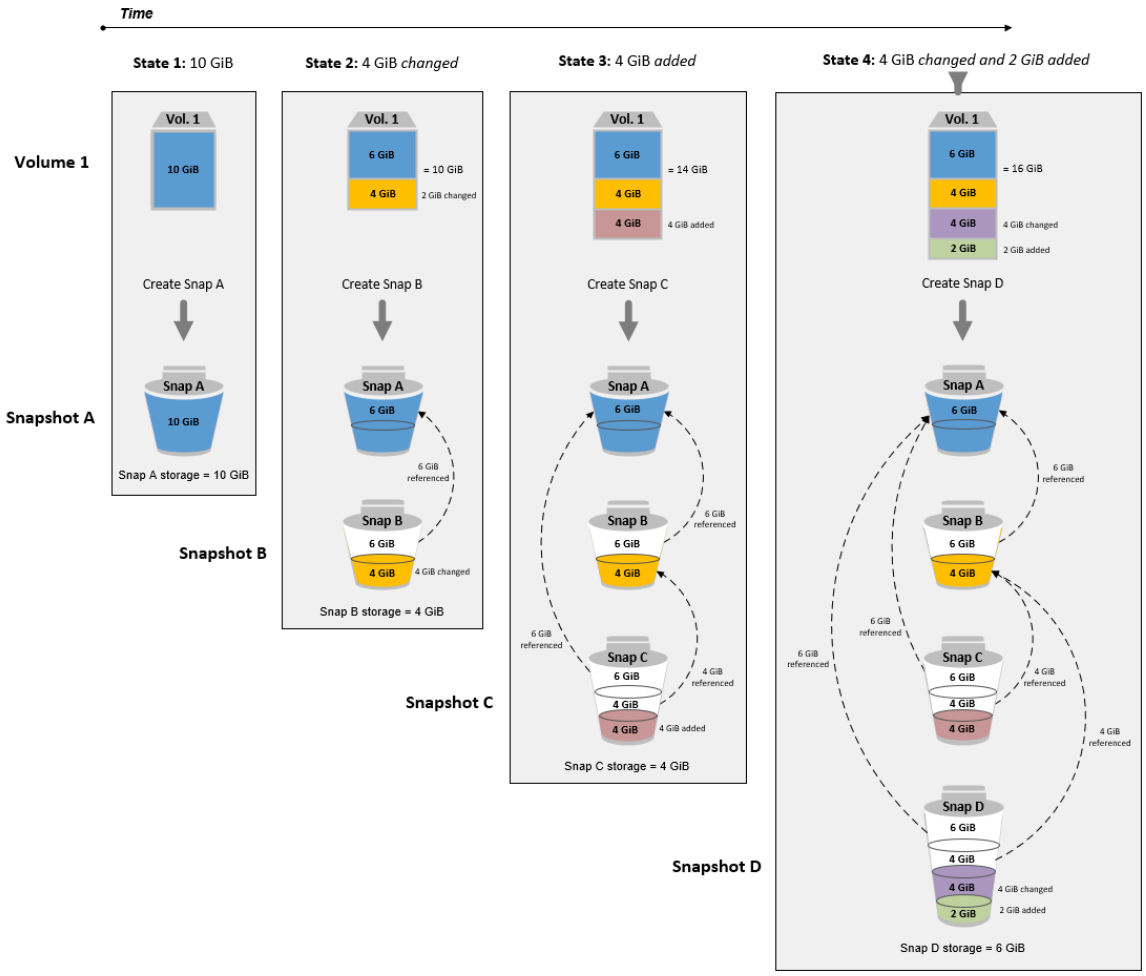
如果只存在卷的一个快照，则快照的大小始终与创建快照时写入卷的块的大小相同。归档此类快照时，标准层中的快照将转换为同等大小的完整快照，然后从标准层移动到归档层。

归档这些快照可以帮助您以更低的存储成本节省开支。如果不再需要源卷，则可以删除该卷以进一步节省存储成本。



归档单个卷的增量快照

归档增量快照时，增量快照将转换为完整快照，然后从标准层移动到归档层。例如，在下图中，如果您归档快照 B，快照将转换为大小为 10GiB 的完整快照并移动到归档层。同样，如果您归档快照 C，归档层中的完整快照大小为 14GiB。



如果要归档快照以降低标准层中的存储成本，您不应归档一组增量快照中的第一个快照。快照谱系中的后续快照引用了这些快照。在大多数情况下，归档这些快照不会降低存储成本。

> **Note**
>
> 您不应归档一组增量快照中的最后一个快照。最后一个快照是卷的最新快照。如果要在卷损坏或丢失的情况下从快照中创建卷，则需要在标准层中使用此快照。

如果归档了一个快照，而该快照包含了谱系中后续快照所引用的数据，那么与所引用数据关联的数据存储和存储成本将分配给后续快照。在这种情况下，归档这些快照不会降低数据存储成本。例如，在上一张图片中，如果归档快照 B，它的 4GiB 的数据相当于由快照 C 产生。在这种情况下，总体存储成本将增加，因为您需要为归档层的快照 B 完整版付费，而标准层的存储成本保持不变。

如果归档快照 C，标准层存储将减少 4GiB，因为该数据未被谱系中任何其它后续快照引用。而且，由于快照已转换为完整快照，您的归档层存储将增加 14GiB。

出于合规性原因归档完整快照

出于合规性考虑，您可能需要每月、每季度或每年创建卷的完整备份。对于这些备份，您可能需要独立快照而不向后或向前引用快照谱系中的其它快照。使用 EBS 快照归档功能归档的快照是完整快照，它们没有引用谱系中的其它快照。此外，为了遵循合规性要求，您可能需要保留这些快照数年。EBS 快照归档使归档这些完整快照以长期保留具备良好的成本效益。

确定标准层存储成本的减少程度

如果要归档增量快照以降低存储成本，您应考虑归档层中完整快照的大小和标准层存储空间减少的程度。本部分介绍如何进行设置。

> **Important**
>
> 在调用 API 的时间点，API 响应的数据是准确的。由于与快照相关的数据随着快照谱系的变化而发生变化，API 响应可能会有所不同。

要确定标准层存储空间和存储成本的降低，请使用以下步骤。

1. 检查完整快照的大小。要确定快照的完整大小，请使用 list-snapshot-blocks 命令。对于 `--snapshot-id`，请指定需归档快照 ID。

```
$  aws ebs list-snapshot-blocks --snapshot-id snapshot_id
```

这会返回有关指定快照中所有数据块的信息。该命令返回的最后一个数据块的 `BlockIndex` 表示快照中的数据块数。数据块数乘以 512KiB（即快照数据块大小），结果接近归档层中完整快照的大小（数据块数 x 512KiB = 完整快照大小）。

例如，以下命令会列出快照 `snap-01234567890abcdef` 的数据块。

```
$  aws ebs list-snapshot-blocks --snapshot-id snap-01234567890abcdef
```

以下是命令输出，其中省略了一些数据块。以下输出表明快照包括大约 16383 个数据块。这相当于约 8GiB 的完整快照大小（16383 x 512KiB = 7.99GiB）。

```
 {
    "VolumeSize": 8,
    "Blocks": [
        {
            "BlockToken": "ABgBAeShfa5RwG+RiWUg2pwmnCU/
YMnV7fGMxLbCWfEBEUmmuqac5RmoyVat",
            "BlockIndex": 0
        },
        {
            "BlockToken": "ABgBATdTONyThPUAbQhbUQXsn5TGoY/
J17GfE83j9WN7siupavOTw9E1KpFh",
            "BlockIndex": 1
        },
        {
            "BlockToken": "EBEUmmuqXsn5TGoY/QwmnCU/YMnV74eKE2TSsn5TGoY/
E83j9WQhbUQXsn5T",
            "BlockIndex": 4
        },
        .....
        {
            "BlockToken": "yThPUAbQhb5V8xpwmnCU/
YMnV74eKE2TSFY1sKP/4r05y47WETdTONyThPUA",
            "BlockIndex": 12890
        },
        {
            "BlockToken":
 "ABgBASHKD5V8xEbaRKdxdkZZS4eKE2TSFYlMG1sKP/4r05y47WEHqKaNPcLs",
            "BlockIndex": 12906
        },
        {
            "BlockToken": "ABgBARROGMUJo6P9X3CFHQGZNQ7av9B6vZtTTqV89QqC
+SkO0HWMlwkGXjnA",
            "BlockIndex": 16383
        }
```

```
    ],
    "VolumeSize": 8,
    "ExpiryTime": 1637677800.845,
    "BlockSize": 524288
}
```

2. 找到需归档快照的源卷（快照创建自此卷）。可以使用 describe-hosts 命令。对于 `--snapshot-id`，请指定需归档快照 ID。响应参数 `VolumeId` 表示源卷 ID。

```
$ aws ec2 describe-snapshots --snapshot-id snapshot_id
```

例如，以下命令返回有关快照 `snap-09c9114207084f0d9` 的信息。

```
$ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
```

以下是命令输出，它表示该快照 `snap-09c9114207084f0d9` 通过卷 `vol-0f3e2c292c52b85c3` 创建。

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

3. 查找通过该源卷创建的所有快照。可以使用 describe-hosts 命令。请指定 `volume-id` 筛选条件，并指定在上一步中得到的卷 ID 作为筛选条件值。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

例如，以下命令返回创建自卷的所有快照 `vol-0f3e2c292c52b85c3`。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=vol-0f3e2c292c52b85c3"
```

以下是命令输出，表示三个快照通过卷创建 `vol-0f3e2c292c52b85c3`。

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-08ca60083f86816b0"
```

```
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

4. 使用上一个命令的输出，按照创建时间（从最早到最新）对快照进行排序。每个快照的响应参数 StartTime 表示其创建时间（UTC 时间格式）。

   例如，按创建时间（从最早到最新）排列的上一步返回的快照如下所示：

   1. snap-08ca60083f86816b0（最早 – 在需归档快照产生之前创建）
   2. snap-09c9114207084f0d9（要归档的快照）
   3. snap-024f49fe8dd853fa8（最新 – 紧接着需归档的快照之后创建）

5. 确定在需归档快照产生之前和之后紧邻着创建的快照。在这种情况下，您要归档快照 snap-09c9114207084f0d9，这是在三个快照集中创建的第二个增量快照。快照 snap-08ca60083f86816b0 正好在其之前创建，而快照 snap-024f49fe8dd853fa8 紧接其后创建。

6. 在需归档的快照中找到未引用的数据。首先，找出需归档快照以及正好在其之前创建的快照之间不同的数据块。使用 list-changed-blocks 命令。对于 --first-snapshot-id，请指定正好在需归档快照之前创建的快照 ID。对于 --second-snapshot-id，请指定需归档快照 ID。

   ```
   $ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
   snapshot-id snapshot_to_archive
   ```

   例如，以下命令显示了以下两个快照之间不同数据块的块索引：快照 snap-08ca60083f86816b0（正好在需归档快照之前创建的快照），以及快照 snap-09c9114207084f0d9（需归档快照）。

   ```
   $ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
   snapshot-id snap-09c9114207084f0d9
   ```

   下面显示了命令输出，其中省略了一些数据块。

   ```
   {
       "BlockSize": 524288,
       "ChangedBlocks": [
           {
   ```

```
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue
+cRwUqF",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
            "BlockIndex": 13174
        },
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

接下来，使用相同的命令查找需归档快照与紧接其后创建的快照之间不同的数据块。对于 `--first-snapshot-id`，请指定需归档快照 ID。对于 `--second-snapshot-id`，请指定紧接着需归档快照之后创建的快照 ID。

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-
snapshot-id snapshot_created_after
```

例如，以下命令显示了以下两个快照之间不同块的数据块索引：快照 snap-09c9114207084f0d9（在需归档快照之后立即创建的快照），以及快照 snap-024f49fe8dd853fa8（需归档快照）。

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-
snapshot-id snap-024f49fe8dd853fa8
```

下面显示了命令输出，其中省略了一些数据块。

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
```

```
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ+iSlWVpBIshmeyeS5FD/
M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
            "BlockIndex": 13193
        },
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```


7. 比较上一步中两个命令返回的输出。如果两个命令输出中都显示相同的数据块索引，则表示该数据块包含未引用的数据。

   例如，上一步中的命令输出表明数据块 4、5、13 和 15 对于快照 `snap-09c9114207084f0d9` 来说是唯一的，而且快照谱系中的任何其它快照都不会引用它们。

   要确定标准层存储空间的减少多少，请将两个命令输出中出现的数据块数乘以 512KiB，即得出快照数据块大小。

   例如，如果在两个命令输出中都出现 9950 个数据块索引，则表明您将减少标准层存储大约 4.85GiB（9950 个数据块 x 512KiB = 4.85GiB）。

8. 确定在标准层中存储未引用的数据块达 90 天的存储成本。将此值与归档层中的完整快照存储成本（如步骤 1 所述）进行比较。假设在最短 90 天的期限内没有从归档层还原完整快照，您可以通过比较这些值来确定节省的成本。有关更多信息，请参阅定价和计费 (p. 1382)。

所需的 IAM 权限

默认情况下，用户无权使用快照归档。要允许用户使用快照归档，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy。

要使用快照归档，用户需要以下权限。

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

控制台用户可能还需要其他权限，例如 `ec2:DescribeSnapshots`。

要归档和恢复加密快照，需要以下 Amazon KMS 额外权限。

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`

以下是 IAM policy 示例，授予了 IAM 用户归档、恢复和查看加密及未加密快照的权限。其包括控制台用户的 `ec2:DescribeSnapshots` 权限。如果不需要某些上述权限，您可以从策略中将其删除。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 `kms:GrantIsForAWSResource` 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

使用快照归档

主题

- 归档快照 (p. 1392)
- 还原已归档的快照 (p. 1393)
- 修改临时还原快照的还原期或还原类型 (p. 1395)
- 查看归档快照 (p. 1396)

归档快照

您可以归档任何状态为 `completed` 的快照，以及自己账户中的快照。您无法归档状态为 `pending` 或 `error` 的快照，以及与您共享的快照。有关更多信息，请参阅注意事项和限制 (p. 1381)。

归档的快照保留其快照 ID、加密状态、Amazon Identity and Access Management (IAM) 权限、所有者信息和资源标签。但是，快照还原和快照共享会在快照归档后自动禁用。

在归档处理过程中，您可以继续使用快照。一旦快照分层状态达到 `archival-complete` 状态，您无法再使用快照。

您可以使用以下方法归档快照。

Console

归档快照

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots。
2. 在快照列表中，选择需归档快照，然后选择 Actions（操作）、Archive snapshot（归档快照）。
3. 如要确认，请选择 Archive snapshot（归档快照）。

Amazon CLI

归档快照

使用 modify-snapshot-tier Amazon CLI 命令。对于 `--snapshot-id`，请指定需归档快照的 ID。对于 `--storage-tier`，请指定 `archive`。

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snapshot_id \
--storage-tier archive
```

例如，以下命令可以归档快照 `snap-01234567890abcedf`。

```
$ aws ec2 modify-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--storage-tier archive
```

该命令将显示以下输出。响应参数 `TieringStartTime` 以 UTC 时间格式 (YYYY-MM-DDTHH:MM:SSZ) 表示归档过程的启动日期和时间。

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

还原已归档的快照

在使用归档快照之前，必须先将其还原到标准层。还原的快照具有与归档之前相同的快照 ID、加密状态、IAM 权限、所有者信息和资源标签。还原后，您可以像使用账户中的任何其它快照一样使用它。还原的快照始终是完整快照。

还原快照时，可以选择使用以下两种方式还原快照：permanently（永久）或 temporarily（暂时）。

如果永久还原快照，则快照将从归档层永久移动到标准层。在手动重新归档或手动删除快照之前，快照将保持还原状态并可供使用。永久还原快照时，快照将从归档层中删除。

如果临时还原快照，则在您指定的还原期内，快照将从归档层复制到标准层。快照将保持还原状态，并且只能在还原期间使用。在还原期间，快照的副本将保留在归档层中。超过期限后，快照将自动从标准层中删除。在还原期间，您可以随时延长或缩短还原期，或将还原类型更改为永久。有关更多信息，请参阅修改临时还原快照的还原期或还原类型 (p. 1395)。

您可以使用以下方法还原归档快照。

Console

从归档中还原快照

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots。
2. 在快照列表中，选择要还原的归档快照，然后选择 Actions（操作）、Restore snapshot from archive（从归档还原快照）。
3. 指定要执行的还原类型。在 Restore type（还原类型）中，执行下列操作之一：
   - 要永久还原快照，请选择 Permanent（永久）。
   - 要临时还原快照，请选择 Temporary（临时），然后在 Temporary restore period（临时还原期）中，输入要还原快照的天数。
4. 要确认，请选择 Restore snapshot（还原快照）。

Amazon CLI

永久还原已归档的快照

使用 restore-snapshot-tier Amazon CLI 命令。对于 `--snapshot-id`，请指定要还原的快照的 ID，并包括 `--permanent-restore` 选项。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--permanent-restore
```

例如，以下命令可永久还原快照 `snap-01234567890abcedf`。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
--permanent-restore
```

该命令将显示以下输出。

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

临时还原已归档的快照

使用 restore-snapshot-tier Amazon CLI 命令。忽略 `--permanent-restore` 选项。对于 `--snapshot-id`，请指定要还原的快照的 ID，以及在 `--temporary-restore-days` 中指定要还原快照的天数。

`--temporary-restore-days` 必须以天为单位指定。允许范围是 1 到 180。如果没有指定一个值，默认为 1 天。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snapshot_id \
--temporary-restore-days number_of_days
```

例如，以下命令会临时还原快照 `snap-01234567890abcedf`，还原期为 5 天。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf \
```

```
--temporary-restore-days 5
```

该命令将显示以下输出。

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

修改临时还原快照的还原期或还原类型

临时还原快照时，必须指定快照在账户中保持还原状态的天数。还原期到期后，快照将自动从标准层中删除。

您可以随时更改临时还原快照的还原期。

您可以选择增加或缩短还原期，也可以将还原类型从临时更改为永久。

如果更改还原期，则新的还原期将从当前日期开始生效。例如，如果指定新的还原期 5 天，快照将从当前日期开始到 5 天内保持还原状态。

Note

您可以通过将还原期设置为 1 天，提前结束临时还原。

如果将还原类型从临时更改为永久，则快照副本将从归档层中删除，并且在您手动重新归档或删除快照之前，该快照将保持在账户中并且可用。

您可以使用以下方法修改快照的还原期。

Console

修改还原期或还原类型

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots。
2. 在快照列表中，选择此前暂时还原的快照，然后选择 Actions（操作）、Restore snapshot from archive（从归档还原快照）。
3. 在 Restore type（还原类型）中，执行下列操作之一：
   - 要将还原类型从临时更改为永久，请选择 Permanent（永久）。
   - 要延长或缩短还原期，请保留 Temporary（临时），然后在 Temporary restore period（临时还原期）中输入新的还原期（以天为单位）。
4. 要确认，请选择 Restore snapshot（还原快照）。

Amazon CLI

修改还原期或还原类型

使用 restore-snapshot-tier Amazon CLI 命令。对于 `--snapshot-id`，请指定之前临时还原的快照的 ID。要将还原类型从临时更改为永久性，请指定 `--permanent-restore` 并忽略 `--temporary-restore-days`。要延长或缩短还原期，请省略 `--permanent-restore`，而且对于 `--temporary-restore-days`，请指定新的还原期（以天为单位）。

例如：延长或缩短还原期

以下命令把快照还原期从 `snap-01234567890abcedf` 改到 `10` 天。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--temporary-restore-days 10
```

该命令将显示以下输出。

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

示例：将还原类型更改为永久

以下命令把快照 snap-01234567890abcedf 的还原类型从临时更改为永久。

```
$ aws ec2 restore-snapshot-tier \
--snapshot-id snap-01234567890abcedf
--permanent-restore
```

该命令将显示以下输出。

```
{
    "SnapshotId": "snap-01234567890abcedf",
    "IsPermanentRestore": true
}
```

查看归档快照

您可以使用以下方法查看快照的存储层信息。

Console

查看快照的存储层信息

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots。
2. 在快照列表中，选择快照，然后选择 Storage tier（存储层）选项卡。

   该表提供以下信息：

   - Last tier change started on（上次层别更改始于）– 上次归档或还原的开始日期和时间。
   - Tier change progress（层更改进展）– 以百分比表示的上次归档或还原操作的进度。
   - Storage tier（存储层）– 快照的存储层。归档快照的状态始终为 archive，以及存储在标准层上的快照的状态始终为 standard，包括临时还原的快照。
   - Tiering status（分层状态）– 上次归档或还原操作的状态。
   - Archive completed on（归档完成时间）– 归档完成的日期和时间。
   - Temporary restore expires on（临时还原到期时间）– 设置临时还原的快照过期的日期和时间。

Amazon CLI

查看有关归档快照的归档信息

使用 describe-snapshot-tier-status Amazon CLI 命令。请指定 snapshot-id 筛选条件，请指定快照 ID 为筛选条件值。或者，要查看所有归档的快照，请省略筛选条件。

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snapshot_id"
```

输出包括以下响应参数：

- Status – 快照的状态。归档快照的状态始终为 completed。只有状态为 completed 的快照可以归档。
- LastTieringStartTime – 归档过程开始的日期和时间，采用 UTC 时间格式 (YYYY-MM-DDTHH:MM:SSZ)。
- LastTieringOperationState – 归档过程的当前状态。可能的状态包括：archival-in-progress | archival-completed | archival-failed | permanent-restore-in-progress | permanent-restore-completed | permanent-restore-failed | temporary-restore-in-progress | temporary-restore-completed | temporary-restore-failed
- LastTieringProgress – 快照归档过程的进度，以百分比表示。
- StorageTier – 快照的存储层。归档快照的状态始终为 archive，以及存储在标准层上的快照的状态始终为 standard，包括临时还原的快照。
- ArchivalCompleteTime – 归档过程完成的日期和时间，采用 UTC 时间格式 (YYYY-MM-DDTHH:MM:SSZ)。

示例

以下命令显示有关快照 snap-01234567890abcedf 的信息。

```
$ aws ec2 describe-snapshot-tier-status --filters "Name=snapshot-id,
 Values=snap-01234567890abcedf"
```

该命令将显示以下输出。

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcedf",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890abcedf",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

查看归档和标准层快照

使用 describe-snapshot Amazon CLI 命令。对于 --snapshot-ids，请指定快照视图的 ID。

```
$ aws ec2 describe-snapshots --snapshot-ids snapshot_id
```

例如，以下命令显示有关快照 snap-01234567890abcedf 的信息。

```
$ aws ec2 describe-snapshots --snapshot-ids snap-01234567890abcedf
```

该命令将显示以下输出。响应参数 StorageTier 说明快照当前是否已归档。archive 表示快照当前已归档并存储在归档层中，而 standard 表示快照当前尚未归档，并且存储在标准层中。

在以下示例输出中，只有 Snap A 已归档。Snap B 和 Snap C 尚未归档。

此外，响应参数 RestoreExpiryTime 仅为从归档中暂时还原的快照返回。它表示将何时从标准层中自动删除临时还原的快照。对于永久还原的快照，不会返回该值。

在以下示例输出中，Snap C 已暂时还原，它将在 2021-09-19T21:00:00.000Z（2021 年 9 月 19 日 UTC 21:00）自动从标准级别中移除。

```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
}
```

仅查看存储在归档层或标准层中的快照

使用 describe-snapshot Amazon CLI 命令。包括 --filter 选项，请指定 storage-tier 为筛选条件名称，请指定 archive 或 standard 为筛选条件值。

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive|standard"
```

例如，以下命令只显示归档快照。

```
$ aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

监控快照归档

Amazon EBS 发出与快照归档操作相关的事件。您可以使用 Amazon Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南。

提供的事件如下：

- `archiveSnapshot` – 当快照归档操作成功或失败时发出。

  以下是在快照归档操作成功时发送事件的示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

  以下是在快照归档操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

```
}
```

- permanentRestoreSnapshot – 当永久还原操作成功或失败时发出。

  以下是在快照还原操作成功时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

  以下是在永久还原操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- temporaryRestoreSnapshot – 当临时还原操作成功或失败时发出。

  以下是在快照暂时还原操作成功时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

下面是在临时还原操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `restoreExpiry` – 在临时还原快照的还原期到期时触发。

  以下是示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
```

```
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

查看 Amazon EBS 快照信息

您可以使用以下方法之一查看有关快照的详细信息。

Console

使用控制台查看快照信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 要仅查看您拥有的快照，请在屏幕左上角选择 Owned by me（我拥有的）。您还可以使用标签和快照属性筛选快照列表。在 Filter（筛选条件）字段中，选择属性字段，然后选择或输入属性值。例如，要仅查看加密的快照，请选择 Encryption（加密），然后输入 `true`。
4. 要查看有关特定快照的更多信息，请在列表中选择其 ID。

Amazon CLI

使用命令行查看快照信息

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-snapshots (Amazon CLI)
- Get-EC2Snapshot（Amazon Tools for Windows PowerShell）

Example 示例 1：基于标签进行筛选

以下命令描述具有标签 Stack=production 的快照。

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example 示例 2：基于卷进行筛选

以下命令描述从指定卷创建的快照。

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example 示例 3：基于快照期限进行筛选

使用 Amazon CLI，您可以使用 JMESPath 通过表达式来筛选结果。例如，以下命令显示您的 Amazon 账户在指定日期（由 *2020-03-31* 表示）之前创建的所有快照的 ID（由 *123456789012* 表示）。如果未指定所有者，则结果将包括所有公有快照。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<=`2020-03-31`)].[SnapshotId]" --output text
```

以下命令显示在指定日期范围内创建的所有快照的 ID。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>=`2019-01-01`) && (StartTime<=`2019-12-31`)].[SnapshotId]" --
output text
```

共享 Amazon EBS 快照

如果您想与其他 Amazon 账户共享快照，可以修改快照的权限。您可以与所有其他 Amazon 账户共享快照，或者您可以私下与您指定的个人 Amazon 账户共享快照。您已授权的用户可以使用您共享的快照来创建自己的 EBS 卷，同时您的原始快照不受影响。

> **Important**
>
> 共享快照时，您可以让其他人访问快照上的所有数据。仅与您信任的人共享所有快照数据的快照。

主题

- 共享快照之前 (p. 1403)
- 共享快照 (p. 1403)
- 共享 KMS 密钥 (p. 1404)
- 查看与您共享的快照 (p. 1406)
- 使用与您共享的快照 (p. 1406)
- 确定共享快照的用途 (p. 1406)

共享快照之前

共享快照时需考虑以下事项：

- 快照受限于在其中创建它们的区域。要与其他区域共享快照，请将快照复制到该区域，然后分享副本。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。
- 您无法共享使用默认 Amazon 托管式密钥 加密的快照。您只能共享使用客户托管密钥加密的快照。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。
- 您只能公开共享未加密的快照。
- 共享加密快照时，还必须共享用于加密快照的客户托管密钥。有关更多信息，请参阅共享 KMS 密钥 (p. 1404)。

共享快照

您可以使用本节介绍的方法之一共享快照。

Console

共享快照

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择快照，然后依次选择 Actions（操作）、Modify Permissions（修改权限）。
4. 请指定快照的权限。Current setting（当前设置）表示快照的当前共享权限。
   - 要与所有Amazon账户公开共享快照，选择 Public（公有）。
   - 要与特定Amazon账户私下共享快照，选择 Private（私有）。然后，在 Sharing accounts（共享账户）部分，选择 Add account（添加账户），接着输入要与之共享的账户的 12 位账户 ID（不带连字符）。

5. 选择 Save changes（保存更改）。

Amazon CLI

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要将快照与特定 Amazon 账户共享，请将用户设置为 Amazon 账户的 ID。

公开共享快照

使用以下命令之一。

- modify-snapshot-attribute (Amazon CLI)

  对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于 `--group-names`，请指定 `all`。

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --group-names all
```

- Edit-EC2SnapshotAttribute（Amazon Tools for Windows PowerShell）

  对于 `-Attribute`，请指定 `CreateVolumePermission`。对于 `-OperationType`，请指定 `Add`。对于 `-GroupName`，请指定 `all`。

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -GroupName all
```

私密共享快照

使用以下命令之一。

- modify-snapshot-attribute (Amazon CLI)

  对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于 `--user-ids`，请指定要与之共享快照的 Amazon 账户的 12 位 ID。

```
$  aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute
 createVolumePermission --operation-type add --user-ids 123456789012
```

- Edit-EC2SnapshotAttribute（Amazon Tools for Windows PowerShell）

  对于 `-Attribute`，请指定 `CreateVolumePermission`。对于 `-OperationType`，请指定 `Add`。对于 `UserId`，请指定要与之共享快照的 Amazon 账户的 12 位 ID。

```
PS C:\>  Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute
 CreateVolumePermission -OperationType Add -UserId 123456789012
```

共享 KMS 密钥

共享加密快照时，还必须共享用于加密快照的客户托管密钥。您可以在创建客户托管密钥时或以后的某个时间向客户托管密钥应用跨账户权限。

必须为正在访问加密快照的共享客户托管密钥用户授予对密钥执行以下操作的权限：

- `kms:DescribeKey`

- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:ReEncrypt`
- `kms:Decrypt`

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 `kms:GrantIsForAWSResource` 条件键以允许用户在 KMS 密钥上创建授权。

有关如何控制对客户托管密钥的访问权限的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用 Amazon KMS 中的密钥策略。

要使用 Amazon KMS 控制台共享客户托管密钥

1. 在 Amazon KMShttps://console.aws.amazon.com/kms 打开 控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（区域选择器）。
3. 在导航窗格中，选择 Customer managed keys (客户托管密钥)。
4. 在 Alias (别名) 列中，选择用于加密快照的客户托管密钥的别名（文本链接）。密钥详细信息将在新页面中打开。
5. 在 Key policy (密钥策略) 部分，您会看到策略视图或默认视图。策略视图显示密钥策略文档。默认视图显示 Key administrators (密钥管理员)、Key deletion (密钥删除)、Key Use (密钥使用) 和 Other Amazon accounts (其他亚马逊云科技账户) 几个部分。如果您在控制台中创建了策略，但尚未对其进行自定义，则会显示默认视图。如果默认视图不可用，则需要在策略视图中手动编辑策略。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的查看密钥策略（控制台）。

   使用策略视图或默认视图（具体取决于您可以访问哪个视图）向策略添加一个或多个 Amazon 账户 ID，如下所示：

   - （策略视图）选择 Edit (编辑)。将一个或多个 Amazon 账户 ID 添加到以下语句："`Allow use of the key`" 和 "`Allow attachment of persistent resources`"。选择 Save changes（保存更改）。在以下示例中，会将 Amazon 账户 ID `444455556666` 添加到策略中。

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
```

```
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- （默认视图）向下滚动到 Other Amazon accounts (其他亚马逊云科技账户)。选择 Add other Amazon accounts(添加其他亚马逊云科技账户)，并按提示输入Amazon账户 ID。要添加其他账户，选择 Add another Amazon account（添加其他亚马逊云科技账户）并输入 Amazon 账户 ID。添加完所有 Amazon 账户后，选择 Save changes（保存更改）。

查看与您共享的快照

您可以使用以下方法之一查看与您共享的快照。

Console

使用控制台查看共享快照

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 筛选列出的快照。在屏幕的左上角，选择以下选项之一：
   - Private snapshots (私有快照) – 仅查看与您私下共享的快照。
   - Public snapshots (公有快照) – 仅查看与您公开共享的快照。

Amazon CLI

使用命令行查看快照权限

使用以下命令之一：

- describe-snapshot-attribute (Amazon CLI)
- Get-EC2SnapshotAttribute（Amazon Tools for Windows PowerShell）

使用与您共享的快照

使用共享的未加密快照

按 ID 或描述查找共享快照。有关更多信息，请参阅查看与您共享的快照 (p. 1406)。您可以像使用账户中拥有的任何其他快照一样使用此快照。例如，您可以从快照中创建卷或将卷复制到其他区域。

使用共享的已加密快照

按 ID 或描述查找共享快照。有关更多信息，请参阅查看与您共享的快照 (p. 1406)。在您的账户中创建共享快照的副本，并使用您拥有的 KMS 密钥对副本进行加密。然后，您可以使用副本创建卷，也可以将其复制到不同的区域。

确定共享快照的用途

您可以使用 Amazon CloudTrail 监控是否已复制与他人共享的快照或使用它来创建卷。在 CloudTrail 中登录以下事件：

- SharedSnapshotCopyInitiated — 正在复制共享快照。

- SharedSnapshotVolumeCreated — 正在使用共享快照创建卷。

有关使用 CloudTrail 的更多信息，请参阅使用 Amazon CloudTrail 记录 Amazon EC2 和 Amazon EBS API 调用 (p. 1037)。

从回收站中还原快照

回收站是一项数据恢复功能，支持您还原意外删除的 Amazon EBS 快照和 EBS 支持的 AMI。使用回收站时，如果资源被删除，回收站功能将在您指定的时间段内保留快照，而后永久删除资源。

在资源保留期到期之前，您可以随时从回收站还原资源。从回收站还原资源后，资源将从回收站中删除，您可以像使用账户中任何该类型的其他资源的一样使用此资源。如果保留期过期且资源未还原，则资源将从回收站中永久删除，并且不再可用于恢复。

回收站中快照的计费费率与您账户中的常规快照费率相同。使用回收站和保留规则不会产生额外费用。有关更多信息，请参阅 Amazon EBS 定价。

有关更多信息，请参阅回收站 (p. 1627)。

主题

- 使用回收站中的快照的权限 (p. 1407)
- 在回收站中查看快照 (p. 1408)
- 从回收站中还原快照 (p. 1409)

使用回收站中的快照的权限

默认情况下，用户无权使用回收站中的快照。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

要查看及恢复回收站中的快照，用户必须具有以下权限：

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

要管理回收站中快照的标签，用户需要以下额外权限。

- `ec2:CreateTags`
- `ec2:DeleteTags`

要使用回收站控制台，用户需要 `ec2:DescribeTags` 权限。

以下是 IAM policy 示例。其中包括控制台用户的 `ec2:DescribeTags` 权限，以及用于管理标签的 `ec2:CreateTags` 和 `ec2:DeleteTags` 权限。如果不需要上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
```

```
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用回收站所需权限的更多信息，请参阅 使用回收站和保留规则的权限 (p. 1631)。

在回收站中查看快照

当快照在回收站中时，您可以查看有关该快照的有限信息，包括：

- 快照的 ID。
- 快照描述。
- 从中创建快照的卷的 ID。
- 快照被删除并进入回收站的日期和时间。
- 保留期到期的日期和时间。此时，快照将从回收站中永久删除。

您可以使用以下方法查看回收站中的快照。

Recycle Bin console

使用控制台查看回收站中的快照

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该网格列出了当前在回收站中的所有快照。要查看特定快照的详细信息，请在网格中选择它，然后选择 Actions（操作）、View details（查看详细信息）。

Amazon CLI

使用 Amazon CLI 查看回收站中的快照

使用 list-snapshots-in-recycle-bin Amazon CLI 命令。加入 `--snapshot-id` 选项来查看特定快照。或者省略 `--snapshot-id` 选项以查看回收站中的所有快照。

```
$ aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令提供有关回收站中的快照 snap-01234567890abcdef 的信息。

```
$ aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

输出示例：

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

从回收站中还原快照

当快照在回收站中时，您不能以任何方式使用它。要使用快照，您必须首先还原它。从回收站还原快照时，该快照立即可供使用，回收站会将其删除。还原快照后，您可以像使用账户中任何其它快照一样使用它。

您可以使用以下方法之一从回收站中还原快照。

Recycle Bin console

使用控制台从回收站中还原快照

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该网格列出了当前在回收站中的所有快照。选择要还原的快照，然后选择 Recover（还原）。
4. 系统提示时，选择 Recover（还原）。

Amazon CLI

使用 Amazon CLI 从回收站中还原已删除的快照

使用 restore-snapshot-from-recycle-bin Amazon CLI 命令。对于 --snapshot-id，请指定需还原快照的 ID。

```
$ aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令将快照 snap-01234567890abcdef 从回收站中还原。

```
$ aws restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

命令成功后，不返回任何输出。

Amazon EBS local snapshots on Outposts

Amazon EBS 快照是 EBS 卷的时间点副本。

默认情况下，Outpost 上 EBS 卷的快照存储在 Amazon S3 中的 Outpost 区域中。您也可以使用 Outposts 上的 Amazon EBS 本地快照 在 Outpost 自身的 Amazon S3 中，在本地存储 Outpost 上的卷副本。这可以确保快照数据驻留在您本地的 Outpost 上。此外，您可以使用 Amazon Identity and Access Management（IAM）策略和权限来设置数据驻留执行策略，以确保快照数据不会离开 Outpost。如果您居住在尚未有某个 Amazon 区域提供服务且有数据驻留要求的国家或地区，这将特别有用。

此主题提供有关使用 Outposts 上的 Amazon EBS 本地快照 的信息。有关 Amazon EBS 快照以及在 Amazon 区域中使用快照的更多信息，请参阅 Amazon EBS 快照 (p. 1368)。

有关 Amazon Outposts 的更多信息，请参阅 Amazon Outposts 功能和 Amazon Outposts 用户指南。有关定价信息，请参阅 Amazon Outposts 定价。

主题

- 常见问题 (p. 1410)
- 先决条件 (p. 1411)
- 注意事项 (p. 399)
- 使用 IAM 控制访问 (p. 1412)
- 使用本地快照 (p. 1413)

常见问题

1. 什么是 本地快照？

   默认情况下，Outpost 上卷的 Amazon EBS 快照存储在 Amazon S3 中的 Outpost 区域中。如果 Outpost 预置了 Amazon S3 on Outposts，您可以选择在 Outpost 自身本地存储快照。本地快照采用增量更新，这意味着只保存在最新快照之后更改的卷数据块。您随时可以使用这些快照在快照所在同一 Outpost 上恢复卷。有关 Amazon EBS 快照的更多信息，请参阅 Amazon EBS 快照 (p. 1368)。

2. 为什么应该使用 本地快照？

   快照是备份数据的便捷方法。使用 本地快照，您的所有快照数据都在 Outpost 上本地存储。这意味着数据不会离开您的本地环境。如果您居住在尚未有某个 Amazon 区域提供服务且有数据驻留要求的国家或地区，这将特别有用。

   此外，使用 本地快照 可以在带宽受限环境中帮助减少区域和 Outpost 之间的通信所使用的带宽。

3. 如何在 Outpost 上执行快照数据驻留？

   您可以使用 Amazon Identity and Access Management（IAM）策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在使用本地快照时以及在执行数据驻留时拥有的权限。您可以创建一个策略，禁止委托人从 Outpost 卷和实例创建快照并将快照存储在 Amazon 区域中。目前，不支从 Outpost 向区域复制快照和映像。有关更多信息，请参阅使用 IAM 控制访问 (p. 1412)。

4. 是否支持多卷、崩溃一致性本地快照？

   是的，您可以从 Outpost 上的实例创建多卷、崩溃一致性本地快照。

5. 我该如何创建本地快照？

   您可以使用（Amazon Command Line InterfaceAmazon CLI）或 Amazon EC2 控制台手动创建快照。有关更多信息，请参阅 使用本地快照 (p. 1413)。您还可以使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期。有关更多信息，请参阅 在 Outpost 上自动执行快照 (p. 1418)。

6. 如果我的 Outpost 失去了与其区域的连接，我可以创建、使用或删除本地快照吗？

   不可以。Outpost 必须与其区域建立连接，因为该区域提供对快照的运行状况至关重要的访问、授权、日志记录和监控服务。如果没有连接，则您无法创建新的本地快照、创建卷或从现有本地快照实例启动实例，也无法删除本地快照。

7. 删除本地快照多久后 Amazon S3 存储容量可供使用？

   Amazon S3 存储容量在删除引用它们的本地快照和卷后 72 小时内可供使用。

8. 我如何确保不会在我的 Outpost 上耗尽 Amazon S3 容量？

   我们建议您使用 Amazon CloudWatch 警报来监控 Amazon S3 存储容量，并删除不再需要的快照和卷，以避免存储容量耗尽。如果您在使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期，请确保快照保留策略保留快照的时间不超过所需时长。

9. 如果我的 Outposts 上的本地 Amazon S3 容量用尽，会发生什么情况？

   如果您的 Outposts 上的本地 Amazon S3 容量不足，Amazon Data Lifecycle Manager 将无法在 Outposts 上成功创建本地快照。Amazon Data Lifecycle Manager 将尝试在 Outposts 上创建本地快照，但快照会立即过渡到 `error` 状态，最终会被 Amazon Data Lifecycle Manager 删除。建议使用 `SnapshotsCreateFailed` Amazon CloudWatch 指标监控快照生命周期策略，以监控快照创建失败的情况。有关更多信息，请参阅使用 Amazon CloudWatch 监控您的策略 (p. 1487)。

10. 我能否将本地快照以及由本地快照支持的 AMI 与竞价型实例和竞价型实例集一起使用？

    不能，您不能使用本地快照以及由本地快照支持的 AMI 启动竞价型实例或竞价型实例集。

11. 我是否可以对本地快照及由本地快照支持的 AMI 使用 Amazon EC2 Auto Scaling？

    是的，您可以使用本地快照及由本地快照支持的 AMI，在与快照位于同一个 Outpost 的子网中启动 Auto Scaling 组。Amazon EC2 Auto Scaling 组服务相关角色必须具有使用用于加密快照的 KMS 密钥 的权限。

    您不能使用本地快照或由本地快照支持的 AMI 在 Amazon 区域中启动 Auto Scaling 组。

先决条件

要在 Outpost 上存储快照，您必须拥有配置了 Amazon S3 on Outposts 的 Outpost。有关 Amazon S3 on Outposts 的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用 Amazon S3 on Outposts。

注意事项

使用本地快照时请记住以下事项。

- Outpost 必须具有与其 Amazon 区域的连接才能使用本地快照。
- 快照元数据存储在与 Outpost 关联的 Amazon 区域中。其中不包括任何快照数据。
- 存储在 Outpost 上的快照默认处于加密状态。不支持非加密快照。在 Outpost 上创建的快照和复制到 Outpost 的快照，将使用区域的默认 KMS 密钥 或您在请求时指定的其他 KMS 密钥 进行加密。
- 当您从 本地快照 在 Outpost 上创建卷时，不能使用其他 KMS 密钥 对卷重新加密。从 本地快照 创建的卷必须使用与源快照相同的 KMS 密钥 进行加密。
- 从 Outpost 中删除本地快照后，删除的快照所使用的 Amazon S3 存储容量将在 72 小时内可供使用。有关更多信息，请参阅删除本地快照 (p. 1418)。
- 您不能从 Outpost 导出本地快照。
- 您不能为本地快照启用快速快照还原。
- EBS direct API 不支持本地快照。
- 您不能将本地快照或 AMI 从 Outpost 复制到某个 Amazon 区域、在 Outpost 之间或在 Outpost 内复制。但是，您可以将快照从 Amazon 区域复制到 Outpost。有关更多信息，请参阅将快照从 Amazon 区域复制到 Outpost (p. 1416)。
- 将快照从 Amazon 区域复制到 Outpost 时，数据将通过服务链路传输。同时复制多个快照可能会影响在 Outpost 上运行的其他服务。

- 您不能共享本地快照。
- 您必须使用 IAM policy 来确保满足数据驻留要求。有关更多信息，请参阅使用 IAM 控制访问 (p. 1412)。
- 本地快照执行增量备份。只保存卷中在最近快照之后发生更改的数据块。每个本地快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的全部信息。有关更多信息，请参阅快照的工作原理 (p. 1369)。
- 您不能使用 IAM policy 为 CopySnapshot 和 CopyImage 操作执行数据驻留。

使用 IAM 控制访问

您可以使用 Amazon Identity and Access Management（IAM）策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在使用本地快照时拥有的权限。以下示例策略可用于授予或拒绝对本地快照执行特定操作的权限。

> **Important**
>
> 目前不支持将快照和映像从 Outpost 复制到区域。因此，您目前无法使用 IAM policy 为 CopySnapshot 和 CopyImage 操作执行数据驻留。

主题

- 为快照执行数据驻留 (p. 1412)
- 禁止委托人删除本地快照 (p. 1413)

为快照执行数据驻留

以下示例策略禁止所有委托人从 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef` 上的卷和实例创建快照并将快照数据存储在 Amazon 区域中。委托人仍然可以创建本地快照。此策略可确保所有快照都保留在 Outpost 上。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

禁止委托人删除本地快照

以下示例策略禁止所有委托人删除存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上的本地快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

使用本地快照

下面几节介绍如何使用本地快照。

主题

- 存储快照的规则 (p. 1413)
- 从 Outpost 上的卷创建本地快照 (p. 1414)
- 从 Outpost 上的实例创建多卷本地快照 (p. 1414)
- 从本地快照创建 AMI (p. 1415)
- 将快照从 Amazon 区域复制到 Outpost (p. 1416)
- 将 AMI 从 Amazon 区域复制到 Outpost (p. 1417)
- 从本地快照创建卷 (p. 1417)
- 从由本地快照支持的 AMI 启动实例 (p. 236)
- 删除本地快照 (p. 1418)
- 在 Outpost 上自动执行快照 (p. 1418)

存储快照的规则

以下规则适用于快照存储：

- 如果卷的最新快照存储在某个 Outpost 中，则所有后续快照都必须存储在同一个 Outpost 中。
- 如果卷的最新快照存储在某个 Amazon 区域中，则所有后续快照都必须存储在同一区域中。要开始从该卷创建本地快照，请执行以下操作：

  1. 在 Amazon 区域中创建卷的快照。

2. 将快照从 Amazon 区域复制到 Outpost。
3. 从本地快照创建新卷：
4. 将卷附加到 Outpost 上的实例。

对于 Outpost 上的新卷，下一个快照可以存储在 Outpost 或 Amazon 区域中。然后必须将所有后续快照存储在同一位置。

- 本地快照，包括在 Outpost 上创建的快照以及从 Amazon 区域复制到 Outpost 的快照，只能用于在同一个 Outpost 上创建卷。
- 如果您从某个区域中的快照在 Outpost 上创建卷，则该新卷的所有后续快照都必须位于同一区域中。
- 如果您从本地快照在 Outpost 上创建卷，则该新卷的所有后续快照都必须位于同一个 Outpost 中。

从 Outpost 上的卷创建本地快照

您可以从 Outpost 上的卷创建本地快照。您可以选择将快照存储在源卷所在的同一 Outpost 中，也可以选择将快照存储在 Outpost 的区域中。

本地快照只能用于在同一个 Outpost 上创建卷。

您可以使用以下方法之一从 Outpost 上的卷创建本地快照。

Console

从 Outpost 上的卷创建本地快照

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Volumes。
2. 选择 Outpost 上的卷，依次选择 Actions (操作) 和 Create Snapshot (创建快照)。
3. （可选）对于 Description (描述)，输入对快照的简短描述。
4. 对于 Snapshot destination (快照目标)，选择 Amazon Outpost。快照将在源卷所在的同一 Outpost 上创建。Outpost ARN 字段显示了目标 Outpost 的 Amazon Resource Name (ARN)。
5. （可选）选择添加标签以向快照添加标签。对于每个标签，提供标签键和标签值。
6. 选择 Create Snapshot (创建快照)。

Command line

从 Outpost 上的卷创建本地快照

使用 create-snapshot 命令。指定要从中创建快照的卷的 ID，以及存储快照的目标 Outpost 的 ARN。如果省略 Outpost ARN，则快照将存储在该 Outpost 的 Amazon 区域中。

例如，以下命令创建卷 `vol-1234567890abcdef0` 的本地快照，然后将快照存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上。

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --outpost-arn
 arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description
 "single volume local snapshot"
```

从 Outpost 上的实例创建多卷本地快照

您可以从 Outpost 上的实例创建崩溃一致性多卷本地快照。您可以选择将快照存储在源实例所在的同一 Outpost 中，也可以存储在 Outpost 的区域中。

多卷本地快照只能用于在同一个 Outpost 上创建卷。

您可以使用以下方法之一从 Outpost 上的实例创建多卷本地快照。

Console

从 Outpost 上的实例创建多卷本地快照

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots (快照)。
2. 选择 Create Snapshot (创建快照)。
3. 对于选择资源类型，选择实例。
4. 对于 Instance ID (实例 ID)，在 Outpost 上选择要从中创建快照的实例。
5. （可选）对于 Description (描述)，输入对快照的简短描述。
6. 对于 Snapshot destination (快照目标)，选择 Amazon Outpost。快照将在源实例所在的同一 Outpost 上创建。前 Outpost ARN (哨站 ARN) 显示了目标 Outpost 的 ARN。
7. 若要从多卷快照集中排除实例的根卷，选择 Exclude root volume（排除根卷）。如果这样做，Amazon EBS 将不会创建实例根卷的快照。
8. 若要从多卷快照集中排除特定数据卷，请选择 Exclude specific data volumes（排除特定数据卷）。Attached data volumes（附加的数据卷）部分列出了当前附加到所选实例的所有数据卷。

   在 Attached data volumes（附加的数据卷）部分，取消选择要从多卷快照集中排除的数据卷。只有选中的卷才会包含在多卷快照集中。
9. （可选）若要自动将标签从源卷复制到相应快照，请为 Copy tags from source volume（从源卷复制标签）选择 Copy tags（复制标签）。这将设置快照元数据（如访问策略、附件信息和成本分配）以匹配源卷。
10. （可选）若要为快照分配自定义标签，请在 Tags（标签）部分选择 Add tag（添加标签），然后输入键值对。您最多可以添加 50 个标签。
11. 选择 Create Snapshot (创建快照)。

    快照创建期间，将一起管理快照。如果卷集中的某个快照失败，则卷集中的其他快照将移至错误状态。

Command line

从 Outpost 上的实例创建多卷本地快照

使用 create-snapshots 命令。指定要从中创建快照的实例的 ID，以及存储快照的目标 Outpost 的 ARN。如果省略 Outpost ARN，则快照将存储在 Outpost 的 Amazon 区域中。

例如，以下命令创建附加到实例 `i-1234567890abcdef0` 的卷的快照，并将快照存储在 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0` 上。

```
$ aws ec2 create-snapshots --instance-specification InstanceId=i-1234567890abcdef0 --
outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --
description "multi-volume local snapshots"
```

从本地快照创建 AMI

您可以使用本地快照和存储在 Outpost 区域中的快照组合来创建 Amazon Machine Image (AMI)。例如，如果您在 `us-east-1` 中有一个 Outpost，则可以使用由该 Outpost 上的本地快照支持的数据卷，以及由 `us-east-1` 区域中的快照支持的根卷来创建一个 AMI。

Note

- 您不能创建包含存储在多个 Outpost 中的备份快照的 AMI。
- 目前，您无法使用 CreateImage API 或 Amazon EC2 控制台，为通过 Amazon S3 on Outposts 启用的 Outpost，直接从 Outpost 上的实例创建 AMI。
- 由本地快照支持的 AMI 只能用于在同一个 Outpost 上启动实例。

从区域中的快照在 Outpost 上创建 AMI

1. 将快照从区域复制到 Outpost。有关更多信息，请参阅将快照从 Amazon 区域复制到 Outpost (p. 1416)。
2. 通过 Amazon EC2 控制台或 register-image 命令使用 Outpost 上的快照副本创建 AMI。有关更多信息，请参阅从快照创建 AMI。

从 Outpost 上的实例在 Outpost 上创建 AMI

1. 从 Outpost 上的实例创建快照并将快照存储在该 Outpost 中。有关更多信息，请参阅从 Outpost 上的实例创建多卷本地快照 (p. 1414)。
2. 通过 Amazon EC2 控制台或 register-image 命令使用本地快照创建 AMI。有关更多信息，请参阅从快照创建 AMI。

从 Outpost 上的实例在区域中创建 AMI

1. 从 Outpost 上的实例创建快照并将快照存储在区域中。有关更多信息，请参阅 从 Outpost 上的卷创建本地快照 (p. 1414) 或 从 Outpost 上的实例创建多卷本地快照 (p. 1414)。
2. 使用 Amazon EC2 控制台或 寄存器映像 命令使用区域中的快照副本创建 AMI。有关更多信息，请参阅从快照创建 AMI。

将快照从 Amazon 区域复制到 Outpost

您可以将快照从 Amazon 区域复制到 Outpost。仅当快照位于 Outpost 的区域中时，才能执行此操作。如果快照位于其他区域，则必须先将快照复制到该 Outpost 的区域，再将其从该区域复制到该 Outpost。

Note

您不能将本地快照从 Outpost 复制到某个区域、在 Outpost 之间或在 Outpost 内复制。

您可以使用以下方法之一将快照从区域复制到 Outpost。

Console

将快照从 Amazon 区域复制到 Outpost

通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择 Snapshots。
2. 在区域中选择快照，然后选择 Actions (操作) 和 Copy (复制)。
3. 对于 Destination Region (目标区域)，选择目标 Outpost 的区域。
4. 对于 Snapshot Destination (快照目标)，选择 Amazon Outpost。

   仅当您在所选目标区域中有 Outpost 时，才会显示 Snapshot Destination (快照目标)字段。如果该字段未显示，则表示选定的目标区域中没有任何 Outpost。
5. 对于 Destination Outpost ARN (目标 Outpost ARN)，输入要将快照复制到的 Outpost 的 ARN。
6. （可选）对于 Description (描述)，输入对复制的快照的简要描述。
7. 默认情况下，快照副本启用加密。无法禁用加密。对于 KMS 密钥，选择要使用的 KMS 密钥。

8. 选择 Copy (复制)。

Command line

将快照从区域复制到 Outpost

使用 copy-snapshot 命令。指定要复制的快照的 ID、要从中复制快照的区域以及目标 Outpost 的 ARN。

例如，以下命令将快照 snap-1234567890abcdef0 从 us-east-1 区域复制到 Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0。

```
$ aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-
id snap-1234567890abcdef0 --destination-outpost-arn arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0 --description "Local snapshot copy"
```

将 AMI 从 Amazon 区域复制到 Outpost

您可以将 AMI 从 Amazon 区域复制到 Outpost。当您将 AMI 从区域复制到 Outpost 时，与该 AMI 关联的所有快照都将从该区域复制到该 Outpost。

仅当与 AMI 关联的快照位于 Outpost 的区域中时，您才能将该 AMI 从该区域复制到该 Outpost。如果快照位于其他区域，则必须先将 AMI 复制到该 Outpost 的区域，再将其从该区域复制到该 Outpost。

Note

您不能将 AMI 从 Outpost 复制到某个区域、在 Outpost 之间或在 Outpost 内复制。

您只能使用 Amazon CLI 将 AMI 从区域复制到 Outpost。

Command line

将 AMI 从区域复制到 Outpost

使用 copy-image 命令。指定要复制的 AMI 的 ID、源区域和目标 Outpost 的 ARN。

例如，以下命令将 AMI ami-1234567890abcdef0 从 us-east-1 区域复制到 Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0。

```
$ aws ec2 copy-image --source-region us-east-1 --source-image-id ami-1234567890abcdef0
 --name "Local AMI copy"  --destination-outpost-arn arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0
```

从本地快照创建卷

您可以从本地快照在 Outpost 上创建卷。卷必须在源快照所在同一个 Outpost 上创建。您不能使用本地快照在 Outpost 的区域中创建卷。

从 本地快照 创建卷时，不能使用不同的 KMS 密钥 对卷重新加密。从 本地快照 创建的卷必须使用与源快照相同的 KMS 密钥 进行加密。

有关更多信息，请参阅从快照创建卷 (p. 1346)。

从由本地快照支持的 AMI 启动实例

您可以从由本地快照支持的 AMI 启动实例。您必须在源 AMI 所在的同一 Outpost 中启动实例。有关更多信息，请参阅 Amazon Outposts 用户指南中的在 Outpost 中启动实例。

删除本地快照

您可以从 Outpost 中删除本地快照。从 Outpost 中删除快照后，已删除快照使用的 Amazon S3 存储容量将在删除快照和引用该快照的卷后 72 小时内可用。

由于 Amazon S3 存储容量不会立即可用，我们建议您使用 Amazon CloudWatch 警报来监控 Amazon S3 存储容量。应删除不再需要的快照和卷，以避免存储容量耗尽。

有关删除快照的更多信息，请参阅删除快照 (p. 1376)。

在 Outpost 上自动执行快照

您可以创建 Amazon Data Lifecycle Manager 快照生命周期策略，使之自动创建、复制、保留和删除 Outpost 上卷和实例的快照。您可以选择是将快照存储在区域中，还是在 Outpost 上本地存储。此外，您还可以将在 Amazon 区域中创建和存储的快照自动复制到 Outpost。

下表显示了支持的功能的概述。

资源位置	快照目标	跨区域复制		快速快照还原	跨账户共享
		复制到区域	复制到 Outpost		
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

注意事项

- 目前仅支持 Amazon EBS 快照生命周期策略。不支持由 EBS 支持的 AMI 策略和跨账户共享事件策略。
- 如果有策略管理某个区域中卷或实例的快照，则快照将在源资源所在同一区域中创建。
- 如果有策略管理 Outpost 上卷或实例的快照，则可以在源 Outpost 或该 Outpost 的区域中创建快照。
- 单个策略无法同时管理区域中的快照和 Outpost 上的快照。如果您需要在区域和 Outpost 中自动执行快照，则必须分别创建策略。
- 在 Outpost 上创建的快照或复制到 Outpost 的快照不支持快照还原。
- 在 Outpost 上创建的快照不支持跨账户共享。

有关创建可管理本地快照的快照生命周期的更多信息，请参阅自动化快照生命周期 (p. 1451)。

使用 EBS direct API 访问 EBS 快照的内容

您可以使用 Amazon Elastic Block Store (Amazon EBS) 直接 API 创建 EBS 快照，将数据直接写入快照，读取快照上的数据，并标识两个快照之间的差异或发生的更改。如果您是为 Amazon EBS 提供备份服务的独立软件供应商 (ISV)，则利用 EBS direct API，可以更高效、更具成本效益地通过快照跟踪 EBS 卷上的增量更改。无需从快照创建新卷，然后使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例来比较差异，即可完成此操作。

您可以从本地数据直接创建增量快照到 EBS 卷和云中，以用于快速灾难恢复。通过写入和读取快照的功能，您可以在发生灾难时将本地数据写入 EBS 快照。然后在灾难恢复后，您可以将其从快照恢复到 Amazon 或本地。您不再需要构建和维护复杂的机制来将数据复制到 Amazon EBS 或从中复制数据。

本用户指南概述了构成 EBS direct API 的元素，并提供了如何有效使用这些元素的示例。有关 API 的操作、数据类型、参数和错误的更多信息，请参阅 EBS direct API 参考。有关支持的 Amazon 区域、终端节点以及

EBS 直接 API 的服务配额的更多信息，请参阅 Amazon General Reference 中的 Amazon EBS 终端节点和配额。

目录

- 了解 EBS direct API (p. 1419)
- EBS 直接 API 的 IAM 权限 (p. 1420)
- 使用 EBS 直接 API (p. 1424)
- EBS 直接 API 的定价 (p. 1440)
- 将接口 VPC 终端节点与 EBS 直接 API 结合使用 (p. 1441)
- 使用 Amazon CloudTrail 记录 EBS 直接 API 的 API 调用 (p. 1441)
- 常见问题 (p. 1447)

了解 EBS direct API

下面是您在开始使用 EBS direct API 前应了解的关键元素。

快照

快照是备份 EBS 卷中的数据的主要方式。使用 EBS direct API，您还可以将数据从本地磁盘备份到快照。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。有关更多信息，请参阅Amazon EBS 快照 (p. 1368)。

> **Note**
>
> EBS direct API 不支持公有快照。

数据块

数据块是快照中的数据片段。每个快照可以包含数千个数据块。快照中的所有数据块都具有固定大小。

数据块索引

数据块索引是以 512 KiB 数据块为单位的逻辑索引。若要确定数据块索引，请用逻辑卷中数据的逻辑偏移量除以数据块大小（数据的逻辑偏移量/524288）。数据的逻辑偏移量必须与 512 KiB 一致。

数据块令牌

数据块令牌是快照中的数据块的标识哈希，它用于查找数据块数据。EBS direct API 返回的数据块令牌是临时的。它们根据为其指定的到期时间戳发生更改，或者在您为同一个快照运行 ListSnapshotBlocks 或 ListChangedBlocks 请求时发生更改。

校验和

校验和是从数据块中派生的大小很小的基准值，用于检测其传输或存储过程中引入的错误。EBS direct API 使用校验和验证数据完整性。从 EBS 快照读取数据时，该服务会为传输的每个数据块提供 Base64 编码的 SHA256 校验和，您可以使用这些校验和进行验证。向 EBS 快照写入数据时，您必须为传输的每个数据块提供一个 Base64 编码的 SHA256 校验和。服务使用提供的校验和验证接收的数据。有关更多信息，请参阅本指南下文中的使用校验和 (p. 1436)。

加密

通过加密，您的数据将转换为无法读取的代码，只能由有权访问加密数据所用 KMS 密钥 的人员破译这些代码，从而为数据提供保护。您可以使用 EBS direct API 读取和写入加密快照，但存在一些限制。有关更多信息，请参阅本指南下文中的使用加密 (p. 1433)。

API 操作

EBS direct API 由六个操作组成。包含三个读取操作和三个写入操作。读取操作包括：

- ListSnapshotBlocks — 返回指定快照中数据块的数据块索引和数据块令牌。
- ListChangedBlocks — 返回同一卷和快照谱系的两个指定快照之间，存在不同的数据块的数据块索引和数据块令牌。
- GetSnapshotBlock — 返回指定快照 ID、数据块索引和数据块令牌的数据块中的数据。

写入操作包括：

- StartSnapshot — 开始拍照，可以是现有快照的增量快照，或者全新的快照。已开始快照会停留在“待处理”状态，直到通过使用 CompleteSnapshot 操作将其完成。
- PutSnapshotBlock — 将数据以单个数据块的形式添加到已开始快照中。您必须为传输的数据块指定一个 Base64 编码的 SHA256 校验和。该服务会在传输完成以后验证校验和。若该服务计算的校验和与您指定值的不匹配，请求将会失败。
- CompleteSnapshot — 完成一个处于“待处理”状态的已开始快照。然后，该快照的状态会更改为“已完成”。

EBS 直接 API 的 IAM 权限

用户必须具有以下策略才能使用 EBS direct API。有关更多信息，请参阅更改用户权限。

有关 EBS 直接 API 资源、操作和用于 IAM 权限策略中的条件上下文键的更多信息，请参阅服务授权参考中的 Amazon Elastic Block Store 的操作、资源和条件键。

> **Important**
>
> 向 用户分配以下策略时请小心谨慎。通过分配这些策略，您可以向通过 Amazon EC2 API（例如 CopySnapshot 或 CreateVolume 操作）拒绝其访问同一资源的用户授予访问权限。

读取快照的权限

以下策略允许对指定 Amazon 区域中的所有快照使用读取 EBS 直接 API。在该策略中，将 *<Region>* 替换为快照的区域。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

以下策略允许在对具有特定键/值标记的快照使用读取 EBS 直接 API。在策略中，将 *<Key>* 替换为标签的键值，并将 *<Value>* 替换为标签的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

以下策略允许仅对账户中特定时间范围内的所有快照使用读取 EBS 直接 API。此策略授权基于 `aws:CurrentTime` 全局条件键使用 EBS 直接 API。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

写入快照的权限

以下策略允许对指定 Amazon 区域中的所有快照使用写入 EBS 直接 API。在该策略中，将 *<Region>* 替换为快照的区域。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
```

```
}
```

以下策略允许在对具有特定键/值标记的快照使用写入 EBS 直接 API。在策略中，将 *<Key>* 替换为标签的键值，并将 *<Value>* 替换为标签的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

以下策略允许使用所有 EBS direct API。只有在指定了父快照 ID 时，它才允许执行 `StartSnapshot` 操作。因此，此策略会阻止在不使用父快照的情况下开始新快照的功能。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

以下策略允许使用所有 EBS direct API。它还允许只为新快照创建 `user` 标签键。此策略还确保用户有权创建标签。`StartSnapshot` 操作是唯一可以指定标签的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
            }
        },
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

以下策略允许仅对账户中特定时间范围内的所有快照使用写入 EBS 直接 API。此策略授权基于 `aws:CurrentTime` 全局条件键使用 EBS 直接 API。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

Amazon KMS keys 使用权限

以下策略授予使用特定 KMS 密钥解密已加密快照的权限。该策略还授予使用 EBS 加密的默认 KMS 密钥来加密新快照的权限。在策略中，将 *<Region>* 替换为 KMS 密钥的区域，将 *<AccountId>* 替换为 KMS 密钥的 Amazon 账户 ID，并将 *<KeyId>* 替换为 KMS 密钥 ID。

> **Note**
>
> 默认情况下，账户中的所有主体都可以访问用于 Amazon EBS 加密的默认 Amazon 托管式 KMS 密钥，并可将其用于 EBS 加密和解密操作。如果您使用的是客户托管式密钥，则必须创建新的密钥策略或修改客户托管式密钥的现有密钥策略，以便授予主体对客户托管式密钥的访问权限。有关更多信息，请参阅Amazon Key Management Service开发人员指南中的在 Amazon KMS 中使用密钥策略。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 `kms:GrantIsForAWSResource` 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "ec2:CreateTags",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

使用 EBS 直接 API

以下主题介绍如何使用 EBS 直接 API 读取和写入快照。您只能使用 Amazon CLI、Amazon API 和 Amazon 开发工具包读取和写入快照。有关更多信息，请参阅：

- 安装 Amazon CLI和配置 Amazon CLI
- EBS 直接 API 参考
- Amazon 开发工具包

> **Important**
>
> EBS direct API 需要 Amazon 签名版本 4 签名。有关更多信息，请参阅使用签名版本 4 签名 (p. 1435)。

主题

- 使用 EBS 直接 API 读取快照 (p. 1424)
- 使用 EBS 直接 API 写入快照 (p. 1430)
- 使用加密 (p. 1433)
- 使用签名版本 4 签名 (p. 1435)
- 使用校验和 (p. 1436)
- StartSnapshot API 的幂等性 (p. 1436)
- 错误重试 (p. 1437)
- 优化性能 (p. 1438)
- EBS 直接 API 服务端点 (p. 1438)

使用 EBS 直接 API 读取快照

以下步骤介绍了如何使用 EBS direct API 读取快照：

1. 使用 ListSnapshotBlocks 操作可查看快照中数据块的数据块索引和数据块令牌。使用 ListChangedBlocks 操作也可查看同一卷和快照谱系的两个指定快照之间，存在不同的数据块的数据块索引和数据块令牌。这些操作可帮助您标识可能希望获取其数据的数据块的数据块令牌和数据块索引。

2. 使用 GetSnapshotBlock 操作，请指定要获取其数据的数据块的数据块索引和数据块令牌。

以下示例显示如何使用 EBS 直接 API 读取快照。

主题

- 列出快照中的数据块 (p. 1425)
- 列出两个快照之间存在不同的数据块 (p. 1426)
- 从快照获取数据块数据 (p. 1429)

列出快照中的数据块

Amazon CLI

以下 list-snapshot-blocks 示例命令返回快照 snap-0987654321 中数据块的数据块索引和数据块令牌。--starting-block-index 参数将结果限制为索引大于 1000 的数据块，并且 --max-results 参数将结果限制为前 100 个数据块。

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000
 --max-results 100
```

以下为上一个命令的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
              "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
          },
          {
              "BlockIndex": 1002,
              "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
          },
          {
              "BlockIndex": 1007,
              "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
          },
          {
              "BlockIndex": 1012,
              "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
          },
          {
              "BlockIndex": 1030,
              "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
          },
          {
              "BlockIndex": 1031,
              "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
          },
          ...
      ],
      "ExpiryTime": 1576287332.806,
```

```
      "VolumeSize": 32212254720,
      "BlockSize": 524288
  }
```

Amazon API

以下 ListSnapshotBlocks 示例请求返回快照 snap-0acEXAMPLEcf41648 中数据块的数据块索引和数据块令牌。startingBlockIndex 参数将结果限制为索引大于 1000 的数据块，并且 maxResults 参数将结果限制为前 100 个数据块。

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 GetSnapshotBlock 操作，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
              "BlockToken":
 "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
          },
          {
              "BlockIndex": 3073,
              "BlockToken":
 "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
          },
          ...
      ],
      "ExpiryTime": 1.59298379649E9,
      "VolumeSize": 3
  }
```

列出两个快照之间存在不同的数据块

在发出分页请求以列出两个快照之间发生更改的块时应注意以下几点：

- 响应可能包含一个或多个空的 ChangedBlocks 数组。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 0 – 999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 999 的增量快照。

  使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照发生更改的块时，将返回一个空的 ChangedBlocks 数组。您必须使用 nextToken 请求剩余的结果，直到第十个结果集（其中包括块索引为 900 - 999 的块）返回发生更改的块为止。
- 响应可能回跳过快照中未写入的块。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 2000 – 2999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 2000 的增量快照。

  使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照中发生更改的块时，响应将跳过块索引 0 - 1999 并将包含块索引 2000。响应不会包含空的 ChangedBlocks 数组。

Amazon CLI

以下 list-changed-blocks 示例命令返回快照 snap-1234567890 与 snap-0987654321 之间存在不同的数据块的数据块索引和数据块令牌。--starting-block-index 参数将结果限制为索引大于 0 的数据块，并且 --max-results 参数将结果限制为前 500 个数据块。

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

以下为上一个命令的示例响应，其中显示了两个快照的数据块索引 0、6000、6001、6002 和 6003 存在不同。此外，数据块索引 6001、6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
              "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
          },
          {
              "BlockIndex": 6000,
              "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
              "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
          },
          {
              "BlockIndex": 6001,
              "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
          },
          {
              "BlockIndex": 6003,
```

```
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
         },
         ...
     ],
     "ExpiryTime": 1576308931.973,
     "VolumeSize": 32212254720,
     "BlockSize": 524288,
     "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//O6Mdi/
BbJarBnp8h"
  }
```

Amazon API

以下 ListChangedBlocks 示例请求返回快照 snap-0acEXAMPLEcf41648 与 snap-0c9EXAMPLE1b30e2f 之间存在不同的数据块的数据块索引和数据块令牌。startingBlockIndex 参数将结果限制为索引大于 0 的数据块，并且 maxResults 参数将结果限制为前 500 个数据块。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了两个快照的数据块索引 0、3072、6002 和 6003 存在不同。此外，数据块索引 6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 GetSnapshotBlock 操作，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
              "FirstBlockToken": "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/
Yb24MaS",
              "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
```

```
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1.592976647009E9,
    "VolumeSize": 3
 }
```

从快照获取数据块数据

Amazon CLI

以下 get-snapshot-block 示例命令返回快照 6001 中，数据块令牌为 AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR 的数据块索引 snap-1234567890 中的数据。在 Windows 计算机上，二进制数据将输出到 data 目录中的 C:\Temp 文件。如果您在 Linux 或 Unix 计算机上运行该命令，请将输出路径替换为 /tmp/data 以将数据输出到 data 目录中的 /tmp 文件。

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-
token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

以下为上一个命令的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及校验和的算法。二进制数据会自动保存到您在请求命令中指定的目录和文件中。

```
{
     "DataLength": "524288",
     "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
     "ChecksumAlgorithm": "SHA256"
 }
```

Amazon API

以下 GetSnapshotBlock 示例请求返回快照 3072 中，数据块令牌为 AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid 的数据块索引 snap-0c9EXAMPLE1b30e2f 中的数据。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及用于生成校验和的算法。二进制数据在响应的正文中传输，并在以下示例中以 *BlockData* 表示。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
```

```
Date: Wed, 17 Jun 2020 23:28:38 GMT
Connection: keep-alive

BlockData
```

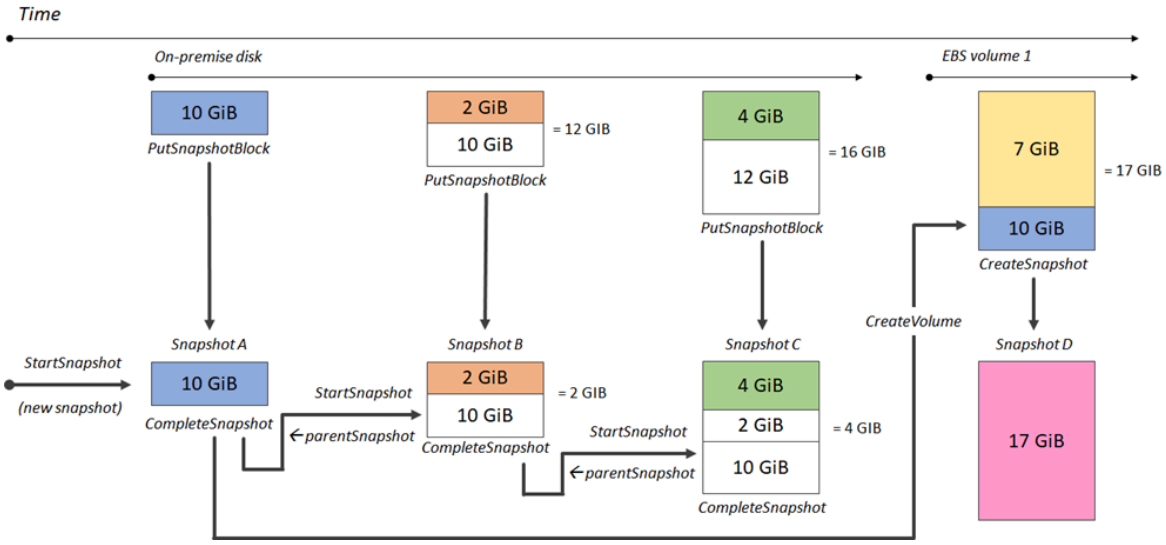
使用 EBS 直接 API 写入快照

以下步骤介绍了如何使用 EBS direct API 写入增量快照：

1. 使用 StartSnapshot 操作并指定父快照 ID，可以启动一个快照作为现有快照的增量快照，忽略父快照 ID 可启动新快照。此操作返回处于“待处理”状态的新快照 ID。
2. 使用 PutSnapshotBlock 操作并指定待处理快照的 ID，以便以单个数据块的形式向其添加数据。您必须为传输的数据块指定一个 Base64 编码的 SHA256 校验和。服务将计算接收到的数据的校验和，并使用您指定的校验和对其进行验证。如果校验和不匹配，则操作失败。
3. 当您完成将数据添加到待处理快照的操作后，使用 CompleteSnapshot 操作启动一个异步工作流，用于密封快照并将其移动到已完成状态。

重复这些步骤，使用之前创建的快照作为父级创建新的增量快照。

例如，在下图中，快照 A 是启动的第一个新快照。快照 A 用作父快照来启动快照 B。快照 B 用作父快照来启动和创建快照 C。快照 A、B 和 C 均为增量快照。快照 A 用于创建 EBS 卷 1。快照 D 创建自 EBS 卷 1。快照 D 是 A 的增量快照；它不是 B 或 C 的增量快照。



以下示例显示如何使用 EBS 直接 API 写入快照。

主题

- 启动快照 (p. 1430)
- 将数据放入快照 (p. 1432)
- 完成快照 (p. 1433)

启动快照

Amazon CLI

以下 start-snapshot 示例命令启动 8 GiB 快照，使用快照 snap-123EXAMPLE1234567 作为父快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或完成请

求，则快照将转为错误状态。550e8400-e29b-41d4-a716-446655440000 客户端令牌确保请求的幂等性。如果省略了客户端令牌，Amazon 开发工具包会自动为您生成一个。有关幂等性的更多信息，请参阅 StartSnapshot API 的幂等性 (p. 1436)。

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

以下为上一个命令的示例响应，其中显示了快照 ID、Amazon 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以 pending 状态启动。在后续 put-snapshot-block 命令中指定快照 ID 以将数据写入快照，然后使用 complete-snapshot 命令完成快照并将其状态更改为 completed。

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

Amazon API

以下 StartSnapshot 示例请求启动 8 GiB 快照，使用快照 snap-123EXAMPLE1234567 作为父快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或完成请求，则快照将转为错误状态。550e8400-e29b-41d4-a716-446655440000 客户端令牌确保请求的幂等性。如果省略了客户端令牌，Amazon 开发工具包会自动为您生成一个。有关幂等性的更多信息，请参阅 StartSnapshot API 的幂等性 (p. 1436)。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

以下为上一个请求的示例响应，其中显示了快照 ID、Amazon 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以“待处理”状态开始。在后续 PutSnapshotBlocks 请求中指定快照 ID，以将数据写入快照。

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
```

```
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

将数据放入快照

Amazon CLI

以下 put-snapshot 示例命令将 524288 字节的数据写入快照 1000 上的数据块索引 snap-0aaEXAMPLEe306d62。Base64 编码的 QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= 校验和使用 SHA256 算法生成。传输的数据位于 /tmp/data 文件中。

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

以下为上一个命令的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```
{
    "DataLength": "524288",
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

Amazon API

以下 PutSnapshot 示例请求将 524288 字节的数据写入快照 1000 上的数据块索引 snap-052EXAMPLEc85d8dd。Base64 编码的 QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= 校验和使用 SHA256 算法生成。数据在请求的正文中传输，并在以下示例中以 *BlockData* 表示。

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

          BlockData
```

以下为上一个请求的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive
```

```
{}
```

完成快照

Amazon CLI

以下 complete-snapshot 示例命令完成快照 snap-0aaEXAMPLEe306d62。该命令指定将 5 数据块写入快照。6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= 校验和表示写入快照的完整数据集的校验和。有关校验和的更多信息，请参阅本指南前文中的使用校验和 (p. 1436)。

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-count 5
 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-algorithm SHA256 --
checksum-aggregation-method LINEAR
```

以下为上一个命令的示例响应。

```
{
    "Status": "pending"
}
```

Amazon API

以下 CompleteSnapshot 示例请求完成快照 snap-052EXAMPLEc85d8dd。该命令指定将 5 数据块写入快照。6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= 校验和表示写入快照的完整数据集的校验和。

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应。

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

使用加密

使用 StartSnapshot 开启新快照时，加密状态取决于为 Encrypted、KmsKeyArn 和 ParentSnapshotId 指定的值，以及 Amazon 账户是否已启用默认加密 (p. 1507)。

Note

- 您可能需要其他 IAM 权限才能对 EBS direct API 使用加密。有关更多信息，请参阅 Amazon KMS keys 使用权限 (p. 1423)。

- 如果 Amazon 账户默认启用了 Amazon EBS 加密，则您无法创建未加密的快照。
- 如果 Amazon 账户默认启用了 Amazon EBS 加密，则您无法使用未加密父快照来开启新快照。您必须首先通过复制父快照来对其进行加密。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。

主题

- 加密结果：未加密父快照 (p. 1434)
- 加密结果：已加密父快照 (p. 1434)
- 加密结果：无父快照 (p. 1435)

加密结果：未加密父快照

下表描述了指定未加密父快照时每种可能的设置组合的加密结果。

ParentSnapshotI	已加密	KmsKeyArn	默认加密	结果
未加密	已忽略	已忽略	启用	请求失败并显示 ValidationException。
			已禁用	快照未加密。
		指定	启用	
			已禁用	
未加密	True	已忽略	启用	请求失败并显示 ValidationException。
			已禁用	
		指定	启用	
			已禁用	
未加密	False	已忽略	启用	请求失败并显示 ValidationException。
			已禁用	
		指定	启用	
			已禁用	

加密结果：已加密父快照

下表描述了指定已加密父快照时每种可能的设置组合的加密结果。

ParentSnapshotI	已加密	KmsKeyArn	默认加密	结果
已加密	已忽略	已忽略	启用	已使用与父快照相同的 KMS 密钥对快照进行加密。
			已禁用	
		指定	启用	请求失败并显示 ValidationException。
			已禁用	
已加密	True	已忽略	启用	请求失败并显示 ValidationException。

ParentSnapshotI	已加密	KmsKeyArn	默认加密	结果
			已禁用	
		指定	启用	
			已禁用	
已加密	False	已忽略	启用	请求失败并显示 `ValidationException`。
			已禁用	
		指定	启用	
			已禁用	

加密结果：无父快照

下表描述了未使用父快照时每种可能的设置组合的加密结果。

ParentSnapshotI	已加密	KmsKeyArn	默认加密	结果
已忽略	True	已忽略	启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	
		指定	启用	已使用为 KmsKeyArn 指定的 KMS 密钥对快照进行加密。
			已禁用	
已忽略	False	已忽略	启用	请求失败并显示 `ValidationException`。
			已禁用	快照未加密。
		指定	启用	请求失败并显示 `ValidationException`。
			已禁用	
已忽略	已忽略	已忽略	启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	快照未加密。
		指定	启用	已使用为 KmsKeyArn 指定的 KMS 密钥对快照进行加密。
			已禁用	

*此默认 KMS 密钥可以是客户托管式密钥或用于 Amazon EBS 加密的默认 Amazon 托管式 KMS 密钥。

使用签名版本 4 签名

签名版本 4 是将身份验证信息添加到通过 HTTP 发送的 Amazon 请求的流程。出于安全考虑，大多数 Amazon 请求都必须使用访问密钥（包括访问密钥 ID 和秘密访问密钥）进行签名。这两个密钥通常称为您的安全凭证。有关如何获取账户凭证的信息，请参阅了解并获取您的凭证。

如果您打算手动创建 HTTP 请求，则必须了解如何对其签名。当您使用（Amazon Command Line InterfaceAmazon CLI）或其中一个 Amazon 开发工具包来向 Amazon 发出请求时，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。当您使用这些工具时，您不必了解如何亲自签署这些请求。

有关更多信息，请参阅 Amazon General Reference 中的使用签名版本 4 签名 Amazon 请求。

使用校验和

GetSnapshotBlock 操作返回快照的数据块中的数据，而 PutSnapShotBlock 操作会将数据添加到快照的数据块中。传输的数据块数据不在签名版本 4 签名流程中进行签名。因此，使用校验和来验证数据的完整性，如下所示：

- 使用 GetSnapshotBlock 操作时，响应会使用 x-amz-Checksum 标头为数据块数据提供 Base64 编码的 SHA256 校验和，并使用 x-amz-Checksum-Algorithm 标头提供校验和算法。使用返回的校验和验证数据的完整性。如果生成的校验和与 Amazon EBS 提供的校验和不匹配，您应将数据视为无效，然后重试请求。
- 使用 PutSnapshotBlock 操作时，您的请求必须使用 x-amz-Checksum 标头为数据块数据提供 Base64 编码的 SHA256 校验和，并使用 x-amz-Checksum-Algorithm 标头提供校验和算法。您提供的校验和将根据 Amazon EBS 生成的校验和进行验证，以验证数据的完整性。如果校验和不相符，请求将失败。
- 当您使用 CompleteSnapshot 操作时，您的请求可以选择针对添加到快照的完整数据集，提供聚合的 Base64 编码的 SHA256 校验和。使用 x-amz-Checksum 标头提供校验和，使用 x-amz-Checksum-Algorithm 标头提供校验和算法，并使用 x-amz-Checksum-Aggregation-Method 标头提供校验和聚合方法。要使用线性聚合方法生成聚合校验和，请按照数据块索引的升序排列各个写入数据块的校验和，将它们连接成单个字符串，然后使用 SHA256 算法生成整个字符串的校验和。

这些操作中的校验和是签名版本 4 签名流程的一部分。

StartSnapshot API 的幂等性

幂等性确保 API 请求仅完成一次。对于幂等请求，如果原始请求成功完成，则后续重试将返回原始成功请求的结果，它们不会有额外的影响。

StartSnapshot API 使用客户端令牌 支持幂等性。客户端令牌是您在发出 API 请求时指定的唯一字符串。如果在某个 API 请求成功完成后，您使用相同的客户端令牌和相同的请求参数重试该请求，则返回原始请求的结果。如果使用相同的客户端令牌重试请求，但更改了一个或多个请求参数，则返回 `ConflictException` 错误。

如果您没有指定自己的客户端令牌，Amazon 开发工具包会自动为请求生成客户端令牌，以确保其幂等性。

客户端令牌可以是包含最多 64 个 ASCII 字符的任意字符串。您不应为不同的请求重复使用相同的客户端令牌。

通过 API，使用您自己的客户端令牌发出幂等 StartSnapshot 请求

指定 `ClientToken` 请求参数。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

通过 Amazon CLI，使用您自己的客户端令牌发出幂等 StartSnapshot 请求

指定 client-token 请求参数。

```
$ aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-snapshot
 snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

错误重试

Amazon SDK 对返回错误响应的请求实施自动重试逻辑。您可以为 Amazon SDK 配置重试设置。有关更多信息，请参阅 SDK 文档。

Amazon CLI 可以配置为自动重试部分失败的请求。有关配置 Amazon CLI 的重试次数的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的 Amazon CLI 重试次数。

Amazon 查询 API 不支持失败的请求的重试逻辑。如果您使用的是 HTTP 或 HTTPS 请求，则必须在客户端应用程序中实现重试逻辑。

有关更多信息，请参阅《Amazon 一般参考》中的 Amazon 中的错误重试和指数回退。

下表显示了可能的 API 错误响应。部分 API 错误是可重试的。客户端应用程序始终可以重试收到可重试错误的失败请求。

错误	响应代码	描述	由以下对象引发	可重试？
InternalServerException	500	由于网络或 Amazon 服务器端问题，请求失败。	所有 API	是
ThrottlingException	400	API 请求的数量已超过账户允许的最大 API 请求节流限制。	所有 API	是
RequestThrottledException	400	API 请求的数量已超过快照允许的最大 API 请求节流限制。	GetSnapshotBlock | PutSnapshotBlock	是
显示消息“Failed to read block data”的 ValidationException	400	提供的数据块不可读。	PutSnapshotBlock	是
显示任何其他消息的 ValidationException	400	请求语法格式错误，或输入不满足 Amazon Web Service 规定的约束。	所有 API	否
ResourceNotFoundException	404	指定的快照 ID 不存在。	所有 API	否
ConflictException	409	指定的客户端令牌曾在具有不同请求参数的类似请求中使用过。有关更多信息，请参阅StartSnapshot	StartSnapshot	否

错误	响应代码	描述	由以下对象引发	可重试？
		API 的幂等性 (p. 1436)。		
AccessDeniedException	401	您无权执行请求的操作。	所有 API	否
ServiceQuotaExceededException	402	请求失败，因为执行请求将超出您账户的一项或多项相关服务限额。	所有 API	否
InvalidSignatureException	403	请求授权签名已过期。必须刷新授权签名才能重试请求。	所有 API	否

优化性能

您可以并发运行 API 请求。假设 PutSnapshotBlock 数据块延迟为 100 毫秒，那么一个线程在一秒内可以处理 10 个请求。此外，假设您的客户端应用程序创建多个线程和连接（例如 100 个连接），那么它每秒可以发出 1000 (10 * 100) 个请求。这对应于大约每秒 500 MB 的吞吐量。

以下列表包含在您应用程序中需要了解的几点：

- 每个线程是否使用单独的连接？ 如果应用程序上的连接受限制，则多线程将等待可用连接，而您会发现吞吐量较低。
- 应用程序的两个放置请求之间是否有任何等待时间？ 这将降低线程的有效吞吐量。
- 实例的带宽限制 – 如果实例上的带宽与其他应用程序共享，则会限制 PutSnapshotBlock 请求的可用吞吐量。

请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应将重试机制内置到 EBS direct API 工作流中，以处理限制、超时和服务不可用性。

查看 EBS direct API 服务配额以确定您每秒可运行的最大 API 请求数。有关更多信息，请参阅 Amazon 一般参考 中的 Amazon Elastic Block Store 终端节点和配额。

EBS 直接 API 服务端点

端点是作为 Amazon Web 服务入口点的 URL。EBS 直接 API 支持以下端点类型：

- IPv4 端点
- 同时支持 IPv4 和 IPv6 的双堆栈端点

当您发出请求时，您可以指定要使用的端点和区域。如果不指定端点，则默认使用 IPv4 端点。要使用不同的端点类型，您必须在请求中指定。有关如何执行此操作的示例，请参阅指定端点 (p. 1439)。

有关区域的信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的区域和可用区。有关 EBS 直接 API 的端点列表，请参阅《Amazon Web Services 一般参考》中的 EBS 直接 API 的端点。

主题

- IPv4 端点 (p. 1439)
- 双栈（IPv4 和 IPv6）端点 (p. 1439)
- 指定端点 (p. 1439)

IPv4 端点

IPv4 端点仅支持 IPv4 流量。IPv4 端点适用于所有区域。

IPv4 端点名称使用以下命名约定：

- `ebs.region.amazonaws.com.cn`

例如，北京区域的 IPv4 端点名称是 `ebs.cn-northwest-1.amazonaws.com.cn`。

定价

在相同区域使用 IPv4 端点时，EBS 直接 API 和 Amazon EC2 实例之间直接传输数据是免费的。但是，如果存在中间服务，如 Amazon PrivateLink 端点、NAT 网关或 Amazon VPC Transit Gateway，则需要向您收取相关费用。

双栈（IPv4 和 IPv6）端点

同时支持 IPv4 和 IPv6 流量的双堆栈端点。双堆栈端点适用于所有区域。

要使用 IPv6，您必须使用双堆栈端点。当您向双堆栈端点发出请求时，端点 URL 解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

EBS 直接 API 只支持区域双堆栈端点，这意味着，您必须将区域指定为端点名称的一部分。双堆栈端点名称使用以下命名约定：

- `ebs.region.api.amazonwebservices.com.cn`

例如，北京区域的双堆栈端点名称为 `ebs.cn-northwest-1.api.aws`。

定价

在相同区域使用双堆栈端点时，EBS 直接 API 和 Amazon EC2 实例之间直接传输数据是免费的。但是，如果存在中间服务，如 Amazon PrivateLink 端点、NAT 网关或 Amazon VPC Transit Gateway，则需要向您收取相关费用。

指定端点

本节提供了一些在发出请求时如何指定端点的示例。

Amazon CLI

以下示例显示如何使用 Amazon CLI 为北京区域指定端点。

- 双堆栈

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.cn-northwest-1.api.amazonwebservices.com.cn
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.cn-northwest-1.amazonaws.com.cn
```

Amazon SDK for Java 2.x

以下示例显示如何使用 Amazon SDK for Java 2.x 为北京区域指定端点。

- 双堆栈

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.cn-
northwest-1.api.amazonwebservices.com.cn", "cn-northwest-1");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.cn-
northwest-1.amazonaws.com.cn", "cn-northwest-1");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

Amazon SDK for Go

以下示例显示如何使用 Amazon SDK for Go 为北京区域指定端点。

- 双堆栈

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.CnNorth1RegionID),
    Endpoint: aws.String("https://ebs.cn-northwest-1.api.amazonwebservices.com.cn")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.CnNorth1RegionID),
    Endpoint: aws.String("https://ebs.cn-northwest-1.amazonaws.com.cn")
})
```

EBS 直接 API 的定价

主题

- API 的定价 (p. 1440)
- 联网成本 (p. 1441)

API 的定价

您为使用 EBS direct API 支付的费用取决于您发出的请求数。有关更多信息，请参阅 Amazon EBS 定价。

- ListChangedBlocks 和 ListSnapshotBlocks API 按每个请求收费。例如，如果您在每 1000 个请求收取 0.0006 USD 的区域发出 100,000 个 ListSnapshotBlocks API 请求，则将向您收取 0.06 USD（每 1000 个请求 0.0006 USD x 100）的费用。
- GetSnapshotBlock 按返回的每个数据块收费。例如，如果您在针对每 1,000 个返回的数据块收取 0.003 USD 的区域发出 100,000 个 GetSnapshotBlock API 请求，则将向您收取 0.30 USD（每 1000 个返回的数据块 0.003 USD x 100）的费用。

- PutSnapshotBlock 按每个写入的数据块收费。例如，如果您在针对每 1,000 个写入的数据块收取 0.006 USD 的区域发出 100,000 个 PutSnapshotBlock API 请求，则将向您收取 0.60 USD（每 1000 个写入的数据块 0.006 USD x 100）的费用。

联网成本

数据传输成本

当使用非 FIPS 终端节点时，在相同 Amazon 区域的 EBS 直接 API 与 Amazon EC2 实例之间直接传输数据是免费的。有关更多信息，请参阅Amazon服务终端节点。如果其他 Amazon 服务处于您的数据传输路径中，将向您收取相关的数据处理费用。这些服务包括但不限于 PrivateLink 终端节点、NAT 网关和 Transit Gateway。

VPC 接口终端节点

如果您在私有子网中使用来自 Amazon EC2 实例的 EBS 直接 API 或 Amazon Lambda 函数，您可以使用 VPC 接口终端节点而不是使用 NAT 网关来降低网络数据传输成本。有关更多信息，请参阅将接口 VPC 终端节点与 EBS 直接 API 结合使用 (p. 1441)。

将接口 VPC 终端节点与 EBS 直接 API 结合使用

您可以通过创建由 Amazon PrivateLink 提供支持的接口 VPC 终端节点在 VPC 和 EBS 直接 API 之间建立私有连接。您可以访问 EBS 直接 API，就像它在您的 VPC 中一样，而无需使用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。VPC 中的实例即使没有公有 IP 地址也可与 EBS direct API 进行通信。

我们将在您为接口终端节点启用的每个子网中创建一个终端节点网络接口。

有关更多信息，请参阅 Amazon PrivateLink 指南中的通过 Amazon PrivateLink 访问 Amazon Web Services。

关于 EBS direct API VPC 终端节点的注意事项

在为 EBS 直接 API 设置接口 VPC 终端节点之前，请查看 Amazon PrivateLink 指南中的注意事项。

EBS direct API 不支持 VPC 终端节点策略。默认情况下，允许通过终端节点对 EBS direct API 进行完全访问。但是，您可以使用安全组控制对接口终端节点的访问。

为 EBS direct API 创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 Amazon Command Line Interface (Amazon CLI) 为 EBS 直接 API 创建 VPC 终端节点。有关更多信息，请参阅 Amazon PrivateLink 指南中的创建 VPC 终端节点。

使用以下服务名称为 EBS direct API 创建 VPC 终端节点：

- `com.amazonaws.region.ebs`

如果为终端节点启用私有 DNS，则可以使用其默认 DNS 名称作为区域，向 EBS direct API 发送 API 请求，例如 `ebs.us-east-1.amazonaws.com`。

使用 Amazon CloudTrail 记录 EBS 直接 API 的 API 调用

EBS direct API 服务已与 Amazon CloudTrail 集成。CloudTrail 是提供用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 将在 EBS 直接 API 中执行的所有 API 调用作为事件捕获。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新管理事件。事件

历史记录中不会捕获数据事件。可以使用 CloudTrail 收集的信息确定向 EBS 直接 API 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

有关 CloudTrail 的更多信息，请参阅 Amazon CloudTrail 用户指南。

CloudTrail 中的 EBS direct API 信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。当 EBS 直接 API 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon 账户中的事件（包括 EBS 直接 API 的事件），请创建跟踪记录。通过跟踪，CloudTrail 可将日志文件传送至 S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 S3 存储桶。此外，您可以配置其他 Amazon 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

支持的 API 操作

对于 EBS 直接 API，您可以使用 CloudTrail 记录两种类型的事件：

- 管理事件 — 通过管理事件，可以了解对在您 Amazon 账户内的快照上执行的管理操作。以下 API 操作预设情况下将作为管理事件记录在跟踪记录中：
  - StartSnapshot
  - CompleteSnapshot

  有关日志记录管理事件的更多信息，请参阅 CloudTrail 用户指南中的记录跟踪记录的管理事件。
- Data events（数据事件）— 通过这些事件，可以了解对快照执行的或在快照内执行的快照操作。以下 API 操作可以选择作为跟踪中的数据事件记录：
  - ListSnapshotBlocks
  - ListChangedBlocks
  - GetSnapshotBlock
  - PutSnapshotBlock

  预设情况下，在您创建跟踪记录时，未记录数据事件。您只能使用 advanced event selectors（高级事件选择器）来记录 EBS 直接 API 调用上的数据事件。有关更多信息，请参阅 CloudTrail 用户指南中的记录数据事件以便跟踪。

  > **Note**
  >
  > 如果您对与您共享的快照执行操作，则数据事件不会发送到拥有快照的 Amazon 账户。

身份信息

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。

- 请求是否由其它 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentityElement。

了解 EBS direct API 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下是示例 CloudTrail 日志条目。

StartSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


CompleteSnapshot


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
```

```
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```


ListSnapshotBlocks


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

ListChangedBlocks


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```


GetSnapshotBlock


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
```

```
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

常见问题

如果快照具有挂起状态，是否可以使用 EBS direct API 访问该快照？

不可以。仅当快照具有已完成状态时，才能访问该快照。

EBS direct API 是否按数字顺序返回数据块索引？

是。返回的数据块索引是唯一的，并按数字顺序排列。

我是否可以提交 MaxResults 参数值低于 100 的请求？

不可以。您可以使用的最小 MaxResult 参数值为 100。如果您提交 MaxResult 参数值低于 100 的请求，并且快照中的数据块超过 100 个，则 API 将返回至少 100 个结果。

我是否可以并发运行 API 请求？

您可以并发运行 API 请求。请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应将重试机制内置到 EBS direct API 工作流中，以处理限制、超时和服务不可用性。有关更多信息，请参阅优化性能 (p. 1438)。

查看 EBS direct API 服务配额以确定您每秒可运行的 API 请求数。有关更多信息，请参阅 Amazon General Reference 中的 Amazon Elastic Block Store 终端节点和配额。

运行 ListChangedBlocks 操作时，是否即使快照中有数据块，也有可能获得空响应？

是。如果快照中几乎没有更改的数据块，则响应可能为空，但 API 将返回下一页令牌值。使用下一页令牌值来继续转到下一页结果。当 API 返回的下一页令牌值为 null 时，您可以确认已到达最后一页结果。

如果同时指定了 NextToken 参数和 StartingBlockIndex 参数，将使用这两者中的哪一个？

使用 NextToken，并忽略 StartingBlockIndex。

数据块令牌和下一个令牌的有效期是多久？

数据块令牌的有效期为七天，下一个令牌的有效期为 60 分钟。

是否支持已加密快照？

是。可以使用 EBS direct API 访问加密快照。

要访问已加密快照，用户必须有权访问用于加密快照的 KMS 密钥和 Amazon KMS 解密操作。有关要分配给用户的 EBS 直接 API 的 IAM 权限 (p. 1420) 策略，请参阅本指南前面的 Amazon KMS部分。

是否支持公有快照？

不支持公有快照。

list snapshot block 是返回快照中的所有数据块索引和数据块令牌，还是仅返回那些写入数据的数据块索引和数据块令牌？

它只返回写入数据的数据块索引和令牌。

我能否获得 EBS direct API 在我的账户上发起的所有 API 调用的历史记录，以便用于安全分析和运营方面的故障排除？

是。要获取您账户上的 EBS direct API 的 API 调用的历史记录，请在 Amazon Web Services Management Console 中打开 Amazon CloudTrail。有关更多信息，请参阅使用 Amazon CloudTrail 记录 EBS 直接 API 的 API 调用 (p. 1441)。

自动化快照生命周期

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除用于备份 Amazon EBS 卷的快照。

有关更多信息，请参阅Amazon Data Lifecycle Manager (p. 1448)。

Amazon Data Lifecycle Manager

您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除 EBS 快照和 EBS 支持的 AMI。当您执行自动快照和 AMI 管理时，它可以帮助您：

- 通过实施定期备份计划来保护重要数据。
- 创建可定期刷新的标准化 AMI。
- 按照审核员的要求或内部合规性保留备份。
- 通过删除过时的备份来降低存储成本。
- 创建将数据备份到隔离账户的灾难恢复备份策略。

结合使用 Amazon CloudWatch Events 和 Amazon CloudTrail 的监控功能时，Amazon Data Lifecycle Manager 可提供针对 Amazon EC2 实例和单独的 EBS 卷的完整备份解决方案，而不会额外收费。

Important

Amazon Data Lifecycle Manager 不能用于管理通过任何其他方式创建的快照或 AMI。
Amazon Data Lifecycle Manager 不能用于自动创建、保留和删除由实例存储支持的 AMI。

目录

- Amazon Data Lifecycle Manager 的工作原理 (p. 1448)
- 配额 (p. 1450)
- 自动化快照生命周期 (p. 1451)
- 自动化 AMI 生命周期 (p. 1462)
- 自动执行跨账户快照副本 (p. 1467)
- 查看、修改和删除生命周期策略 (p. 1475)
- Amazon Identity and Access Management (p. 1478)
- 监控快照和 AMI 的生命周期 (p. 1486)

Amazon Data Lifecycle Manager 的工作原理

以下是 Amazon Data Lifecycle Manager 的关键要素。

元素

- 快照 (p. 1449)
- EBS 支持的 AMI (p. 1449)
- 定位资源标签 (p. 1449)
- Amazon Data Lifecycle Manager 标签 (p. 1449)
- 生命周期策略 (p. 1449)
- 政策计划 (p. 1450)

快照

快照是备份 EBS 卷中的数据的主要方式。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。在您删除卷的一系列快照中的一个快照时，只删除该快照独有的数据。将保留卷的其余捕获历史记录。有关更多信息，请参阅Amazon EBS 快照 (p. 1368)。

EBS 支持的 AMI

Amazon Machine Image (AMI) 提供启动实例所需的信息。在需要具有相同配置的多个实例时，您可以从单个 AMI 启动多个实例。Amazon Data Lifecycle Manager 仅支持 EBS 支持的 AMI。EBS 支持的 AMI 包括挂载到源实例的每个 EBS 卷的快照。有关更多信息，请参阅Amazon Machine Images (AMI) (p. 101)。

定位资源标签

Amazon Data Lifecycle Manager 使用资源标签来标识要备份的资源。在创建快照或 EBS 支持的 AMI 策略时，可以指定多个目标资源标签。至少具有指定目标资源标签之一的指定类型（实例或卷）的所有资源都将根据策略被设为目标。例如，如果您创建以卷为目标的快照策略并指定 `purpose=prod`、`costcenter=prod` 和 `environment=live` 作为目标资源标签，则该策略将以具有上述任意标签键值对的所有卷为目标。

如果要在资源上运行多个策略，可以为目标资源分配多个标签，然后创建单独的策略，每个策略都以特定的资源标签为目标。

您不能在标签键中使用 \ 或 = 字符。目标资源标签区分大小写。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。

Amazon Data Lifecycle Manager 标签

Amazon Data Lifecycle Manager 对通过策略创建的所有快照和 AMI 应用以下系统标签，以便与通过任何其他方法创建的快照和 AMI 区分开来：

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` – 适用于根据基于期限的计划创建的快照。指示何时从标准层中删除快照。
- `aws:dlm:managed`
- `aws:dlm:archived` – 适用于按计划存档的快照。

还可以在创建时指定要应用于快照和 AMI 的自定义标签。您不能在标签键中使用 \ 或 = 字符。

Amazon Data Lifecycle Manager 用于将卷与快照策略关联的目标标签可以选择性地应用于策略创建的快照。同样，用于将实例与 AMI 策略关联的目标标签也可以选择性地应用于策略创建的 AMI。

生命周期策略

生命周期策略包括以下核心设置：

- Policy type (策略类型) – 定义策略可以管理的资源类型。Amazon Data Lifecycle Manager 支持以下类型的生命周期策略：
  - 快照生命周期策略—用于自动化 EBS 快照的生命周期。这些策略可以针对连接到实例的单个 EBS 卷或所有 EBS 卷。
  - EBS 支持的 AMI 生命周期策略—用于自动化 EBS 支持的 AMI 及其备份快照的生命周期。这些策略只能针对实例。
  - 跨账户复制事件策略—用于自动执行跨账户快照副本 将此策略类型与跨账户共享快照的 EBS 快照策略结合使用。
- Resource type (资源类型)—定义策略所针对的资源类型。快照生命周期策略可以针对实例或卷。使用 `VOLUME` 创建单个卷的快照，或使用 `INSTANCE` 创建挂载到实例的所有卷的多卷快照。有关更多信息，请参阅多卷快照 (p. 1372)。AMI 生命周期策略只能针对实例。创建一个 AMI，其中包含挂载到目标实例的所有卷的快照。
- Target tags (目标标签)—指定必须分配给 EBS 卷或 Amazon EC2 实例才能成为策略目标的标签。
- 策略计划（仅限快照和 AMI 策略）— 定义创建快照或 AMI 的时间以及将它们保留多长时间。有关更多信息，请参阅政策计划 (p. 1450)。

例如，您可以使用类似以下内容的设置创建策略：

- 管理标签中包含 `account` 键和 `finance` 值的所有 EBS 卷。
- 每 24 小时在 `0900` UTC 创建快照。
- 只保留最新的五个快照。
- 每天不晚于 `0959` UTC 开始创建快照。

政策计划

策略计划定义策略创建快照或 AMI 的时间。策略最多可以有四个计划—一个强制要求的计划和最多三个可选计划。

在单个策略中添加多个计划，可让您使用同一策略按不同频率创建快照或 AMI。例如，您可以创建一个策略来按每日、每周、每月和每年的频率创建快照。这样就无需管理多个策略。

对于每个计划，您可以定义频率、快速快照还原设置（仅限快照生命周期策略）、跨区域复制规则和标签。分配给计划的标签将自动分配给启动计划时创建的快照或 AMI。此外，Amazon Data Lifecycle Manager 还会根据计划的频率自动为每个快照或 AMI 分配系统生成的标签。

每个计划都会根据其频率单独启动。如果同时启动多个计划，Amazon Data Lifecycle Manager 只会创建一个快照或 AMI，并采用保留期限最长的计划保留设置。启动的所有计划的标签都会应用于该快照或 AMI。

- （仅限快照生命周期策略）如果为启动的多个计划启用了快速快照还原，则会在所有启动的计划中指定的所有可用区内为该快照启用快速快照还原。为每个可用区使用所启动计划的最长保留期限设置。
- 如果为启动的多个计划启用了跨区域复制，则该快照或 AMI 会被复制到启动的所有计划中指定的所有区域。应用所启动计划的最长保留期限。

配额

您的 Amazon 账户具有以下与 Amazon Data Lifecycle Manager 相关的配额：

描述	配额
每区域的生命周期策略	100
每个资源的标签	45

自动化快照生命周期

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 Amazon EBS 快照生命周期。

主题

- 创建快照生命周期策略 (p. 1451)
- 快照生命周期策略的注意事项 (p. 1459)
- 其他资源 (p. 1462)

创建快照生命周期策略

使用以下过程之一创建快照生命周期策略。

Console

要创建快照策略

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在 Select policy type (选择策略类型) 页面，选择 EBS snapshot policy (EBS 快照策略)，然后选择 Next (下一步)。
4. 在 Target Resources (目标资源) 部分，执行以下操作：
   a. 对于 Target resource types (目标资源类型)，选择要备份的资源的类型。选择 `Volume` 创建各个卷的快照，或选择 `Instance` 从挂载到实例的卷创建多卷快照。
   b. （仅限 Amazon Outpost 客户）对于 Target resource location（目标资源位置），请指定目标资源的位置。
      - 如果目标资源位于某个 Amazon 区域中，请选择 Amazon 区域。Amazon Data Lifecycle Manager 仅备份当前区域中所有具有匹配目标标签的指定类型资源。如果资源位于某个区域中，则由策略创建的快照将存储在同一区域中。
      - 如果目标资源位于您账户中的 Outpost 上，请选择 Amazon Outpost。Amazon Data Lifecycle Manager 将备份您的账户中所有 Outpost 上具有匹配目标标签的全部指定类型资源。如果资源位于 Outpost 上，则策略创建的快照可以存储在资源所在同一区域或 Outpost 上。
      - 如果您的账户中没有任何 Outposts，此选项将被隐藏，且已为您选择 Amazon 区域。
   c. 对于 Target resource tags (目标资源标签)，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。
5. 对于 Description (描述)，输入策略的简短描述。
6. 对于 IAM role (IAM 角色)，选择一个有权管理快照以及描述卷和实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择 Default role (默认角色)。或者，要使用您之前创建的自定义 IAM 角色，请选择 Choose another role (选择其他角色)，然后选择要使用的角色。
7. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
8. 对于 Policy status（策略状态），选择 Enable（启用），以在下次计划时间开启策略运行，或者选择 Disable policy（禁用策略）以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始创建快照。
9. （仅适用于以实例为目标的策略）默认情况下，Amazon Data Lifecycle Manager 将创建附加到目标实例的所有卷的快照。不过，您可以选择创建附加卷子集的快照。在 Parameters（参数）部分，执行以下操作：

- 如果您不想创建附加到目标实例的根卷的快照，请选择 Exclude root volume（排除根卷）。如果选择此选项，则只有附加到目标实例的数据（非根）卷才会包含在多卷快照集中。
- 如果要创建附加到目标实例的数据（非根）卷子集的快照，请选择 Exclude specific data volumes（排除特定数据卷），然后指定用于标识不应创建快照的数据卷的标签。Amazon Data Lifecycle Manager 不会为具有任何指定标签的数据卷创建快照。Amazon Data Lifecycle Manager 仅为不具有任何指定标签的数据卷创建快照。

10. 选择 Next（下一步）。
11. 在 Configure schedule (配置计划) 页面配置策略计划。一个策略最多可以有 4 个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：

    a. 在 Schedule details (计划详细信息) 部分执行以下操作：

       i. 对于 Schedule name (计划名称)，请指定计划的描述性名称。

       ii. 在 Frequency (频率) 和相关字段中配置策略运行之间的间隔。您可以按每日、每周、每月或每年计划配置策略运行。或者，选择 Custom cron expression (自定义 Cron 表达式) 以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南 中的 Cron 表达式。

          Note

          如果您需要为此计划启用 snapshot archiving（快照存档），则必须选择 monthly（每月）或 yearly（每年）频率，或者指定一个创建频率至少为 28 天的 cron 表达式。
          如果指定一个将在特定周次的特定日期（例如，当月第二周星期四）创建快照的每月频率，则对于基于计数的计划，存档层的保留计数必须为 4 或以上。

       iii. 对于 Starting at (开始于)，请指定计划开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。时间必须输入 hh:mm UTC 格式。

       iv. 对于 Retention type (保留类型)，请指定计划创建的快照的保留策略。您可以根据其总计数或存在时间保留快照。

          - （基于计数的保留计划）如果未启用快照存档，则范围为 1 到 1000。如果您启用了快照存档，则范围为 0 到 1000。如果您指定计数为 0，则快照将在创建后立即存档。
          - （基于期限的保留计划）如果未启用快照存档，则范围为 1 天到 100 年。如果您启用了快照存档，则范围为 0 天到 100 年。如果您指定了 0 天，则快照将在创建后立即存档。

          Note

          - 所有计划必须具有相同的保留类型（基于期限或基于计数）。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。
          - 如果您启用了快速快照还原、跨区域复制或快照共享，则必须指定 1 或更大的保留计数，或者 1 天或更长的保留期。
          - 如果您启用了快照存档，则此保留规则将决定快照在存档之前在标准层中的保留时间。达到标准层的保留阈值时，快照将转换为完整快照，然后从标准层移动到存档层。

       v. （仅限 Amazon Outposts 客户）对于 Snapshot destination（快照目标），请为此策略创建的快照指定目标位置。

          - 如果策略以区域中的资源为目标，则须在同一区域中创建快照。Amazon已选定您的区域。
          - 如果策略的目标是 Outpost 上的资源，您可以选择在源资源所在同一 Outpost 上创建快照，或者在与 Outpost 关联的区域中创建快照。
          - 如果您的账户中没有任何 Outposts，此选项将被隐藏，且已为您选择 Amazon 区域。

b. 请在 Tagging (标记) 部分执行以下操作：

   i. 要将所有用户定义的标签从源卷复制到计划创建的快照，请选择 Copy tags from source (从源复制标记)。

   ii. 要指定分配给由该计划创建的快照的其他标签，请选择 Add tags (添加标签)。

c. （仅适用于以卷为目标的策略）在 Snapshot archiving（快照存档）部分中，执行以下操作：

   Note

   您在一个策略中只能为一个计划启用快照存档。

   i. 要为此计划启用快照存档，请选择 Archive snapshots created by this schedule（将此计划创建的快照存档）。

      Note

      只有在快照创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

   ii. 为存档层中的快照指定保留规则。

   - 对于基于计数的计划，指定要在存档层中保留的快照数量。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 3，则计划将在存档层中最多保留 3 个快照。存档第四个快照时，系统将会删除存档层中三个现有快照中最老的一个。
   - 对于基于期限的计划，指定要在存档层中保留快照的期限。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 120 天，则计划将在该期限届满时自动从存档层中删除快照。

      Important

      存档快照的最短保留期为 90 天。必须指定一个会将快照保留至少 90 天的保留规则。

d. 要为计划创建的快照启用快速快照还原，请在 Fast snapshot restore (快速快照还原) 部分选择 Enable fast snapshot restore (启用快速快照还原)。如果您启用快速快照还原，则必须选择要在其中启用该功能的可用区。如果计划使用基于时间的保留计划，则必须指定为每个快照启用快速快照还原的时间段。如果计划使用基于计数的保留，您必须指定要启用快速快照还原的最大快照数。

   如果计划在 Outpost 上创建快照，则无法启用快速快照还原。存储在 Outpost 上的本地快照不支持快速快照还原。

   Note

   对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。

e. 要将计划创建的快照复制到 Outpost 或其他区域，请在 Cross-Region copy (跨区域复制) 部分选择 Enable cross-Region copy (启用跨区域复制)。

   如果计划在区域中创建快照，则您可以将快照复制到账户中最多三个其他区域 或 Outpost。您必须为每个目标区域或 Outpost 指定单独的跨区域复制规则。

   对于每个区域或 Outpost，您可以选择不同的保留策略，还可以选择复制所有标签还是不复制任何标签。如果源快照已加密或默认启用加密，则会加密已复制的快照。如果源快照未加密，您可以启用加密。如果未指定 KMS 密钥，则会在每个目标区域中使用 EBS 加密的默认 KMS 密钥 对快照进行加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥 的访问权限。

Note

您必须确保没有超过每个区域的并发快照副本数。

如果策略在 Outpost 上创建快照，则无法将快照复制到区域或另一个 Outpost，并且跨区域复制设置不可用。

f. 在 Cross-account sharing (跨账户共享) 中，将策略配置为自动共享计划创建的快照与其他 Amazon 账户。执行以下操作：

   i. 要启用与其他 Amazon 账户共享，请选择 Enable cross-account sharing (启用跨账户共享)。
   ii. 要添加要与之共享快照的账户，请选择 Add account (添加账户)，输入 12 位 Amazon 账户 ID，然后选择 Add (添加)。
   iii. 要在特定时间段后自动取消共享所共享的快照，请选择 Unshare automatically（自动取消共享）。如果您选择自动将共享快照取消共享，则自动取消快照共享前的持续时间不能超过策略保留其快照的期限。例如，如果策略的保留配置可将快照保留 5 天，则您可以将策略配置为在最多 4 天的时间后自动取消快照共享。这适用于采用基于存在时间和基于计数的快照保留配置的策略。

   如果不启用自动取消共享，快照将一直共享直至删除。

   Note

   您只能共享未加密的快照或使用 客户托管密钥 加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。

g. 要添加其他计划，请选择位于页面顶部的 Add another schedule (添加其他计划)。每个其他计划请按照本主题之前所述填写字段。
h. 添加所需计划之后，请选择 Review policy (查看策略)。

12. 查看策略摘要，然后选择 Create policy (创建策略)。

Command line

可使用 create-lifecycle-policy 命令创建快照生命周期策略。对于 `PolicyType`，请指定 `EBS_SNAPSHOT_MANAGEMENT`。

Note

为简化语法，以下示例使用包含策略详细信息的 JSON 文件 `policyDetails.json`。

示例 1 – 具有两个计划的快照生命周期策略

此示例创建的快照生命周期策略可创建标签键 `costcenter` 的值为 115 的所有卷的快照。该策略包含两个计划。第一个计划在每天 3:00 UTC 创建快照。第二个计划在每周五 17:00 UTC 创建一个周快照。

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
```

```
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

示例 2 - 以实例为目标并创建数据（非根）卷子集快照的快照生命周期策略

此示例创建的快照生命周期策略可从标记为 code=production 的实例创建多卷快照集。该策略仅包含一个计划。该计划不会创建标记为 code=temp 的数据卷的快照。

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
```

```
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

示例 3 - 自动执行 Outpost 资源本地快照的快照生命周期策略

此示例创建一个快照生命周期策略，该策略创建所有 Outpost 中带有 `team=dev` 标记的卷的快照。该策略在源卷所在的同一 Outpost 上创建快照。该策略从 12 UTC 开始每 `00:00` 小时创建一次快照。

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
```

```
        "Name": "on-site backup",
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
        },
        "CopyTags": false
    }
]}
```

示例 4 - 在区域中创建快照并将其复制到 Outpost 的快照生命周期策略

以下示例策略创建带 team=dev 标记的卷的快照。快照在源卷所在的同一区域中创建。从 12 UTC 开始，每 00:00 小时创建一次快照，并保留最多 1 个快照。该策略还会将快照复制到 Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0，使用默认加密 KMS 密钥 对复制的快照进行加密，并将副本保留 1 个月。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
```

```
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

示例 5 – 快照生命周期策略，具有已启用归档并基于期限的计划

此示例将创建一个以带有 Name=Prod 标签的卷为目标的快照生命周期策略。此策略采用基于期限的计划，该计划会在每月第一天 09:00 创建快照。此计划会在标准层中将每个快照保留一天，之后将其转移到至存档层。快照在存档层中存储 90 天后将被删除。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

示例 6 – 快照生命周期策略，具有已启用归档并基于计数的计划

此示例将创建一个以带有 Purpose=Test 标签的卷为目标的快照生命周期策略。此策略采用基于计数的计划，该计划会在每月第一天 09:00 创建快照。此计划将在快照创建后立即将其存档，并在存档层中最多保留三个快照。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
}
```

快照生命周期策略的注意事项

以下一般注意事项适用于快照生命周期策略：

- 快照生命周期策略仅针对与策略位于同一区域的实例或卷。
- 第一个快照创建操作将在指定的开始时间后一小时内开始。后续快照创建操作将在计划时间的一小时内开始。
- 您可以创建多个策略来备份卷或实例。例如，假设一个卷有两个标签，其中标签 A 是每 12 小时创建一次快照的策略 A 的目标，标签 B 是每 24 小时创建一次快照的策略 B 的目标，则 Amazon Data Lifecycle Manager 将根据这两个策略的计划创建快照。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 目标资源标签区分大小写。
- 如果从策略所针对的资源中删除目标标签，则 Amazon Data Lifecycle Manager 不再管理标准层和存档层中的现有快照；如不再需要，您必须手动将其删除。
- 如果您创建了以实例为目标的策略，并且在创建策略后将新卷挂载到目标实例，则在下次运行策略时，新添加的卷将包含在备份中。策略运行时挂载到实例的所有卷都包括在内。

- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个快照，则该策略不会在达到保留阈值时自动删除该快照。如果不再需要快照，则必须手动删除该快照。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一张快照，直到创建下一张快照。例如，如果基于存在时间的策略每月创建一个快照，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个快照保留一个月，即使保留期为七天。

共享快照 (p. 1381)时需考虑以下事项：

- 您只能为将卷作为目标的快照策略启用快照存档。
- 对于每个策略，您只能为一个计划指定一个存档规则。
- 如果您使用控制台，则只有在创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

  如果您使用 Amazon CLI、Amazon API 或 Amazon SDK，则只有在指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。
- 存档层中的最短保留期为 90 天。
- 快照存档时，快照将在移动到存档层时转换为完整快照。这可能会导致快照存储成本增加。有关更多信息，请参阅定价和计费 (p. 1382)。
- 快照存档时将会禁用快速快照还原和快照共享。
- 如果在某个闰年中，您的保留规则导致存档保留期少于 90 天，则 Amazon Data Lifecycle Manager 会确保快照至少保留 90 天。
- 如果您手动将 Amazon Data Lifecycle Manager 创建的快照存档，并且该快照在达到计划的保留阈值时仍在存档，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前将快照还原到标准层，则该计划将继续按照保留规则管理快照。
- 如果您将 Amazon Data Lifecycle Manager 创建的快照永久或临时还原到标准层，并且该快照在达到计划的保留阈值时仍处于标准层中，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前重新将快照存档，则计划将在达到保留阈值时删除快照。
- Amazon Data Lifecycle Manager 存档的快照会使用您的 `Archived snapshots per volume` 和 `In-progress snapshot archives per account` 限额。
- 如果计划在重试 24 小时后仍无法将快照存档，则该快照将保留在标准层中，并按照本应从存档层中删除的时间来计划删除时间。例如，假设计划将快照存档 120 天，则在存档失败后，快照会保留在标准层中 120 天，然后才会被永久删除。对于基于计数的计划，快照不会计入计划的保留计数。
- 快照存档的区域必须与创建快照的区域相同。如果您启用了跨区域复制和快照存档，Amazon Data Lifecycle Manager 不会将快照副本存档。
- Amazon Data Lifecycle Manager 存档的快照将会使用 `aws:dlm:archived=true` 系统标签进行标记。此外，如果创建快照的计划已启用存档并且基于期限，则将会使用 `aws:dlm:expirationTime` 系统标签标记所创建的快照，以注明计划将快照存档的日期和时间。

以下注意事项适用于排除根卷和数据（非根）卷：

- 如果您选择排除启动卷，并且指定标签以排除附加到实例的所有其他数据卷，则 Amazon Data Lifecycle Manager 不会为受影响的实例创建任何快照，并且会发出 `SnapshotsCreateFailed` CloudWatch 指标。有关更多信息，请参阅使用 CloudWatch 监控您的策略。

删除或终止快照生命周期策略用作目标的卷或实例时应注意以下事项：

- 对于具有基于计数的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则 Amazon Data Lifecycle Manager 将不再管理标准层和存档层中之前从已删除的卷或已终止的实例创建的快照。如果不再需要较早版本的快照，您必须手动将其删除。
- 对于具有基于期限的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则该策略将继续按照既定计划从标准层和存档层中删除从已删除的卷或实例创建的快照，直到但不包括最后一个快照。如果不再需要最后一个快照，则必须手动删除该快照。

快照生命周期策略和快速快照还原 (p. 1514)应注意以下事项：

- Amazon Data Lifecycle Manager 只能为大小为 16 TiB 或以下的快照启用快速快照还原。有关更多信息，请参阅Amazon EBS 快速快照还原 (p. 1514)。
- 即使您删除或禁用了策略，为该策略禁用了快速快照还原，或者为该可用区禁用了快速快照还原，已启用快速快照还原的快照仍会保持启用状态。您必须手动为这些快照禁用快速快照还原。
- 如果您为策略启用了快速快照还原，并且超出了可启用快速快照还原的最大快照数，Amazon Data Lifecycle Manager 将按计划创建快照，但不会为其启用快速快照还原。在删除启用了快速快照还原的快照后，将为 Amazon Data Lifecycle Manager 创建的下一个快照启用快速快照还原。
- 快照启用快速快照还原后，每 TiB 需要 60 分钟来优化快照。我们建议您配置相应的计划，以确保在 Amazon Data Lifecycle Manager 创建下一个快照之前对每个快照进行完全优化。
- 如果您为以实例为目标的策略启用快速快照还原，Amazon Data Lifecycle Manager 会为多卷快照集中的各个快照单独启用快速快照还原。如果 Amazon Data Lifecycle Manager 无法为多卷快照集中的其中一个快照启用快速快照还原，它仍会尝试为快照集中的其余快照启用快速快照还原。
- 对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。有关更多信息，请参阅定价和计费 (p. 1518)。

  Note

  根据生命周期策略的配置，您可以在多个可用区同时为多个快照启用快速快照还原。

跨账户共享快照时需注意以下事项：

- 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。
- 您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。
- 如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。

快照策略和回收站 (p. 1627)应注意以下事项：

- 如果 Amazon Data Lifecycle Manager 删除快照并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原快照，则必须在不再需要该快照时手动删除它。Amazon Data Lifecycle Manager 将不再管理该快照。
- 如果您手动删除由策略创建的快照，并且该快照在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在回收站中时，Amazon Data Lifecycle Manager 不管理快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，那么当达到策略的保留阈值时，Amazon Data Lifecycle Manager 将删除快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，则 Amazon Data Lifecycle Manager 将不再删除快照。如果不再需要快照，则必须手动删除该快照。

以下注意事项适用于处于 error（错误）状态的快照生命周期策略：

- 对于具有基于存在时间的保留计划的策略，则设置为在策略处于 `error` 状态时过期的快照将无限期保留。您必须手动删除快照。重新启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时恢复删除快照。
- 对于具有基于计数的保留计划的策略，策略会在其处于 `error` 状态时停止创建和删除快照。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建快照，并在达到保留阈值时恢复删除快照。

其他资源

有关更多信息，请参阅 Amazon 存储博客文章 Automating Amazon EBS snapshot and AMI management using Amazon Data Lifecycle Manager（使用 Amazon Data Lifecycle Manager 实现 Amazon EBS 快照和 AMI 管理的自动化）。

自动化 AMI 生命周期

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 EBS 支持的 AMI 生命周期。

主题

- 创建 AMI 生命周期策略。 (p. 1462)
- AMI 生命周期策略的注意事项 (p. 1466)
- 其他资源 (p. 1467)

创建 AMI 生命周期策略。

使用以下程序之一创建 AMI 生命周期策略。

Console

创建 AMI 策略

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在 Select policy type (选择策略类型) 页面，选择 EBS-backed AMI policy (EBS 支持的 AMI 策略)，然后选择 Next (下一步)。
4. 在 Target resources (目标资源) 部分，对于 Target resource tags (目标资源标签)，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。
5. 对于 Description (描述)，输入策略的简短描述。
6. 对于 IAM role (IAM 角色)，选择一个有权管理 AMI 和快照以及描述实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择 Default role (默认角色)。或者，要使用您之前创建的自定义 IAM 角色，请选择 Choose another role (选择其他角色)，然后选择要使用的角色。
7. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
8. 对于 Policy status after creation (创建后的策略状态)，选择 Enable policy (启用策略)，以在下次计划时间启动策略运行，或者选择 Disable policy (禁用策略)，以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始创建 AMI。
9. 在 Instance reboot (实例重启) 部分，指明是否在创建 AMI 之前重启实例。为了防止目标实例重启，请选择 No (否)。选择 No (否) 可能会导致数据一致性问题。要在创建 AMI 之前重启实例，请选择 Yes (是)。选择此选项可确保数据一致性，但可能导致多个目标实例同时重新启动。
10. 选择 Next（下一步）。
11. 在 Configure schedule (配置计划) 页面配置策略计划。一个策略最多可以有四个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：

    a. 在 Schedule details (计划详细信息) 部分执行以下操作：

       i. 对于 Schedule name (计划名称)，请指定计划的描述性名称。

       ii. 在 Frequency (频率) 和相关字段中配置策略运行之间的间隔。您可以按每日、每周、每月或每年计划配置策略运行。或者，选择 Custom cron expression (自定义 Cron 表达式) 以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南 中的 Cron 表达式。

iii. 对于 Starting at (开始于)，请指定策略开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。您必须输入 hh:mm UTC 格式的时间。

iv. 对于 Retention type (保留类型)，请指定计划创建的 AMI 的保留策略。您可以根据其总计数或存在时间保留 AMI。

对于基于计数的保留，范围为 1 到 1000。在达到最大计数后，将在创建新 AMI 时注销最早 AMI。

对于基于存在时间的保留，范围是 1 天到 100 年。在每个 AMI 的保留期限过期后，会将其注销。

Note

所有计划必须具有相同的保留类型。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。

b. 请在 Tagging (标记) 部分执行以下操作：

i. 要将所有用户定义的标签从源实例复制到计划创建的 AMI，请选择 Copy tags from source (从源复制标记)。

ii. 默认情况下，计划创建的 AMI 会自动标记为源实例的 ID。要防止发生此自动标记，请在 Variable tags (变量标签) 中，删除 instance-id:$(instance-id) 平铺。

iii. 要指定分配给由该计划创建的 AMI 的其他标签，请选择 Add tags (添加标签)。

c. 要在不应再使用AMI时将其弃用，请在 AMI deprecation（AMI 弃用）部分选择 Enable AMI deprecation for this schedule（为此计划启用 AMI 弃用），然后指定 AMI 弃用规则。AMI 弃用规则指定何时弃用 AMI。

如果计划使用基于计数的 AMI 保留，您必须指定要弃用的最早 AMI 的数量。弃用计数必须小于或等于计划的 AMI 保留计数，并且不能大于 1000。例如，如果计划配置为最多保留 5 个 AMI，则可以将计划配置为弃用最多 5 个最早的 AMI。

如果计划使用基于存在时间的 AMI 保留，则必须指定弃用 AMI 的期限。弃用计数必须小于或等于计划的 AMI 保留期限，并且不能超过 10 年（120 个月、520 周或 3650 天）。例如，如果计划配置为将 AMI 保留 10 天，则可以将计划配置为在创建后最多 10 天的期限后弃用 AMI。

d. 要将计划创建的 AMI 复制到其他区域，请在 Cross-Region copy (跨区域复制) 部分选择 Enable cross-Region copy (启用跨区域复制)。您可以将 AMI 复制到账户中最多三个其他区域。您必须为每个目标区域指定单独的跨区域复制规则。

对于每个目标地区，您可以指定以下内容：

- AMI 副本的保留策略。保留期限过期后，将自动取消注册目标区域中的副本。
- AMI 副本的加密状态。如果源 AMI 已加密或预设情况下启用加密，则会始终加密复制的 AMI。如果源 AMI 未加密，并且预设情况下禁用加密，则您可以选择启用加密。如果未指定 KMS 密钥，则会在每个目标区域中使用 EBS 加密的默认 KMS 密钥 对 AMI 进行加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥 的访问权限。
- AMI 副本的弃用规则。当弃用期限过期时，将自动弃用 AMI 副本。弃用期限必须小于或等于副本保留期限，并且不能超过 10 年。
- 是从源 AMI 复制所有标签还是不复制标签。

Note

请勿超过每个区域的并发 AMI 副本数。

e. 要添加其他计划，请选择位于页面顶部的 Add another schedule (添加其他计划)。每个其他计划请按照本主题之前所述填写字段。

f. 添加所需计划之后，请选择 Review policy (查看策略)。

12. 查看策略摘要，然后选择 Create policy (创建策略)。

Command line

可使用 create-lifecycle-policy 命令创建 AMI 生命周期策略。对于 PolicyType，请指定 IMAGE_MANAGEMENT。

Note

为简化语法，以下示例使用包含策略详细信息的 JSON 文件 policyDetails.json。

示例 1：基于存在时间的保留和 AMI 弃用

此示例创建的 AMI 生命周期策略可在不重新启动目标实例的情况下创建标签键 purpose 的值为 production 的所有实例的 AMI。该策略包括一个每天可在 UTC 01:00 创建 AMI 的计划。该策略保留 AMI 2 天，并在 1 天后弃用。还会将标签从源实例复制到其创建的 AMI。

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
```

```
}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

示例 2：基于计数的保留和使用跨区域复制的 AMI 弃用

此示例创建的 AMI 生命周期策略可创建标签键 purpose 的值为 production 的所有实例的 AMI，并重新启动目标实例。该策略包括一个可在 UTC 17:30 起每 6 小时创建 AMI 的计划。该策略保留 3 AMI 并自动弃用 2 最早的 AMI。它还具有跨区域复制规则，该规则会将 AMI 复制到 us-east-1，保留 2 AMI 副本，并自动弃用最早的 AMI。

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
                "IntervalUnit": "DAYS",
                "Interval": 1
            },
```

```
            "CopyTags": true
        }]
    }]
}
```

AMI 生命周期策略的注意事项

创建 AMI 生命周期策略时应注意以下一般注意事项：

- AMI 生命周期策略仅针对与策略位于同一区域的实例。
- 第一个 AMI 创建操作将在指定开始时间之后的一小时内启动。后续 AMI 创建操作将在计划时间的一小时内开始。
- 当 Amazon Data Lifecycle Manager 注销 AMI 时，它会自动删除其支持的快照。
- 目标资源标签区分大小写。
- 如果从策略所针对的实例中删除目标标签，则 Amazon Data Lifecycle Manager 不再管理标准中的现有 AMI；如不再需要，您必须手动将其删除。
- 您可以创建多个策略来备份实例。例如，假设一个实例有两个标签，其中标签 A 是每 12 小时创建一个 AMI 的策略 A 的目标，标签 B 是每 24 小时创建一个 AMI 的策略 B 的目标，则 Amazon Data Lifecycle Manager 将根据这两个策略的计划创建 AMI。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 在下次运行策略时，备份中将自动包含在创建策略后挂载到目标实例的新卷。策略运行时挂载到实例的所有卷都包括在内。
- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个 AMI，则该策略不会在达到保留阈值时自动注销该 AMI。如果不再需要该 AMI，则必须手动将其注销。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一个 AMI，直到创建下一个 AMI。例如，如果基于存在时间的策略每月创建一个 AMI，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个 AMI 保留一个月，即使保留期为七天。
- 对于基于计数的策略，Amazon Data Lifecycle Manager 在尝试根据保留策略取消注册最旧的 AMI 之前，始终根据创建频率创建 AMI。
- 成功取消注册 AMI 并删除其关联的备份快照可能需要几小时。如果 Amazon Data Lifecycle Manager 在之前创建的 AMI 成功取消注册之前创建了下一个 AMI，则您可以临时保留一些大于保留次数的 AMI。

终止策略针对的实例时应注意以下注意事项：

- 如果您终止某个策略按照基于计数的保留计划针对的实例，则该策略将不再管理以前从已终止的实例创建的 AMI。如果不再需要较早版本的 AMI，您必须手动将其注销。
- 如果您终止某个策略按照基于存在时间的保留计划针对的实例，则该策略将继续按照原定计划取消注册之前从已终止的实例创建的 AMI，直至（但不包括）最后一个 AMI。如果不再需要最后一个 AMI，则必须手动将其注销。

AMI 策略和 AMI 弃用应注意以下事项：

- 如果您针对具有基于计数的保留的计划增加 AMI 弃用计数，则更改将应用于该计划创建的所有 AMI（现有 AMI 和新 AMI）。
- 如果您针对具有基于存在时间的保留的计划增加 AMI 弃用期限，则更改仅应用于新 AMI。现有 AMI 不受影响。
- 如果您从计划中删除 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将不会取消该计划之前弃用的 AMI 弃用。
- 如果您要减少计划的 AMI 弃用计数或期限，则 Amazon Data Lifecycle Manager 将不会取消该计划之前弃用的 AMI 弃用。

- 如果您手动弃用由 AMI 策略创建的 AMI，则 Amazon Data Lifecycle Manager 将不会覆盖弃用操作。
- 如果您手动取消之前已被 AMI 策略弃用的 AMI 的弃用，则 Amazon Data Lifecycle Manager 将不会覆盖取消操作。
- 如果 AMI 由多个冲突的计划创建，并且其中一个或多个计划没有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将不会弃用该 AMI。
- 如果 AMI 由多个相互冲突的计划创建，并且其中所有计划都有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将会使用导致最新弃用日期的弃用规则。

以下注意事项适用于 AMI 策略和 回收站 (p. 1627)：

- 如果 Amazon Data Lifecycle Manager 注销 AMI 并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原 AMI，则必须在不再需要该 AMI 时手动注销 AMI。Amazon Data Lifecycle Manager 将不再管理该 AMI。
- 如果您手动注销由策略创建的 AMI，并且该 AMI 在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会注销该 AMI。当 AMI 在回收站中时，Amazon Data Lifecycle Manager 不管理 AMI。

  如果在达到策略的保留阈值之前从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将在达到策略的保留阈值时注销 AMI。

  如果在达到策略的保留阈值之后从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将不再注销 AMI。如果不再需要 AMI，则必须手动将其删除。

以下注意事项适用于处于错误状态的 AMI 策略：

- 对于具有基于存在时间的保留计划的策略，则设置为在策略处于 `error` 状态时过期的 AMI 将无限期保留。您必须手动取消注册 AMI。重新启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时恢复取消注册 AMI。
- 对于具有基于计数的保留计划的策略，策略会在其处于 `error` 状态时停止创建和取消注册 AMI。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建 AMI，并在达到保留阈值时恢复取消注册 AMI。

其他资源

有关更多信息，请参阅 Amazon 存储博客文章 Automating Amazon EBS snapshot and AMI management using Amazon Data Lifecycle Manager（使用 Amazon Data Lifecycle Manager 实现 Amazon EBS 快照和 AMI 管理的自动化）。

自动执行跨账户快照副本

通过自动执行跨账户快照副本，您可以将 Amazon EBS 快照复制到隔离账户中的特定区域，并使用加密密钥对这些快照进行加密。这样，您能够在账户遭到泄露时防止自己的数据丢失。

自动执行跨账户快照副本涉及两个账户：

- Source account (源账户)—源账户是创建快照并与目标账户共享快照的账户。在此账户中，您必须创建 EBS 快照策略，以便按设定的时间间隔创建快照，然后与其他 Amazon 账户共享这些快照。
- Target account (目标账户)—目标账户是与之共享快照的目标账户，它也是创建共享快照副本的账户。在此账户中，您必须创建跨账户复制事件策略，以自动复制由一个或多个指定源账户共享的快照。

主题

- 创建跨账户快照复制策略 (p. 1468)
- 指定快照描述筛选条件 (p. 1474)

- 跨账户快照复制策略的注意事项 (p. 1474)
- 其他资源 (p. 1475)

创建跨账户快照复制策略

要为跨账户快照复制准备源账户和目标账户，您需要执行以下步骤：

主题

- 第 1 步：创建 EBS 快照策略（Source account (源账户)）(p. 1468)
- 步骤 2：共享 客户托管密钥（ 源账户 ）(p. 1468)
- 第 3 步：创建跨账户复制事件策略（Target account (目标账户)）(p. 1470)
- 第 4 步：允许 IAM 角色使用所需的 KMS 密钥（Target account （目标账户））(p. 1472)

第 1 步：创建 EBS 快照策略（Source account (源账户)）

在源账户中，创建一个 EBS 快照策略，该策略将创建快照并与所需的目标账户共享。

创建策略时，请确保启用跨账户共享，并指定目标 Amazon 账户，用于共享快照。这些是您要与之共享快照的账户。如果您要共享加密快照，则必须授予所选目标账户使用用于加密源卷的 KMS 密钥 的权限。有关更多信息，请参阅步骤 2：共享 客户托管密钥（ 源账户 ）(p. 1468)。

> **Note**
>
> 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 密钥。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。

有关手动创建 EBS 快照策略的更多信息，请参阅 自动化快照生命周期 (p. 1451)。

使用以下方法之一创建 EBS 快照策略。

步骤 2：共享 客户托管密钥（ 源账户 ）

如果您要共享加密快照，则必须授予 IAM 角色和（您在上一步中选择的）目标Amazon账户使用用于加密源卷的客户托管密钥的权限。

> **Note**
>
> 仅在共享加密快照时执行此步骤。如果您正在共享的是未加密快照，请跳过此步骤。

Console

1. 在 Amazon KMShttps://console.aws.amazon.com/kms 打开 控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector（区域选择器）。
3. 在导航窗格中，选择 Customer managed key (客户托管密钥)，然后选择您需要与目标账户共享的 KMS 密钥。

   记下 KMS 密钥 ARN，稍后您将用到它。
4. 在 Key policy (密钥策略) 选项卡上，向下滚动到 Key users (密钥用户) 部分。选择 Add (添加)，输入您在上一步中选择的 IAM 角色的名称，然后选择 Add (添加)。
5. 在密钥政策选项卡上，向下滚动到其他 Amazon 账户部分。选择 Add other Amazon accounts（添加其他亚马逊云科技账户），然后添加您在上一步中选择与之共享快照的所有目标 Amazon 账户。
6. 选择 Save changes（保存更改）。

Command line

使用 get-key-policy 命令检索当前附加到 KMS 密钥 的密钥策略。

例如，以下命令检索 ID 为 9d5e2b3d-e410-4a27-a958-19e220d83a1e 的 KMS 密钥 的密钥策略，并将其写入名为 snapshotKey.json 的文件。

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

使用首选文本编辑器打开密钥策略。添加您在创建快照策略时指定的 IAM 角色的 ARN 以及要与之共享 KMS 密钥 的目标账户的 ARN。

例如，在以下策略中，我们添加了默认 IAM 角色的 ARN 以及目标账户 222222222222. 的根账户的 ARN

Tip

为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 kms:GrantIsForAWSResource 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
```

```
    }
}
```

保存并关闭 文件。然后使用 put-key-policy 命令将更新后的密钥策略附加到 KMS 密钥。

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

第 3 步：创建跨账户复制事件策略（Target account (目标账户)）

在目标账户中，您必须创建跨账户复制事件策略，该策略将自动复制由所需源账户共享的快照。

只有当指定的源账户之一与该账户共享快照时，此策略才会在目标账户中运行。

使用以下方法之一创建跨账户复制事件策略。

Console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在 Select policy type (选择策略类型) 页面，选择 Cross-account copy event policy (跨账户复制事件策略)，然后选择 Next (下一步)。
4. 对于 Policy Description (策略描述)，输入策略的简短描述。
5. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
6. 在 Event settings (事件设置) 部分，定义将导致策略运行的快照共享事件。执行以下操作：

   a. 对于 Sharing accounts (共享账户)，请指定您想从中复制共享快照的源 Amazon 账户。选择 Add account (添加账户)，输入 12 位 Amazon 账户 ID，然后选择 Add (添加)。

   b. 对于 Filter by description (按描述筛选)，请使用正则表达式输入所需的快照描述。该策略仅复制由指定源账户共享且其描述与指定筛选条件匹配的快照。有关更多信息，请参阅指定快照描述筛选条件 (p. 1474)。
7. 对于 IAM role (IAM 角色)，请选择有权执行快照复制操作的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择 Default role (默认角色)。或者，要使用您之前创建的自定义 IAM 角色，请选择 Choose another role (选择其他角色)，然后选择要使用的角色。

   如果您要复制加密快照，您必须授予所选 IAM 角色使用用于加密源卷的加密 KMS 密钥 的权限。同样，如果您使用不同的 KMS 密钥 对目标区域中的快照进行加密，则必须授予 IAM 角色使用目标 KMS 密钥 的权限。有关更多信息，请参阅第 4 步：允许 IAM 角色使用所需的 KMS 密钥（Target account （目标账户））(p. 1472)。
8. 在 Copy action (复制操作) 部分，定义激活策略时应执行的快照复制操作。该策略最多可以将快照复制到三个区域。您必须为每个目标区域指定单独的复制规则。对要添加的每个规则执行以下操作：

   a. 对于 Name (名称)，为复制操作输入一个描述性名称。

   b. 对于 Target Region (目标区域)，选择要将快照复制到的区域。

   c. 对于 Expire (过期)，请指定快照副本创建之后在目标区域中保留多长时间。

   d. 要加密快照副本，请在 Encryption (加密) 中选择Enable encryption (启用加密)。如果源快照已加密，或者预设情况下为您的账户启用了加密，则快照副本将始终加密，即使您在此处没有启用加密也一样。如果源快照未加密，并且默认情况下未为您的账户启用加密，则您可以选择启用或禁用加密。如果启用了加密但未指定 KMS 密钥，则快照在每个目标区域中都将使用默认

加密 KMS 密钥 进行加密。如果您为目标区域指定 KMS 密钥，则您必须具有对 KMS 密钥 的访问权限。

9. 要添加其他快照复制操作，请选择 Add new Regions (添加新区域)。
10. 对于创建后的策略状态，选择启用策略，以在下次计划时间启动策略运行，或者选择禁用策略，以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始复制快照。
11. 选择 Create policy。

Command line

使用 create-lifecycle-policy 命令创建策略。要创建跨账户复制事件策略，请为 PolicyType 指定 EVENT_BASED_POLICY。

例如，以下命令可在目标账户 222222222222 中创建跨账户复制事件策略。该策略会复制由源账户 111111111111 共享的快照。该策略将快照复制到 sa-east-1 和 eu-west-2。复制到 sa-east-1 的快照未加密，它们将保留 3 天。复制到 eu-west-2 的快照使用 KMS 密钥 8af79514-350d-4c52-bac8-8985e84171c7 进行加密，它们将保留 1 个月。该策略使用默认 IAM 角色。

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

下面显示的是 policyDetails.json 文件的内容。

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-west-2:222222222222:key/8af79514-350d-4c52-
bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
```

```
}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

第 4 步：允许 IAM 角色使用所需的 KMS 密钥（Target account （目标账户））

如果您要复制加密快照，则必须授予（您在上一步中选择的）IAM 角色使用用于加密源卷的 客户托管密钥 的权限。

Note

仅在复制加密快照时执行此步骤。如果您要复制的是未加密快照，请跳过此步骤。

使用以下方法之一将所需策略添加到 IAM 角色。

Console

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles (角色)。搜索并选择您在上一步中创建跨账户复制事件策略时选择的 IAM 角色。如果您选择使用默认角色，则该角色名为 Amazon Web Services DataLifecycleManagerDefaultRole。
3. 选择 Add inline policy (添加内联策略)，然后选择 JSON 选项卡。
4. 将现有策略替换为以下内容，然后指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

   Note

   如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

   在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

   Tip

   为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 kms:GrantIsForAWSResource 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
```

```
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

5. 选择查看策略
6. 对于 Name (名称)，为策略输入描述性名称，然后选择 Create policy (创建策略)。

Command line

使用首选文本编辑器，创建一个名为 `policyDetails.json` 的新 JSON 文件。添加以下策略并指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

Note

如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

Tip

为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 `kms:GrantIsForAWSResource` 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
```

```
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

保存并关闭 文件。然后使用 put-role-policy 命令将策略添加到 IAM 角色。

例如

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

指定快照描述筛选条件

在目标账户中创建快照复制策略时，必须指定快照描述筛选条件。通过快照描述筛选条件，您可指定额外的筛选级别，从而控制策略应复制哪些快照。这意味着只有当快照由指定源账户之一共享，并且其快照描述与指定筛选条件匹配时，策略才会复制该快照。换句话说，如果快照由指定源账户之一共享，但其描述不符合指定的筛选条件，则策略不会复制该快照。

必须使用正则表达式指定快照描述筛选条件。使用控制台和命令行创建跨账户复制事件策略时，它是必填字段。下面是可以使用的示例正则表达式：

- `.*`—此筛选条件匹配所有快照描述。如果使用此表达式，该策略将复制由指定源账户之一共享的所有快照。
- `Created for policy: policy-0123456789abcdef0.*`—此筛选条件仅匹配由 ID 为 的策略创建的快照。`policy-0123456789abcdef0`如果您使用类似这样的表达式，则该策略仅复制由指定源账户之一与您的账户共享以及由具有指定 ID 的策略创建的快照。
- `.*production.*`—此筛选条件匹配描述中任意位置包含词语 `production` 的任何快照。如果使用此表达式，该策略将复制由指定源账户之一共享且描述中包含指定文本的所有快照。

跨账户快照复制策略的注意事项

跨账户复制事件策略时需考虑以下事项：

- 您只能复制未加密的快照或使用 客户托管密钥 加密的快照。
- 您可以创建跨账户复制事件策略，用于复制在 Amazon Data Lifecycle Manager 外部共享的快照。

- 如果要加密目标账户中的快照，则为跨账户复制事件策略选择的 IAM 角色必须拥有使用所需 KMS 密钥 的权限。

其他资源

有关更多信息，请参阅 Amazon 存储博客文章 Automating copying encrypted Amazon EBS snapshots across Amazon accounts（跨 账户自动复制加密的 Amazon EBS 快照）。

查看、修改和删除生命周期策略

使用以下程序查看、修改和删除现有生命周期策略。

主题

- 查看生命周期策略 (p. 1475)
- 修改生命周期策略 (p. 1476)
- 删除生命周期策略 (p. 1478)

查看生命周期策略

使用以下程序之一查看生命周期策略。

Console

查看生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。Details (详细信息) 选项卡显示有关策略的信息。

Command line

可使用 get-lifecycle-policy 命令来显示有关生命周期策略的信息。

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

下面是示例输出。它包括您指定的信息以及 Amazon 插入的元数据。

```
{
   "Policy":{
      "Description": "My first policy",
      "DateCreated": "2018-05-15T00:16:21+0000",
      "State": "ENABLED",
      "ExecutionRoleArn":
 "arn:aws:iam::210774411744:role/AWSDataLifecycleManagerDefaultRole",
      "PolicyId": "policy-0123456789abcdef0",
      "DateModified": "2018-05-15T00:16:22+0000",
      "PolicyDetails": {
        "PolicyType":"EBS_SNAPSHOT_MANAGEMENT",
         "ResourceTypes": [
            "VOLUME"
         ],
         "TargetTags": [
            {
               "Value": "115",
               "Key": "costcenter"
            }
```

```
        ],
        "Schedules": [
           {
              "TagsToAdd": [
                 {
                    "Value": "myDailySnapshot",
                    "Key": "type"
                 }
              ],
              "RetainRule": {
                 "Count": 5
              },
              "CopyTags": false,
              "CreateRule": {
                 "Interval": 24,
                 "IntervalUnit": "HOURS",
                 "Times": [
                    "03:00"
                 ]
              },
              "Name": "DailySnapshots"
           }
        ]
     }
  }
}
```

修改生命周期策略

修改策略的注意事项

- 如果您通过删除其目标标签来修改了 AMI 或快照策略，则具有这些标签的卷或实例将不再受此策略管理。
- 如果您修改了计划的名称，则使用旧计划名称创建的快照或 AMI 将不再由此策略管理。
- 如果您修改了基于存在时间的保留计划以使用新的时间间隔，则新间隔仅适用于在更改之后创建的新快照或 AMI。新计划不影响更改之前创建的快照或 AMI 的保留计划。
- 创建后，您无法将策略的保留计划从基于计数更改为基于存在时间。要进行该更改，您必须创建新的策略。
- 如果您禁用了其保留计划基于存在时间的策略，则设置为在禁用策略期间过期的快照或 AMI 将无限期地保留。您必须删除快照或手动注销 AMI。再次启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时继续删除快照或取消注册 AMI。
- 如果您禁用了具有基于计数的保留计划的策略，则该策略将停止创建和删除快照或 AMI。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建快照和 AMI，并在达到保留阈值时恢复删除快照或 AMI。
- 如果您禁用了某个具有已启用快照存档策略的策略，则禁用该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您按某个基于计数的计划启用了快照存档，则存档规则适用于由该计划创建和存档的所有新快照，也适用于之前由该计划创建和存档的现有快照。
- 如果您按某个基于期限的计划启用了快照存档，则存档规则仅适用于启用快照存档后创建的新快照。对于在启用快照存档之前创建的现有快照，将继续根据最初创建和存档快照时设定的计划，从各自的存储层中删除。
- 如果您为某个基于计数的计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。
- 如果您为某个基于期限的计划禁用了快照存档，则由该策略创建并计划存档的快照将在 `aws:dlm:expirationTime` 系统标签注明发原定存档日期和时间永久删除。
- 如果您为某个计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。

- 如果您为基于计数的计划修改了存档保留计数，则新的保留计数将包括之前由该计划存档的现有快照。
- 如果您为基于期限的计划修改了存档保留期，则新的保留期仅适用于修改保留规则后存档的快照。

使用以下程序之一修改生命周期策略。

Console

修改生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择 Actions (操作)，然后选择 Modify Lifecycle Policy (修改生命周期策略)。
5. 根据需要，修改策略设置。例如，您可以修改计划，添加或删除标签，或者启用或禁用策略。
6. 选择 Update policy。

Command line

可使用 update-lifecycle-policy 命令来修改生命周期策略中的信息。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetailsUpdated.json`。

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
    --policy-details file://policyDetailsUpdated.json
```

以下是 `policyDetailsUpdated.json` 文件的示例。

```
{
   "ResourceTypes":[
      "VOLUME"
   ],
   "TargetTags":[
      {
         "Key": "costcenter",
         "Value": "120"
      }
   ],
   "Schedules":[
      {
         "Name": "DailySnapshots",
         "TagsToAdd": [
            {
               "Key": "type",
               "Value": "myDailySnapshot"
            }
         ],
         "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
               "15:00"
            ]
         },
         "RetainRule": {
            "Count" :5
         },
```

```
        "CopyTags": false
      }
   ]
}
```

要查看更新后的策略，请使用 `get-lifecycle-policy` 命令。您可以看到更改了状态、标签的值、快照时间间隔和快照开始时间。

删除生命周期策略

修改策略的注意事项

- 如果您删除了某个策略，则该策略创建的快照或 AMI 不会自动删除。如果您不再需要快照或 AMI，则必须手动将其删除。
- 如果您删除了某个具有已启用快照存档策略的策略，则删除该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您删除了某个策略，并且该策略具有已启用存档并且基于期限的计划，则由该策略创建并计划存档的快照将在 `aws:dlm:expirationtime` 系统标签注明发原定存档日期和时间永久删除。

使用以下程序之一删除生命周期策略。

Console

删除生命周期策略

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择 Actions (操作)，然后选择 Delete Lifecycle Policy (删除生命周期策略)。
5. 在提示确认时，选择 Delete Lifecycle Policy (删除生命周期策略)。

Command line

可使用 delete-lifecycle-policy 命令来删除生命周期策略并释放策略中指定的目标标签以供重复使用。

> **Note**
>
> 您可以仅删除由 Amazon Data Lifecycle Manager 创建的快照。

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Amazon Data Lifecycle Manager API 参考提供了 Amazon Data Lifecycle Manager 查询 API 的各种操作和数据类型的描述和语法。

或者，您可以使用 Amazon 开发工具包之一，通过适用于您所用编程语言或平台的方法来访问该 API。有关更多信息，请参阅 Amazon 软件开发工具包。

Amazon Identity and Access Management

Amazon Data Lifecycle Manager 的访问需要凭据。这些凭证必须拥有权限访问 Amazon 资源，如实例、卷、快照和 AMI。下列各节详述如何使用 Amazon Identity and Access Management (IAM) 和如何帮助保护对您的资源的访问。

主题

- Amazon 托管策略 (p. 1479)
- IAM 服务角色 (p. 1481)
- 用户的权限 (p. 1484)
- 加密权限 (p. 1485)

Amazon 托管策略

Amazon 托管式策略是由 Amazon 创建和管理的独立策略。Amazon 托管策略可用于为很多常用案例提供权限。与必须自己编写策略相比，通过 Amazon 托管策略可以更高效地将适当的权限分配给用户、组和角色。

但是，您不能更改 Amazon 托管式策略中定义的权限。Amazon 有时会更新 Amazon 托管策略中定义的权限。当发生此情况时，更新会影响策略附加到的所有委托人实体（用户、组和角色）。

Amazon Data Lifecycle Manager 提供了适用于常见使用案例的两个 Amazon 托管策略。通过这些策略可以更高效地定义适当的权限，并控制对资源的访问。Amazon Data Lifecycle Manager 提供的 Amazon 托管策略旨在附加到您传递给 Amazon Data Lifecycle Manager 的角色。

以下是 Amazon Data Lifecycle Manager 提供的 Amazon 托管策略。您还可以在 IAM 控制台的 Policies（策略）部分中找到这些 Amazon 托管策略。

AWSDataLifecycleManagerServiceRole

AWSDataLifecycleManagerServiceRole 策略为 Amazon Data Lifecycle Manager 提供了相应权限，以创建和管理 Amazon EBS 快照策略和跨帐户复制事件策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
```

```
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

AWSDataLifecycleManagerServiceRoleForAMIManagement 策略为 Amazon Data Lifecycle Manager 提供了相应权限，以创建和管理Amazon EBS-backed AMI 策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

Amazon 托管式策略更新

Amazon 服务负责维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

下表提供了关于 Amazon Data Lifecycle Manager 的 Amazon 托管式策略更新的详细信息（从该服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 1757) 上的 RSS 源。

更改	说明	日期
AWSDataLifecycleManagerServiceRole – 增加了支持快照存档的权限。	AmazonDataLifecycleManagerServiceRole Lifecycle Manager 增加了 `ec2:ModifySnapshotTier` 和 `ec2:DescribeSnapshotTierStatus` 操作，以向快照策略授予将快照存档和检查快照存档状态的权限。	2022 年 9 月 30 日
AWSDataLifecycleManagerServiceRole — 添加了支持 AMI 弃用的权限。	AmazonDataLifecycleManagerServiceRoleForAMIManagement Lifecycle Manager 添加了 `ec2:EnableImageDeprecation` 和 `ec2:DisableImageDeprecation` 操作以授予 EBS 支持的 AMI 策略权限，从而启用和禁用 AMI 弃用。	2021 年 8 月 23 日
Amazon Data Lifecycle Manager 已开启跟踪更改	Amazon Data Lifecycle Manager 已开始跟踪其 Amazon 托管式策略的更改。	2021 年 8 月 23 日

IAM 服务角色

Amazon Identity and Access Management (IAM) 角色类似于用户，因为它是一个 Amazon 身份，具有确定其在 Amazon 中可执行和不可执行的操作的权限策略。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。服务角色是 Amazon 服务代入以代表您执行操作的角色。作为代表您执行备份操作的服务，Amazon Data Lifecycle Manager 要求您在该服务代表您执行策略操作时将其传递给要代入的角色。有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

您传递到 Amazon Data Lifecycle Manager 的角色必须拥有一个 IAM policy，该策略具有的权限可让 Amazon Data Lifecycle Manager 执行策略操作关联的操作，如创建快照和 AMI、复制快照和 AMI、删除快照以及取消注册 AMI。每种 Amazon Data Lifecycle Manager 策略类型需要不同的权限。该角色还必须将 Amazon Data Lifecycle Manager 列为可信实体，这使得 Amazon Data Lifecycle Manager 能够代入该角色。

主题

- Amazon Data Lifecycle Manager 的原定设置服务角色 (p. 1482)
- Amazon Data Lifecycle Manager 的自定义服务角色 (p. 1482)

Amazon Data Lifecycle Manager 的原定设置服务角色

Amazon Data Lifecycle Manager 使用以下原定设置的服务角色：

- Amazon Web Services DataLifecycleManagerDefaultRole 用于管理快照的 — 默认角色。它只信任 `dlm.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行快照和跨账户快照复制策略所需的操作。此角色使用 `AWSDataLifecycleManagerServiceRole` Amazon 托管式策略。

  Note

  角色的 ARN 格式会有所不同，具体取决于使用控制台还是 Amazon CLI 创建角色。如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果使用 Amazon CLI 创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`。
- Amazon Web Services DataLifecycleManagerDefaultRoleForAMIManagement 用于管理 AMI 的 — 默认角色。它只信任 `dlm.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行由 EBS 支持的 AMI 策略所需的操作。此角色使用 `AWSDataLifecycleManagerServiceRoleForAMIManagement` Amazon 托管式策略。

如果您使用的是 Amazon Data Lifecycle Manager 控制台，Amazon Data Lifecycle Manager 会在您首次创建快照或跨账户快照复制策略时，自动创建 AWSDataLifecycleManagerDefaultRole 服务角色，并且它会在您首次创建由 EBS 支持的 AMI 策略时自动创建 AWSDataLifecycleManagerDefaultRoleForAMIManagement 服务角色。

如果您不使用控制台，可以使用 create-default-role 命令手动创建服务角色。对于 `--resource-type`，指定 `snapshot` 以创建 AWSDataLifecycleManagerDefaultRole，或 `image` 以创建 AWSDataLifecycleManagerDefaultRoleForAMIManagement。

```
$ aws dlm create-default-role --resource-type snapshot|image
```

如果您删除了原定设置服务角色，然后需要再次创建，则可以使用相同的流程在您的账户中重新创建它们。

Amazon Data Lifecycle Manager 的自定义服务角色

作为使用原定设置服务角色的替代方案，您可以在创建生命周期策略时创建具有所需权限的自定义 IAM 角色，然后选择它们。

创建自定义 IAM 角色

1. 创建具有以下权限的角色。

   - 管理快照生命周期策略所需的权限

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
```

```
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
        }
    ]
}
```

- 管理 AMI 生命周期策略所需的权限

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
```

```
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

有关更多信息，请参阅IAM 用户指南中的创建角色。

2. 向角色添加信任关系。

   a. 在 IAM 控制台中，选择角色。

   b. 选择您创建的角色，然后选择信任关系。

   c. 选择编辑信任关系，添加以下策略，然后选择更新信任策略。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": "dlm.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
 }]
}
```

建议您使用 aws:SourceAccount 和 aws:SourceArn 条件键来防止出现混淆代理人问题。例如，您可以将以下条件块添加到以前的信任策略。aws:SourceAccount 是生命周期策略的所有者，aws:SourceArn 是生命周期策略的 ARN。如果您不知道生命周期策略的 ID，可以用通配符 (*) 替换 ARN 的该部分，然后在创建生命周期策略后更新信任策略。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

用户的权限

用户必须具有以下权限才能使用 Amazon Data Lifecycle Manager。

Note

- 仅控制台用户需要 ec2:DescribeAvailabilityZones、ec2:DescribeRegions、kms:ListAliases 和 kms:DescribeKey 权限。如果不需要访问控制台，则可以删除权限。

- AWSDataLifecycleManagerDefaultRole 角色的 ARN 格式会有所不同，具体取决于使用控制台还是 Amazon CLI 创建角色。如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果使用 Amazon CLI 创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`。以下策略假定使用 Amazon CLI 创建角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
                ]
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

加密权限

使用 Amazon Data Lifecycle Manager 和加密资源时，请考虑以下情况。

- 如果源卷已加密，请确保 Amazon Data Lifecycle Manager 默认角色（Amazon Web Services DataLifecycleManagerDefaultRole 和Amazon Web Services DataLifecycleManagerDefaultRoleForAMIManagement）有权使用用于加密卷的 KMS 密钥。
- 如果您为未加密快照或未加密快照支持的 AMI 启用跨区域复制，并选择在目标区域中启用加密，请确保默认角色有权使用在目标区域中执行加密所需的 KMS 密钥。
- 如果您为加密快照或加密快照支持的 AMI 启用跨区域复制，请确保默认角色有权同时使用源和目标 KMS 密钥。
- 如果您为加密快照启用快照归档，请确保 Amazon Data Lifecycle Manager 默认角色（AWSDataLifecycleManagerDefaultRole）有权使用用于加密快照的 KMS 密钥。

有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的允许其他账户中的用户使用 KMS 密钥。

监控快照和 AMI 的生命周期

您可以使用以下功能来监控快照和 AMI 的生命周期。

功能

- 控制台和 Amazon CLI (p. 1486)
- Amazon CloudTrail (p. 1486)
- 使用 CloudWatch Events 监控您的策略 (p. 1486)
- 使用 Amazon CloudWatch 监控您的策略 (p. 1487)

控制台和 Amazon CLI

您可以使用 Amazon EC2 控制台或 Amazon CLI 来查看生命周期策略。策略创建的每个快照和 AMI 均具有时间戳以及与策略相关的标签。您可以使用这些标签来筛选快照和 AMI 以验证是否按您的预期创建备份。有关使用控制台查看生命周期策略的信息，请参阅查看生命周期策略 (p. 1475)。

Amazon CloudTrail

使用 Amazon CloudTrail，您可以跟踪用户活动和 API 使用率来证明符合内部策略和监管标准。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

使用 CloudWatch Events 监控您的策略

Amazon EBS 和 Amazon Data Lifecycle Manager 发出与生命周期策略操作相关的事件。您可以使用 Amazon Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon CloudWatch Events 用户指南。

提供的事件如下：

> **Note**
>
> AMI 生命周期策略操作不会触发任何事件。

- `createSnapshot` – 当 `CreateSnapshot` 操作成功或失败时，会发出 Amazon EBS 事件。有关更多信息，请参阅适用于 Amazon EBS 的 EventBridge (p. 1569)。
- `DLM Policy State Change` – 当生命周期策略进入错误状态时，会发出 Amazon Data Lifecycle Manager 事件。此事件包含有关导致错误的问题的描述。下面是在 IAM 角色授予的权限不足时发出的事件的示例。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    }
```

```
}
```

下面是在超过限制时发出的事件的示例。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    }
}
```

使用 Amazon CloudWatch 监控您的策略

您可以使用 CloudWatch 监控您的 Amazon Data Lifecycle Manager 生命周期策略，此工具可收集原始数据并将其处理为易读的近乎实时的指标。您可以使用这些指标来准确查看您的策略随着时间的推移创建、删除和复制了多少 Amazon EBS 快照和 EBS 支持的 AMI。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。

指标的保留期限为 15 个月，以便您可以访问历史信息，并更好地了解生命周期策略在较长时间内的表现。

有关 Amazon CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南。

主题

- 受支持的指标 (p. 1487)
- 查看适用于您策略的 CloudWatch 指标 (p. 1490)
- 绘制策略的指标图表 (p. 1490)
- 为策略创建 CloudWatch 警报 (p. 1491)
- 使用案例示例 (p. 179)
- 管理报告失败操作的策略 (p. 1493)

受支持的指标

`Data Lifecycle Manager` 命名空间包括 Amazon Data Lifecycle Manager 生命周期策略的以下指标。支持的指标因策略类型而异。

所有指标都可以在 `DLMPolicyId` 维度上衡量。最有用的统计工具为 `sum` 和 `average`，并且度量单位为 `count`。

选择选项卡以查看该策略类型支持的指标。

EBS snapshot policies

指标	描述
`ResourcesTargeted`	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。

指标	描述
SnapshotsCreateStarted	快照策略启动的快照创建操作数。即使有多次后续重试，每个操作也只记录一次。 如果快照创建操作失败，Amazon Data Lifecycle Manager 会发送 SnapshotsCreateFailed 指标。
SnapshotsCreateCompleted	快照策略创建的快照数量。这包括在计划时间后 60 分钟内的成功重试。
SnapshotsCreateFailed	不能由快照策略创建的快照数量。这包括在计划时间后 60 分钟内的不成功重试。
SnapshotsSharedCompleted	快照策略跨账户共享的快照数量。
SnapshotsDeleteCompleted	快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。
SnapshotsDeleteFailed	不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。
SnapshotsCopiedRegionStarted	快照策略启动的跨区域快照复制操作数。
SnapshotsCopiedRegionCompleted	快照策略创建的跨区域快照副本数量。这包括在计划时间的 24 小时内的成功重试。
SnapshotsCopiedRegionFailed	不能由快照策略创建的跨区域快照副本的数量。这包括在计划时间后 24 小时内的不成功重试。
SnapshotsCopiedRegionDeleteCompleted	快照策略删除的跨区域快照副本的数量，由保留规则指定。
SnapshotsCopiedRegionDeleteFailed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
snapshotsArchiveDeleteCompleted	成功由快照策略从存档层中删除的存档快照数量。
snapshotsArchiveScheduled	计划由快照策略存档的快照数量。
snapshotsArchiveCompleted	成功由快照策略存档的快照数量。
snapshotsArchiveFailed	不能由快照策略存档的快照数量。
snapshotsArchiveDeleteCompleted	成功由快照策略从存档层中删除的存档快照数量。

EBS-backed AMI policies

以下指标可与 EBS 支持的 AMI 策略一起使用：

指标	描述
ResourcesTargeted	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。
SnapshotsDeleteCompleted	快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。

指标	描述
SnapshotsDeleteFailed	不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 此指标包括在 EBS 支持的 AMI 策略取消注册 AMI 时删除的快照。
SnapshotsCopiedRegionDeleteCompleted	快照策略删除的跨区域快照副本的数量，由保留规则指定。
SnapshotsCopiedRegionDeleteFailed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
ImagesCreateStarted	由 EBS 支持的 AMI 策略启动的 CreateImage 操作的数量。
ImagesCreateCompleted	由 EBS 支持的 AMI 策略创建的 AMI 数量。
ImagesCreateFailed	不能由 EBS 支持的 AMI 策略创建的 AMI 数量。
ImagesDeregisterCompleted	由 EBS 支持的 AMI 策略取消注册的 AMI 数量。
ImagesDeregisterFailed	不能由 EBS 支持的 AMI 策略取消注册的 AMI 数量。
ImagesCopiedRegionStarted	由 EBS 支持的 AMI 策略启动的跨区域复制操作的数量。
ImagesCopiedRegionCompleted	由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。
ImagesCopiedRegionFailed	不能由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。
ImagesCopiedRegionDeregisterCompleted	由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。
ImagesCopiedRegionDeregisterFailed	不能由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。
EnableImageDeprecationCompleted	由 EBS 支持的 AMI 策略标记为弃用的 AMI 数量。
EnableImageDeprecationFailed	EBS 支持的 AMI 策略无法标记为弃用的 AMI 数。
EnableCopiedImageDeprecationCompleted	由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。
EnableCopiedImageDeprecationFailed	不能由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。

Cross-account copy event policies

跨账户复制事件策略可以使用以下指标：

指标	描述
SnapshotsCopiedAccountStarted	跨账户复制事件策略启动的跨账户快照复制操作的数量。
SnapshotsCopiedAccountCompleted	跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的成功重试。
SnapshotsCopiedAccountFailed	不能由跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的不成功重试。
SnapshotsCopiedAccountDeleteCompleted	跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。
SnapshotsCopiedAccountDeleteFailed	不能由跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。

查看适用于您策略的 CloudWatch 指标

您可以使用 Amazon Web Services Management Console 或命令行工具来列出 Amazon Data Lifecycle Manager 发送给 Amazon CloudWatch 的指标。

Amazon EC2 console

使用 Amazon EC2 控制台查看指标

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Lifecycle Manager（生命周期管理器）。
3. 在网格中选择一个策略，然后选择 Monitoring（监控）选项卡。

CloudWatch console

使用 Amazon CloudWatch 控制台查看指标

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，请选择指标。
3. 选择 EBS 命名空间，然后选择 Data Lifecycle Manager metrics（数据生命周期管理器指标）。

Amazon CLI

列出 Amazon Data Lifecycle Manager 的所有可用指标

使用 list-metrics 命令。

```
$ aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

列出特定策略的所有指标

使用 list-metrics 命令并指定 DLMPolicyId 维度。

```
$ aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

列出所有策略的单个指标

使用 list-metrics 命令并指定 --metric-name 选项。

```
$ aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

绘制策略的指标图表

在您创建策略后，可以打开 Amazon EC2 控制台并在 Monitoring（监控）选项卡上查看策略的监控图表。每个图表以一个可用的 Amazon EC2 指标为基础。

可供使用图表指标如下：

- 资源目标已确定（基于 ResourcesTargeted）
- 快照创建已启动（基于 SnapshotsCreateStarted）

- 快照创建已完成（基于 SnapshotsCreateCompleted）
- 快照创建已失败（基于 SnapshotsCreateFailed）
- 快照共享已完成（基于 SnapshotsSharedCompleted）
- 快照删除已完成（基于 SnapshotsDeleteCompleted）
- 快照删除已失败（基于 SnapshotsDeleteFailed）
- 快照跨区域复制已启动（基于 SnapshotsCopiedRegionStarted）
- 快照跨区域复制已完成（基于 SnapshotsCopiedRegionCompleted）
- 快照跨区域复制已失败（基于 SnapshotsCopiedRegionFailed）
- 快照跨区域复制删除已完成（基于 SnapshotsCopiedRegionDeleteCompleted）
- 快照跨区域复制删除已失败（基于 SnapshotsCopiedRegionDeleteFailed）
- 快照跨账户复制已启动（基于 SnapshotsCopiedAccountStarted）
- 快照跨账户复制已完成（基于 SnapshotsCopiedAccountCompleted）
- 快照跨账户复制已失败（基于 SnapshotsCopiedAccountFailed）
- 快照跨账户复制删除已完成（基于 SnapshotsCopiedAccountDeleteCompleted）
- 快照跨账户复制删除已失败（基于 SnapshotsCopiedAccountDeleteFailed）
- AMI 创建已开始（基于ImagesCreateStarted）
- AMI 创建已完成（基于 ImagesCreateCompleted）
- AMI 创建已失败（基于 ImagesCreateFailed）
- AMI 取消注册已完成（基于 ImagesDeregisterCompleted）
- AMI 取消注册已失败（基于 ImagesDeregisterFailed）
- AMI 跨区域复制已启动（基于 ImagesCopiedRegionStarted）
- AMI 跨区域复制已完成（基于 ImagesCopiedRegionCompleted）
- AMI 跨区域复制已失败（基于 ImagesCopiedRegionFailed）
- AMI 跨区域取消注册已完成（基于 ImagesCopiedRegionDeregisterCompleted）
- AMI 跨区域复制取消注册已失败（基于 ImagesCopiedRegionDeregisteredFailed）
- AMI 启用弃用已完成（基于 EnableImageDeprecationCompleted）
- AMI 启用弃用已失败（基于 EnableImageDeprecationFailed）
- AMI 跨区域复制启用弃用已完成（基于 EnableCopiedImageDeprecationCompleted）
- AMI 跨区域复制启用弃用已失败（基于 EnableCopiedImageDeprecationFailed）

为策略创建 CloudWatch 警报

您可以创建 CloudWatch 警报来监控您的策略的 CloudWatch 指标。当该指标达到指定阈值时，CloudWatch 自动向您发送通知。您可以使用 CloudWatch 控制台创建警报。

有关使用 CloudWatch 控制台创建警报的信息，请参阅 Amazon CloudWatch 用户指南 中的下列主题。

- 根据静态阈值创建 CloudWatch 警报
- 根据异常检测创建 CloudWatch 警报

使用案例示例

以下是使用案例示例：

主题

- 示例 1：ResourcesTargeted 指标 (p. 1492)
- 示例 2：SnapshotDeleteFailed 指标 (p. 1492)
- 示例 3：SnapshotsCopiedRegionFailed 指标 (p. 1492)

示例 1：ResourcesTargeted 指标

您可以使用 ResourcesTargeted 指标来监控特定策略每次运行时所针对的资源总数。这使您能够在目标资源的数量低于或高于预期阈值时触发告警。

例如，如果您希望每日策略创建不超过 50 卷的备份，可以创建告警，该告警会在 ResourcesTargeted 的 sum 大于 50 超过 1 小时时发送电子邮件通知。通过这种方式，您可以确保没有从已错误标记的卷意外创建任何快照。

可以使用以下命令创建此告警：

```
$ aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

示例 2：SnapshotDeleteFailed 指标

您可以使用 SnapshotDeleteFailed 指标，以根据策略的快照保留规则来监控删除快照的故障情况。

例如，如果您已创建应每 12 小时自动删除一次快照的策略，则可以创建一个告警，该告警会在 SnapshotDeletionFailed 的 sum 大于 0 超过 1 小时通知您的工程团队。这有助于调查不正确的快照保留，并确保您的存储成本不会因不必要的快照而增加。

可以使用以下命令创建此告警：

```
$ aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

示例 3：SnapshotsCopiedRegionFailed 指标

使用 SnapshotsCopiedRegionFailed 指标以确定您的策略何时无法将快照复制到其他区域。

例如，如果您的策略每天跨区域复制快照，则可以创建告警，该告警会在 SnapshotCrossRegionCopyFailed 的 sum 大于 0 超过 1 小时时向您的工程团队发送 SMS。这对于验证策略是否成功复制了谱系中的后续快照非常有用。

可以使用以下命令创建此告警：

```
$ aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
```

```
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

管理报告失败操作的策略

有关当其中一个策略报告失败操作指标的意外非零值时该怎么办的更多信息，请参阅如果 Amazon Data Lifecycle Manager 在 CloudWatch 指标中报告失败的操作，我该怎么办？ Amazon 。

Amazon EBS 数据服务

Amazon EBS 提供以下数据服务。

数据服务

- Amazon EBS 弹性卷 (p. 1493)
- Amazon EBS 加密 (p. 1504)
- Amazon EBS 快速快照还原 (p. 1514)

Amazon EBS 弹性卷

通过使用 Amazon EBS 弹性卷，您可以增加卷大小，更改卷类型或调整 EBS 卷的性能。如果您的实例支持弹性卷，您可以执行这些操作，而无需分离卷或重新启动实例。这样，您就可以在更改生效时继续使用应用程序。

修改卷配置是免费的。卷修改开始后，您需要支付新卷配置的费用。有关更多信息，请参阅Amazon EBS 定价页面。

目录

- 修改卷时的要求 (p. 1493)
- 请求对您的 EBS 卷进行修改 (p. 1495)
- 监控卷修改的进度 (p. 1498)
- 调整卷大小后扩展 Linux 文件系统 (p. 1500)

修改卷时的要求

您修改 Amazon EBS 卷时存在以下要求和限制。若要了解有关 EBS 卷的常规要求的更多信息，请参阅 针对 EBS 卷的大小和配置的限制 (p. 1342)。

主题

- 支持的实例类型 (p. 1493)
- 针对 Linux 卷的要求 (p. 1494)
- 限制 (p. 1494)

支持的实例类型

以下实例上支持弹性卷：

- 所有最新一代的实例 (p. 239)

- 以下上一代的实例：C1、C3、CC2、CR1、G2、I2、M1、M3 和 R3

如果您的实例类型不支持弹性卷，请参阅在不支持弹性卷的情况下修改 EBS 卷 (p. 1497)。

针对 Linux 卷的要求

Linux AMI 需要将 GUID 分区表 (GPT) 和 GRUB 2 用于 2 TiB (2048 GiB) 或更大的引导卷。现在的很多 Linux AMI 仍使用 MBR 分区方案，此方案仅支持最高 2 TiB 的引导卷大小。如果您的实例不通过大于 2 TiB 的引导卷启动，您要使用的 AMI 可能限制为小于 2 TiB 的引导卷大小。非引导卷对 Linux 实例没有这种限制。有关影响 Windows 卷的要求，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的针对 Windows 卷的要求。

在尝试调整超过 2 TiB 的引导卷大小之前，您可以通过在您的实例上运行以下命令来决定该卷是使用 MBR 分区还是使用 GPT 分区：

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

使用 GPT 分区的 Amazon Linux 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.10

  Partition table scan:
    MBR: protective
    BSD: not present
    APM: not present
    GPT: present

  Found valid GPT with protective MBR; using GPT.
```

使用 MBR 分区的 SUSE 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.8

  Partition table scan:
    MBR: MBR only
    BSD: not present
    APM: not present
    GPT: not present
```

限制

- 卷修改过程中可以请求的最大聚合存储空间存在限制。有关更多信息，请参阅 Amazon Web Services General Reference 中的 Amazon EBS 服务配额。
- 修改卷后，您须等待至少六个小时并确保卷处于 `in-use` 或 `available` 状态，然后再对同一个卷进行其他修改。这有时也称为冷却时间。
- 如果卷是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的，您必须初始化弹性卷支持。有关更多信息，请参阅初始化弹性卷支持 (p. 1496)。
- 如果在尝试修改 EBS 卷时遇到错误消息，或者要修改附加到上一代实例类型的 EBS 卷，请执行以下步骤之一：
  - 对于非根卷，将卷与实例分离，应用修改，然后重新附加卷。
  - 对于根卷，停止实例，应用修改，然后重新启动实例。
- 尚未完全初始化的卷的修改时间会增加。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。
- 新卷大小不能超过其文件系统和分区方案所支持的容量。有关更多信息，请参阅针对 EBS 卷的大小和配置的限制 (p. 1342)。
- 如果要修改卷类型，则大小和性能必须在目标卷类型的限制范围内。有关更多信息，请参阅 Amazon EBS 卷类型 (p. 1327)

- 您无法减小 EBS 卷的大小。但是，您可以创建较小的卷，然后使用应用程序级工具（如 rsync）将数据迁移到该卷。
- 在现有 io1 或 io2 卷预置超 32,000 IOPS 后，您可能需要分离并重新连接卷，或重新启动实例以查看完整的性能改进。
- 对于 io2 卷，当其连接至不支持 io2 Block Express 的实例类型时，您无法将其大小增加超过 16TiB 或 IOPS 超过 64,000。有关更多信息，请参阅io2 Block Express 卷 (p. 1334)。
- 您不能修改启用多重挂载的 io2 卷的卷类型。
- 您无法修改启用了多重挂载的 io1 卷的卷类型、大小或预置 IOPS。
- 无法将类型 io1、io2、gp2、gp3 或 standard 的根卷修改为 st1 或 sc1 卷，即使已将它与实例分离也是如此。
- 虽然 m3.medium 实例完全支持卷修改，但 m3.large、m3.xlarge 和 m3.2xlarge 实例可能不支持所有卷修改功能。

请求对您的 EBS 卷进行修改

对于弹性卷，您可以在不分离 Amazon EBS 卷的情况下动态增加卷的大小或降低其性能，以及修改卷类型。

修改卷时使用以下过程：

1. （可选）在修改包含有用数据的卷之前，最佳实践是创建卷的快照（如果您需要回滚您的更改）。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。
2. 请求卷修改。
3. 监控卷修改进度。有关更多信息，请参阅监控卷修改的进度 (p. 1498)。
4. 如果修改了卷的大小，请扩展卷的文件系统以利用增加的存储容量。有关更多信息，请参阅调整卷大小后扩展 Linux 文件系统 (p. 1500)。

目录

- 使用弹性卷修改 EBS 卷 (p. 1495)
- 初始化弹性卷支持（如果需要） (p. 1496)
- 在不支持弹性卷的情况下修改 EBS 卷 (p. 1497)

使用弹性卷修改 EBS 卷

注意事项

修改 卷时请牢记以下事项：

- 提交卷修改请求后，您将无法取消该请求。
- 您只能增加卷的大小。您无法减小卷的大小。
- 您可以提高或降低卷的性能。
- 如果您没有修改卷类型，则卷的大小和性能修改必须在当前卷类型的限制范围内。如果您更改卷类型，则卷的大小和性能修改必须在目标卷类型的限制范围内
- 如果您将卷类型从 gp2 更改为 gp3，并且您未指定 IOPS 或吞吐量性能，则 Amazon EBS 将自动预调配与源 gp2 卷的性能或基准 gp3 性能相当的性能（以二者中较高者为准）。

  例如，如果您将具有 250 MiB/s 吞吐量和 1500 IOPS 的 500 GiB gp2 卷修改为 gp3，但未指定 IOPS 或吞吐量性能，Amazon EBS 会自动预调配具有 3000 IOPS（基准gp3 IOPS）和 250 MiB/s（用于匹配源 gp2 卷吞吐量）的 gp3 卷。

要修改 EBS 卷，请使用以下方法之一。

Console

使用控制台修改 EBS 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择要修改的卷，然后选择 Actions（操作）、Modify Volume（修改卷）。
4. Modify Volume（修改卷）窗口显示卷 ID 和卷的当前配置，包括类型、大小、IOPS 和吞吐量。设置新的配置值，如下所述：
   - 要修改类型，请为 Volume type（卷类型）选择一个值。
   - 要修改大小，请为 Size (大小) 输入新值。
   - （仅限于 gp3、io1 和 io2）要修改 IOPS，为 IOPS 输入新值。
   - （仅限于 gp3）要修改吞吐量，为 Throughput（吞吐量）输入新值。
5. 完成更改卷设置后，请选择 Modify (修改)。当系统提示您确认时，选择 Modify（修改）。
6. Important

   如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅调整卷大小后扩展 Linux 文件系统 (p. 1500)。

Amazon CLI

使用 Amazon CLI 修改 EBS 卷

使用 modify-volume 命令修改卷的一个或多个配置设置。如果您有一个类型为 gp2 且大小为 100 GiB 的卷，以下命令会将其配置更改为类型为 io1、包含 10000 IOPS 且大小为 200 GiB 的卷。

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-
id vol-11111111111111111
```

下面是示例输出：

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-11111111111111111",
        "TargetIops": 10000,
        "StartTime": "2017-01-19T22:21:02.959Z",
        "Progress": 0,
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
    }
}
```

Important

如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅调整卷大小后扩展 Linux 文件系统 (p. 1500)。

初始化弹性卷支持（如果需要）

您必须先使用以下操作之一初始化卷修改支持，然后才能修改在 UTC 时间 2016 年 11 月 3 日 23:40 前附加到实例的卷：

- 分离和附加卷
- 停止和启动实例

使用以下过程之一来确定您的实例是否已准备好进行卷修改。

Console

使用控制台确定您的实例是否已准备就绪

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择 Show/Hide Columns 图标 (齿轮)。选择启动时间属性列，然后选择确认。
4. 按 Launch Time 列对实例列表进行排序。对于在截止日期之前启动的每个实例，选择存储选项卡，并检查连接时间列以查看其卷附加的时间。

Amazon CLI

使用 CLI 确定您的实例是否已准备就绪

使用以下 describe-instances 命令确定卷是否是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的。

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" --output text
```

每个实例的输出的第一行都将显示其 ID，无论实例是否在截止日期前启动（True 或 False）。第一行后跟一行或多行，以显示是否在截止日期前已附加每个 EBS 卷（True 或 False）。在以下示例输出中，您必须为第一个实例初始化卷修改，因为该实例是在截止日期前启动的，并且其根卷是在截止日期前附加的。其他实例已准备就绪，因为它们是在截止日期后启动的。

```
i-e905622e              True
True
i-719f99a8              False
True
i-006b02c1b78381e57     False
False
False
i-e3d172ed              False
True
```

在不支持弹性卷的情况下修改 EBS 卷

如果您使用的是支持的实例类型，则可以使用弹性卷来在不分离 Amazon EBS 卷的情况下动态修改卷的大小、性能和卷类型。

如果您无法使用弹性卷但需要修改根（启动）卷，则必须停止实例，修改卷，然后重新启动实例。

实例启动之后，可以检查文件系统大小，看实例是否识别这个更大的卷空间。在 Linux 上，请使用 df -h 命令检查文件系统大小。

```
[ec2-user ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

如果大小没有反映新扩展的卷，则必须扩展设备的文件系统，以便实例可以使用新的空间。有关更多信息，请参阅调整卷大小后扩展 Linux 文件系统 (p. 1500)。

监控卷修改的进度

当您修改 EBS 卷时，它将经历一系列状态。卷将依次进入 `modifying` 状态、`optimizing` 状态和 `completed` 状态。此时，卷已准备好做进一步的修改。

> **Note**
>
> 在极少数情况下，暂时的 Amazon 故障可能会导致 `failed` 状态。这并不指示卷的运行状况；它仅指示卷修改失败。如果发生这种情况，请重试卷修改。

当卷处于 `optimizing` 状态时，卷性能介于源配置规范和目标配置规范之间。过渡卷的性能将不会低于源卷的性能。如果您降级 IOPS，则过渡卷的性能不会低于目标卷的性能。

卷修改更改将生效，如下所示：

- 大小更改通常需要几秒钟才能完成，并在卷转为 `0ptimizing` 状态后生效。
- 性能 (IOPS) 更改可能需要几分钟到几小时才能完成，具体视所做的配置更改而定。
- 在某些情况下，新配置生效最长需要 24 个小时，例如卷未完全初始化时。通常，完全使用的 1 TiB 卷需要约 6 个小时才能迁移到新的性能配置。

要监控卷修改的进度，请使用以下方法之一。

Console

使用 Amazon EC2 控制台监控修改的进度

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 在 Details（详细信息）选项卡的 Volume state（卷状态）列和 Volume state（卷状态）字段包含以下格式的信息：*volume-state* - *modification-state* (*progress*%)。

   可能的卷状态包括 `creating`、`available`、`in-use`、`deleting`、`deleted` 和 `error`。

   可能的代码状态是 `modifying`、`optimizing` 和 `completed`。

Amazon CLI

要使用 Amazon CLI 监控修改进度

使用 describe-volumes-modifications 命令查看一个或多个卷修改的进度。以下示例描述了两个卷的卷修改。

```
aws ec2 describe-volumes-modifications --volume-
ids vol-11111111111111111 vol-22222222222222222
```

在以下示例输出中，卷修改仍处于 `modifying` 状态。以百分比形式报告进展情况。

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
            "ModificationState": "modifying",
            "VolumeId": "vol-11111111111111111",
```

```
            "TargetIops": 10000,
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-22222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

下一个示例描述了修改状态为 `optimizing` 或 `completed` 的所有卷，然后筛选和格式化结果以只显示于 2017 年 2 月 1 日及之后做出的修改：

```
aws ec2 describe-volumes-modifications --filters Name=modification-
state,Values="optimizing","completed" --query "VolumesModifications[?
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

以下是包含有关两个卷的信息的示例输出：

```
[
    {
        "STATE": "optimizing",
        "ID": "vol-06397e7a0eEXAMPLE"
    },
    {
        "STATE": "completed",
        "ID": "vol-ba74e18c2aEXAMPLE"
    }
]
```

CloudWatch Events console

利用 CloudWatch Events，您可以为卷修改事件创建通知规则。您可以使用规则生成使用 Amazon SNS 的通知消息，或调用 Lambda 函数来响应匹配事件。尽最大努力发出事件。

使用 CloudWatch Events 监控修改进度

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 依次选择 Events、Create rule。
3. 对于 Build event pattern to match events by service，选择 Custom event pattern。
4. 对于 Build custom event pattern (构建自定义事件模式)，将内容替换为以下内容并选择 Save (保存)。

```
{
  "source": [
    "aws.ec2"
  ],
  "detail-type": [
    "EBS Volume Notification"
  ],
```

```
  "detail": {
    "event": [
      "modifyVolume"
    ]
  }
}
```

下面是示例事件数据：

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "2017-01-12T21:09:07Z",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

调整卷大小后扩展 Linux 文件系统

Note

以下主题将引导您完成为 Linux 扩展 XFS 和 Ext4 文件系统的过程。有关其他文件系统的信息，请参阅其文档了解相关说明。

增加 EBS 卷的大小后 (p. 1495)，您必须使用文件系统特定的命令将文件系统扩展到新的较大大小。您可以在卷进入 optimizing 状态后立即执行此操作。

若要在 Linux 上扩展文件系统，您需要执行以下操作：

1. 如果卷有分区，则扩展分区。
2. 扩展文件系统。

开始前的准备工作

- 如果需要回滚更改，则创建卷的快照。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。
- 确认卷修改成功并且其处于 optimizing 或 completed 状态。有关更多信息，请参阅监控卷修改的进度 (p. 1498)。
- 确保卷已附加到实例，并且已格式化和挂载。有关更多信息，请参阅格式化并挂载附加的卷 (p. 1348)。
- 如果在 Amazon EBS 卷上使用逻辑卷，则必须使用逻辑卷管理器 (LVM) 来扩展逻辑卷。有关如何执行此操作的说明，请参阅 Amazon 知识中心文章如何在整个 EBS 卷上创建 LVM 逻辑卷？中的扩展逻辑卷部分。

扩展 EBS 卷的文件系统

按照以下过程扩展调整大小后的卷的文件系统。请注意，Xen 实例和 Nitro 实例 (p. 246)的设备和分区命名有所不同。若要确定您的实例是 Xen 实例还是 Nitro 实例，请使用以下命令：

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-type instance_type --query
 "InstanceTypes[].Hypervisor"
```

扩展 EBS 卷的文件系统

1. 连接到您的 实例 (p. 644)。
2. 如果需要，调整分区的大小。为此，请执行以下操作：

   a. 检查卷是否有分区。使用 lsblk 命令。

      Nitro instance example

      在以下示例输出中，根卷 (nvme0n1) 有两个分区（nvme0n1p1 和 nvme0n1p128），而额外的卷 (nvme1n1) 没有分区。

      ```
      [ec2-user ~]$ sudo lsblk
      NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      nvme1n1       259:0    0  30G  0 disk /data
      nvme0n1       259:1    0  16G  0 disk
      ##nvme0n1p1   259:2    0   8G  0 part /
      ##nvme0n1p128 259:3    0   1M  0 part
      ```

      Xen instance example

      在以下示例输出中，根卷 (xvda) 有一个分区 (xvda1)，而额外的卷 (xvdf) 没有分区。

      ```
      [ec2-user ~]$ sudo lsblk
      NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
      xvda    202:0    0  16G  0 disk
      ##xvda1 202:1    0   8G  0 part /
      xvdf    202:80   0  24G  0 disk
      ```

      如果该卷具有分区，则继续执行以下步骤（2b）。如果该卷没有分区，请跳过步骤 2b、2c 和 2d，然后继续执行步骤 3。

      故障排除技巧

      如果没有在命令输出中看到该卷，请确保该卷已附加到实例 (p. 1347)并且已格式化和挂载 (p. 1348)。

   b. 检查是否需要扩展分区。在上一步的 lsblk 命令输出中，比较分区大小和卷大小。

      如果分区大小小于卷大小，则继续执行下一步。如果分区大小等于卷大小，则无法扩展分区。

      故障排除技巧

      如果卷仍然反映原始大小，则请确认卷修改成功 (p. 1498)。

   c. 扩展分区。使用 growpart 命令并指定要扩展的分区。

      Nitro instance example

      例如，若要扩展名为 nvme0n1p1 的分区，请使用以下命令。

      Important

      请注意，设备名称 (nvme0n1) 和分区编号 (1) 之间有空格。

      ```
      [ec2-user ~]$ sudo growpart /dev/nvme0n1 1
      ```

Xen instance example

例如，若要扩展名为 xvda1 的分区，请使用以下命令。

Important

请注意，设备名称 (xvda) 和分区编号 (1) 之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

故障排除技巧

- mkdir: cannot create directory ‘/tmp/growpart.31171’: No space left on device FAILED: failed to make temp dir：表示卷上没有足够的可用磁盘空间供 growpart 创建执行调整大小所需的临时目录。请释放一些磁盘空间并重试。
- must supply partition-number：表示您指定的分区不正确。使用 lsblk 命令以确认分区名称，并确保在设备名称和分区编号之间输入空格。
- NOCHANGE: partition 1 is size 16773087. it cannot be grown：表示分区已经扩展了整个卷，无法再扩展。确认卷修改成功 (p. 1498)。

d. 验证是否已扩展分区。使用 lsblk 命令。分区大小现在应等于卷大小。

Nitro instance example

以下示例输出显示卷 (nvme0n1) 和分区 (nvme0n1p1) 的大小相同 (16 GB)。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0  16G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

以下示例输出显示卷 (xvda) 和分区 (xvda1) 的大小相同 (16 GB)。

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. 扩展文件系统。

a. 获取需要扩展的文件系统的名称、大小、类型和挂载点。使用 df -hT 命令。

Nitro instance example

以下示例输出显示了 /dev/nvme0n1p1 文件系统的大小为 8 GB，其类型为 xfs，其挂载点是 /。

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
```

```
...
```

Xen instance example

以下示例输出显示了 /dev/xvda1 文件系统的大小为 8 GB，其类型为 ext4，其挂载点是 /。

```
[ec2-user ~]$ df -hT
Filesystem      Type   Size    Used   Avail   Use%   Mounted on
/dev/xvda1      ext4   8.0G    1.9G   6.2G    24%    /
/dev/xvdf1      xfs    24.0G   45M    8.0G    1%     /data
...
```

b. 扩展文件系统的命令因文件系统类型而异。根据您在上一步中记录的文件系统类型选择以下正确命令。

- [XFS 文件系统] 使用 xfs_growfs 命令并指定您在上一步中记录的文件系统的挂载点。

  Nitro and Xen instance example

  例如，若要扩展挂载在 / 上的文件系统，请使用以下命令。

  ```
  [ec2-user ~]$ sudo xfs_growfs -d /
  ```

  故障排除技巧

  - `xfs_growfs: /data is not a mounted XFS filesystem`：表示指定的挂载点不正确，或者文件系统不是 XFS。若要验证挂载点和文件系统类型，请使用 df -hT 命令。
  - `data size unchanged, skipping`：表示文件系统已经扩展了整个卷。如果卷没有分区，则请确认卷修改成功 (p. 1498)。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [Ext4 文件系统] 使用 resize2fs 命令并指定您在上一步中记录的文件系统的名称。

  Nitro instance example

  例如，若要扩展名为 /dev/nvme0n1p1 的挂载文件系统，请使用以下命令。

  ```
  [ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
  ```

  Xen instance example

  例如，若要扩展名为 /dev/xvda1 的挂载文件系统，请使用以下命令。

  ```
  [ec2-user ~]$ sudo resize2fs /dev/xvda1
  ```

  故障排除技巧

  - `resize2fs: Bad magic number in super-block while trying to open /dev/xvda1`：表示文件系统不是 Ext4。若要验证文件系统类型，请使用 df -hT 命令。
  - `open: No such file or directory while opening /dev/xvdb1`：表示您指定的分区不正确。若要验证分区，请使用 df -hT 命令。
  - `The filesystem is already 3932160 blocks long. Nothing to do!`：表示文件系统已经扩展了整个卷。如果卷没有分区，则请确认卷修改成功 (p. 1498)。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [其他文件系统]，请参阅文件系统的文档，了解相关说明。

c. 验证是否已扩展文件系统。使用 df -hT 命令并确认文件系统大小等于卷大小。

Amazon EBS 加密

使用 Amazon EBS 加密 作为与 EC2 实例关联的 EBS 资源的直接加密解决方案。借助 Amazon EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。创建加密卷和快照时，Amazon EBS 加密使用 Amazon KMS keys。

加密操作在托管 EC2 实例的服务器上进行，用于确保静态数据安全性以及在实例和其附加的 EBS 存储之间传输的数据的安全性。

您可以同时将加密卷和未加密卷附加到实例。

目录

- EBS 加密的工作原理 (p. 1504)
- 要求 (p. 1505)
- EBS 加密的默认 KMS 密钥 (p. 1506)
- 默认加密 (p. 1507)
- 加密 EBS 资源 (p. 1508)
- 轮换 Amazon KMS 密钥 (p. 1508)
- 加密方案 (p. 1509)
- 使用 API 和 CLI 设置加密默认值 (p. 1513)

EBS 加密的工作原理

您可以加密 EC2 实例的引导卷和数据卷。

在创建加密的 EBS 卷并将其附加到支持的实例类型后，将对以下类型的数据进行加密：

- 卷中的静态数据
- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照
- 从这些快照创建的所有卷

Amazon EBS 通过数据密钥使用行业标准的 AES-256 数据加密来加密您的卷。数据密钥由 Amazon KMS 生成，然后由 Amazon KMS 使用您的 Amazon KMS 密钥加密，然后再与您的卷信息一起存储。同一数据密钥将由所有快照以及使用相同 Amazon KMS 密钥从这些快照创建的任何后续卷共享。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的数据密钥。

根据用于创建加密卷的快照是加密还是未加密，Amazon EC2 和 Amazon KMS 结合使用以稍有不同的方式对 EBS 卷进行加密和解密。

快照加密时 EBS 加密的工作原理

当您从自己拥有的加密快照创建加密卷时，Amazon EC2 和 Amazon KMS 结合使用对 EBS 卷进行加密和解密，如下所示：

1. Amazon EC2 将 GenerateDataKeyWithoutPlaintext 请求发送到 Amazon KMS，并指定您为卷加密选择的 KMS 密钥。
2. 如果使用与快照相同的 KMS 密钥加密卷，Amazon KMS 将使用与快照相同的数据密钥，并在同一 KMS 密钥下对其进行加密。如果使用不同的 KMS 密钥加密卷，Amazon KMS 会生成一个新的数据密钥，并在您指定的 KMS 密钥下对其进行加密。加密的数据密钥会发送到 Amazon EBS，并与卷元数据存储在一起。

3. 当您将加密卷附加到实例时，Amazon EC2 将 CreateGrant 请求发送到 Amazon KMS，以便它可以解密数据密钥。
4. Amazon KMS 解密加密的数据密钥，然后将解密的数据密钥发送到 Amazon EC2。
5. Amazon EC2 使用管理程序内存中的明文数据密钥来加密卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

快照未加密时 EBS 加密的工作原理

当您从未加密的快照创建加密卷时，Amazon EC2 和 Amazon KMS 结合使用对 EBS 卷进行加密和解密，如下所示：

1. Amazon EC2 将 CreateGrant 请求发送到 Amazon KMS，以便它可以对从快照创建的卷进行加密。
2. Amazon EC2 将 GenerateDataKeyWithoutPlaintext 请求发送到 Amazon KMS，并指定您为卷加密选择的 KMS 密钥。
3. Amazon KMS 会生成一个新的数据密钥，在您为卷加密选择的 KMS 密钥下加密该密钥，然后将加密后的数据密钥发送到 Amazon EBS 以便与卷元数据一起存储。
4. Amazon EC2 将 Decrypt 请求发送到 Amazon KMS 以获取用于加密卷数据的加密密钥。
5. 当您将加密卷附加到实例时，Amazon EC2 将 CreateGrant 请求发送到 Amazon KMS，以便它可以解密数据密钥。
6. 当您将加密卷附加到实例时，Amazon EC2 将 Decrypt 请求发送到 Amazon KMS，同时指定加密的数据密钥。
7. Amazon KMS 解密加密的数据密钥，然后将解密的数据密钥发送到 Amazon EC2。
8. Amazon EC2 使用管理程序内存中的明文数据密钥来加密卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon Elastic Block Store (Amazon EBS) 如何使用 Amazon KMS 和 Amazon EC2 示例 2。

要求

在您开始之前，确认您满足以下要求。

支持的卷类型

所有 EBS 卷类型都支持加密。您可能希望加密卷具有与未加密卷相同的 IOPS 性能，同时对延迟的影响最低。您可以采用与访问未加密卷相同的方式来访问加密卷。加密和解密是以透明方式处理的，并且不需要您或您的应用程序执行额外操作。

支持的实例类型

Amazon EBS 加密适用于所有当前一代 (p. 239)实例类型以及下列上一代 (p. 244)实例类型：
A1、C1、C3、cr1.8xlarge、G2、I2、M1、M2、M3 和 R3。

用户的权限

当您将 KMS 密钥配置为用于 EBS 加密的默认密钥时，默认 KMS 密钥政策允许任何有权访问所需 KMS 操作的用户使用此 KMS 密钥加密或解密 EBS 资源。您必须授予用户调用以下操作的权限才能使用 EBS 加密：

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

Tip

为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。而是仅当 Amazon 服务代表用户创建授权时，才使用 kms:GrantIsForAWSResource 条件键以允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中默认密钥策略部分中的允许访问 Amazon账户并启用 IAM policy。

EBS 加密的默认 KMS 密钥

Amazon EBS 自动在您存储 Amazon 资源的每个区域中创建唯一的 Amazon 托管式密钥。此 KMS 密钥 具有别名 alias/aws/ebs。默认情况下，Amazon EBS 使用此 KMS 密钥 进行加密。您也可以指定一个您创建的对称客户管理加密密钥，以作为 EBS 加密的原定设置 KMS 密钥。使用您自己的 KMS 密钥 可以提高灵活性，包括提供创建、轮换和禁用 KMS 密钥 的能力。

Important

Amazon EBS 不支持非对称加密 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的使用对称和非对称加密 KMS 密钥。

New console

针对某个区域配置用于 EBS 加密的默认 KMS 密钥

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择 EBS 加密。
5. 选择管理。
6. 对于 Default encryption key（原定设置加密密钥），选择对称客户管理加密密钥。
7. 选择更新 EBS 加密。

Old console

针对某个区域配置用于 EBS 加密的默认 KMS 密钥

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择设置。
5. 选择 Change the default key（更改默认密钥），然后选择可用 KMS 密钥。
6. 选择 Save settings (保存设置)。

默认加密

您可以配置 Amazon 账户对您创建的新 EBS 卷和快照副本进行加密。例如，Amazon EBS 加密当您启动实例时创建的 EBS 卷以及您从未加密的快照复制的快照。有关从未加密转换为加密 EBS 资源的示例，请参阅加密未加密的资源 (p. 1508)。

默认情况下，加密对现有 EBS 卷或快照没有影响。

注意事项

- 默认加密是区域特定的设置。如果您为某个区域启用了它，则无法为该区域中单独的卷或快照禁用。
- 当您启用默认加密时，您只能在实例类型支持 EBS 加密时启动实例。有关更多信息，请参阅支持的实例类型 (p. 1505)。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 在使用 Amazon Server Migration Service (SMS) 迁移服务器时，默认情况下不会启用加密。如果默认情况下已启用加密，并且您遇到增量复制失败，请默认关闭加密。改为在创建复制作业时启用 AMI 加密。

New console

默认为某个区域启用加密

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择 EBS 加密。
5. 选择管理。
6. 选择 Enable (启用)。您可以将系统代表您创建的 Amazon 托管式密钥（别名为 `alias/aws/ebs`）保留为默认加密密钥，或者选择对称客户管理加密密钥。
7. 选择更新 EBS 加密。

Old console

默认为某个区域启用加密

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择区域。
3. 从导航窗格中，选择 EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择设置。
5. 在 EBS Storage (EBS 存储) 下，选择 Always encrypt new EBS volumes (始终加密新的 EBS 卷)。
6. 选择 Save settings (保存设置)。

您无法更改与现有快照或加密卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

加密 EBS 资源

您可以通过启用加密来加密 EBS 卷：使用默认加密 (p. 1507)，或者在创建要加密的卷时启用加密。

加密卷时，可以指定用于加密该卷的对称加密 KMS 密钥。如果未指定 KMS 密钥，则用于加密的 KMS 密钥取决于源快照的加密状态及其所有权。有关更多信息，请参阅加密结果表 (p. 1512)。

> Note
>
> 如果您正在使用 API 或 Amazon CLI 指定 KMS 密钥，请注意 Amazon 将异步对 KMS 密钥 进行身份验证。如果您指定了无效的 KMS 密钥 ID、别名或 ARN，则操作可能会显示完成，但最终失败。

您无法更改与现有快照或卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

在创建时加密空卷

创建新的空 EBS 卷时，可以通过为特定卷创建操作启用加密来对其进行加密。如果默认情况下启用了 EBS 加密，则会使用 EBS 加密的默认 KMS 密钥 自动加密卷。您也可以为特定的卷创建操作指定不同的对称加密 KMS 密钥。卷从其首次可用时开始加密，因此您的数据始终安全。有关详细步骤，请参阅创建 Amazon EBS 卷 (p. 1344)。

默认情况下，您在创建卷时选择的 KMS 密钥 会对从该卷拍摄的快照加密，并对从这些加密的快照还原的卷加密。您无法从加密卷或快照删除加密，这意味着从加密快照还原的卷或者加密快照的副本始终加密。

加密卷的快照无法公开，但您可以与特定账户共享加密快照。有关详细指导，请参阅共享 Amazon EBS 快照 (p. 1403)。

加密未加密的资源

您无法直接加密现有未加密卷或快照。但是，您可以从未加密的卷或快照创建加密卷或快照。如果预设情况下启用加密，Amazon EBS 将使用 EBS 加密的原定设置 KMS 密钥自动加密新卷和快照。否则，您可以在创建单个卷或快照时启用加密，使用用于 Amazon EBS 加密的原定设置 KMS 密钥或对称客户管理加密密钥。有关更多信息，请参阅 创建 Amazon EBS 卷 (p. 1344) 和 复制 Amazon EBS 快照 (p. 1377)。

要将快照副本加密到 客户托管密钥，您必须同时启用加密并指定 KMS 密钥，如 复制未加密的快照（未启用默认加密） (p. 1510) 中所示。

> Important
>
> Amazon EBS 不支持非对称加密 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的使用对称和非对称加密 KMS 密钥。

在从由 EBS 支持的 AMI 启动实例时，您还可以应用新的加密状态。这是因为 EBS 支持的 AMI 包括可以按照所述进行加密的 EBS 卷的快照。有关更多信息，请参阅将加密与 EBS 支持的 AMI 结合使用 (p. 196)。

轮换 Amazon KMS 密钥

加密最佳实践建议不要广泛重复使用加密密钥。要为您的 KMS 密钥创建新的加密材料，您可以创建新的 KMS 密钥，然后更改您的应用程序或别名来使用新的 KMS 密钥。或者，您可以为现有 KMS 密钥启用自动密钥轮换。

如果您为 KMS 密钥启用自动密钥轮换，Amazon KMS 会每年为该 KMS 密钥生成新的加密材料。Amazon KMS 会保留所有以前版本的加密材料，以便解密使用该 KMS 密钥加密的任何数据。Amazon KMS 不会删除任何轮换的密钥材料，直至您删除 KMS 密钥。

当您使用轮换 KMS 密钥加密数据时，Amazon KMS 会使用当前的密钥材料。当您使用轮换 KMS 密钥解密数据时，Amazon KMS 会使用加密时所用的密钥材料版本。您可以在应用程序和 Amazon 服务中安全地使用轮换的 KMS 密钥，而无需代码更改。

Note

只有具有 Amazon KMS 创建的密钥材料的对称客户托管密钥才支持自动轮换密钥。Amazon KMS 每年自动轮换 Amazon 托管式密钥。您无法启用或禁用 Amazon 托管式密钥 的密钥轮换。

有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 轮换 KMS 密钥。

加密方案

创建加密 EBS 资源时，除非您在卷创建参数或 AMI 或实例的块设备映射中指定了不同的 客户托管密钥，否则它将使用您账户的用于 EBS 加密的默认 KMS 密钥 进行加密。有关更多信息，请参阅EBS 加密的默认 KMS 密钥 (p. 1506)。

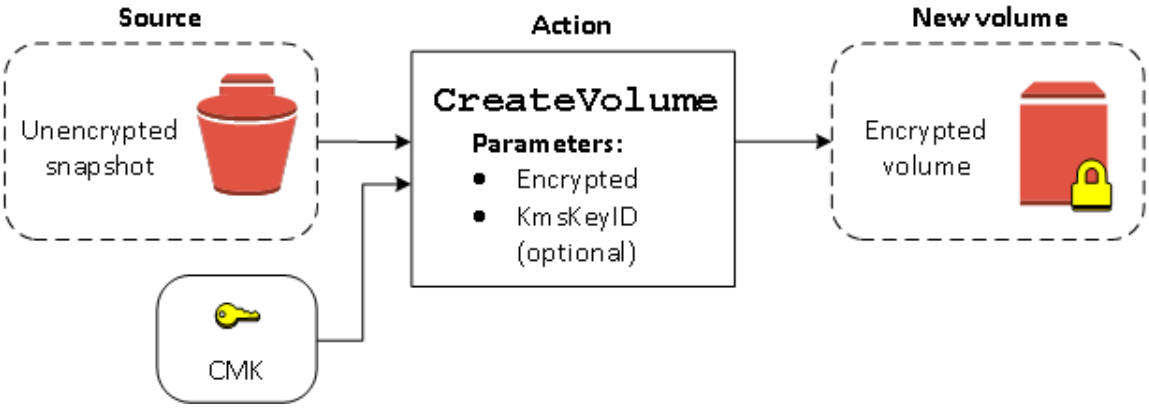
以下示例说明如何管理卷和快照的加密状态。有关加密案例的完整列表，请参阅加密结果表 (p. 1512)。

示例

- 还原未加密的卷（未启用默认加密） (p. 1509)
- 还原未加密的卷（启用了默认加密） (p. 1509)
- 复制未加密的快照（未启用默认加密） (p. 1510)
- 复制未加密的快照（启用了默认加密） (p. 1510)
- 重新加密已加密卷 (p. 1511)
- 重新加密已加密快照 (p. 1511)
- 在加密卷与未加密卷之间迁移数据 (p. 1512)
- 加密结果 (p. 1512)

还原未加密的卷（未启用默认加密）

未启用默认加密时，从未加密快照还原的卷在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的卷。下图说明了该过程。

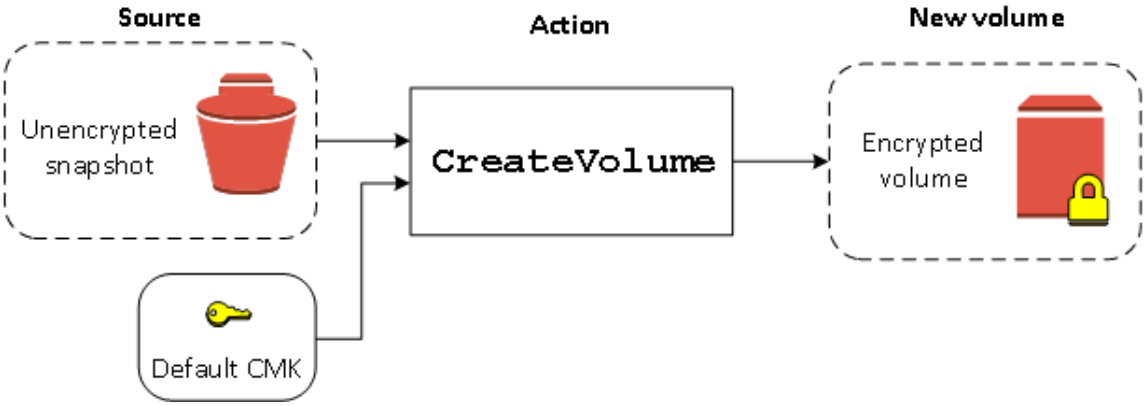


如果您省略 `KmsKeyId` 参数，则将使用您用于 EBS 加密的默认 KMS 密钥 加密生成的卷。您必须指定 KMS 密钥 ID 以使用不同的 KMS 密钥 加密卷。

有关更多信息，请参阅从快照创建卷 (p. 1346)。

还原未加密的卷（启用了默认加密）

在您启用了默认加密时，从未加密快照还原的卷必须加密，无需使用默认 KMS 密钥 的加密参数。下图说明了这种简单默认案例：

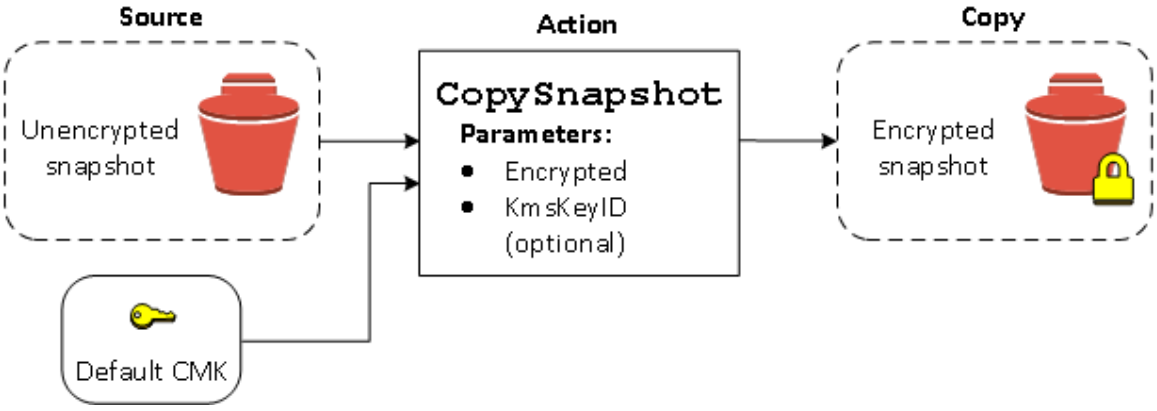


如果您要使用对称客户管理加密密钥来加密还原的卷，则必须提供 Encrypted 和 KmsKeyId 参数，如 还原未加密的卷（未启用默认加密）(p. 1509) 中所示。

复制未加密的快照（未启用默认加密）

未启用默认加密时，未加密快照的副本在默认情况下不加密。但是，您可以设置 Encrypted 参数和可选的 KmsKeyId 参数来加密生成的快照。如果省略 KmsKeyId，则使用默认 KMS 密钥 加密生成的快照。您必须指定 KMS 密钥 ID 以使用不同的对称加密 KMS 密钥对卷进行加密。

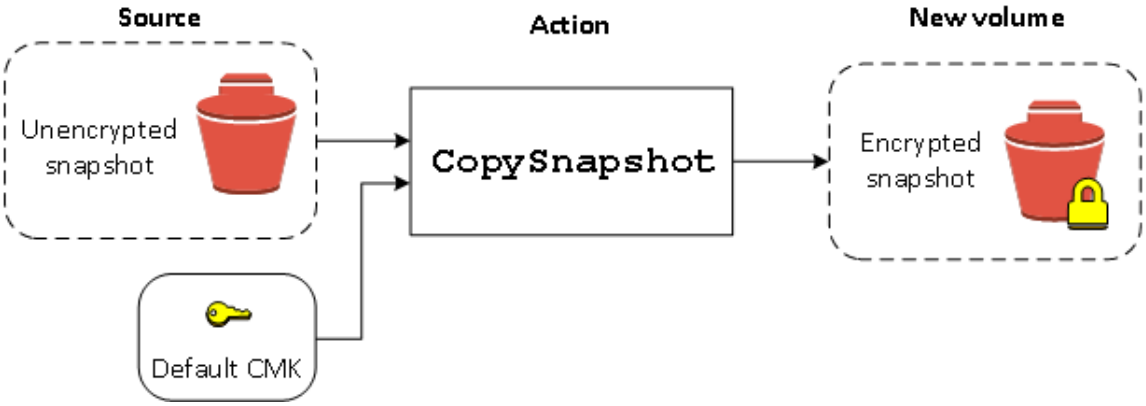
下图说明了该过程。



您可以将未加密的快照复制到加密的快照，然后从加密的快照中创建卷来加密 EBS 卷。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。

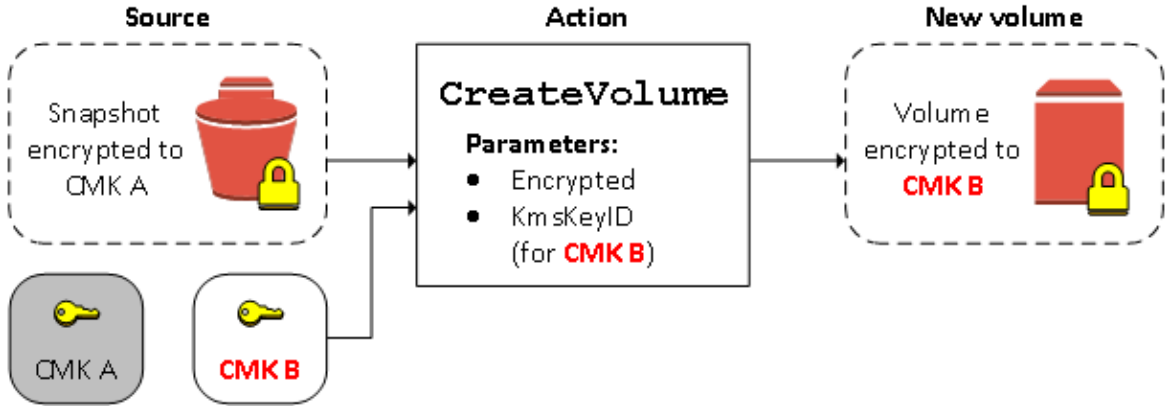
复制未加密的快照（启用了默认加密）

在您启用了默认加密时，未加密快照的副本必须加密，无需使用默认 KMS 密钥 的加密参数。下图说明了这种默认情况：



重新加密已加密卷

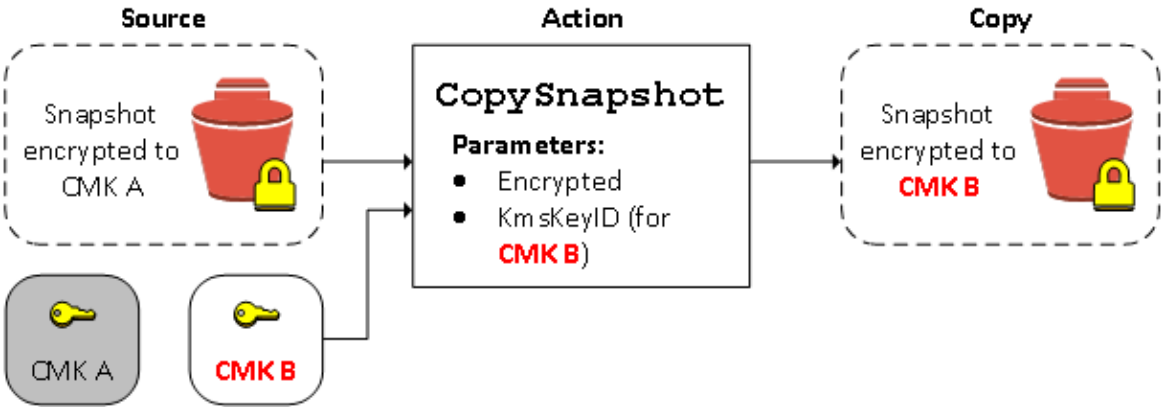
对加密快照执行 `CreateVolume` 操作时，您可以选择使用不同的 KMS 密钥 重新加密它。下图说明了该过程。在本例中，您拥有两个 KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在卷创建期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据被自动解密，然后由 KMS 密钥 B 重新加密。



有关更多信息，请参阅从快照创建卷 (p. 1346)。

重新加密已加密快照

由于能够在复制过程中加密快照，您可以将新的对称加密 KMS 密钥应用于您拥有的已加密过的快照。从生成的副本还原的卷只能使用新的 KMS 密钥 进行访问。下图说明了该过程。在本例中，您拥有两个 KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在复制期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据由 KMS 密钥 B 自动重新加密。



在相关的场景中，您可以选择将新加密参数应用于已与您共享的快照的副本。默认情况下，系统会使用快照拥有者共享的 KMS 密钥 对该副本进行加密。但是，我们建议您使用您控制的其他 KMS 密钥 创建共享快照的副本。这样，即使原始 KMS 密钥 遭到泄露或拥有者出于任何原因撤销了 KMS 密钥，您也不会失去对卷的访问权限。有关更多信息，请参阅加密和快照复制 (p. 1378)。

在加密卷与未加密卷之间迁移数据

当您对加密卷和未加密卷都可以访问时，就可以在它们之间自由传输数据了。EC2 透明地执行加密和解密操作。

例如，使用 rsync 命令复制数据。在以下命令中，源数据位于 `/mnt/source` 中，目标卷挂载在 `/mnt/destination` 中。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

加密结果

下表描述了每种可能的设置组合的加密结果。

是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
否	否	新（空）卷	未加密	不适用
否	否	您拥有的未加密快照	未加密	
否	否	您拥有的加密快照	按相同密钥加密	
否	否	与您共享的未加密快照	未加密	
否	否	与您共享的加密快照	由默认客户托管密钥加密*	
是	否	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密**
是	否	您拥有的未加密快照	由默认客户托管密钥加密	
是	否	您拥有的加密快照	按相同密钥加密	
是	否	与您共享的未加密快照	由默认客户托管密钥加密	

是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
是	否	与您共享的加密快照	由默认客户托管密钥加密	
否	是	新（空）卷	由默认客户托管密钥加密	不适用
否	是	您拥有的未加密快照	由默认客户托管密钥加密	
否	是	您拥有的加密快照	按相同密钥加密	
否	是	与您共享的未加密快照	由默认客户托管密钥加密	
否	是	与您共享的加密快照	由默认客户托管密钥加密	
是	是	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密
是	是	您拥有的未加密快照	由默认客户托管密钥加密	
是	是	您拥有的加密快照	按相同密钥加密	
是	是	与您共享的未加密快照	由默认客户托管密钥加密	
是	是	与您共享的加密快照	由默认客户托管密钥加密	

* 这是用于Amazon账户和区域的 EBS 加密的默认客户托管密钥。默认情况下，这是 EBS 唯一的 Amazon 托管式密钥，您也可以指定自定义的托管密钥。有关更多信息，请参阅EBS 加密的默认 KMS 密钥 (p. 1506)。

**这是在启动时为卷指定的客户托管密钥。将为 Amazon 账户和区域使用此客户托管密钥，而不是使用默认的客户托管密钥。

使用 API 和 CLI 设置加密默认值

您可以使用以下 API 操作和 CLI 命令默认管理加密和默认 KMS 密钥。

API 操作	CLI 命令	描述
DisableEbsEncryptionByDefault	disable-ebs-encryption-by-default	默认禁用加密。
EnableEbsEncryptionByDefault	enable-ebs-encryption-by-default	默认启用加密。
GetEbsDefaultKmsKeyId	get-ebs-default-kms-key-id	描述默认 KMS 密钥。
GetEbsEncryptionByDefault	get-ebs-encryption-by-default	指示是否默认启用了加密。
ModifyEbsDefaultKmsKeyId	modify-ebs-default-kms-key-id	更改用于加密 EBS 卷的默认 KMS 密钥。

API 操作	CLI 命令	描述
ResetEbsDefaultKmsKeyId	reset-ebs-default-kms-key-id	将 Amazon 托管式密钥重置为用于加密 EBS 卷的默认 KMS 密钥。

Amazon EBS 快速快照还原

Amazon EBS 快速快照还原 (FSR) 使您能够从创建时已完全初始化的快照创建卷。这会消除首次访问块时对其执行 I/O 操作的延迟。使用快速快照还原创建的卷可以立即交付其所有预置性能。

要开始使用，请在特定可用区中为特定快照启用快速快照还原。每一对快照和可用区指代一个快速快照还原。当您从其中一个已启用该功能的可用区中的快照创建卷时，该卷将使用快速快照还原进行还原。

必须在每个快照的基础上明确启用快照还原。如果从已启用快速快照还原的快照还原卷创建新的快照，则新快照不会自动启用快速快照恢复功能。您必须明确启用新快照的该功能。

您可以使用快速快照还原的全部性能优势还原的卷数是由快照的卷创建积分决定的。有关更多信息，请参阅卷创建积分 (p. 1514)。

您可以为您拥有的快照以及与您共享的公有快照和私有快照启用快速快照还原。

目录

- 注意事项 (p. 1514)
- 卷创建积分 (p. 1514)
- 管理快速快照还原 (p. 1515)
- 监控快速快照还原 (p. 1518)
- 快速快照还原配额 (p. 1518)
- 定价和计费 (p. 1518)

注意事项

- 可以为大小为 16 TiB 或以下的快照启用快速快照还原。
- 预调配性能高达 64,000 IOPS 和 1,000 MiB/s 吞吐量的卷能够实现快速快照还原的全部性能。对于预调配性能超过 64,000 IOPS 或 1,000 MiB/s 吞吐量的卷，我们建议您初始化该卷 (p. 1554)以实现其全部性能。

卷创建积分

获得快速快照还原的全部性能优势的卷数是由快照的卷创建积分决定的。每个可用区的每个快照具有一积分存储桶。从快照中创建并启用了快速快照还原的每个卷使用积分存储桶中的一积分。您必须在存储桶中至少有一积分才能从快照创建初始化卷。如果您创建卷但存储桶中的积分少于一个，则创建卷时不能获得快速快照还原的优势。

当您为与您共享的快照启用快速快照还原时，您的账户中的共享快照会获得单独的信用存储桶。如果您从共享快照创建卷，则配额将从您的信用存储桶中消耗；这些配额不会从快照所有者的信用存储桶中消耗。

积分存储桶大小及其重填速率取决于快照的大小，而不是取决于从快照中创建的卷的大小。

当您为快照启用快速快照还原时，积分存储桶从零积分开始，并以设定的速率填满，直到达到最大积分容量。此外，在使用积分时，将随着时间的推移重填积分存储桶，直到其达到最大积分容量。

每积分存储桶的填充率计算如下：

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

积分存储桶的大小计算如下：

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

例如，如果为大小为 128 GiB 的快照启用快速快照还原，则填充率为每分钟 0.1333 积分。

```
MIN (10, (1024 ÷ 128))
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

积分存储桶的最大大小为 8 积分。

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
 = MAX (1, 8)
 = 8 credits
```

在此示例中，启用快速快照还原时，积分存储桶以零积分开始。8 分钟后，积分存储桶有足够的积分来创建一个初始化卷 (0.1333 credits × 8 minutes = 1.066 credits)。如果积分存储桶已满，您可以同时创建 8 个初始化卷（8 积分）。当存储桶低于其最大容量时，它将每分钟重填 0.1333 积分。

您可以使用 Cloudwatch 指标来监控积分余额存储桶的大小以及各个存储桶中可用的积分数量。有关更多信息，请参阅快速快照还原指标 (p. 1567)。

从启用了快速快照还原的存储桶创建卷之后，您可以使用 describe-volumes 来描述卷，并检查输出中的 fastRestored 字段以确定是否使用快速快照还原将该卷创建为已初始化卷。

管理快速快照还原

主题

- 启用或禁用快速快照还原 (p. 1515)
- 查看快照的快速快照还原状态 (p. 1516)
- 查看使用快速快照还原功能还原的卷 (p. 1517)

启用或禁用快速快照还原

默认情况下，对于快照禁用快速快照还原。您可以为您拥有的快照以及与您共享的快照启用或禁用快速快照还原。为快照启用或禁用快速快照还原时，所做的更改仅适用于您的账户。

> **Note**
>
> 当您为快照启用快速快照还原时，您的账户将按特定可用区中启用快速快照还原的每分钟计费。收费按比例计算，最少 1 小时。

当您删除您拥有的快照时，系统会在账户中自动禁用该快照的快速快照还原。如果您为与您共享的快照启用了快速快照还原，并且快照所有者删除或取消共享，则会自动为您账户中的共享快照禁用快速快照还原。

如果为共享的快照启用了快速快照还原，并且使用自定义 CMK 对其进行了加密，则在快照所有者撤消对自定义 CMK 的访问权限时，快速快照还原不会自动为快照禁用。您必须手动为该快照禁用快速快照还原。

使用以下方法之一为您拥有的快照或与您共享的快照启用或禁用快速快照还原。

Console

启用或禁用快速快照还原

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择快照，然后选择 Actions（操作）、Manage fast snapshot restore（管理快速快照还原）。
4. Fast snapshot restore settings（快速快照还原设置）部分列出了所有可用区、Local Zones 和 Wavelength 区域，您可以在其中为所选快照启用快速快照还原功能。Current status（当前状态）卷说明每个区域当前是启用还是禁用快速快照还原。

   要在当前禁用快照的区域中启用快速快照还原，选择该区域，然后选择 Enable（启用），并选择 Enable（启用）以确认。

   要在当前启用快照还原的区域中禁用快速快照还原，请选择该区域，然后选择 Disable（禁用）。
5. 进行必要的更改后，选择 Close（关闭）。

Amazon CLI

使用 Amazon CLI 管理快速快照还原

- enable-fast-snapshot-restores
- disable-fast-snapshot-restores
- describe-fast-snapshot-restores

Note

为快照启用快速快照还原后，快照将进入 `optimizing` 状态。处于 `optimizing` 状态的快照在使用快照恢复卷时可以提供一些性能优势。只有在进入 `enabled` 状态后，它们才开始发挥快速快照还原的全部性能优势。

查看快照的快速快照还原状态

快照的快速快照还原可能处于以下状态之一。

- `enabling` — 发出了启用快速快照还原的请求。
- `optimizing` — 正在启用快速快照还原。对于快照优化，每个 TiB 需要 60 分钟的时间。处于此状态的快照在还原卷时提供了一些性能优势。
- `enabled` — 启用了快速快照还原。处于此状态的快照在还原卷时提供了全面的性能优势。
- `disabling` — 发出了禁用快速快照还原的请求，或者启用快速快照还原的请求失败。
- `disabled` — 禁用了快速快照还原。您可以根据需要再次启用快速快照还原。

使用以下方法之一查看所拥有或共享的快照的快速快照还原状态。

Console

使用控制台查看快速快照还原的状态

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots。
3. 选择快照。
4. 在 Details（详细信息）选项卡上，查看 Fast Snapshot Restore（快速快照还原），该选项卡表示快速快照还原的状态。

Amazon CLI

使用 Amazon CLI 查看已启用快速快照还原的快照

使用 describe-fast-snapshot-restores 命令，描述已启用快速快照还原的快照。

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

下面是示例输出。

```
{
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        }
    ]
}
```

查看使用快速快照还原功能还原的卷

当您在可用区中，从已启用快速快照还原的快照创建卷时，将使用快速快照还原进行还原。

使用 describe-volumes 命令，查看从已启用快速快照还原的快照创建的卷。

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

下面是示例输出。

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
            "SnapshotId": "snap-0e946653493cb0447",
            "State": "available",
            "VolumeId": "vol-0d371921d4ca797b0",
```

```
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

监控快速快照还原

Amazon EBS 会在快照的快速快照还原状态发生变化时发出 Amazon CloudWatch Events。有关更多信息，请参阅EBS 快速快照还原事件 (p. 1576)。

快速快照还原配额

每个区域最多可启用 5 个快照以用于快速快照还原。配额适用于您拥有的快照以及与您共享的快照。如果为与您共享的快照启用快速快照还原，则它将计入快速快照还原配额。它不计入快照所有者的快速快照还原配额。

定价和计费

对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。

例如，假设您在 cn-northwest-1a 中为一个快照启用了一个月（30 天）的快速快照还原，则需要支付 ¥3905.28（1 个快照 x 1 个可用区 x 720 小时 x 每小时 ¥5.424）的费用。如果您按照同样的期限在 cn-northwest-1a、cn-northwest-1b 和 cn-northwest-1c 中为两个快照启用了快速快照还原，则需要支付 ¥23431.68（2 个快照 x 3 个可用区 x 720 小时 x 每小时 ¥5.424）的费用。

如果为与您共享的公有快照或私有快照启用快速快照还原，则会对您的账户进行计费；不会对快照所有者进行计费。当快照所有者删除与您共享的快照或取消其共享时，系统会为您账户中的快照禁用快速快照还原，并停止计费。

有关更多信息，请参阅 Amazon EBS 定价。

Linux 实例上的 Amazon EBS 和 NVMe

EBS 卷作为 NVMe 块存储设备在基于 Nitro 系统 (p. 246)构建的实例上公开。设备名称为 /dev/nvme0n1、/dev/nvme1n1，以此类推。您在块储存设备映射中指定的设备名称将使用 NVMe 设备名称 (/dev/nvme[0-26]n1) 进行重命名。块储存设备驱动程序可以使用不同于您在块储存设备映射中为卷指定的顺序来分配 NVMe 设备名称。

无论块储存设备接口如何，Amazon EBS 产品详细信息中所述的 EBS 性能保证都有效。

有关 Windows 实例上的 EBS 卷和 NVME 的信息，请参阅用户指南（适用于 Windows 实例）。

目录

- 安装或升级 NVMe 驱动程序 (p. 1518)
- 识别 EBS 设备 (p. 1520)
- 使用 NVMe EBS 卷 (p. 1521)
- I/O 操作超时 (p. 1522)
- Abort command (p. 1522)

安装或升级 NVMe 驱动程序

要访问 NVMe 卷，必须安装 NVMe 驱动程序。实例可以支持 NVMe EBS 卷和 NVMe 实例存储卷（要么两种类型的 NVMe 卷均支持，要么均不支持）。有关更多信息，请参阅 联网和存储功能摘要 (p. 247)。

以下 AMI 包含所需的 NVMe 驱动程序：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

  Note

  Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

有关 Windows 实例上的 NVMe 驱动程序的更多信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 Windows 实例上的 Amazon EBS 和 NVMe。

确认实例具有 NVMe 驱动程序

您可以使用以下命令确认您的实例是否具有 NVMe 驱动程序。

- Amazon Linux、RHEL、CentOS 和 SUSE Linux Enterprise Server

```
$ modinfo nvme
```

  如果实例具有 NVMe 驱动程序，则该命令将返回有关该驱动程序的信息。
- Amazon Linux 2 和 Ubuntu

```
$ ls /sys/module/ | grep nvme
```

  如果实例具有 NVMe 驱动程序，该命令将返回已安装的驱动程序。

更新 NVMe 驱动程序

如果您的实例具有 NVMe 驱动程序，您可以使用以下过程将驱动程序更新到最新版本。

1. 连接到您的 实例。
2. 更新程序包缓存以获取必需程序包更新，如下所示。
   - 对于 Amazon Linux 2、Amazon Linux、CentOS 和 Red Hat Enterprise Linux：

     ```
     [ec2-user ~]$ sudo yum update -y
     ```
   - 对于 Ubuntu 和 Debian：

     ```
     [ec2-user ~]$ sudo apt-get update -y
     ```
3. Ubuntu 16.04 及更高版本包含 `linux-aws` 程序包，该程序包包含基于 Nitro 的实例所需的 NVMe 和 ENA 驱动程序。升级 `linux-aws` 程序包以接收最新版本，如下所示：

   ```
   [ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
   ```

   对于 Ubuntu 14.04，您可以安装最新的 `linux-aws` 程序包，如下所示：

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. 重启实例以加载最新内核版本。

```
sudo reboot
```

5. 重启之后重新连接到实例。

识别 EBS 设备

EBS 使用单一根 I/O 虚拟化 (SR-IOV) 在使用 NVMe 规范的基于 Nitro 的实例上提供卷附加。这些设备依赖于操作系统上的标准 NVMe 驱动程序。这些驱动程序通常在实例启动期间通过扫描 PCI 总线来发现附加的设备，然后根据设备响应的顺序创建设备节点，而不是按照在块储存设备映射中指定设备的顺序。在 Linux 中，NVMe 设备名称遵循 /dev/nvme<x>n<y> 模式，其中 <x> 是枚举顺序，对于 EBS，<y> 为 1。有时候，在接下来的实例启动时，设备会以不同顺序响应发现过程，这会导致设备名称更改。此外，块储存设备驱动程序分配的设备名称可以不同于块储存设备映射中指定的名称。

建议您在实例中为 EBS 卷使用静态标识符，例如以下之一：

- 对基于 Nitro 的实例，您在附加 EBS 卷或者在 `AttachVolume` 或 `RunInstances` API 调用期间通过 Amazon EC2 控制台指定的块储存设备映射，将在 NVMe 控制器标识的供应商特定数据字段中捕获。对版本高于 2017.09.01 的 Amazon Linux AMI，我们提供了 udev 规则，该规则读取此数据并创建指向块储存设备映射的符号链接。
- EBS 卷 ID 和挂载点在实例状态更改之间保持稳定。NVMe 设备名称可以根据设备在实例启动期间响应的顺序进行更改。我们建议使用 EBS 卷 ID 和挂载点以实现一致的设备标识。
- NVMe EBS 卷在设备标识中将 EBS 卷 ID 设置为序列号。使用 `lsblk -o +SERIAL` 命令列出序列号。
- NVMe 设备名称格式可能会有所不同，具体取决于 EBS 卷是在实例启动期间还是之后附上。实例启动后附上卷的 NVMe 设备名称包括 /dev/ 前缀，而实例启动期间附上卷的 NVMe 设备名称不包括 /dev/ 前缀。如果您使用的是 Amazon Linux 或 FreeBSD AMI，请使用 `sudo ebsnvme-id /dev/nvme0n1 -u` 命令获得一致的 NVMe 设备名称。对于其他发布版本，请使用 `sudo ebsnvme-id /dev/nvme0n1 -u` 命令确定 NVMe 设备名称。
- 格式化设备时，将生成在文件系统的使用寿命内保持的 UUID。此时可指定设备标签。有关更多信息，请参阅 使 Amazon EBS 卷可在 Linux 上使用 (p. 1348) 和 从错误的卷启动 (p. 1726)。

Amazon Linux AMI

利用 Amazon Linux AMI 2017.09.01 或更高版本（包括 Amazon Linux 2），您可以按下面所示运行 ebsnvme-id 命令以将 NVMe 设备名称映射到卷 ID 和设备名称：

以下示例显示实例启动期间附上的卷的命令和输出。请注意，NVMe 设备名称不包括 /dev/ 前缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

以下示例显示实例启动后附上的卷的命令和输出。请注意，NVMe 设备名称包括 /dev/ 前缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux 还将创建从块储存设备映射中的设备名称（例如，/dev/sdf）到 NVMe 设备名称的符号链接。

FreeBSD AMI

从 FreeBSD 12.2-RELEASE 开始，您可以运行如上所示的 ebsnvme-id 命令。传递 NVMe 设备的名称（例如，nvme0）或磁盘设备的名称（例如，nvd0 或 nda0）。FreeBSD 还创建到磁盘设备的符号链接（例如，/dev/aws/disk/ebs/*volume_id*）。

其他 Linux AMI

利用内核版本 4.2 或更高版本，您可以按下面所示运行 nvme id-ctrl 命令以将 NVMe 设备映射到卷 ID。首先，使用您的 Linux 发行版的程序包管理工具安装 NVMe 命令行程序包 nvme-cli。有关其他发行版的下载和安装说明，请参阅特定于您的发行版的文档。

以下示例将获取实例启动期间附上的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称不包括 /dev/ 前缀。设备名称通过特定于 NVMe 控制器供应商的扩展（控制器标识的字节 384:4095）提供：

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

以下示例将获取实例启动后附上的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称包括 /dev/ 前缀。

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

lsblk 命令可列出可用设备及其挂载点（如果适用）。这有助于确定要使用的正确设备名称。在本示例中，/dev/nvme0n1p1 作为根设备挂载，/dev/nvme1n1 会附加但不会挂载。

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:3   0  100G  0 disk
nvme0n1       259:0   0    8G  0 disk
  nvme0n1p1   259:1   0    8G  0 part /
  nvme0n1p128 259:2   0    1M  0 part
```

使用 NVMe EBS 卷

要格式化并挂载 NVMe EBS 卷，请参阅 使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)。

如果您使用的是 Linux 内核 4.2 或更高版本，您对 NVMe EBS 卷的卷大小进行的所有更改将自动在实例中反映。对于旧版 Linux 内核，您可能需要分离然后附加 EBS 卷或者重启实例才能反映大小更改。对于 Linux 内核 3.19 或更高版本，您可以按下面所示使用 hdparm 命令强制重新扫描 NVMe 设备：

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

当您分离 NVMe EBS 卷时，实例在分离卷之前将没有机会刷新文件系统缓存或元数据。在分离 NVMe EBS 卷之前，您应该首先同步并卸载它。如果卷无法分离，您可以按照force-detach中所述尝试执行 从 Linux 实例分离 Amazon EBS 卷 (p. 1364) 命令。

I/O 操作超时

附加到基于 Nitro 系统的实例的 EBS 卷使用操作系统提供的默认 NVMe 驱动程序。大多数操作系统为提交到 NVMe 设备的 I/O 操作指定一个超时。默认超时为 30 秒，可以使用 `nvme_core.io_timeout` 引导参数更改该超时。对于 4.6 版之前的大多数 Linux 内核版本，此参数为 `nvme.io_timeout`。

如果 I/O 延迟超过了此超时参数的值，则 Linux NVMe 驱动程序会使 I/O 失败，并将错误返回文件系统或应用程序。根据 I/O 操作，您的文件系统或应用程序可以重试错误。在某些情况下，您的文件系统可能会通过只读方式重新挂载。

为了获得与附加到 Xen 实例的 EBS 卷类似的体验，我们建议将 `nvme_core.io_timeout` 设置为可能的最大值。对于当前内核，最大值为 4294967295，而对于较早的内核，最大值为 255。根据 Linux 版本的不同，超时时间可能已设置为支持的最大值。例如，对于 Amazon Linux AMI 2017.09.01 以及更高的版本，超时时间默认设置为 4294967295。

您可以通过将高于建议最大值的值写入 `/sys/module/nvme_core/parameters/io_timeout` 并在尝试保存文件时检查 Numerical result out of range (数值结果超出范围) 错误，以此来验证您的 Linux 发行版的最大值。

`Abort` command

`Abort` 命令是一个 NVMe 管理员命令，用于中止之前提交给控制器的特定命令。此命令通常由设备驱动程序向超过输入/输出操作超时阈值的存储设备发出。默认支持 `Abort` 命令的 Amazon EC2 实例类型，将中止先前提交给已向其发出 `Abort` 命令的所附加 Amazon EBS 设备的控制器的特定命令。

默认情况下，以下实例类型支持所有附加的 Amazon EBS 卷的 `Abort` 命令：`R5b`、`R6i`、`M6i`、`M6a`、`C6gn`、`C6i`、`X2gd`、`X2iezn`、`Im4gn`、`Is4gen`。

向附加的 Amazon EBS 卷发出 `Abort` 命令时，其他实例类型不采取任何操作。

NVMe 设备为 `1.4` 版本或更高版本的 Amazon EBS 设备支持 `Abort` 命令。

有关更多信息，请参阅 NVM Express 基本规范的 5.1 Abort 命令部分。

Amazon EBS 优化的实例

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

EBS 优化的实例将专用带宽提供给 Amazon EBS。当附加到 EBS 优化实例时，通用型 SSD（`gp2` 和 `gp3`）卷可在给定年度 99% 的时间内提供至少 90% 的预置 IOPS 性能，而预置 IOPS SSD（`io1` 和 `io2`）卷可在给定年度 99.9% 的时间内提供至少 90% 的预置 IOPS 性能。吞吐量优化型 HDD（`st1`）和 Cold HDD（`sc1`）在给定年度 99% 的时间内提供至少 90% 的预期吞吐量性能。不合规时间近似均匀分配，目标是达到 99% 的每小时预计总吞吐量。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。

目录

- 支持的实例类型 (p. 1522)
- 获得最佳性能 (p. 1547)
- 查看支持 EBS 优化的实例类型 (p. 1548)
- 在启动时启用 EBS 优化 (p. 1549)
- 为现有实例启用 EBS 优化 (p. 1549)

支持的实例类型

下面的表显示了支持 EBS 优化的实例类型。它们包括针对 Amazon EBS 的专用带宽、在具有流式处理读取工作负载和 128 KiB I/O 大小的连接上可实现的典型最大聚合吞吐量，以及实例可以支持的最大 IOPS（如果使用的是 16 KiB I/O 大小）。

请选择提供的专用 Amazon EBS 吞吐量大于应用程序所需的 EBS 优化实例；否则，Amazon EBS 与 Amazon EC2 的连接将成为性能障碍。

主题

- 默认为 EBS 优化 (p. 1523)
- 支持的 EBS 优化 (p. 1546)

默认为 EBS 优化

下表列出了支持 EBS 优化且默认情况下启用 EBS 优化的实例类型。无需启用 EBS 优化，禁用 EBS 优化也没有效果。

> **Note**
>
> 您还可以使用 Amazon CLI 以编程方式查看此信息。有关更多信息，请参阅查看支持 EBS 优化的实例类型 (p. 1548)。

主题

- 通用型 (p. 1523)
- 计算优化 (p. 1530)
- 内存优化 (p. 1534)
- 存储优化 (p. 1542)
- 加速计算 (p. 1544)

通用型

> **Important**
>
> 标有星号（*）的实例可以至少每 24 小时支持一次 30 分钟的最大性能，之后会恢复到基线性能。未标星号的实例保持最高性能的时间不确定。如果工作负载需要在超过 30 分钟的时长内保持最大性能，请选择以下任一实例。

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
a1.medium *	300	3500	37.50	437.50	2500	20000
a1.large *	525	3500	65.62	437.50	4000	20000
a1.xlarge *	800	3500	100.00	437.50	6000	20000
a1.2xlarge *	1750	3500	218.75	437.50	10000	20000
a1.4xlarge	3500		437.5		20000	
a1.metal	3500		437.5		20000	
m4.large	450		56.25		3600	
m4.xlarge	750		93.75		6000	
m4.2xlarge	1000		125.0		8000	
m4.4xlarge	2000		250.0		16000	
m4.10xlarge	4000		500.0		32000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m4.16xlarge	10000		1250.0		65000	
m5.large *	650	4750	81.25	593.75	3600	18750
m5.xlarge *	1150	4750	143.75	593.75	6000	18750
m5.2xlarge *	2300	4750	287.50	593.75	12000	18750
m5.4xlarge	4750		593.75		18750	
m5.8xlarge	6800		850.0		30000	
m5.12xlarge	9500		1187.5		40000	
m5.16xlarge	13600		1700.0		60000	
m5.24xlarge	19000		2375.0		80000	
m5.metal	19000		2375.0		80000	
m5a.large *	650	2880	81.25	360.00	3600	16000
m5a.xlarge *	1085	2880	135.62	360.00	6000	16000
m5a.2xlarge *	1580	2880	197.50	360.00	8333	16000
m5a.4xlarge	2880		360.0		16000	
m5a.8xlarge	4750		593.75		20000	
m5a.12xlarge	6780		847.5		30000	
m5a.16xlarge	9500		1187.5		40000	
m5a.24xlarge	13750		1718.75		60000	
m5ad.large *	650	2880	81.25	360.00	3600	16000
m5ad.xlarge *	1085	2880	135.62	360.00	6000	16000
m5ad.2xlarge *	1580	2880	197.50	360.00	8333	16000
m5ad.4xlarge	2880		360.0		16000	
m5ad.8xlarge	4750		593.75		20000	
m5ad.12xlarge	6780		847.5		30000	
m5ad.16xlarge	9500		1187.5		40000	
m5ad.24xlarge	13750		1718.75		60000	
m5d.large *	650	4750	81.25	593.75	3600	18750
m5d.xlarge *	1150	4750	143.75	593.75	6000	18750

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m5d.2xlarge *	2300	4750	287.50	593.75	12000	18750
m5d.4xlarge	4750		593.75		18750	
m5d.8xlarge	6800		850.0		30000	
m5d.12xlarge	9500		1187.5		40000	
m5d.16xlarge	13600		1700.0		60000	
m5d.24xlarge	19000		2375.0		80000	
m5d.metal	19000		2375.0		80000	
m5dn.large *	650	4750	81.25	593.75	3600	18750
m5dn.xlarge *	1150	4750	143.75	593.75	6000	18750
m5dn.2xlarge *	2300	4750	287.50	593.75	12000	18750
m5dn.4xlarge	4750		593.75		18750	
m5dn.8xlarge	6800		850.0		30000	
m5dn.12xlarge	9500		1187.5		40000	
m5dn.16xlarge	13600		1700.0		60000	
m5dn.24xlarge	19000		2375.0		80000	
m5dn.metal	19000		2375.0		80000	
m5n.large *	650	4750	81.25	593.75	3600	18750
m5n.xlarge *	1150	4750	143.75	593.75	6000	18750
m5n.2xlarge *	2300	4750	287.50	593.75	12000	18750
m5n.4xlarge	4750		593.75		18750	
m5n.8xlarge	6800		850.0		30000	
m5n.12xlarge	9500		1187.5		40000	
m5n.16xlarge	13600		1700.0		60000	
m5n.24xlarge	19000		2375.0		80000	
m5n.metal	19000		2375.0		80000	
m5zn.large *	800	3170	100.00	396.25	3333	13333

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m5zn.xlarge *	1564	3170	195.50	396.25	6667	13333
m5zn.2xlarge	3170		396.25		13333	
m5zn.3xlarge	4750		593.75		20000	
m5zn.6xlarge	9500		1187.5		40000	
m5zn.12xlarge	19000		2375.0		80000	
m5zn.metal	19000		2375.0		80000	
m6a.large *	531	6666	66.38	833.33	3600	26667
m6a.xlarge *	1061	6666	132.62	833.33	6000	26667
m6a.2xlarge *	2122	6666	265.25	833.33	8333	26667
m6a.4xlarge *	4245	6666	530.62	833.33	16000	26667
m6a.8xlarge	6666		833.333333		26667	
m6a.12xlarge	10000		1250.0		40000	
m6a.16xlarge	13300		1662.5		53333	
m6a.24xlarge	20000		2500.0		80000	
m6a.32xlarge	26666		3333.333333		100000	
m6a.48xlarge	40000		5000.0		160000	
m6a.metal	40000		5000.0		160000	
m6g.medium *	315	4750	39.38	593.75	2500	20000
m6g.large *	630	4750	78.75	593.75	3600	20000
m6g.xlarge *	1188	4750	148.50	593.75	6000	20000
m6g.2xlarge *	2375	4750	296.88	593.75	12000	20000
m6g.4xlarge	4750		593.75		20000	
m6g.8xlarge	9500		1187.5		40000	
m6g.12xlarge	14250		1781.25		50000	
m6g.16xlarge	19000		2375.0		80000	
m6g.metal	19000		2375.0		80000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m6gd.medium*	315	4750	39.38	593.75	2500	20000
m6gd.large*	630	4750	78.75	593.75	3600	20000
m6gd.xlarge*	1188	4750	148.50	593.75	6000	20000
m6gd.2xlarge*	2375	4750	296.88	593.75	12000	20000
m6gd.4xlarge	4750		593.75		20000	
m6gd.8xlarge	9500		1187.5		40000	
m6gd.12xlarge	14250		1781.25		50000	
m6gd.16xlarge	19000		2375.0		80000	
m6gd.metal	19000		2375.0		80000	
m6i.large *	650	10000	81.25	1250.00	3600	40000
m6i.xlarge *	1250	10000	156.25	1250.00	6000	40000
m6i.2xlarge *	2500	10000	312.50	1250.00	12000	40000
m6i.4xlarge *	5000	10000	625.00	1250.00	20000	40000
m6i.8xlarge	10000		1250.0		40000	
m6i.12xlarge	15000		1875.0		60000	
m6i.16xlarge	20000		2500.0		80000	
m6i.24xlarge	30000		3750.0		120000	
m6i.32xlarge	40000		5000.0		160000	
m6i.metal	40000		5000.0		160000	
m6id.large *	650	10000	81.25	1250.00	3600	40000
m6id.xlarge *	1250	10000	156.25	1250.00	6000	40000
m6id.2xlarge*	2500	10000	312.50	1250.00	12000	40000
m6id.4xlarge*	5000	10000	625.00	1250.00	20000	40000
m6id.8xlarge	10000		1250.0		40000	
m6id.12xlarge	15000		1875.0		60000	
m6id.16xlarge	20000		2500.0		80000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m6id.24xlarge	30000		3750.0		120000	
m6id.32xlarge	40000		5000.0		160000	
m6id.metal	40000		5000.0		160000	
m6idn.large *	1250	20000	156.25	2500.00	5468	87500
m6idn.xlarge *	2500	20000	312.50	2500.00	10937	87500
m6idn.2xlarge *	5000	20000	625.00	2500.00	21875	87500
m6idn.4xlarge *	10000	20000	1250.00	2500.00	43750	87500
m6idn.8xlarge	20000		2500.0		87500	
m6idn.12xlarge	30000		3750.0		131250	
m6idn.16xlarge	40000		5000.0		175000	
m6idn.24xlarge	60000		7500.0		262500	
m6idn.32xlarge	80000		10000.0		350000	
m6idn.metal	80000		10000.0		350000	
m6in.large *	1250	20000	156.25	2500.00	5468	87500
m6in.xlarge *	2500	20000	312.50	2500.00	10937	87500
m6in.2xlarge *	5000	20000	625.00	2500.00	21875	87500
m6in.4xlarge *	10000	20000	1250.00	2500.00	43750	87500
m6in.8xlarge	20000		2500.0		87500	
m6in.12xlarge	30000		3750.0		131250	
m6in.16xlarge	40000		5000.0		175000	
m6in.24xlarge	60000		7500.0		262500	
m6in.32xlarge	80000		10000.0		350000	
m6in.metal	80000		10000.0		350000	
m7g.medium *	315	10000	39.38	1250.00	2500	40000
m7g.large *	630	10000	78.75	1250.00	3600	40000

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
m7g.xlarge *	1250	10000	156.25	1250.00	6000	40000
m7g.2xlarge *	2500	10000	312.50	1250.00	12000	40000
m7g.4xlarge *	5000	10000	625.00	1250.00	20000	40000
m7g.8xlarge	10000		1250.0		40000	
m7g.12xlarge	15000		1875.0		60000	
m7g.16xlarge	20000		2500.0		80000	
m7g.metal	20000		2500.0		80000	
mac1.metal	14000		1750.0		80000	
mac2.metal	10000		1250.0		55000	
t3.nano *	43	2085	5.38	260.62	250	11800
t3.micro *	87	2085	10.88	260.62	500	11800
t3.small *	174	2085	21.75	260.62	1000	11800
t3.medium *	347	2085	43.38	260.62	2000	11800
t3.large *	695	2780	86.88	347.50	4000	15700
t3.xlarge *	695	2780	86.88	347.50	4000	15700
t3.2xlarge *	695	2780	86.88	347.50	4000	15700
t3a.nano *	45	2085	5.62	260.62	250	11800
t3a.micro *	90	2085	11.25	260.62	500	11800
t3a.small *	175	2085	21.88	260.62	1000	11800
t3a.medium *	350	2085	43.75	260.62	2000	11800
t3a.large *	695	2780	86.88	347.50	4000	15700
t3a.xlarge *	695	2780	86.88	347.50	4000	15700
t3a.2xlarge *	695	2780	86.88	347.50	4000	15700
t4g.nano *	43	2085	5.38	260.62	250	11800
t4g.micro *	87	2085	10.88	260.62	500	11800
t4g.small *	174	2085	21.75	260.62	1000	11800
t4g.medium *	347	2085	43.38	260.62	2000	11800

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
t4g.large *	695	2780	86.88	347.50	4000	15700
t4g.xlarge *	695	2780	86.88	347.50	4000	15700
t4g.2xlarge *	695	2780	86.88	347.50	4000	15700

计算优化

Important

标有星号（*）的实例可以至少每 24 小时支持一次 30 分钟的最大性能，之后会恢复到基线性能。未标星号的实例保持最高性能的时间不确定。如果工作负载需要在超过 30 分钟的时长内保持最大性能，请选择以下任一实例。

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
c4.large	500		62.5		4000	
c4.xlarge	750		93.75		6000	
c4.2xlarge	1000		125.0		8000	
c4.4xlarge	2000		250.0		16000	
c4.8xlarge	4000		500.0		32000	
c5.large *	650	4750	81.25	593.75	4000	20000
c5.xlarge *	1150	4750	143.75	593.75	6000	20000
c5.2xlarge *	2300	4750	287.50	593.75	10000	20000
c5.4xlarge	4750		593.75		20000	
c5.9xlarge	9500		1187.5		40000	
c5.12xlarge	9500		1187.5		40000	
c5.18xlarge	19000		2375.0		80000	
c5.24xlarge	19000		2375.0		80000	
c5.metal	19000		2375.0		80000	
c5a.large *	200	3170	25.00	396.25	800	13300
c5a.xlarge *	400	3170	50.00	396.25	1600	13300
c5a.2xlarge *	800	3170	100.00	396.25	3200	13300
c5a.4xlarge *	1580	3170	197.50	396.25	6600	13300
c5a.8xlarge	3170		396.25		13300	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
c5a.12xlarge	4750		593.75		20000	
c5a.16xlarge	6300		787.5		26700	
c5a.24xlarge	9500		1187.5		40000	
c5ad.large *	200	3170	25.00	396.25	800	13300
c5ad.xlarge *	400	3170	50.00	396.25	1600	13300
c5ad.2xlarge *	800	3170	100.00	396.25	3200	13300
c5ad.4xlarge *	1580	3170	197.50	396.25	6600	13300
c5ad.8xlarge	3170		396.25		13300	
c5ad.12xlarge	4750		593.75		20000	
c5ad.16xlarge	6300		787.5		26700	
c5ad.24xlarge	9500		1187.5		40000	
c5d.large *	650	4750	81.25	593.75	4000	20000
c5d.xlarge *	1150	4750	143.75	593.75	6000	20000
c5d.2xlarge *	2300	4750	287.50	593.75	10000	20000
c5d.4xlarge	4750		593.75		20000	
c5d.9xlarge	9500		1187.5		40000	
c5d.12xlarge	9500		1187.5		40000	
c5d.18xlarge	19000		2375.0		80000	
c5d.24xlarge	19000		2375.0		80000	
c5d.metal	19000		2375.0		80000	
c5n.large *	650	4750	81.25	593.75	4000	20000
c5n.xlarge *	1150	4750	143.75	593.75	6000	20000
c5n.2xlarge *	2300	4750	287.50	593.75	10000	20000
c5n.4xlarge	4750		593.75		20000	
c5n.9xlarge	9500		1187.5		40000	
c5n.18xlarge	19000		2375.0		80000	
c5n.metal	19000		2375.0		80000	
c6a.large *	531	6666	66.38	833.33	3600	26667

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
c6a.xlarge *	1061	6666	132.62	833.33	6000	26667
c6a.2xlarge *	2122	6666	265.25	833.33	8333	26667
c6a.4xlarge *	4245	6666	530.62	833.33	16000	26667
c6a.8xlarge	6666		833.333333		26667	
c6a.12xlarge	10000		1250.0		40000	
c6a.16xlarge	13300		1662.5		53333	
c6a.24xlarge	20000		2500.0		80000	
c6a.32xlarge	26666		3333.333333		100000	
c6a.48xlarge	40000		5000.0		160000	
c6a.metal	40000		5000.0		160000	
c6g.medium *	315	4750	39.38	593.75	2500	20000
c6g.large *	630	4750	78.75	593.75	3600	20000
c6g.xlarge *	1188	4750	148.50	593.75	6000	20000
c6g.2xlarge *	2375	4750	296.88	593.75	12000	20000
c6g.4xlarge	4750		593.75		20000	
c6g.8xlarge	9500		1187.5		40000	
c6g.12xlarge	14250		1781.25		50000	
c6g.16xlarge	19000		2375.0		80000	
c6g.metal	19000		2375.0		80000	
c6gd.medium *	315	4750	39.38	593.75	2500	20000
c6gd.large *	630	4750	78.75	593.75	3600	20000
c6gd.xlarge *	1188	4750	148.50	593.75	6000	20000
c6gd.2xlarge *	2375	4750	296.88	593.75	12000	20000
c6gd.4xlarge	4750		593.75		20000	
c6gd.8xlarge	9500		1187.5		40000	
c6gd.12xlarge	14250		1781.25		50000	
c6gd.16xlarge	19000		2375.0		80000	
c6gd.metal	19000		2375.0		80000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
c6gn.medium *	760	9500	95.00	1187.50	2500	40000
c6gn.large *	1235	9500	154.38	1187.50	5000	40000
c6gn.xlarge *	2375	9500	296.88	1187.50	10000	40000
c6gn.2xlarge *	4750	9500	593.75	1187.50	20000	40000
c6gn.4xlarge	9500		1187.5		40000	
c6gn.8xlarge	19000		2375.0		80000	
c6gn.12xlarge	28500		3562.5		120000	
c6gn.16xlarge	38000		4750.0		160000	
c6i.large *	650	10000	81.25	1250.00	3600	40000
c6i.xlarge *	1250	10000	156.25	1250.00	6000	40000
c6i.2xlarge *	2500	10000	312.50	1250.00	12000	40000
c6i.4xlarge *	5000	10000	625.00	1250.00	20000	40000
c6i.8xlarge	10000		1250.0		40000	
c6i.12xlarge	15000		1875.0		60000	
c6i.16xlarge	20000		2500.0		80000	
c6i.24xlarge	30000		3750.0		120000	
c6i.32xlarge	40000		5000.0		160000	
c6i.metal	40000		5000.0		160000	
c6id.large *	650	10000	81.25	1250.00	3600	40000
c6id.xlarge *	1250	10000	156.25	1250.00	6000	40000
c6id.2xlarge *	2500	10000	312.50	1250.00	12000	40000
c6id.4xlarge *	5000	10000	625.00	1250.00	20000	40000
c6id.8xlarge	10000		1250.0		40000	
c6id.12xlarge	15000		1875.0		60000	
c6id.16xlarge	20000		2500.0		80000	
c6id.24xlarge	30000		3750.0		120000	
c6id.32xlarge	40000		5000.0		160000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
c6id.metal	40000		5000.0		160000	
c6in.large *	1250	20000	156.25	2500.00	5468	87500
c6in.xlarge *	2500	20000	312.50	2500.00	10937	87500
c6in.2xlarge *	5000	20000	625.00	2500.00	21875	87500
c6in.4xlarge *	10000	20000	1250.00	2500.00	43750	87500
c6in.8xlarge	20000		2500.0		87500	
c6in.12xlarge	30000		3750.0		131250	
c6in.16xlarge	40000		5000.0		175000	
c6in.24xlarge	60000		7500.0		262500	
c6in.32xlarge	80000		10000.0		350000	
c6in.metal	80000		10000.0		350000	
c7g.medium *	315	10000	39.38	1250.00	2500	40000
c7g.large *	630	10000	78.75	1250.00	3600	40000
c7g.xlarge *	1250	10000	156.25	1250.00	6000	40000
c7g.2xlarge *	2500	10000	312.50	1250.00	12000	40000
c7g.4xlarge *	5000	10000	625.00	1250.00	20000	40000
c7g.8xlarge	10000		1250.0		40000	
c7g.12xlarge	15000		1875.0		60000	
c7g.16xlarge	20000		2500.0		80000	
c7g.metal	20000		2500.0		80000	
hpc6a.48xlarge *	87	2085	10.88	260.62	500	11000

内存优化

Important

标有星号（*）的实例可以至少每 24 小时支持一次 30 分钟的最大性能，之后会恢复到基线性能。未标星号的实例保持最高性能的时间不确定。如果工作负载需要在超过 30 分钟的时长内保持最大性能，请选择以下任一实例。

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
hpc6id.32xlarge *	87	2085	10.88	260.62	500	11000
r4.large	425		53.125		3000	
r4.xlarge	850		106.25		6000	
r4.2xlarge	1700		212.5		12000	
r4.4xlarge	3500		437.5		18750	
r4.8xlarge	7000		875.0		37500	
r4.16xlarge	14000		1750.0		75000	
r5.large *	650	4750	81.25	593.75	3600	18750
r5.xlarge *	1150	4750	143.75	593.75	6000	18750
r5.2xlarge *	2300	4750	287.50	593.75	12000	18750
r5.4xlarge	4750		593.75		18750	
r5.8xlarge	6800		850.0		30000	
r5.12xlarge	9500		1187.5		40000	
r5.16xlarge	13600		1700.0		60000	
r5.24xlarge	19000		2375.0		80000	
r5.metal	19000		2375.0		80000	
r5a.large *	650	2880	81.25	360.00	3600	16000
r5a.xlarge *	1085	2880	135.62	360.00	6000	16000
r5a.2xlarge *	1580	2880	197.50	360.00	8333	16000
r5a.4xlarge	2880		360.0		16000	
r5a.8xlarge	4750		593.75		20000	
r5a.12xlarge	6780		847.5		30000	
r5a.16xlarge	9500		1187.5		40000	
r5a.24xlarge	13570		1696.25		60000	
r5ad.large *	650	2880	81.25	360.00	3600	16000
r5ad.xlarge *	1085	2880	135.62	360.00	6000	16000
r5ad.2xlarge *	1580	2880	197.50	360.00	8333	16000
r5ad.4xlarge	2880		360.0		16000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
r5ad.8xlarge	4750		593.75		20000	
r5ad.12xlarge	6780		847.5		30000	
r5ad.16xlarge	9500		1187.5		40000	
r5ad.24xlarge	13570		1696.25		60000	
r5b.large *	1250	10000	156.25	1250.00	5417	43333
r5b.xlarge *	2500	10000	312.50	1250.00	10833	43333
r5b.2xlarge *	5000	10000	625.00	1250.00	21667	43333
r5b.4xlarge	10000		1250.0		43333	
r5b.8xlarge	20000		2500.0		86667	
r5b.12xlarge	30000		3750.0		130000	
r5b.16xlarge	40000		5000.0		173333	
r5b.24xlarge	60000		7500.0		260000	
r5b.metal	60000		7500.0		260000	
r5d.large *	650	4750	81.25	593.75	3600	18750
r5d.xlarge *	1150	4750	143.75	593.75	6000	18750
r5d.2xlarge *	2300	4750	287.50	593.75	12000	18750
r5d.4xlarge	4750		593.75		18750	
r5d.8xlarge	6800		850.0		30000	
r5d.12xlarge	9500		1187.5		40000	
r5d.16xlarge	13600		1700.0		60000	
r5d.24xlarge	19000		2375.0		80000	
r5d.metal	19000		2375.0		80000	
r5dn.large *	650	4750	81.25	593.75	3600	18750
r5dn.xlarge *	1150	4750	143.75	593.75	6000	18750
r5dn.2xlarge *	2300	4750	287.50	593.75	12000	18750
r5dn.4xlarge	4750		593.75		18750	
r5dn.8xlarge	6800		850.0		30000	
r5dn.12xlarge	9500		1187.5		40000	
r5dn.16xlarge	13600		1700.0		60000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
r5dn.24xlarge	19000		2375.0		80000	
r5dn.metal	19000		2375.0		80000	
r5n.large *	650	4750	81.25	593.75	3600	18750
r5n.xlarge *	1150	4750	143.75	593.75	6000	18750
r5n.2xlarge *	2300	4750	287.50	593.75	12000	18750
r5n.4xlarge	4750		593.75		18750	
r5n.8xlarge	6800		850.0		30000	
r5n.12xlarge	9500		1187.5		40000	
r5n.16xlarge	13600		1700.0		60000	
r5n.24xlarge	19000		2375.0		80000	
r5n.metal	19000		2375.0		80000	
r6a.large *	531	6666	66.38	833.33	3600	26667
r6a.xlarge *	1061	6666	132.62	833.33	6000	26667
r6a.2xlarge *	2122	6666	265.25	833.33	8333	26667
r6a.4xlarge *	4245	6666	530.62	833.33	16000	26667
r6a.8xlarge	6666		833.333333		26667	
r6a.12xlarge	10000		1250.0		40000	
r6a.16xlarge	13300		1662.5		53333	
r6a.24xlarge	20000		2500.0		80000	
r6a.32xlarge	26666		3333.333333		100000	
r6a.48xlarge	40000		5000.0		160000	
r6a.metal	40000		5000.0		160000	
r6g.medium *	315	4750	39.38	593.75	2500	20000
r6g.large *	630	4750	78.75	593.75	3600	20000
r6g.xlarge *	1188	4750	148.50	593.75	6000	20000
r6g.2xlarge *	2375	4750	296.88	593.75	12000	20000
r6g.4xlarge	4750		593.75		20000	
r6g.8xlarge	9500		1187.5		40000	
r6g.12xlarge	14250		1781.25		50000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
r6g.16xlarge	19000		2375.0		80000	
r6g.metal	19000		2375.0		80000	
r6gd.medium *	315	4750	39.38	593.75	2500	20000
r6gd.large *	630	4750	78.75	593.75	3600	20000
r6gd.xlarge *	1188	4750	148.50	593.75	6000	20000
r6gd.2xlarge *	2375	4750	296.88	593.75	12000	20000
r6gd.4xlarge	4750		593.75		20000	
r6gd.8xlarge	9500		1187.5		40000	
r6gd.12xlarge	14250		1781.25		50000	
r6gd.16xlarge	19000		2375.0		80000	
r6gd.metal	19000		2375.0		80000	
r6i.large *	650	10000	81.25	1250.00	3600	40000
r6i.xlarge *	1250	10000	156.25	1250.00	6000	40000
r6i.2xlarge *	2500	10000	312.50	1250.00	12000	40000
r6i.4xlarge *	5000	10000	625.00	1250.00	20000	40000
r6i.8xlarge	10000		1250.0		40000	
r6i.12xlarge	15000		1875.0		60000	
r6i.16xlarge	20000		2500.0		80000	
r6i.24xlarge	30000		3750.0		120000	
r6i.32xlarge	40000		5000.0		160000	
r6i.metal	40000		5000.0		160000	
r6idn.large *	1250	20000	156.25	2500.00	5468	87500
r6idn.xlarge *	2500	20000	312.50	2500.00	10937	87500
r6idn.2xlarge *	5000	20000	625.00	2500.00	21875	87500
r6idn.4xlarge *	10000	20000	1250.00	2500.00	43750	87500
r6idn.8xlarge	20000		2500.0		87500	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
r6idn.12xlarge	30000		3750.0		131250	
r6idn.16xlarge	40000		5000.0		175000	
r6idn.24xlarge	60000		7500.0		262500	
r6idn.32xlarge	80000		10000.0		350000	
r6idn.metal	80000		10000.0		350000	
r6in.large *	1250	20000	156.25	2500.00	5468	87500
r6in.xlarge *	2500	20000	312.50	2500.00	10937	87500
r6in.2xlarge *	5000	20000	625.00	2500.00	21875	87500
r6in.4xlarge *	10000	20000	1250.00	2500.00	43750	87500
r6in.8xlarge	20000		2500.0		87500	
r6in.12xlarge	30000		3750.0		131250	
r6in.16xlarge	40000		5000.0		175000	
r6in.24xlarge	60000		7500.0		262500	
r6in.32xlarge	80000		10000.0		350000	
r6in.metal	80000		10000.0		350000	
r6id.large *	650	10000	81.25	1250.00	3600	40000
r6id.xlarge *	1250	10000	156.25	1250.00	6000	40000
r6id.2xlarge *	2500	10000	312.50	1250.00	12000	40000
r6id.4xlarge *	5000	10000	625.00	1250.00	20000	40000
r6id.8xlarge	10000		1250.0		40000	
r6id.12xlarge	15000		1875.0		60000	
r6id.16xlarge	20000		2500.0		80000	
r6id.24xlarge	30000		3750.0		120000	
r6id.32xlarge	40000		5000.0		160000	
r6id.metal	40000		5000.0		160000	
r7g.medium *	315	10000	39.38	1250.00	2500	40000

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
r7g.large *	630	10000	78.75	1250.00	3600	40000
r7g.xlarge *	1250	10000	156.25	1250.00	6000	40000
r7g.2xlarge *	2500	10000	312.50	1250.00	12000	40000
r7g.4xlarge *	5000	10000	625.00	1250.00	20000	40000
r7g.8xlarge	10000		1250.0		40000	
r7g.12xlarge	15000		1875.0		60000	
r7g.16xlarge	20000		2500.0		80000	
r7g.metal	20000		2500.0		80000	
u-3tb1.56xlarge	19000		2375.0		80000	
u-6tb1.56xlarge	38000		4750.0		160000	
u-6tb1.112xlarge	38000		4750.0		160000	
u-6tb1.metal	38000		4750.0		160000	
u-9tb1.112xlarge	38000		4750.0		160000	
u-9tb1.metal	38000		4750.0		160000	
u-12tb1.112xlarge	38000		4750.0		160000	
u-12tb1.metal	38000		4750.0		160000	
u-18tb1.metal	38000		4750.0		160000	
u-24tb1.metal	38000		4750.0		160000	
x1.16xlarge	7000		875.0		40000	
x1.32xlarge	14000		1750.0		80000	
x2gd.medium *	315	4750	39.38	593.75	2500	20000
x2gd.large *	630	4750	78.75	593.75	3600	20000
x2gd.xlarge *	1188	4750	148.50	593.75	6000	20000
x2gd.2xlarge *	2375	4750	296.88	593.75	12000	20000
x2gd.4xlarge	4750		593.75		20000	
x2gd.8xlarge	9500		1187.5		40000	
x2gd.12xlarge	14250		1781.25		60000	
x2gd.16xlarge	19000		2375.0		80000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
x2gd.metal	19000		2375.0		80000	
x2idn.16xlarge	40000		5000.0		173333	
x2idn.24xlarge	60000		7500.0		260000	
x2idn.32xlarge	80000		10000.0		260000	
x2idn.metal	80000		10000.0		260000	
x2iedn.xlarge *	2500	20000	312.50	2500.00	8125	65000
x2iedn.2xlarge *	5000	20000	625.00	2500.00	16250	65000
x2iedn.4xlarge *	10000	20000	1250.00	2500.00	32500	65000
x2iedn.8xlarge	20000		2500.0		65000	
x2iedn.16xlarge	40000		5000.0		130000	
x2iedn.24xlarge	60000		7500.0		195000	
x2iedn.32xlarge	80000		10000.0		260000	
x2iedn.metal	80000		10000.0		260000	
x2iezn.2xlarge	3170		396.25		13333	
x2iezn.4xlarge	4750		593.75		20000	
x2iezn.6xlarge	9500		1187.5		40000	
x2iezn.8xlarge	12000		1500.0		55000	
x2iezn.12xlarge	19000		2375.0		80000	
x2iezn.metal	19000		2375.0		80000	
x1e.xlarge	500		62.5		3700	
x1e.2xlarge	1000		125.0		7400	
x1e.4xlarge	1750		218.75		10000	
x1e.8xlarge	3500		437.5		20000	
x1e.16xlarge	7000		875.0		40000	
x1e.32xlarge	14000		1750.0		80000	
z1d.large *	800	3170	100.00	396.25	3333	13333
z1d.xlarge *	1580	3170	197.50	396.25	6667	13333
z1d.2xlarge	3170		396.25		13333	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
z1d.3xlarge	4750		593.75		20000	
z1d.6xlarge	9500		1187.5		40000	
z1d.12xlarge	19000		2375.0		80000	
z1d.metal	19000		2375.0		80000	

存储优化

Important

标有星号（*）的实例可以至少每 24 小时支持一次 30 分钟的最大性能，之后会恢复到基线性能。未标星号的实例保持最高性能的时间不确定。如果工作负载需要在超过 30 分钟的时长内保持最大性能，请选择以下任一实例。

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
d2.xlarge	750		93.75		6000	
d2.2xlarge	1000		125.0		8000	
d2.4xlarge	2000		250.0		16000	
d2.8xlarge	4000		500.0		32000	
d3.xlarge *	850	2800	106.25	350.00	5000	15000
d3.2xlarge *	1700	2800	212.50	350.00	10000	15000
d3.4xlarge	2800		350.0		15000	
d3.8xlarge	5000		625.0		30000	
d3en.xlarge *	850	2800	106.25	350.00	5000	15000
d3en.2xlarge *	1700	2800	212.50	350.00	10000	15000
d3en.4xlarge	2800		350.0		15000	
d3en.6xlarge	4000		500.0		25000	
d3en.8xlarge	5000		625.0		30000	
d3en.12xlarge	7000		875.0		40000	
h1.2xlarge	1750		218.75		12000	
h1.4xlarge	3500		437.5		20000	

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
h1.8xlarge	7000		875.0		40000	
h1.16xlarge	14000		1750.0		80000	
i3.large	425		53.125		3000	
i3.xlarge	850		106.25		6000	
i3.2xlarge	1700		212.5		12000	
i3.4xlarge	3500		437.5		16000	
i3.8xlarge	7000		875.0		32500	
i3.16xlarge	14000		1750.0		65000	
i3.metal	19000		2375.0		80000	
i3en.large *	576	4750	72.10	593.75	3000	20000
i3en.xlarge *	1153	4750	144.20	593.75	6000	20000
i3en.2xlarge *	2307	4750	288.39	593.75	12000	20000
i3en.3xlarge *	3800	4750	475.00	593.75	15000	20000
i3en.6xlarge	4750		593.75		20000	
i3en.12xlarge	9500		1187.5		40000	
i3en.24xlarge	19000		2375.0		80000	
i3en.metal	19000		2375.0		80000	
i4i.large *	625	10000	78.12	1250.00	2500	40000
i4i.xlarge *	1250	10000	156.25	1250.00	5000	40000
i4i.2xlarge *	2500	10000	312.50	1250.00	10000	40000
i4i.4xlarge *	5000	10000	625.00	1250.00	20000	40000
i4i.8xlarge	10000		1250.0		40000	
i4i.16xlarge	20000		2500.0		80000	
i4i.32xlarge	40000		5000.0		160000	
i4i.metal	40000		5000.0		160000	
im4gn.large *	1250	10000	156.25	1250.00	5000	40000
im4gn.xlarge *	2500	10000	312.50	1250.00	10000	40000

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
im4gn.2xlarge *	5000	10000	625.00	1250.00	20000	40000
im4gn.4xlarge	10000		1250.0		40000	
im4gn.8xlarge	20000		2500.0		80000	
im4gn.16xlarge	40000		5000.0		160000	
is4gen.medium *	625	10000	78.12	1250.00	2500	40000
is4gen.large *	1250	10000	156.25	1250.00	5000	40000
is4gen.xlarge *	2500	10000	312.50	1250.00	10000	40000
is4gen.2xlarge *	5000	10000	625.00	1250.00	20000	40000
is4gen.4xlarge	10000		1250.0		40000	
is4gen.8xlarge	20000		2500.0		80000	

加速计算

Important

标有星号（*）的实例可以至少每 24 小时支持一次 30 分钟的最大性能，之后会恢复到基线性能。未标星号的实例保持最高性能的时间不确定。如果工作负载需要在超过 30 分钟的时长内保持最大性能，请选择以下任一实例。

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
dl1.24xlarge	19000		2375.0		80000	
f1.2xlarge	1700		212.5		12000	
f1.4xlarge	3500		437.5		44000	
f1.16xlarge	14000		1750.0		75000	
g3.4xlarge	3500		437.5		20000	
g3.8xlarge	7000		875.0		40000	
g3.16xlarge	14000		1750.0		80000	
g4ad.xlarge *	400	3170	50.00	396.25	1700	13333

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
g4ad.2xlarge *	800	3170	100.00	396.25	3400	13333
g4ad.4xlarge *	1580	3170	197.50	396.25	6700	13333
g4ad.8xlarge	3170		396.25		13333	
g4ad.16xlarge	6300		787.5		26667	
g4dn.xlarge *	950	3500	118.75	437.50	3000	20000
g4dn.2xlarge *	1150	3500	143.75	437.50	6000	20000
g4dn.4xlarge	4750		593.75		20000	
g4dn.8xlarge	9500		1187.5		40000	
g4dn.12xlarge	9500		1187.5		40000	
g4dn.16xlarge	9500		1187.5		40000	
g4dn.metal	19000		2375.0		80000	
g5.xlarge *	700	3500	87.50	437.50	3000	15000
g5.2xlarge *	850	3500	106.25	437.50	3500	15000
g5.4xlarge	4750		593.75		20000	
g5.8xlarge	16000		2000.0		65000	
g5.12xlarge	16000		2000.0		65000	
g5.16xlarge	16000		2000.0		65000	
g5.24xlarge	19000		2375.0		80000	
g5.48xlarge	19000		2375.0		80000	
g5g.xlarge *	1188	4750	148.50	593.75	6000	20000
g5g.2xlarge *	2375	4750	296.88	593.75	12000	20000
g5g.4xlarge	4750		593.75		20000	
g5g.8xlarge	9500		1187.5		40000	
g5g.16xlarge	19000		2375.0		80000	
g5g.metal	19000		2375.0		80000	
inf1.xlarge *	1190	4750	148.75	593.75	4000	20000

实例大小	基准带宽 (Mbps)	最大带宽 (Mbps)	基准吞吐量（MB/s，128 KiB I/O）	最大吞吐量（MB/s，128 KiB I/O）	基准 IOPS (16 KiB I/O)	最大 IOPS (16 KiB I/O)
inf1.2xlarge *	1190	4750	148.75	593.75	6000	20000
inf1.6xlarge	4750		593.75		20000	
inf1.24xlarge	19000		2375.0		80000	
p2.xlarge	750		93.75		6000	
p2.8xlarge	5000		625.0		32500	
p2.16xlarge	10000		1250.0		65000	
p3.2xlarge	1750		218.75		10000	
p3.8xlarge	7000		875.0		40000	
p3.16xlarge	14000		1750.0		80000	
p3dn.24xlarge	19000		2375.0		80000	
p4d.24xlarge	19000		2375.0		80000	
p4de.24xlarge	19000		2375.0		80000	
trn1.2xlarge *	5000	20000	625.00	2500.00	16250	65000
trn1.32xlarge	80000		10000.0		260000	
vt1.3xlarge *	2375	4750	296.88	593.75	10000	20000
vt1.6xlarge	4750		593.75		20000	
vt1.24xlarge	19000		2375.0		80000	

支持的 EBS 优化

下表列出了支持 EBS 优化的实例类型，但默认情况下不启用 EBS 优化。您可以在启动这些实例时或在它们运行后启用 EBS 优化。实例必须启用了 EBS 优化才能实现所述的性能级别。当您对默认情况下不会进行 EBS 优化的实例启用 EBS 优化时，您需为专用容量支付一笔较小的按小时计算的额外费用。有关定价信息，请参阅上的“EBS 优化实例”。

> **Note**
>
> 您还可以使用 Amazon CLI 以编程方式查看此信息。有关更多信息，请参阅查看支持 EBS 优化的实例类型 (p. 1548)。

实例大小	最大带宽 (Mbps)	最大吞吐量（MB/s，128 KiB I/O）	最大 IOPS (16 KiB I/O)
c1.xlarge	1000	125.0	8000
c3.xlarge	500	62.5	4000
c3.2xlarge	1000	125.0	8000

实例大小	最大带宽 (Mbps)	最大吞吐量（MB/s，128 KiB I/O）	最大 IOPS (16 KiB I/O)
c3.4xlarge	2000	250.0	16000
g2.2xlarge	1000	125.0	8000
i2.xlarge	500	62.5	4000
i2.2xlarge	1000	125.0	8000
i2.4xlarge	2000	250.0	16000
m1.large	500	62.5	4000
m1.xlarge	1000	125.0	8000
m2.2xlarge	500	62.5	4000
m2.4xlarge	1000	125.0	8000
m3.xlarge	500	62.5	4000
m3.2xlarge	1000	125.0	8000
r3.xlarge	500	62.5	4000
r3.2xlarge	1000	125.0	8000
r3.4xlarge	2000	250.0	16000

`i2.8xlarge`、`c3.8xlarge` 和 `r3.8xlarge` 实例没有专用 EBS 带宽，因此不提供 EBS 优化。在这些实例上，网络流量和 Amazon EBS 流量将共用同一 10 Gb 网络接口。

获得最佳性能

您可以使用 `EBSIOBalance%` 和 `EBSByteBalance%` 指标来帮助您确定您的实例是否正确调整了大小。您可以在 CloudWatch 控制台中查看这些指标，并设置将根据您指定的阈值触发的警报。这些指标以百分比形式表示。具有持续低余额百分比的实例是上调大小的候选对象。余额百分比从未低于 100% 的实例是下调大小的候选对象。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。

内存增强型实例适合在云中运行大型内存中数据库，包括 SAP HANA 内存中数据库的生产部署。要最大限度提高 EBS 性能，请使用包含偶数个 `io1` 或 `io2` 卷（具有相同的预置性能）的内存增强型实例。例如，对于 IOPS 密集型工作负载，请使用 4 个具有 40,000 预置 IOPS 的 `io1` 或 `io2` 卷以获得最高 160,000 的实例 IOPS。同样，对于吞吐量密集型工作负载，请使用 6 个具有 48,000 预置 IOPS 的 `io1` 或 `io2` 卷以获得最高 4,750 MB/s 的吞吐量。有关其他建议，请参阅 SAP HANA 的存储配置。

注意事项

- 2020 年 2 月 26 日之后启动的 G4dn、I3en、Inf1、M5a、M5ad、R5a、R5ad、T3、T3a 和 Z1d 实例提供上表中列出的最高性能。要从 2020 年 2 月 26 日之前启动的实例中获得最高性能，请停止该实例，然后重新启动。
- 2019 年 12 月 3 日之后启动的 C5、C5d、C5n、M5、M5d、M5n、M5dn、R5、R5d、R5n、R5dn 和 P3dn 实例提供上表中列出的最高性能。要从 2019 年 12 月 3 日之前启动的实例中获得最高性能，请停止该实例，然后重新启动。
- 2020 年 3 月 12 日之后启动的 `u-6tb1.metal`、`u-9tb1.metal` 和 `u-12tb1.metal` 实例提供上表中的性能。2020 年 3 月 12 日之前启动的这些类型的实例可能会提供较低的性能。要从 2020 年 3 月 12 日之前启动的实例中获得最高性能，请与客户团队联系以免费升级实例。

查看支持 EBS 优化的实例类型

您可以使用 Amazon CLI 查看当前区域中支持 EBS 优化的实例类型。

要查看支持 EBS 优化并默认启用了优化的实例类型

使用以下 describe-instance-types 命令。

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops,"MaxTh
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

eu-west-1 的示例输出：

```
----------------------------------------------------------------------------------------------
|                                    DescribeInstanceTypes
    |
+--------------+--------------------+---------------------+-----------
+-----------------------+
| EBSOptimized |   InstanceType     | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/
s)  |
+--------------+--------------------+---------------------+-----------
+-----------------------+
|  default     |  m5dn.8xlarge      |  6800               |  30000    |  850.0
    |
|  default     |  m6gd.xlarge       |  4750               |  20000    |  593.75
    |
|  default     |  c4.4xlarge        |  2000               |  16000    |  250.0
    |
|  default     |  r4.16xlarge       |  14000              |  75000    |  1750.0
    |
|  default     |  m5ad.large        |  2880               |  16000    |  360.0
    |
...
```

查看支持 EBS 优化但默认未启用优化的实例类型

使用以下 describe-instance-types 命令。

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops,"MaxTh
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

eu-west-1 的示例输出：

```
-----------------------------------------------------------------------------------------
|                                  DescribeInstanceTypes                                |
+--------------+--------------+---------------------+----------+-----------------------+
| EBSOptimized | InstanceType  | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+--------------+---------------------+----------+-----------------------+
|  supported   |  m2.4xlarge  |  1000               |  8000    |  125.0                |
|  supported   |  i2.2xlarge  |  1000               |  8000    |  125.0                |
|  supported   |  r3.4xlarge  |  2000               |  16000   |  250.0                |
|  supported   |  m3.xlarge   |  500                |  4000    |  62.5                 |
|  supported   |  r3.2xlarge  |  1000               |  8000    |  125.0                |
...
```

在启动时启用 EBS 优化

您可以通过针对 EBS 优化设置某个实例的属性来为该实例启用优化。

使用控制台在启动实例时启用 Amazon EBS 优化

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Launch Instance（启动实例）。
3. 在步骤 1：选择 Amazon Machine Image (AMI) 中，选择 AMI。
4. 在步骤 2：选择实例类型 中，选择作为支持性 Amazon EBS 优化列出的实例类型。
5. 在 Step 3: Configure Instance Details 中，填写所需的字段并选择 Launch as EBS-optimized instance。如果您在上一步中选择的实例类型不支持 Amazon EBS 优化，则该选项将不存在。如果您选择的实例类型在默认情况下会进行 Amazon EBS 优化，则会选择此选项，并且无法取消选择。
6. 按照说明来完成向导和启动实例。

在启动实例时使用命令行启用 EBS 优化

您可以将下列命令之一与对应的选项结合使用。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- run-instances 与 `--ebs-optimized` (Amazon CLI)
- New-EC2Instance 与 `-EbsOptimized` (Amazon Tools for Windows PowerShell)

为现有实例启用 EBS 优化

您可以修改现有实例的 Amazon EBS 优化实例属性来为该实例启用或禁用优化。如果实例正在运行，则必须先停止实例。

> **Warning**
>
> 当您停止某个实例时，任何实例存储卷上的数据都将被擦除。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

使用控制台为现有实例启用 EBS 优化

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 要停止实例，请依次选择操作、实例状态、停止实例。停止实例可能需要几分钟时间。
4. 在实例处于选中状态时，依次选择操作、实例设置、更改实例类型。
5. 对于更改实例类型，请执行以下操作之一：
   - 如果您的实例在默认情况下是 Amazon EBS 优化实例，则将选择 EBS-optimized (EBS 优化)，并且您无法更改它。您可以选择取消，因为已为该实例启用 Amazon EBS 优化。
   - 如果实例的实例类型支持 Amazon EBS 优化，请选择 EBS 优化，然后选择应用。
   - 如果您的实例的实例类型不支持 Amazon EBS 优化，则您无法选择 EBS 优化。您可以从实例类型中选择一个支持 Amazon EBS 优化的实例类型，选择 EBS 优化，再选择应用。
6. 依次选择实例状态、启动实例。

使用命令行为现有实例启用 EBS 优化

1. 如果实例正在运行，请使用下列命令之一将其停止：

- stop-instances (Amazon CLI)
- Stop-EC2Instance (Amazon Tools for Windows PowerShell)

2. 要启用 EBS 优化，请将下列命令之一与相应的选项结合使用：

   - modify-instance-attribute 与 `--ebs-optimized` (Amazon CLI)
   - Edit-EC2InstanceAttribute 与 `-EbsOptimized` (Amazon Tools for Windows PowerShell)

Linux 实例上的 Amazon EBS 卷性能

几个因素 (包括 I/O 特性以及实例和卷的配置) 会对 Amazon EBS 的性能造成影响。客户如按照 Amazon EBS 和 Amazon EC2 产品详细信息页面上的指导操作，通常能获得很好的性能。但是，在某些情况下，您可能需要进行一些调整才能在此平台上获得最好的性能。本主题讨论特定于某些使用案例的一般最佳实践和性能调整。除了基准测试之外，我们建议您根据实际工作负载信息来调整性能，以确定最佳配置。当您学习了使用 EBS 卷的基础知识后，最好了解一下所需的 I/O 性能，以及可用于提升 Amazon EBS 性能以满足这些要求的选项。

EBS 卷类型性能的 Amazon 更新可能不会立即在您的现有卷上生效。要查看较早卷上的全部性能，您需要先在其上执行 `ModifyVolume` 操作。有关更多信息，请参阅在 Linux 上修改 EBS 卷的大小、IOPS 或类型。

目录

- Amazon EBS 性能提示 (p. 1550)
- I/O 特性和监控 (p. 1552)
- 初始化 Amazon EBS 卷 (p. 1554)
- Linux 上的 RAID 配置 (p. 1556)
- 对 EBS 卷进行基准测试 (p. 1559)

Amazon EBS 性能提示

这些提示代表了在各种用户场景下能够获得最佳 EBS 卷性能的最佳实践。

使用 EBS 优化的实例

对于不支持 EBS 优化吞吐量的实例，网络流量可能会与实例和 EBS 卷之间的流量产生冲突；而在 EBS 优化实例中，这两种流量相互独立。部分 EBS 优化实例配置 (如 C3、R3 和 M3) 会产生额外成本，另一些实例 (如 M4、C4、C5 和 D2) 始终可进行 EBS 优化而不会产生额外成本。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

了解如何计算性能

度量 EBS 卷的性能时，应了解所需采用的度量单位以及如何计算性能，这十分重要。有关更多信息，请参阅I/O 特性和监控 (p. 1552)。

了解工作负载

EBS 卷的最高性能、I/O 操作的大小和数量，以及完成每个操作所需时间之间存在着某种关系。这些因素 (性能、I/O 和延迟) 相互影响，不同应用程序对各个因素的敏感程度也不同。有关更多信息，请参阅 对 EBS 卷进行基准测试 (p. 1559)。

请注意，从快照中初始化卷时，性能将会下降

当您首次访问从快照创建的新 EBS 卷上的每个数据块时，延迟会大大增加。您可以使用以下其中一个选项来避免这一性能下降：

- 在将卷部署到生产环境之前访问每个块。此过程称为初始化（以前称为预热）。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅Amazon EBS 快速快照还原 (p. 1514)。

可能导致 HDD 性能下降的因素

如果创建吞吐量优化型 HDD (st1) 卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。这种情况是这些卷类型特有的。其他可能会限制性能的因素包括迫使吞吐量超过实例的支持能力，在初始化从快照创建的卷时损失性能，以及卷上的小型随机 I/O 过多。有关计算 HDD 卷吞吐量的更多信息，请参阅 Amazon EBS 卷类型 (p. 1327)。

如果您的应用程序没有发送足够多的 I/O 请求，性能可能也会受影响。这可通过查看卷的队列长度和 I/O 大小来监控。队列长度是您的应用程序向卷发起的待处理 I/O 请求的数量。为实现最大程度的一致性，在执行 1MiB 的顺序 I/O 时，HDD 卷必须保持 4 或更大的队列长度（四舍五入为最近的整数）。有关确保稳定的卷性能的更多信息，请参阅 I/O 特性和监控 (p. 1552)

为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值

一些工作负载读取操作量大，并会访问操作系统页缓存中的块储存设备 (例如，从文件系统访问)。在这种情况下，为了实现最大的吞吐量，我们建议您将预读取设置配置为 1 MiB。每个块储存设备的设置不同，应该只应用于您的 HDD 卷。

要检查您的块储存设备的当前预读数值，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

块储存设备信息采用以下格式返回：

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

以上显示的设备报告预读取值为 256 (默认值)。将此数字乘以扇区大小 (512 字节) 就可获得预读取缓冲区的大小，在此例中为 128 KiB。要将缓冲区值设置为 1 MiB，请使用以下命令：

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

再次运行第一个命令，验证预读取设置现在显示 2048。

仅当您的工作负载包括大型顺序 I/O 时，才使用此设置。如果它主要包含的是小型随机 I/O，则此设置会降低性能。一般来说，如果工作负载主要包括小型随机 I/O，则应考虑使用通用型 SSD（gp2 和 gp3）卷，而不是 st1 或 sc1 卷。

使用现代 Linux 内核

借助对间接描述符的支持，使用现代 Linux 内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，以及任何当代 EC2 实例。如果您的平均 I/O 大小达到或接近 44 KiB，则说明您可能是在不支持间接描述符的情况下使用实例或内核。有关根据 Amazon CloudWatch 指标得出平均 I/O 大小的信息，请参阅 I/O 特性和监控 (p. 1552)。

要在 st1 或 sc1卷上实现最大吞吐量，建议您将值 256 应用于 xen_blkfront.max 参数（对于低于 4.6 的 Linux 内核版本）或 xen_blkfront.max_indirect_segments 参数（对于 Linux 内核版本 4.6 及更高版本）。可在操作系统 boot 命令行中设置相应的参数。

例如，在具有较早内核的 Amazon Linux AMI 中，您可以将它添加到在 /boot/grub/menu.lst 中找到的 GRUB 配置的 kernel 行末尾：

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

对于更高版本的内核，该命令将类似于以下内容：

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

重启实例，让此设置生效。

有关更多信息，请参阅Configuring GRUB (p. 228)。对于其他 Linux 发行版（尤其是不使用 GRUB 引导加载程序的版本）可能需要采用不同方法来调整内核参数。

使用 RAID 0 以最大限度利用实例资源

某些实例类型可以实现的 I/O 吞吐量大于可以为单个 EBS 卷配置的量。可以将多个卷一起加入到 RAID 0 配置中，以将可用带宽用于这些实例。有关更多信息，请参阅Linux 上的 RAID 配置 (p. 1556)。

使用 Amazon CloudWatch 跟踪性能

Amazon Web Services 提供了您可以使用 Amazon CloudWatch 来分析和查看的 Amazon EBS 性能指标，以及可以用于监控卷运行状况的状态检查。有关更多信息，请参阅监控您的卷状态 (p. 1359)。

I/O 特性和监控

在给定卷配置中，某些 I/O 特性会对 EBS 卷的性能表现造成影响。支持 SSD 的卷（即通用型 SSD（gp2 和 gp3）和预置 IOPS SSD（io1 和 io2）能够提供一致的性能，无论 I/O 操作是随机的还是顺序的。支持 HDD 的卷（即吞吐量优化型 HDD（st1）和 Cold HDD（sc1）仅当 I/O 操作是大型顺序操作时才能提供最佳性能。要了解 SSD 和 HDD 卷在您的应用程序中性能如何，务必要知道卷上的需求之间的联系、卷能支持的 IOPS 数量、完成 I/O 操作所需的时间，以及卷的吞吐量限制。

主题

- IOPS (p. 1552)
- 卷队列长度和延迟 (p. 1553)
- I/O 大小和卷吞吐量限制 (p. 1553)
- 使用 CloudWatch 监控 I/O 特性 (p. 1554)
- 相关资源 (p. 1554)

IOPS

IOPS 是表示每秒输入/输出操作数的度量单位。这些操作以 KiB 为单位，而底层驱动程序技术决定了卷类型将作为单个 I/O 计数的最大数据量。由于 SSD 卷处理小型或随机 I/O 比 HDD 卷更有效，因此 SSD 卷的 I/O 大小上限为 256 KiB，而 HDD 卷的 I/O 大小上限为 1,024 KiB。

当小型 I/O 操作在物理上连续进行时，Amazon EBS 会尝试将这些操作合并为单个 I/O 操作，直至最大 I/O 大小。同样，当 I/O 操作大于最大 I/O 大小时，Amazon EBS 会尝试将这些操作分为较小的 I/O 操作。下表显示了一些示例。

卷类型	最大 I/O 大小	来自应用程序的 I/O 操作	IOPS 数量	备注
SSD	256 KiB	1 个 1024 KiB I/O 操作	4 (1,024÷256=4)	Amazon EBS 将 1,024 个 I/O 操作拆分为四个较小的 256 KiB 操作。

卷类型	最大 I/O 大小	来自应用程序的 I/O 操作	IOPS 数量	备注
		8 个连续 32KiB I/O 操作	1 (8x32=256)	Amazon EBS 将 8 个连续 32 KiB I/O 操作合并为一个 256 KiB 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。
HDD	1,024 KiB	1 个 1024 KiB I/O 操作	1	I/O 操作已经等于最大 I/O 大小。它不会被合并或拆分。
		8 个连续 128KiB I/O 操作	1 (8x128=1,024)	Amazon EBS 将 8 个连续 128 KiB I/O 操作合并为一个 1,024 KiB I/O 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。

这样，当您创建支持 3,000 IOPS（通过将 Provisioned IOPS SSD 卷预置为 3000 IOPS 或将 通用型 SSD 卷大小确定为 1000 GiB）的 SSD 卷时，您就可以将它挂载到一个 EBS 优化实例，该实例可以提供足够的带宽，您可以每秒传输最高 3000 次数据 I/O，其吞吐量由 I/O 大小决定。

卷队列长度和延迟

卷队列长度是指等待设备处理的 I/O 请求的数量。延迟为 I/O 操作的实际端到端客户端时间，也就是说，从将 I/O 发送到 EBS 到接收来自 EBS 的确认以表示 I/O 读取或写入完成所经过的时间。队列长度必须进行适当调整，以便与 I/O 大小和延迟匹配，避免在访客操作系统上或在到 EBS 的网络链路上产生瓶颈。

每个工作负载的最佳队列长度不同，具体取决于您的特定应用程序对于 IOPS 和延迟的敏感程度。如果您的工作负载未提供足够的 I/O 请求来充分利用 EBS 卷的可用性能，则卷可能无法提供您预置 IOPS 或吞吐量。

事务密集型应用程序对 I/O 延迟增加很敏感，很适合支持 SSD 的卷。您可以通过使卷保持较小的队列长度和较高的 IOPS 数量，来维持高 IOPS 和低延迟。持续迫使一个卷的 IOPS 高于它能够支持的 IOPS 可能增加 I/O 延迟。

吞吐量密集型应用程序对 I/O 延迟增加较不敏感，很适合使用 HDD 支持的卷。您可以在执行大型顺序 I/O 时维持大队列长度，从而对 HDD 卷保持高吞吐量。

I/O 大小和卷吞吐量限制

对于 SSD 卷，如果 I/O 大小非常大，由于达到卷的吞吐量限制，您的 IOPS 数可能会少于预配置数量。例如，对于具有可用突增积分的 1000GiB 以下的 gp2 卷，IOPS 限制为 3000，卷吞吐量限制为 250 MiB/s。如果您正在使用 256 KiB 的 I/O 大小，则您的卷在 IOPS 为 1000 时将达到其吞吐量限制 (1000 x 256 KiB = 250 MiB)。当 I/O 大小较小（如 16 KiB）时，这个卷可以支持 3000 IOPS，这是因为吞吐量远低于 250 MiB/s。（这些示例都假设卷的 I/O 不会达到实例的吞吐量限制。）有关每种 EBS 卷类型吞吐量限制的更多信息，请参阅 Amazon EBS 卷类型 (p. 1327)。

对于较小的 I/O 操作，从实例内部进行度量时，您可能会看到 IOPS 值高于预配置值。当实例操作系统在将小型 I/O 操作传递到 Amazon EBS 之前将其合并为一个较大的操作时，会发生这种情况。

如果您的工作负载在 HDD 支持的 `st1` 和 `sc1` 卷上使用顺序 I/O，则从实例内部进行度量时，您的 IOPS 值可能会高于预期数量。当实例操作系统将顺序 I/O 进行合并，并以 1024 KiB 大小为单位来对其进行计数时，会发生这种情况。如果您的工作负载使用小型随机 I/O，则吞吐量可能会低于您的预期。这是因为我们会将每个随机的非顺序 I/O 计入总的 IOPS 计数，这可能导致您比预期更快达到卷的 IOPS 限制。

Important

无论您采用何种 EBS 卷类型，如果您的 IOPS 或吞吐量与您在配置中的预期不同，请确保 EC2 实例带宽并不是导致这种结果的限制因素。您应始终使用最新一代的 EBS 优化实例 (或包含 10 Gb/s 网络连接的实例) 以实现最佳性能。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。未达到预期 IOPS 的另一个可能原因是未对 EBS 卷执行足够多的 I/O 操作。

使用 CloudWatch 监控 I/O 特性

您可以通过每个卷的 CloudWatch 卷指标 (p. 1564)监控这些 I/O 特性。要考虑的重要指标包括以下内容：

- `BurstBalance`
- `VolumeReadBytes`
- `VolumeWriteBytes`
- `VolumeReadOps`
- `VolumeWriteOps`
- `VolumeQueueLength`

`BurstBalance` 以剩余余额百分比的形式显示 `gp2`、`st1` 和 `sc1` 卷的突增存储桶余额。当您的突增存储桶耗尽时，卷 I/O（对于 `gp2` 卷）或卷吞吐量（对于 `st1` 和 `sc1` 卷）会限定在基准水平。检查 `BurstBalance` 值以确定卷是否因为此原因而受限制。有关可用 Amazon EBS 指标的完整列表，请参阅 Amazon EBS 指标 (p. 1564) 和 基于 Nitro 的实例的 Amazon EBS 指标 (p. 1006)。

HDD 支持的 `st1` 和 `sc1` 卷经过特别设计，旨在对使用 1024 KiB 最大 I/O 大小的工作负载提供最佳性能。要确定卷的平均 I/O 大小，请将 `VolumeWriteBytes` 除以 `VolumeWriteOps`。同样的计算也适用于读取操作。如果平均 I/O 大小低于 64 KiB，则提高发送到 `st1` 或 `sc1` 卷的 I/O 操作的大小应该能够提高性能。

Note

如果平均 I/O 大小达到或接近 44 KiB，说明您可能是在不支持间接描述符的情况下使用实例或内核。所有 Linux 内核 3.8 及更高版本的内核上具有此支持，任何当代实例也具有此支持。

如果您的 I/O 延迟高于您的所需，请检查 `VolumeQueueLength`，以确保应用程序尝试驱动的 IOPS 不会超过您的配置。如果您的应用程序需要的 IOPS 数量超出您的卷所能提供的数量，则应考虑使用以下选项之一：

- 更大的 `gp2` 卷，提供足够的基准 IOPS 性能
- `gp3`、`io1` 或 `io2` 卷，预置了足够 IOPS 以实现所需延迟。

相关资源

有关 Amazon EBS I/O 特征的更多信息，请参阅以下 re:Invent 演示文稿：Amazon EBS：为性能而设计。

初始化 Amazon EBS 卷

空的 EBS 卷一经创建便能实现其最高性能，而不需要初始化（以前称为预热）。

对于从快照创建的卷，必须先从 Amazon S3 下载存储块并将其写入到卷中，然后才能访问这些块。该预备操作需要一些时间才能完成，并且可能会导致首次访问每个块时的 I/O 操作延迟大大提高。在下载所有块并将其写入到卷后，才会实现卷性能。

Important

在初始化已从快照创建的 Provisioned IOPS SSD 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O 性能状态检查中显示 `warning` 状态。这是预期行为，并且您可在初始

化 Provisioned IOPS SSD 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅EBS 卷状态检查 (p. 1359)。

对于大部分应用程序，可将此初始化成本分摊到卷的整个使用期限。为了避免最初在生产环境中出现这种性能下降，您可以使用以下其中一种方案：

- 强制立即初始化整个卷。有关更多信息，请参阅在 Linux 上初始化 Amazon EBS 卷 (p. 1555)。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅Amazon EBS 快速快照还原 (p. 1514)。

在 Linux 上初始化 Amazon EBS 卷

空的 EBS 卷一旦可用便能实现其最高性能，而不需要初始化（以前称为预热）。对于已从快照创建的卷，请使用 dd 或 fio 实用程序读取卷上的所有数据块。卷上的所有现有数据都会保留。

有关在 Windows 上初始化 Amazon EBS 卷的信息，请参阅在 Windows 上初始化 Amazon EBS 卷。

在 Linux 上初始化从快照创建的卷

1. 将新还原的卷附加到您的 Linux 实例。
2. 使用 lsblk 命令列出实例上的块储存设备。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

在此处可以看到新卷 /dev/xvdf 已附加，但是未挂载 (因为 MOUNTPOINT 列下没有列出任何路径)。

3. 使用 dd 或 fio 实用程序对设备上的所有数据块进行读取。默认情况下，dd 命令将安装在 Linux 系统上，但 fio 要快得多，因为它允很多线程读取。

   Note

   此步骤可能需要几分钟到几个小时，具体取决于 EC2 实例带宽、为卷配置的 IOPS 和卷的大小。

   [dd] 应将 if（输入文件）参数设置为要初始化的驱动器。应将 of (输出文件) 参数设置为 Linux 空虚拟设备 /dev/null。bs 参数设置读取操作的数据块大小；要获得最佳性能，这应设置为 1 MB。

   Important

   不当使用 dd 可能容易损坏卷的数据。请务必严格遵循下面的示例命令。只有 if=/dev/*xvdf* 参数将因您要读取的设备的名称而异。

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] 如果您在系统上安装了 fio，请使用以下命令初始化您的卷。应将 --filename（输入文件）参数设置为要初始化的驱动器。

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=128k --iodepth=32 --
ioengine=libaio --direct=1 --name=volume-initialize
```

要在 Amazon Linux 上安装 fio，请使用以下命令：

```
sudo yum install -y fio
```

要在 Ubuntu 上安装 fio，请使用以下命令：

```
sudo apt-get install -y fio
```

操作完成时，您会看到读取操作的报告。卷现在已准备就绪，可供使用。有关更多信息，请参阅使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)。

Linux 上的 RAID 配置

通过 Amazon EBS，您可以使用可与传统裸机服务器结合使用的任何标准 RAID 配置，只要实例的操作系统支持该特定 RAID 配置。这是因为，所有 RAID 都是在软件级别上实现的。

Amazon EBS 卷的数据可在可用区内多个服务器间进行复制，以防由于任何单个组件发生故障导致数据丢失。此复制使得 Amazon EBS 卷的可靠程度比普通磁盘高 10 倍。更多信息，请参阅 Amazon EBS 产品详细信息页面中的 Amazon EBS 可用性与持久性。

> **Note**
>
> 您应避免从 RAID 卷启动。Grub 通常只安装在 RAID 阵列中的一台设备上，如果某台镜像设备发生故障，您可能无法启动操作系统。

如果您需要在 Windows 实例上创建一个 RAID 阵列，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 Windows 上的 RAID 配置。

目录

- RAID 配置选项 (p. 1556)
- 在 Linux 上创建 RAID 0 阵列 (p. 1556)
- 创建 RAID 阵列中卷的快照 (p. 1559)

RAID 配置选项

相比在单个 Amazon EBS 卷上配置，通过创建 RAID 0 阵列，文件系统可以获得更高性能。如果 I/O 性能至关重要，请使用 RAID 0。I/O 通过 RAID 0 在卷内以条带状分布。如果您添加卷，则会直接增加吞吐量和 IOPS。但是，请记住，条带的性能仅限于集中性能最差的卷，并且集中的单个卷丢失会导致阵列数据完全丢失。

RAID 0 阵列的最终大小是阵列中各个卷的大小之和，带宽是阵列中各个卷的可用带宽之和。例如，预置 IOPS 为 4000 的两个 500 GiB `io1` 卷将创建可用带宽为 8000 IOPS、吞吐量为 1000 MiB/s 的 1000 GiB RAID 0 阵列。

> **Important**
>
> 不建议对 Amazon EBS 使用 RAID 5 和 RAID 6，因为这些 RAID 模式的奇偶校验写入操作会使用您的卷的一些可用 IOPS。根据您的 RAID 阵列配置，这些 RAID 模式提供的可用 IOPS 比 RAID 0 配置少 20-30%。成本增加也是与这些 RAID 模式有关的一个因素；在使用相同的卷大小和速度时，一个 2 卷 RAID 0 阵列明显胜过两倍成本的 4 卷 RAID 6 阵列。
> RAID 1 也不建议用于 Amazon EBS。RAID 1 需要比非 RAID 配置更大的 Amazon EC2 到 Amazon EBS 带宽，因为数据将同时写入多个卷。此外，RAID 1 不提供任何写入性能改进。

在 Linux 上创建 RAID 0 阵列

本文档提供基本的 RAID 0 设置示例。

在执行此步骤之前，您需要确定 RAID 0 阵列的大小以及需要配置多少 IOPS。

使用以下过程创建 RAID 0 阵列。请注意，您可以从 Amazon EC2 用户指南（适用于 Windows 实例）中的在 Windows 上创建 RAID 0 阵列中获得有关 Windows 实例的说明。

在 Linux 上创建 RAID 0 阵列

1. 为阵列创建 Amazon EBS 卷。有关更多信息，请参阅创建 Amazon EBS 卷 (p. 1344)。

   Important

   为阵列创建具有相等大小和 IOPS 性能值的卷。确保不创建超过 EC2 实例的可用带宽的阵列。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。
2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅将 Amazon EBS 卷挂载到实例 (p. 1347)。
3. 使用 mdadm 命令从新附加的 Amazon EBS 卷创建逻辑 RAID 设备。用阵列中的卷数替换 *number_of_volumes*，用阵列中每个卷的设备名称 (例如 /dev/xvdf) 替换 *device_name*。您还可以将 *MY_RAID* 替代为阵列的唯一名称。

   Note

   您可以使用 lsblk 命令列出实例上的设备以找到设备名称。

   要创建 RAID 0 阵列，请运行以下命令（注意，--level=0 选项用于将阵列条带化）：

   ```
   [ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
   ```

   Tip

   如您遇到 mdadm: command not found 错误，请使用以下命令安装 mdadm：sudo yum install mdadm。
4. 给 RAID 阵列一些时间进行初始化和同步。您可以借助下面的命令跟踪这些操作的进度：

   ```
   [ec2-user ~]$ sudo cat /proc/mdstat
   ```

   下面是示例输出：

   ```
   Personalities : [raid0]
   md0 : active raid0 xvdc[1] xvdb[0]
         41910272 blocks super 1.2 512k chunks

   unused devices: <none>
   ```

   通常，您可以通过下面的命令显示有关 RAID 阵列的详细信息：

   ```
   [ec2-user ~]$ sudo mdadm --detail /dev/md0
   ```

   下面是示例输出：

   ```
   /dev/md0:
              Version : 1.2
        Creation Time : Wed May 19 11:12:56 2021
           Raid Level : raid0
           Array Size : 41910272 (39.97 GiB 42.92 GB)
         Raid Devices : 2
        Total Devices : 2
          Persistence : Superblock is persistent
   ```

```
       Update Time : Wed May 19 11:12:56 2021
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

        Chunk Size : 512K

Consistency Policy : none

              Name : MY_RAID
              UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
            Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. 在您的 RAID 阵列上创建一个文件系统，并为该文件系统分配一个稍后在装载该文件系统时使用的标签。例如，要使用标签 *MY_RAID* 创建 ext4 文件系统，请运行以下命令：

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

根据应用程序的要求或操作系统的限制，您可以使用其他文件系统类型，如 ext3 或 XFS (请参阅您的文件系统文档以了解相应的文件系统创建命令)。

6. 要确保 RAID 阵列在启动时自动重组，请创建一个包含 RAID 信息的配置文件：

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

Note

如果您使用的是 Linux 发行版而非 Amazon Linux，您可能需要修改此命令。例如，您可能需要将文件放在不同的位置，或者添加 `--examine` 参数。有关更多信息，请在 Linux 实例上运行 man mdadm.conf。

7. 创建新的 Ramdisk Image 以为新的 RAID 配置正确地预加载块储存设备模块：

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. 为 RAID 阵列创建装载点。

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. 最后，在已创建的装载点上安装 RAID 设备：

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

RAID 设备现已准备就绪，可供使用。

10. （可选）要在每次系统重启时装载此 Amazon EBS 卷，可在 `/etc/fstab` 文件中为该设备添加一个条目。

    a. 创建 `/etc/fstab` 文件的备份，当您进行编辑时意外损坏或删除了此文件的情况下，可以使用该备份。

    ```
    [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
    ```

    b. 使用您常用的文本编辑器（如 `/etc/fstab` 或 nano）打开 vim 文件。

c. 注释掉任何以“UUID=”开头的行，然后，在文件末尾，使用以下格式为您的 RAID 卷添加新行：

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

此行的最后三个字段分别是文件系统装载选项、文件系统转储频率和启动时的文件系统检查顺序。如果您不知道这些值应该是什么，请使用以下示例中的值 (defaults,nofail 0 2))。有关 /etc/fstab 条目的更多信息，请参阅 fstab 手册页面（方法：在命令行输入 man fstab）。例如，要在设备上的装载点 /mnt/raid 装载带 MY_RAID 标签的 ext4 文件系统，请将以下条目添加到 /etc/fstab。

Note

如果您要在未附加该卷的情况下启动实例 (例如，以便该卷可以在不同实例之间向后和向前移动)，则应添加 nofail 装载选项，该选项允许实例即使在卷安装过程中出现错误时也可启动。Debian 衍生物 (如 Ubuntu) 还必须添加 nobootwait 装载选项。

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. 在您将新条目添加到 /etc/fstab 后，需要检查您的条目是否有效。运行 sudo mount -a 命令以在 /etc/fstab 中装载所有文件系统。

```
[ec2-user ~]$ sudo mount -a
```

如果上述命令未产生错误，说明您的 /etc/fstab 文件正常，您的文件系统会在下次启动时自动装载。如果该命令产生了任何错误，请检查这些错误并尝试更正 /etc/fstab。

Warning

/etc/fstab 文件中的错误可能显示系统无法启动。请勿关闭 /etc/fstab 文件中有错误的系统。

e. (可选) 如果您无法确定如何更正 /etc/fstab 错误，则始终可以使用以下命令还原您的备份 /etc/fstab 文件。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

创建 RAID 阵列中卷的快照

如果要使用快照备份 RAID 阵列中 EBS 卷上的数据，则必须确保快照的一致性。原因在于这些卷的快照是独立创建的。从不同步的快照恢复 RAID 阵列中的 EBS 卷会降低阵列的完整性。

要为 RAID 阵列创建一组一致的快照，请使用 EBS 多卷快照。利用多卷快照，您可以跨附加到 EC2 实例的多个 EBS 卷拍摄时间点、数据协调和崩溃一致性快照。您不需要停止实例以在多个卷之间协调来确保一致性，因为快照将跨多个 EBS 卷自动拍摄。有关更多信息，请参阅创建 Amazon EBS 快照下的有关创建多卷快照的步骤。

对 EBS 卷进行基准测试

您可以通过模拟 I/O 工作负载来测试 Amazon EBS 卷的性能。过程如下所述：

1. 启动 EBS 优化实例。
2. 创建新的 EBS 卷。
3. 将这些卷附加到您的 EBS 优化实例。
4. 配置并挂载块储存设备。
5. 安装工具以便测试 I/O 性能。

6. 测试卷的 I/O 性能。
7. 删除卷并终止实例，确保不会继续引发更改。

> **Important**
>
> 某些过程可能会对您进行基准测试的 EBS 卷上的现有数据造成破坏。基准测试程序适用于出于测试目的而特别创建的卷，并不适用于生产卷。

设置实例

为了获得最佳的 EBS 卷性能，我们建议您使用 EBS 优化实例。EBS 优化实例可在 Amazon EC2 和 Amazon EBS 之间提供实例专用吞吐量。EBS 优化的实例在 Amazon EC2 与 Amazon EBS 之间提供了专用带宽，其规格取决于实例类型。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

要创建 EBS 优化实例，可在使用 Amazon EC2 控制台启动实例时选择作为 EBS 优化的实例启动，或在使用命令行时指定 --ebs-optimized。请确保您启动的实例是支持该选项的最新一代实例。有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。

设置 Provisioned IOPS SSD 或 通用型 SSD 卷

要使用 Amazon EC2 控制台创建预置 IOPS SSD（`io1` 和 `io2`）或通用型 SSD（`gp2` 和 `gp3`）卷，对于 Volume type (卷类型)，选择 Provisioned IOPS SSD (io1) (预置 IOPS SSD [io1])、Provisioned IOPS SSD (io2) (预置 IOPS SSD [io2])、General Purpose SSD (gp2) (通用型 SSD [gp2])，或 General Purpose SSD (gp3) (通用型 SSD [gp3])。在命令行中，为 `io1` 参数指定 `io2`、`gp2`、`gp3` 或 --volume-type。对于 `io1`、`io2` 和 `gp3` 卷，请指定 --iops 参数的每秒 I/O 操作数 (IOPS)。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)和创建 Amazon EBS 卷 (p. 1344)。

要了解这些示例测试，我们建议您创建一个包含 6 个卷的高性能 RAID 0 阵列。因为您是按照预配置的 GB 数量（以及为 io1、io2 和 gp3 卷预配置的 IOPS 数量，而不是卷的数量）付费，因此创建多个较小卷并使用它们来创建条带集不会产生额外费用。如果您是使用 Oracle Orion 来测试卷的性能，则它可以模拟 Oracle ASM 的条带化操作，因此我们建议您让 Orion 执行条带化分区。如果您使用的是其他基准测试工具，则需要自己对卷执行条带化分区。

有关如何创建包含 6 个卷的 RAID 0 阵列的说明，请参阅 在 Linux 上创建 RAID 0 阵列 (p. 1556)。

设置吞吐量优化型 HDD（`st1`）卷或 Cold HDD（`sc1`）卷

要创建 `st1` 卷，可在使用 Amazon EC2 控制台创建卷时选择 Throughput Optimized HDD (吞吐量优化型 HDD)，或在使用命令行时指定 --type **`st1`**。要创建 `sc1` 卷，可在使用 Amazon EC2 控制台创建卷时选择 Cold HDD，或在使用命令行时指定 --type **`sc1`**。有关创建 EBS 卷的信息，请参阅创建 Amazon EBS 卷 (p. 1344)。有关将这些卷附加到您的实例的信息，请参阅 将 Amazon EBS 卷挂载到实例 (p. 1347)。

Amazon 提供了一个 JSON 模板，以便与 Amazon CloudFormation 配合使用来简化此设置过程。访问模板并将其另存为 JSON 文件。Amazon CloudFormation 允许您配置自己的 SSH 密钥并提供了更简单的方式来设置性能测试环境，以评估 `st1` 卷。此模板会创建一个最新一代的实例以及一个 2 TiB 的 `st1` 卷，然后将该卷附加到 `/dev/xvdf` 处的实例。

使用模板创建 HDD 卷

1. 打开 Amazon CloudFormation 控制台，地址：https://console.aws.amazon.com/cloudformation。
2. 选择 Create Stack。
3. 选择 Upload a Template to Amazon S3，然后选择之前获得的 JSON 模板。
4. 为您的堆栈提供名称 (如“ebs-perf-testing”)，然后选择实例类型 (默认为 r3.8xlarge) 和 SSH 密钥。
5. 选择 Next 两次，然后选择 Create Stack。
6. 新堆栈的状态从 CREATE_IN_PROGRESS 变为 COMPLETE 后，选择 Outputs（输出）以获取新实例的公有 DNS 条目，新实例将附加一个 2TiB 的 `st1` 卷。
7. 以用户 **`ec2-user`** 的身份使用 SSH 连接到您的新堆栈（使用从上一步的 DNS 条目中获得的主机名）。

8. 继续执行安装基准测试工具 (p. 1561)。

安装基准测试工具

下表列出了您可用于对 EBS 卷的性能进行基准测试的部分可用工具。

工具	描述

fio	用于测试 I/O 性能。（请注意，fio 依赖于 `libaio-devel`。）
	要在 Amazon Linux 上安装 fio，请运行以下命令：
	`[ec2-user ~]$ sudo yum install -y fio`
	要在 Ubuntu 上安装 fio，请执行以下命令：
	`sudo apt-get install -y fio`

Oracle Orion 校准工具	用于校准要与 Oracle 数据库搭配使用的存储系统的 I/O 性能。

这些基准测试工具可支持各种测试参数。您应该使用命令来测试您的卷支持的工作负载。下面提供的命令示例可帮助您入门。

选择卷队列长度

基于工作负载和卷类型选择最佳卷队列长度。

SSD 支持的卷的队列长度

要确定支持 SSD 的卷上工作负载的最佳队列长度，建议您将每 1000 IOPS（通用型 SSD 卷的基准量，Provisioned IOPS SSD 卷的预置量）对应 1 个队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。

在达到预配置 IOPS、吞吐量或最佳系统队列长度值之前，增加队列长度有好处，当前队列长度设置为 32。举例来说，预配置 3,000 IOPS 的卷应该将队列长度设置为 3。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

HDD 支持的卷的队列长度

要确定 HDD 卷上工作负载的最佳队列长度，建议您在执行 1MiB 顺序 I/O 时以至少为 4 的队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。例如，突发吞吐量为 500 MiB/s、IOPS 为 500 的 2 TiB `st1` 卷在执行 1024 KiB、512 KiB 或 256 KiB 的顺序 I/O 时，分别应该将队列长度 4、8 或 16 作为目标。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

禁用 C 状态

在运行基准测试之前，您应禁用处理器 C 状态。支持此功能的 CPU 中的核心在暂时空闲时，会进入 C 状态以节省功耗。在调用核心以恢复处理时，将经过一段特定的时间，核心才能再次全速运行。此延迟可能会干扰处理器基准测试例程。有关 C 状态以及哪些 EC2 实例类型支持此状态的更多信息，请参阅 EC2 实例的处理器状态控制。

在 Linux 上禁用 C 状态

您可在 Amazon Linux、RHEL 和 CentOS 上按以下所示禁用 C 状态：

1. 获取 C 状态数。

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. 从 c1 到 cN 禁用 C 状态。理想情况下，核心应处于状态 c0。

```
$ for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

执行基准测试

以下步骤介绍各种 EBS 卷类型的基准测试命令。

对附加了 EBS 卷的 EBS 优化实例运行以下命令。如果已从快照创建 EBS 卷，在执行基准测试之前，请确保初始化这些卷。有关更多信息，请参阅初始化 Amazon EBS 卷 (p. 1554)。

完成对卷的测试后，可参阅以下主题来帮助清除卷：删除 Amazon EBS 卷 (p. 1366)和终止实例 (p. 634)。

基准 Provisioned IOPS SSD 和 通用型 SSD 卷

在您创建的 RAID 0 阵列上运行 fio。

以下命令可执行 16 KB 随机写入操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --
name fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based
 --runtime=180 --group_reporting --norandommap
```

以下命令可执行 16 KB 随机读取操作。

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1 --
rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --
norandommap
```

有关解析结果的更多信息，请参阅以下教程：使用 fio 检查磁盘 IO 性能。

基准 st1 和 sc1 卷

在 fio 或 st1 卷上运行 sc1。

> **Note**
>
> 在执行这些测试之前，请按为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值 (p. 1551)所述在实例上设置缓冲 I/O。

以下命令针对附加的 st1 块储存设备（例如 /dev/xvdf）执行 1 MiB 的顺序读取操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

以下命令针对附加的 st1 块储存设备执行 1 MiB 的顺序写入操作：

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

有些工作负载可对块储存设备的不同部分混合执行顺序读取和顺序写入操作。要对此类工作负载进行基准测试，我们建议您为读取和写入操作单独、同时使用 fio 作业，并为每个作业使用 fio offset_increment 选项将块储存设备的不同位置作为目标。

运行此类工作负载比顺序写入或顺序读取工作负载要复杂一些。使用文本编辑器创建一个 fio 作业文件，在此示例中名为 `fio_rw_mix.cfg`，包含以下内容：

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

然后运行以下命令：

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

有关解析结果的更多信息，请参阅以下教程：使用 fio 检查磁盘 IO 性能。

对于 fio 和 `st1` 卷而言，通过多个 `sc1` 作业来执行直接 I/O（即使使用顺序读入或写入操作）可能会导致吞吐量小于预期数值。建议您使用一个直接 I/O 作业并使用 `iodepth` 参数来控制并发 I/O 操作的数量。

Amazon EBS 的 Amazon CloudWatch 指标

Amazon CloudWatch 指标是统计数据，您可以使用这些指标来查看、分析和设置有关卷操作行为的警报。

数据在 1 分钟期间内自动可用，无需收费。

当您从 CloudWatch 得到数据时，您可以列入一个`Period`请求参数来指定返回数据的粒度。这不同于我们收集数据时所用的时间 (1 分钟时间)。我们建议您在请求中指定的时间大于等于收集时间，从而确保返回数据有效。

获取数据时，您可以使用 CloudWatch API 或 Amazon EC2 控制台。控制台从 CloudWatch API 中获取原始数据并根据数据显示一系列图表。根据您的需要，您既可以选择使用从 API 中获得的数据也可以选择使用控制台中的图表。

主题

- Amazon EBS 指标 (p. 1564)
- Amazon EBS 指标的维度 (p. 1567)
- Amazon EC2 控制台中的图表 (p. 1567)

Amazon EBS 指标

Amazon Elastic Block Store (Amazon EBS) 可将若干指标的数据点发送到 CloudWatch。所有 Amazon EBS 卷类型都会自动向 CloudWatch 发送 1 分钟的指标，但只有在卷连接到实例时，才会自动发送。

指标

- 挂载到所有实例类型的卷的卷指标 (p. 1564)
- 挂载到基于 Nitro 实例类型的卷的卷指标 (p. 1567)
- 快速快照还原指标 (p. 1567)

挂载到所有实例类型的卷的卷指标

AWS/EBS 命名空间包括连接到所有实例类型的 EBS 卷的以下指标。要从实例上的操作系统获取有关可用磁盘空间的信息，请参阅查看可用磁盘空间 (p. 1353)。

Note

- 某些指标在基于 Nitro 系统构建的实例上存在差异。有关这些实例类型的列表，请参阅 基于 Nitro 系统构建的实例 (p. 246)。
- AWS/EC2 命名空间包括所添加的卷的基于 Nitro 的实例（非裸机实例）的其他 Amazon EBS 指标。有关这些指标的更多信息，请参阅 基于 Nitro 的实例的 Amazon EBS 指标 (p. 1006)。

指标	描述
VolumeReadBytes	提供有关指定时间段内的读取操作的信息。Sum 统计数据将报告该时间段内传输的总字节数。Average 统计数据报告该时间段内的每个读取操作的平均大小，附加到基于 Nitro 的实例的卷除外，其中的平均值表示指定时间段的平均值。SampleCount 统计数据报告该时间段内的读取操作总数，但附加到基于 Nitro 的实例的卷除外，其中的样本数表示在统计计算中使用的数据点数。对于 Xen 实例，只有在卷上有读取活动时才报告数据。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：字节
VolumeWriteBytes	提供有关指定时间段内的写入操作的信息。Sum 统计数据将报告该时间段内传输的总字节数。Average 统计数据报告该时间段内的每个写入操作的平均大小，附加到基于 Nitro 的实例的卷除外，其中的平均值表示指定时间段的平均值。SampleCount 统计数据报告该时间段内的写入操作总数，但附加到基于 Nitro 的实例的卷除外，其中的样本数表示在统计计算中使用的数据点数。对于 Xen 实例，只有在卷上有写入活动时才报告数据。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：字节
VolumeReadOps	在指定时间的读取操作总数。注意：读取操作在完成时计数。 要计算该时间段的平均每秒读取操作数（读取 IOPS），请将该时间段的总读取操作数除以秒数。

指标	描述
	仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：计数
VolumeWriteOps	在指定时间的写入操作总数。注意：写入操作在完成时计数。 要计算该时间段的平均每秒写入操作数（写入 IOPS），请将该时间段的总写入操作数除以秒数。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：计数
VolumeTotalReadTime	Note 启用多重挂载的卷不支持此指标。 指定时间段中所有读取操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 1 分钟 (60 秒) 的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。对于 Xen 实例，只有在卷上有读取活动时才报告数据。 该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：秒
VolumeTotalWriteTime	Note 启用多重挂载的卷不支持此指标。 指定时间段中所有写入操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 1 分钟 (60 秒) 的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。对于 Xen 实例，只有在卷上有写入活动时才报告数据。 该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：秒

指标	描述
VolumeIdleTime	Note 启用多重挂载的卷不支持此指标。 未提交读取或写入操作的指定时间段中的总秒数。 该指标的 Average 统计数据与附加到基于 Nitro 的实例的卷无关。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：秒
VolumeQueueLength	指定时间段中等待完成的读取和写入操作请求的数量。 该指标的 Sum 统计数据与附加到基于 Nitro 的实例的卷无关。 仅附加到基于 Nitro 的实例的卷支持该指标的 Minimum 和 Maximum 统计数据。 单位：计数
VolumeThroughputPercentage	Note 启用多重挂载的卷不支持此指标。 仅用于 Provisioned IOPS SSD 卷。每秒传输的 I/O 操作数 (IOPS) 在为 Amazon EBS 卷预置的总 IOPS 中所占的百分比。预置 IOPS SSD 卷在 99.9% 的时间里可提供预置性能。 写入过程中，如果一分钟内没有其他待处理的 I/O 请求，指标值就会是 100%。另外，卷的 I/O 性能可能由于已执行的操作而暂时下降 (例如，在使用高峰期创建卷的快照，在非 EBS 优化的实例上运行卷，或者首次访问卷上的数据)。 单位：百分比
VolumeConsumedReadWriteOps	仅用于 Provisioned IOPS SSD 卷。指定时间段内使用的读取和写入操作的总量（规格化为 256K 容量单位）。 每个小于 256K 的 I/O 操作算作使用了 1 IOPS。大于 256K 的 I/O 操作按 256K 容量单位计算。例如，1024K I/O 算作使用了 4 IOPS。 单位：计数

指标	描述
BurstBalance	仅可与通用型 SSD（gp2）、吞吐量优化型 HDD（st1）和 Cold HDD（sc1）卷一同使用。提供有关突增存储桶中剩余的 I/O 积分百分比（对于 gp2）或吞吐量积分（对于 st1 和 sc1）的信息。仅当卷处于活动状态时将数据报告给 CloudWatch。如果未附加卷，则不会报告任何数据。 此指标的 Sum 统计数据与挂载到在 Nitro System 上构建的实例的卷无关。 如果卷的基准性能超过了最大突发性能，则绝不会使用积分。如果卷附加到基于 Nitro 系统构建的实例，则不会报告突增余额。对于其他实例，报告的突增余额是 100%。有关更多信息，请参阅gp2 卷性能 (p. 1331)。 单位：百分比

挂载到基于 Nitro 实例类型的卷的卷指标

AWS/EC2 命名空间包括所添加的卷的基于 Nitro 的实例（非裸机实例）的其他 Amazon EBS 指标。有关这些指标的更多信息，请参阅 基于 Nitro 的实例的 Amazon EBS 指标 (p. 1006)。

快速快照还原指标

AWS/EBS 命名空间包含以下用于快速快照还原 (p. 1514)的指标。

指标	描述
FastSnapshotRestoreCreditsBucketSize	可以累积的最大卷创建积分数。将为每个可用区的每个快照报告该指标。 最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。
FastSnapshotRestoreCreditsBalance	可用的卷创建积分数。将为每个可用区的每个快照报告该指标。 最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。

Amazon EBS 指标的维度

支持的维度是卷 ID (VolumeId)。所有可用的统计数据都是按卷 ID 筛选的。

对于卷指标 (p. 1564)，支持的维度是卷 ID (VolumeId)。所有可用的统计数据都是按卷 ID 筛选的。

对于快速快照还原指标 (p. 1567)，支持的维度是快照 ID (SnapshotId) 和可用区 (AvailabilityZone)。

Amazon EC2 控制台中的图表

创建一个卷后，您可以在 Amazon EC2 控制台中查看该卷的监控图表。在控制台的 Volumes 页面上选择一个卷，然后选择 Monitoring。下表列出了显示的图表。右列说明如何使用从 CloudWatch API 中获得的原始数据指标来生成每一个图表。所有的图表周期都是 5 分钟。

图表	使用原始指标描述
读取带宽 (KiB/s)	`Sum(VolumeReadBytes) / Period / 1024`
写入带宽 (KiB/s)	`Sum(VolumeWriteBytes) / Period / 1024`
读取吞吐量 (IOPS)	`Sum(VolumeReadOps) / Period`
写入吞吐量 (IOPS)	`Sum(VolumeWriteOps) / Period`
平均队列长度 (操作数)	`Avg(VolumeQueueLength)`
空闲花费时间百分比	`Sum(VolumeIdleTime) / Period × 100`

平均读取大小 (KiB/操作)	`Avg(VolumeReadBytes) / 1024`
	
	对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均读取大小：
	
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024`
	
	在 EBS CloudWatch 控制台中提供了 `VolumeReadBytes` 和 `VolumeReadOps` 指标。

平均写入大小 (KiB/操作)	`Avg(VolumeWriteBytes) / 1024`
	
	对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均写入大小：
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`
	
	在 EBS CloudWatch 控制台中提供了 `VolumeWriteBytes` 和 `VolumeWriteOps` 指标。

平均读取延迟 (毫秒/操作)	`Avg(VolumeTotalReadTime) × 1000`
	
	对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均读取延迟：
	
	`(Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000`
	
	在 EBS CloudWatch 控制台中提供了 `VolumeTotalReadTime` 和 `VolumeReadOps` 指标。

平均写入延迟 (毫秒/操作)	`Avg(VolumeTotalWriteTime) × 1000`
	
	对基于 Nitro 的实例，以下公式使用 CloudWatch Metric Math 计算平均写入延迟：
	
	`(Sum(VolumeTotalWriteTime) / Sum(VolumeWriteOps)) * 1000`
	
	在 EBS CloudWatch 控制台中提供了 `VolumeTotalWriteTime` 和 `VolumeWriteOps` 指标。

对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作 (读取或写入，以适用于图表者为准) 总数计算得出。

适用于 Amazon EBS 的 EventBridge

Amazon EBS 将事件发送到 Amazon EventBridge，用于在卷和快照上执行操作。使用 EventBridge，您可以创建规则以触发编程操作，从而响应这些事件。例如，您可以创建一个规则，在启用快照以快速恢复快照时向您的电子邮件发送通知。

EventBridge 中的事件表示为 JSON 对象。该事件独有的字段包含在 JSON 对象的“详细信息”部分。“事件”字段包含事件名称。“结果”字段包含触发事件的操作的已完成状态。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 事件模式。

有关更多信息，请参阅《Amazon EventBridge 用户指南》中的什么是 Amazon EventBridge？。

事件

- EBS 卷事件 (p. 1569)
- EBS 卷修改事件 (p. 1572)
- EBS 快照事件 (p. 1572)
- EBS 快照归档事件 (p. 1576)
- EBS 快速快照还原事件 (p. 1576)
- 使用 Amazon Lambda 处理 EventBridge 事件 (p. 1577)

EBS 卷事件

在发生以下卷事件时，Amazon EBS 会向 EventBridge 发送事件。

事件

- 创建卷 (createVolume) (p. 1569)
- 删除卷 (deleteVolume) (p. 1570)
- 卷附加或重新附加（attachVolume、reattachVolume）(p. 1571)

创建卷 (createVolume)

当创建卷的操作完成后，系统会将 `createVolume` 事件发送至您的 Amazon 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 `available` 或 `failed`。如果提供的 Amazon KMS key 无效，创建操作将失败，如以下示例所示。

事件数据

下面的列表是 EBS 为成功的 `createVolume` 事件发送的 JSON 对象示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
```

```
   "detail": {
      "result": "available",
      "cause": "",
      "event": "createVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

下面的列表是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 被禁用。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
 is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

以下是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 正等待导入。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
 is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

删除卷 (deleteVolume)

当删除卷的操作完成后，系统会将 deleteVolume 事件发送至您的 Amazon 账户。不过，不会保存、记录或存档该事件。此事件具有 deleted 结果。如果删除操作未完成，绝不会发送此事件。

事件数据

下面的列表是 EBS 为成功的 deleteVolume 事件发送的 JSON 对象示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
      "event": "deleteVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

卷附加或重新附加（attachVolume、reattachVolume）

如果卷无法附加或重新附加到实例，系统会将 attachVolume 或 reattachVolume 事件发送至您的 Amazon 账户。不过，不会保存、记录或存档该事件。如果您使用 KMS 密钥 加密 EBS 卷并且该 KMS 密钥变为无效，则日后使用该 KMS 密钥 将卷附加或重新附加到实例时，EBS 会发送一个事件，如以下示例所示。

事件数据

下面的列表是 EBS 在 attachVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 处于待删除状态。

> **Note**
>
> 在对服务器进行日常维护后，Amazon 可能会尝试重新附加卷。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
 is pending deletion.",
    "request-id": ""
  }
}
```

下面的列表是 EBS 在 reattachVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 处于待删除状态。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
```

```
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
 is pending deletion.",
    "request-id": ""
  }
}
```

EBS 卷修改事件

当修改卷时，Amazon EBS 会向 EventBridge 发送 `modifyVolume` 事件。不过，不会保存、记录或存档该事件。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

EBS 快照事件

在发生以下卷事件时，Amazon EBS 会向 EventBridge 发送事件。

事件

- 创建单个快照 (createSnapshot) (p. 1572)
- 创建多个快照 (createSnapshots) (p. 1573)
- 复制快照 (copySnapshot) (p. 1574)
- 共享快照 (shareSnapshot) (p. 1575)

创建单个快照 (createSnapshot)

当创建快照的操作完成后，系统会将 `createSnapshot` 事件发送至您的 Amazon 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 `succeeded` 或 `failed`。

事件数据

下面的列表是 EBS 为成功的 createSnapshot 事件发送的 JSON 对象示例。在 detail 部分，source 字段包含源卷的 ARN。startTime 和 endTime 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

创建多个快照 (createSnapshots)

当创建多卷快照的操作完成后，系统会将 createSnapshots 事件发送至您的 Amazon 账户。此事件的结果可能是 succeeded 或 failed。

事件数据

下面的列表是 EBS 为成功的 createSnapshots 事件发送的 JSON 对象示例。在 detail 部分中，source 字段包含多卷快照集的源卷的 ARN。startTime 和 endTime 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
```

```
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

下面的列表是 EBS 在 createSnapshots 事件失败后发送的 JSON 对象的示例。失败的原因是多卷快照集的一个或多个快照未能完成。snapshot_id 的值是失败的快照的 ARN。startTime 和 endTime 表示创建快照操作开始和结束的时间。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

复制快照 (copySnapshot)

当复制快照的操作完成后，系统会将 copySnapshot 事件发送至您的 Amazon 账户。不过，不会保存、记录或存档该事件。此事件的结果可能是 succeeded 或 failed。

事件数据

下面的列表是 EBS 在 copySnapshot 事件成功后发送的 JSON 对象的示例。snapshot_id 的值为新创建快照的 ARN。在 detail 部分中，source 的值为源快照的 ARN。startTime 和 endTime 表示 copy-snapshot 操作何时开始以及何时结束。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "Incremental": "true"
  }
}
```

下面的列表是 EBS 在 copySnapshot 事件失败后发送的 JSON 对象的示例。失败原因是源快照 ID 无效。snapshot_id 的值为失败快照的 ARN。在 detail 部分中，source 的值为源快照的 ARN。startTime 和 endTime 表示 copy-snapshot 操作何时开始以及何时结束。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

共享快照 (shareSnapshot)

在其他账户与您的 shareSnapshot 账户共享快照时，系统会将 Amazon 事件发送至您的该账户。不过，不会保存、记录或存档该事件。结果始终是 succeeded。

事件数据

下面是 EBS 在 shareSnapshot 事件完成后发送的 JSON 对象的示例。在 detail 部分中，source 的值是与您共享快照的用户的 Amazon 账号。startTime 和 endTime 表示 share-snapshot 操作何时开始以及何时结束。仅在与其他用户共享私有快照时，系统才会发送 shareSnapshot 事件。共享公有快照不会触发该事件。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
```

```
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

EBS 快照归档事件

Amazon EBS 发出与快照归档操作相关的事件。

EBS 快速快照还原事件

在快照的快速快照还原状态发生变化时，Amazon EBS 向 EventBridge 发送事件。尽最大努力发出事件。

以下是此事件的示例数据。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

可能的 state 值为 enabling、optimizing、enabled、disabling 和 disabled。

message 的可能值如下所示：

Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)

启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。无法为该快照启用快速快照还原。

Client.UserInitiated

状态成功转换为 enabling 或 disabling。

`Client.UserInitiated - Lifecycle state transition`

状态成功转换为 optimizing、enabled 或 disabled。

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

由于容量不足而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Server.InternalError - An internal error caused the operation to fail`

由于内部错误而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

快照的快速快照还原状态已转换为 disabling 或 disabled，因为快照已被快照所有者删除或取消共享。无法为已删除或不再与您共享的快照启用快速快照还原。

使用 Amazon Lambda 处理 EventBridge 事件

您可以使用 Amazon EBS 和 Amazon EventBridge 自动执行数据备份工作流。这需要您创建 IAM policy、用于处理事件的 Amazon Lambda 函数，以及与传入事件匹配并能将传入事件路由到 Lambda 函数的 EventBridge 规则。

以下过程使用 `createSnapshot` 事件自动将已完成的快照复制到其他区域，以用于灾难恢复。

将已完成的快照复制到其他区域

1. 创建 IAM policy（例如以下示例中显示的策略），以便提供使用 CopySnapshot 操作和写入 EventBridge 日志所需的权限。将策略分配给要处理 EventBridge 事件的用户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 在 Lambda 中定义一个可在 EventBridge 控制台中使用的函数。在 Amazon EBS 发送匹配的 `createSnapshot` 事件时（表示快照已完成），EventBridge 会调用下方在 Node.js 中编写的示例 Lambda 函数。该函数被调用后，它会将快照从 `us-east-2` 复制到 `us-east-1`。

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
```

```
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot ${snapshotId}
 to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

为确保您的 Lambda 函数在 EventBridge 控制台中可用，请在将发生 EventBridge 事件的区域中创建该函数。有关更多信息，请参见 Amazon Lambda 开发人员指南。

3. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
4. 在导航窗格中，选择 Rules (规则)，然后选择 Create rule (创建规则)。
5. 对于 Step 1: Define rule detail（步骤 1：定义规则详细信息），请执行以下操作：
   a. 为 Name（名称）和 Description（描述）输入值。
   b. 对于 Event bus（事件总线），保持 default（默认）。
   c. 确保 Enable the rule on the selected event bus（在选定的事件总线上启用该规则）已开启。
   d. 对于 Event type（事件类型），选择 Rule with an event pattern（具有事件模式的规则）。
   e. 选择 Next（下一步）。
6. 对于 Step 2: Build event pattern（步骤 2：构建事件模式），执行以下操作：
   a. 对于事件源，选择 Amazon 事件或 EventBridge 合作伙伴事件。

b. 在事件模式部分，对于事件源，请确保选择 Amazon 服务，对于 Amazon 服务，选择 EC2。
c. 对于 Event type（事件类型），选择 EBS Snapshot Notification（EBS 快照通知），选择 Specific event(s)（特定事件），然后选择 createSnapshot。
d. 选择 Specific result(s)（特定结果），然后选择 Succeeded（成功）。
e. 选择 Next（下一步）。

7. 对于 Step 3: Select targets（步骤 3：选择目标），请执行以下操作：
   a. 对于 Target types（目标类型），选择 Amazon service（服务）。
   b. 对于 Select target（选择目标），选择 Lambda function（Lambda 函数），对于 Function（函数），选择之前创建的函数。
   c. 选择 Next（下一步）。
8. 对于 Step 4: Configure tags（步骤 4：配置标签），如果需要，为规则指定标签，然后选择 Next（下一步）。
9. 对于 Step 5: Review and create（步骤 5：查看并创建），查看规则，然后选择 Create rule（创建规则）。

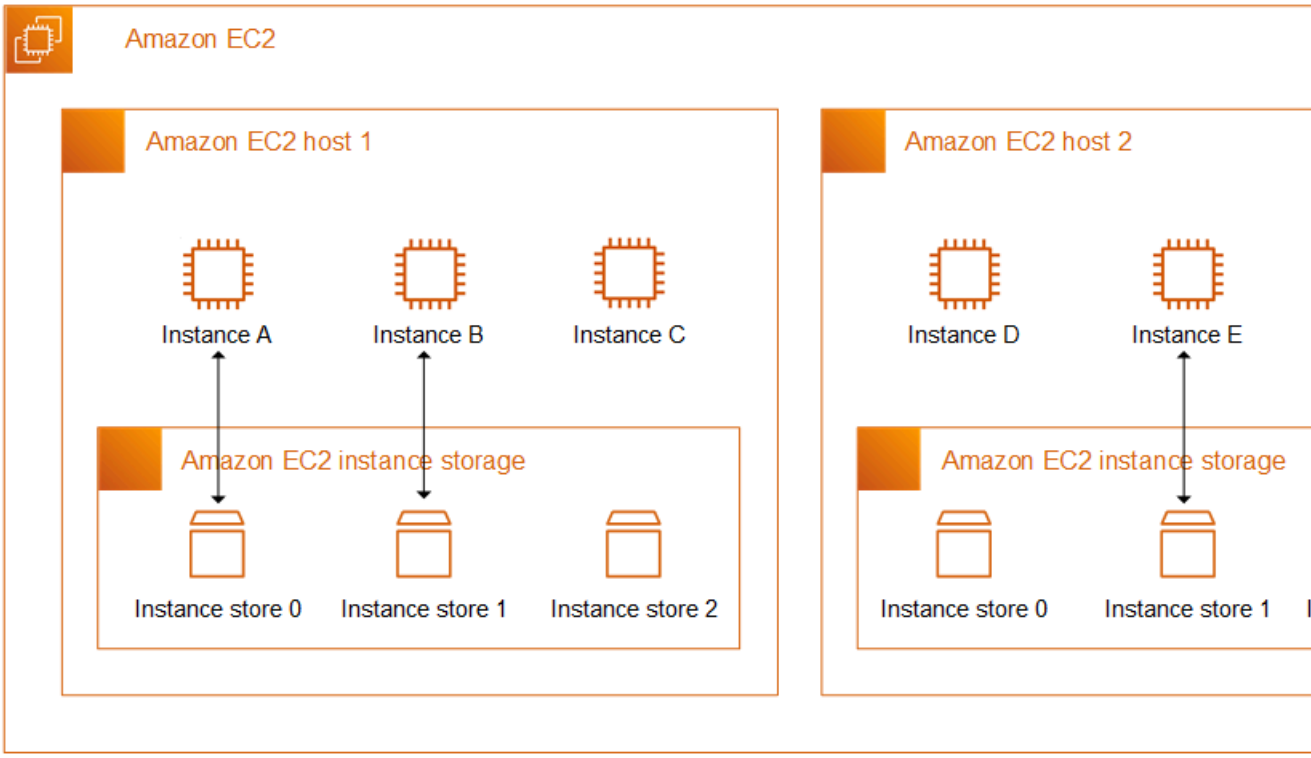
现在，您的规则应该会显示在规则选项卡中。在所示的示例中，当您下次复制快照时，EBS 应该会发送您所配置的事件。

Amazon EC2 实例存储

实例存储 为您的实例提供临时性块级存储。此存储位于已物理附加到主机的磁盘上。实例存储非常适合临时存储频繁更改的信息，例如缓冲区、缓存、Scratch 数据和其他临时内容。它还可用于存储您在一组实例中复制的临时数据，例如负载均衡的 Web 服务器池。

实例存储由一个或多个显示为块储存设备的实例存储卷组成。实例存储的大小以及可用设备的数量因实例类型而异。

实例存储卷的虚拟设备为 `ephemeral[0-23]`。支持一个实例存储卷的实例类型具有 `ephemeral0`。支持两个实例存储卷的实例类型有 `ephemeral0` 和 `ephemeral1` 等。



目录

- 实例存储生命周期 (p. 1580)
- 实例存储卷 (p. 1581)
- 将实例存储卷添加到您的 EC2 实例 (p. 1592)
- SSD 实例存储卷 (p. 1596)
- 实例存储交换卷 (p. 1597)
- 优化实例存储卷的磁盘性能 (p. 1599)

实例存储生命周期

您只能在启动实例时指定实例的实例存储卷。您无法将实例存储卷与一个实例分离并将该卷附加到另一个实例。

实例存储内的数据仅在与关联的实例的生命周期内保留。如果实例重启 (无论是故意还是意外)，实例存储内的数据都会保留下来。然而，在以下任一情况下，实例存储中的数据会丢失：

- 底层磁盘驱动器发生故障
- 实例停止
- 实例休眠
- 实例终止

因此，切勿依赖实例存储来存储珍贵且需要长期保存的数据。应使用更持久的数据存储，如 Amazon S3、Amazon EBS 或 Amazon EFS。

当您停止、休眠或终止某个实例时，实例存储中的每个存储块都会被重置。因此，无法通过另一实例的实例存储访问您的数据。

如果您从实例创建 AMI，则从此 AMI 中启动实例时，实例存储卷上的数据不能保存且不会出现在实例存储卷上。

如果更改实例类型，实例存储不会附加到新实例类型。有关更多信息，请参阅更改实例类型 (p. 399)。

实例存储卷

实例类型决定了可用的实例存储的大小以及用于实例存储卷的硬件类型。实例存储卷包含在实例使用成本中。您必须指定在启动实例时要使用的实例存储卷 (NVMe 实例存储卷除外，因为它们在默认情况下可用)。之后设置实例存储卷的格式并挂载这些卷，然后再使用这些卷。您无法在启动实例后使实例存储卷可用。有关更多信息，请参阅将实例存储卷添加到您的 EC2 实例 (p. 1592)。

某些实例类型使用基于 NVMe 或 SATA 的固态硬盘 (SSD) 来提供高随机 I/O 性能。如果您需要延迟非常低的存储，且实例终止时不需要保留数据或可以使用容错架构，则可以选择这种实例。有关更多信息，请参阅SSD 实例存储卷 (p. 1596)。

NVMe 实例存储卷和某些 HDD 实例存储卷上的数据采用静态加密。有关更多信息，请参阅Amazon EC2 中的数据保护 (p. 1221)。

可用的实例存储卷

下表列出了每种支持的实例类型可以使用的实例存储卷的数量、大小、类型和性能优化。

主题

- 通用型 (p. 1581)
- 计算优化 (p. 1583)
- 内存优化 (p. 1585)
- 存储优化 (p. 1588)
- 加速计算 (p. 1590)

通用型

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
m1.small	1 x 160 GB	HDD	✓	
m1.medium	1 x 410 GB	HDD	✓	
m1.large	2 x 420 GB	HDD	✓	
m1.xlarge	4 x 420 GB	HDD	✓	
m2.xlarge	1 x 420 GB	HDD	✓	
m2.2xlarge	1 x 850 GB	HDD	✓	
m2.4xlarge	2 x 840 GB	HDD	✓	
m3.medium	1 x 4 GB	SSD	✓	
m3.large	1 x 32 GB	SSD	✓	
m3.xlarge	2 x 40 GB	SSD	✓	
m3.2xlarge	2 x 80 GB	SSD	✓	
m5ad.large	1 x 75GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
m5ad.xlarge	1 x 150GB	NVMe SSD		✓
m5ad.2xlarge	1 x 300GB	NVMe SSD		✓
m5ad.4xlarge	2 x 300 GB	NVMe SSD		✓
m5ad.8xlarge	2 x 600 GB	NVMe SSD		✓
m5ad.12xlarge	2 x 900 GB	NVMe SSD		✓
m5ad.16xlarge	4 x 600 GB	NVMe SSD		✓
m5ad.24xlarge	4 x 900 GB	NVMe SSD		✓
m5d.large	1 x 75GB	NVMe SSD		✓
m5d.xlarge	1 x 150GB	NVMe SSD		✓
m5d.2xlarge	1 x 300GB	NVMe SSD		✓
m5d.4xlarge	2 x 300 GB	NVMe SSD		✓
m5d.8xlarge	2 x 600 GB	NVMe SSD		✓
m5d.12xlarge	2 x 900 GB	NVMe SSD		✓
m5d.16xlarge	4 x 600 GB	NVMe SSD		✓
m5d.24xlarge	4 x 900 GB	NVMe SSD		✓
m5d.metal	4 x 900 GB	NVMe SSD		✓
m5dn.large	1 x 75GB	NVMe SSD		✓
m5dn.xlarge	1 x 150GB	NVMe SSD		✓
m5dn.2xlarge	1 x 300GB	NVMe SSD		✓
m5dn.4xlarge	2 x 300 GB	NVMe SSD		✓
m5dn.8xlarge	2 x 600 GB	NVMe SSD		✓
m5dn.12xlarge	2 x 900 GB	NVMe SSD		✓
m5dn.16xlarge	4 x 600 GB	NVMe SSD		✓
m5dn.24xlarge	4 x 900 GB	NVMe SSD		✓
m5dn.metal	4 x 900 GB	NVMe SSD		✓
m6gd.medium	1 x 59 GB	NVMe SSD		✓
m6gd.large	1 x 118 GB	NVMe SSD		✓
m6gd.xlarge	1 x 237 GB	NVMe SSD		✓
m6gd.2xlarge	1 x 474 GB	NVMe SSD		✓
m6gd.4xlarge	1 x 950 GB	NVMe SSD		✓
m6gd.8xlarge	1 x 1900 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
m6gd.12xlarge	2 x 1425 GB	NVMe SSD		✓
m6gd.16xlarge	2 x 1900 GB	NVMe SSD		✓
m6gd.metal	2 x 1900 GB	NVMe SSD		✓
m6id.large	1 x 118 GB	NVMe SSD		✓
m6id.xlarge	1 x 237 GB	NVMe SSD		✓
m6id.2xlarge	1 x 474 GB	NVMe SSD		✓
m6id.4xlarge	1 x 950 GB	NVMe SSD		✓
m6id.8xlarge	1 x 1900 GB	NVMe SSD		✓
m6id.12xlarge	2 x 1425 GB	NVMe SSD		✓
m6id.16xlarge	2 x 1900 GB	NVMe SSD		✓
m6id.24xlarge	4 x 1425 GB	NVMe SSD		✓
m6id.32xlarge	4 x 1900 GB	NVMe SSD		✓
m6id.metal	4 x 1900 GB	NVMe SSD		✓
m6idn.large	1 x 118 GB	NVMe SSD		✓
m6idn.xlarge	1 x 237 GB	NVMe SSD		✓
m6idn.2xlarge	1 x 474 GB	NVMe SSD		✓
m6idn.4xlarge	1 x 950 GB	NVMe SSD		✓
m6idn.8xlarge	1 x 1900 GB	NVMe SSD		✓
m6idn.12xlarge	2 x 1425 GB	NVMe SSD		✓
m6idn.16xlarge	2 x 1900 GB	NVMe SSD		✓
m6idn.24xlarge	4 x 1425 GB	NVMe SSD		✓
m6idn.32xlarge	4 x 1900 GB	NVMe SSD		✓
m6idn.metal	4 x 1900 GB	NVMe SSD		✓

计算优化

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
c1.medium	1 x 350 GB	HDD	✓	
c1.xlarge	4 x 420 GB	HDD	✓	
c3.large	2 x 16 GB	SSD	✓	
c3.xlarge	2 x 40 GB	SSD	✓	

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
c3.2xlarge	2 x 80 GB	SSD	✓	
c3.4xlarge	2 x 160 GB	SSD	✓	
c3.8xlarge	2 x 320 GB	SSD	✓	
c5ad.large	1 x 75GB	NVMe SSD		✓
c5ad.xlarge	1 x 150GB	NVMe SSD		✓
c5ad.2xlarge	1 x 300GB	NVMe SSD		✓
c5ad.4xlarge	2 x 300 GB	NVMe SSD		✓
c5ad.8xlarge	2 x 600 GB	NVMe SSD		✓
c5ad.12xlarge	2 x 900 GB	NVMe SSD		✓
c5ad.16xlarge	2 x 1200 GB	NVMe SSD		✓
c5ad.24xlarge	2 x 1900 GB	NVMe SSD		✓
c5d.large	1 x 50GB	NVMe SSD		✓
c5d.xlarge	1 x 100GB	NVMe SSD		✓
c5d.2xlarge	1 x 200GB	NVMe SSD		✓
c5d.4xlarge	1 x 400GB	NVMe SSD		✓
c5d.9xlarge	1 x 900GB	NVMe SSD		✓
c5d.12xlarge	2 x 900 GB	NVMe SSD		✓
c5d.18xlarge	2 x 900 GB	NVMe SSD		✓
c5d.24xlarge	4 x 900 GB	NVMe SSD		✓
c5d.metal	4 x 900 GB	NVMe SSD		✓
c6gd.medium	1 x 59 GB	NVMe SSD		✓
c6gd.large	1 x 118 GB	NVMe SSD		✓
c6gd.xlarge	1 x 237 GB	NVMe SSD		✓
c6gd.2xlarge	1 x 474 GB	NVMe SSD		✓
c6gd.4xlarge	1 x 950 GB	NVMe SSD		✓
c6gd.8xlarge	1 x 1900 GB	NVMe SSD		✓
c6gd.12xlarge	2 x 1425 GB	NVMe SSD		✓
c6gd.16xlarge	2 x 1900 GB	NVMe SSD		✓
c6gd.metal	2 x 1900 GB	NVMe SSD		✓
c6id.large	1 x 118 GB	NVMe SSD		✓
c6id.xlarge	1 x 237 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
c6id.2xlarge	1 x 474 GB	NVMe SSD		✓
c6id.4xlarge	1 x 950 GB	NVMe SSD		✓
c6id.8xlarge	1 x 1900 GB	NVMe SSD		✓
c6id.12xlarge	2 x 1425 GB	NVMe SSD		✓
c6id.16xlarge	2 x 1900 GB	NVMe SSD		✓
c6id.24xlarge	4 x 1425 GB	NVMe SSD		✓
c6id.32xlarge	4 x 1900 GB	NVMe SSD		✓
c6id.metal	4 x 1900 GB	NVMe SSD		✓
cc2.8xlarge	4 x 840 GB	HDD	✓	

内存优化

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
cr1.8xlarge	2 x 120 GB	HDD	✓	
hpc6id.32xlarge	4 x 3800 GB	NVMe SSD		✓
r3.large	1 x 32 GB	SSD	✓	
r3.xlarge	1 x 80 GB	SSD	✓	
r3.2xlarge	1 x 160 GB	SSD	✓	
r3.4xlarge	1 x 320 GB	SSD	✓	
r3.8xlarge	2 x 320 GB	SSD	✓	
r5ad.large	1 x 75GB	NVMe SSD		✓
r5ad.xlarge	1 x 150GB	NVMe SSD		✓
r5ad.2xlarge	1 x 300GB	NVMe SSD		✓
r5ad.4xlarge	2 x 300 GB	NVMe SSD		✓
r5ad.8xlarge	2 x 600 GB	NVMe SSD		✓
r5ad.12xlarge	2 x 900 GB	NVMe SSD		✓
r5ad.16xlarge	4 x 600 GB	NVMe SSD		✓
r5ad.24xlarge	4 x 900 GB	NVMe SSD		✓
r5d.large	1 x 75GB	NVMe SSD		✓
r5d.xlarge	1 x 150GB	NVMe SSD		✓
r5d.2xlarge	1 x 300GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
r5d.4xlarge	2 x 300 GB	NVMe SSD		✓
r5d.8xlarge	2 x 600 GB	NVMe SSD		✓
r5d.12xlarge	2 x 900 GB	NVMe SSD		✓
r5d.16xlarge	4 x 600 GB	NVMe SSD		✓
r5d.24xlarge	4 x 900 GB	NVMe SSD		✓
r5d.metal	4 x 900 GB	NVMe SSD		✓
r5dn.large	1 x 75GB	NVMe SSD		✓
r5dn.xlarge	1 x 150GB	NVMe SSD		✓
r5dn.2xlarge	1 x 300GB	NVMe SSD		✓
r5dn.4xlarge	2 x 300 GB	NVMe SSD		✓
r5dn.8xlarge	2 x 600 GB	NVMe SSD		✓
r5dn.12xlarge	2 x 900 GB	NVMe SSD		✓
r5dn.16xlarge	4 x 600 GB	NVMe SSD		✓
r5dn.24xlarge	4 x 900 GB	NVMe SSD		✓
r5dn.metal	4 x 900 GB	NVMe SSD		✓
r6gd.medium	1 x 59 GB	NVMe SSD		✓
r6gd.large	1 x 118 GB	NVMe SSD		✓
r6gd.xlarge	1 x 237 GB	NVMe SSD		✓
r6gd.2xlarge	1 x 474 GB	NVMe SSD		✓
r6gd.4xlarge	1 x 950 GB	NVMe SSD		✓
r6gd.8xlarge	1 x 1900 GB	NVMe SSD		✓
r6gd.12xlarge	2 x 1425 GB	NVMe SSD		✓
r6gd.16xlarge	2 x 1900 GB	NVMe SSD		✓
r6gd.metal	2 x 1900 GB	NVMe SSD		✓
r6idn.large	1 x 118 GB	NVMe SSD		✓
r6idn.xlarge	1 x 237 GB	NVMe SSD		✓
r6idn.2xlarge	1 x 474 GB	NVMe SSD		✓
r6idn.4xlarge	1 x 950 GB	NVMe SSD		✓
r6idn.8xlarge	1 x 1900 GB	NVMe SSD		✓
r6idn.12xlarge	2 x 1425 GB	NVMe SSD		✓
r6idn.16xlarge	2 x 1900 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
r6idn.24xlarge	4 x 1425 GB	NVMe SSD		✓
r6idn.32xlarge	4 x 1900 GB	NVMe SSD		✓
r6idn.metal	4 x 1900 GB	NVMe SSD		✓
r6id.large	1 x 118 GB	NVMe SSD		✓
r6id.xlarge	1 x 237 GB	NVMe SSD		✓
r6id.2xlarge	1 x 474 GB	NVMe SSD		✓
r6id.4xlarge	1 x 950 GB	NVMe SSD		✓
r6id.8xlarge	1 x 1900 GB	NVMe SSD		✓
r6id.12xlarge	2 x 1425 GB	NVMe SSD		✓
r6id.16xlarge	2 x 1900 GB	NVMe SSD		✓
r6id.24xlarge	4 x 1425 GB	NVMe SSD		✓
r6id.32xlarge	4 x 1900 GB	NVMe SSD		✓
r6id.metal	4 x 1900 GB	NVMe SSD		✓
x1.16xlarge	1 x 1920 GB	SSD	✓	
x1.32xlarge	2 x 1920 GB	SSD	✓	
x2gd.medium	1 x 59 GB	NVMe SSD		✓
x2gd.large	1 x 118 GB	NVMe SSD		✓
x2gd.xlarge	1 x 237 GB	NVMe SSD		✓
x2gd.2xlarge	1 x 475 GB	NVMe SSD		✓
x2gd.4xlarge	1 x 950 GB	NVMe SSD		✓
x2gd.8xlarge	1 x 1900 GB	NVMe SSD		✓
x2gd.12xlarge	2 x 1425 GB	NVMe SSD		✓
x2gd.16xlarge	2 x 1900 GB	NVMe SSD		✓
x2gd.metal	2 x 1900 GB	NVMe SSD		✓
x2idn.16xlarge	1 x 1900 GB	NVMe SSD		✓
x2idn.24xlarge	2 x 1425 GB	NVMe SSD		✓
x2idn.32xlarge	2 x 1900 GB	NVMe SSD		✓
x2idn.metal	2 x 1900 GB	NVMe SSD		✓
x2iedn.xlarge	1 x 118 GB	NVMe SSD		✓
x2iedn.2xlarge	1 x 237 GB	NVMe SSD		✓
x2iedn.4xlarge	1 x 475 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
x2iedn.8xlarge	1 x 950 GB	NVMe SSD		✓
x2iedn.16xlarge	1 x 1900 GB	NVMe SSD		✓
x2iedn.24xlarge	2 x 1425 GB	NVMe SSD		✓
x2iedn.32xlarge	2 x 1900 GB	NVMe SSD		✓
x2iedn.metal	2 x 1900 GB	NVMe SSD		✓
x1e.xlarge	1 x 120GB	SSD	✓	
x1e.2xlarge	1 x 240GB	SSD	✓	
x1e.4xlarge	1 x 480GB	SSD	✓	
x1e.8xlarge	1 x 960GB	SSD	✓	
x1e.16xlarge	1 x 1920 GB	SSD	✓	
x1e.32xlarge	2 x 1920 GB	SSD	✓	
z1d.large	1 x 75GB	NVMe SSD		✓
z1d.xlarge	1 x 150GB	NVMe SSD		✓
z1d.2xlarge	1 x 300GB	NVMe SSD		✓
z1d.3xlarge	1 x 450GB	NVMe SSD		✓
z1d.6xlarge	1 x 900GB	NVMe SSD		✓
z1d.12xlarge	2 x 900 GB	NVMe SSD		✓
z1d.metal	2 x 900 GB	NVMe SSD		✓

存储优化

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
d2.xlarge	3 x 2048 GB	HDD	✓	
d2.2xlarge	6 x 2048 GB	HDD	✓	
d2.4xlarge	12 x 2048 GB	HDD	✓	
d2.8xlarge	24 x 2048 GB	HDD	✓	
d3.xlarge	3 x 1980 GB	NVMe HDD		✓
d3.2xlarge	6 x 1980 GB	NVMe HDD		✓
d3.4xlarge	12 x 1980 GB	NVMe HDD		✓
d3.8xlarge	24 x 1980 GB	NVMe HDD		✓
d3en.xlarge	2 x 13980 GB	NVMe HDD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
d3en.2xlarge	4 x 13980 GB	NVMe HDD		✓
d3en.4xlarge	8 x 13980 GB	NVMe HDD		✓
d3en.6xlarge	12 x 13980 GB	NVMe HDD		✓
d3en.8xlarge	16 x 13980 GB	NVMe HDD		✓
d3en.12xlarge	24 x 13980 GB	NVMe HDD		✓
h1.2xlarge	1 x 2000 GB	HDD	✓	
h1.4xlarge	2 x 2000 GB	HDD	✓	
h1.8xlarge	4 x 2000 GB	HDD	✓	
h1.16xlarge	8 x 2000 GB	HDD	✓	
hs1.8xlarge	24 x 2048 GB	HDD	✓	
i2.xlarge	1 x 800 GB	SSD	✓	
i2.2xlarge	2 x 800 GB	SSD	✓	
i2.4xlarge	4 x 800 GB	SSD	✓	
i2.8xlarge	8 x 800 GB	SSD	✓	
i3.large	1 x 475 GB	NVMe SSD		✓
i3.xlarge	1 x 950 GB	NVMe SSD		✓
i3.2xlarge	1 x 1900 GB	NVMe SSD		✓
i3.4xlarge	2 x 1900 GB	NVMe SSD		✓
i3.8xlarge	4 x 1900 GB	NVMe SSD		✓
i3.16xlarge	8 x 1900 GB	NVMe SSD		✓
i3.metal	8 x 1900 GB	NVMe SSD		✓
i3en.large	1 x 1250 GB	NVMe SSD		✓
i3en.xlarge	1 x 2500 GB	NVMe SSD		✓
i3en.2xlarge	2 x 2500 GB	NVMe SSD		✓
i3en.3xlarge	1 x 7500 GB	NVMe SSD		✓
i3en.6xlarge	2 x 7500 GB	NVMe SSD		✓
i3en.12xlarge	4 x 7500 GB	NVMe SSD		✓
i3en.24xlarge	8 x 7500 GB	NVMe SSD		✓
i3en.metal	8 x 7500 GB	NVMe SSD		✓
i4i.large	1 x 468 GB	NVMe SSD		✓
i4i.xlarge	1 x 937 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
i4i.2xlarge	1 x 1875 GB	NVMe SSD		✓
i4i.4xlarge	1 x 3750 GB	NVMe SSD		✓
i4i.8xlarge	2 x 3750 GB	NVMe SSD		✓
i4i.16xlarge	4 x 3750 GB	NVMe SSD		✓
i4i.32xlarge	8 x 3750 GB	NVMe SSD		✓
i4i.metal	8 x 3750 GB	NVMe SSD		✓
im4gn.large	1 x 937 GB	NVMe SSD		✓
im4gn.xlarge	1 x 1875 GB	NVMe SSD		✓
im4gn.2xlarge	1 x 3750 GB	NVMe SSD		✓
im4gn.4xlarge	1 x 7500 GB	NVMe SSD		✓
im4gn.8xlarge	2 x 7500 GB	NVMe SSD		✓
im4gn.16xlarge	4 x 7500 GB	NVMe SSD		✓
is4gen.medium	1 x 937 GB	NVMe SSD		✓
is4gen.large	1 x 1875 GB	NVMe SSD		✓
is4gen.xlarge	1 x 3750 GB	NVMe SSD		✓
is4gen.2xlarge	1 x 7500 GB	NVMe SSD		✓
is4gen.4xlarge	2 x 7500 GB	NVMe SSD		✓
is4gen.8xlarge	4 x 7500 GB	NVMe SSD		✓

加速计算

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
dl1.24xlarge	4 x 1000 GB	NVMe SSD		✓
f1.2xlarge	1 x 470GB	NVMe SSD		✓
f1.4xlarge	1 x 940 GB	NVMe SSD		✓
f1.16xlarge	4 x 940 GB	NVMe SSD		✓
g2.2xlarge	1 x 60 GB	SSD	✓	
g2.8xlarge	2 x 120 GB	SSD	✓	
g4ad.xlarge	1 x 150GB	NVMe SSD		✓
g4ad.2xlarge	1 x 300GB	NVMe SSD		✓
g4ad.4xlarge	1 x 600 GB	NVMe SSD		✓

实例类型	实例存储卷	类型	需要初始化*	TRIM 支持**
g4ad.8xlarge	1 x 1200 GB	NVMe SSD		✓
g4ad.16xlarge	2 x 1200 GB	NVMe SSD		✓
g4dn.xlarge	1 x 125 GB	NVMe SSD		✓
g4dn.2xlarge	1 x 225 GB	NVMe SSD		✓
g4dn.4xlarge	1 x 225 GB	NVMe SSD		✓
g4dn.8xlarge	1 x 900GB	NVMe SSD		✓
g4dn.12xlarge	1 x 900GB	NVMe SSD		✓
g4dn.16xlarge	1 x 900GB	NVMe SSD		✓
g4dn.metal	2 x 900 GB	NVMe SSD		✓
g5.xlarge	1 x 250 GB	NVMe SSD		✓
g5.2xlarge	1 x 450GB	NVMe SSD		✓
g5.4xlarge	1 x 600 GB	NVMe SSD		✓
g5.8xlarge	1 x 900GB	NVMe SSD		✓
g5.12xlarge	1 x 3800 GB	NVMe SSD		✓
g5.16xlarge	1 x 1900 GB	NVMe SSD		✓
g5.24xlarge	1 x 3800 GB	NVMe SSD		✓
g5.48xlarge	2 x 3800 GB	NVMe SSD		✓
p3dn.24xlarge	2 x 900 GB	NVMe SSD		✓
p4d.24xlarge	8 x 1000 GB	NVMe SSD		✓
p4de.24xlarge	8 x 1000 GB	NVMe SSD		✓
trn1.2xlarge	1 x 474 GB	NVMe SSD		✓
trn1.32xlarge	4 x 1900 GB	NVMe SSD		✓

* 如果附加到特定实例的卷没有初始化，将会进行初始写入。有关更多信息，请参阅 优化实例存储卷的磁盘性能 (p. 1599)。

** 有关更多信息，请参阅 实例存储卷 TRIM 支持 (p. 1597)。

† c1.medium 和 m1.small 实例类型还包括一个不会在启动时自动启用的 900MB 实例存储交换卷。有关更多信息，请参阅实例存储交换卷 (p. 1597)。

实例存储卷的性能

以下文档说明了实例存储卷的 I/O 性能。

- 通用实例 (p. 271)
- 计算优化型实例 (p. 319)
- 内存优化型实例 (p. 342)

- 存储优化型实例 (p. 354)
- 加速计算实例 (p. 367)

使用 Amazon CLI 查询实例存储卷信息

您可以使用 describe-instance-types Amazon CLI 命令来显示有关实例类型的信息，例如其实例存储卷。以下示例显示了包含实例存储卷的所有 R5 实例的实例存储总大小。

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-supported,Values=true"
 \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

输出示例

```
--------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r5ad.24xlarge |  3600  |
|  r5ad.12xlarge |  1800  |
|  r5dn.8xlarge  |  1200  |
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

以下示例显示指定实例类型的完整实例存储详细信息。

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

示例输出显示，此实例类型有两个 300 GB 的 NVMe SSD 卷，总共 600 GB 的实例存储空间。

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

将实例存储卷添加到您的 EC2 实例

使用块储存设备映射为您的实例指定 EBS 卷和实例存储卷。块储存设备映射中的每个条目均包括设备名称和映射到其上的卷。默认块储存设备映射由使用的 AMI 指定。或者，您可在启动实例时为实例指定块储存设备映射。

某个实例类型支持的所有 NVMe 实例存储卷将在实例启动时自动枚举并为其分配设备名称；将这些卷包含在 AMI 或实例的块储存设备映射中不起作用。有关更多信息，请参阅块设备映射 (p. 1615)。

块储存设备映射始终指定实例的根卷。根卷是一个 Amazon EBS 卷或实例存储卷。有关更多信息，请参阅根设备存储 (p. 103)。将自动挂载根卷。对于根卷的具有实例存储卷的实例，该卷的大小因 AMI 而异，但最大大小为 10 GB。

您可在启动实例时使用块储存设备映射来指定额外的 EBS 卷，或者可在实例运行后附加额外的 EBS 卷。有关更多信息，请参阅Amazon EBS 卷 (p. 1324)。

您只能在启动实例时为其指定实例存储卷。无法在启动实例后将实例存储卷附加到该实例。

如果更改实例类型，实例存储不会附加到新实例类型。有关更多信息，请参阅更改实例类型 (p. 399)。

对您的实例可用的实例存储卷的数量和大小因实例类型而异。一些实例类型不支持实例存储卷。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他卷将被忽略。有关每种实例类型支持的实例存储卷的更多信息，请参阅实例存储卷 (p. 1581)。

如果为您的实例选择的实例类型支持非 NVMe 实例存储卷，则您必须在启动实例时将这些卷添加到实例的块储存设备映射。NVMe 实例存储卷在默认情况下是可用的。在启动实例后，您必须先确保已格式化和挂载实例的实例存储卷，然后才能使用这些存储卷。将自动挂载实例存储支持的实例的根卷。

目录

- 将实例存储卷添加到 AMI (p. 1593)
- 将实例存储卷添加到实例 (p. 1594)
- 使实例存储卷在您的实例上可用 (p. 1595)

将实例存储卷添加到 AMI

您可创建带包括实例存储卷的块储存设备映射的 AMI。如果使用支持实例存储卷的实例类型和在其块储存设备映射中指定实例存储卷的 AMI 启动一个实例，则该实例包括这些实例存储卷。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他实例存储卷将被忽略。

注意事项

- 对于 M3 实例，请在实例的块储存设备映射中指定实例存储卷，而非 AMI。Amazon EC2 可能会忽略仅在 AMI 的块储存设备映射中指定的实例存储卷。
- 启动实例时，可忽略 AMI 块储存设备映射中指定的非 NVMe 实例存储卷，或添加实例存储卷。

New console

使用控制台向 Amazon EBS-backed AMI 添加实例存储卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions (操作)、Image and templates (映像和模板) 和 Create Image (创建映像)。
4. 在 Create image (创建映像) 页面，为您的映像添加一个有意义的名称和描述。
5. 对于要添加的每个实例存储卷，选择 Add New Volume (添加新卷)，从 Volume Type (卷类型) 中选择实例存储卷，并从 Device (设备) 中选择设备名称。（有关更多信息，请参阅 Linux 实例上的设备名称 (p. 1614)。）可用的实例存储卷数量取决于实例类型。对于具有 NVMe 实例存储卷的实例，这些卷的设备映射取决于操作系统枚举这些卷的顺序。
6. 选择创建映像。

Old console

使用控制台向 Amazon EBS-backed AMI 添加实例存储卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Image 和 Create Image。
4. 在 Create Image 对话框中，为您的映像键入有意义的名称和描述。
5. 对于要添加的每个实例存储卷，选择 Add New Volume，从 Volume Type 中选择实例存储卷，并从 Device 中选择设备名称。（有关更多信息，请参阅 Linux 实例上的设备名称 (p. 1614)。）可用的实例存储卷数量取决于实例类型。对于具有 NVMe 实例存储卷的实例，这些卷的设备映射取决于操作系统枚举这些卷的顺序。
6. 选择 Create Image。

使用命令行向 AMI 添加实例存储卷

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- create-image 或 register-image (Amazon CLI)
- New-EC2Image 和 Register-EC2Image (Amazon Tools for Windows PowerShell)

将实例存储卷添加到实例

启动实例时，指定的 AMI 将提供默认块储存设备映射。如果需要额外的实例存储卷，您必须在启动实例时将这些卷添加到实例。您还可忽略 AMI 块储存设备映射中指定的设备。

注意事项

- 对于 M3 实例，即使您未在实例的块储存设备映射中指定实例存储卷，您也可能收到这些卷。
- 对于 HS1 实例，无论您在 AMI 的块储存设备映射中指定了多少个实例存储卷，从 AMI 中启动的实例的块储存设备映射都会自动包括最大数目的支持的实例存储卷。您必须先从块储存设备映射中显式删除不需要的实例存储卷，然后再启动该映射。

使用控制台更新实例的块储存设备映射

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择启动实例。
3. 在 Application and OS Images（应用程序和操作系统映像）部分中，请选择要使用的 AMI。
4. 在配置存储部分中，实例存储卷部分列出了可附加到实例的实例存储卷。可用的实例存储卷数量取决于实例类型。
5. 对于要附加的每个实例存储卷，对于设备名称，选择要使用的设备名称。
6. 根据需要配置剩余的实例设置，然后选择启动实例。

使用命令行更新实例的块储存设备映射

您可将下列选项命令之一与对应的命令结合使用。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- `--block-device-mappings` 与 run-instances (Amazon CLI)
- 带 New-EC2Instance 的 `-BlockDeviceMapping` (Amazon Tools for Windows PowerShell)

使实例存储卷在您的实例上可用

启动实例后，该实例可使用实例存储卷，但是必须先挂载该卷，然后再使用。对于 Linux 实例，实例类型决定应为您挂载哪种实例存储卷，以及哪些存储卷可由您自行挂载。对于 Windows 实例，EC2Config 服务可为实例挂载实例存储卷。该实例的块储存设备驱动程序会在挂载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 建议的名称不同。

很多实例存储卷都预先经过 ext3 文件系统的格式化处理。支持 TRIM 指令的基于 SSD 的实例存储卷不会预先经过任何文件系统的格式化处理。然而，您可以在启动实例后，使用您选择的文件系统将卷格式化。有关更多信息，请参阅实例存储卷 TRIM 支持 (p. 1597)。对于 Windows 实例，EC2Config 服务可利用 NTFS 文件系统重新格式化实例存储卷。

您可以确认，可以从使用自身元数据的实例内使用实例存储设备。有关更多信息，请参阅查看实例存储卷的实例块储存设备映射 (p. 1622)。

对于 Windows 实例，您还可以使用 Windows 磁盘管理来查看实例存储卷。有关更多信息，请参阅使用 Windows 磁盘管理列出磁盘。

对于 Linux 实例，您可按照以下过程所述操作来查看和挂载实例存储卷。

使实例存储卷在 Linux 上可用

1. 使用 SSH 客户端连接到实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 使用 `df -h` 命令查看已格式化并挂载的卷。

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. 使用 `lsblk` 查看在启动时已映射但未格式化和装载的所有卷。

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. 要格式化并挂载仅映射的实例存储卷，请执行以下操作：
   a. 使用 `mkfs` 命令在设备上创建文件系统。

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/nvme1n1
```

   b. 使用 `mkdir` 命令创建要将设备挂载到的目录。

```
[ec2-user ~]$ sudo mkdir /data
```

   c. 使用 `mount` 命令在新建目录上挂载设备。

```
[ec2-user ~]$ sudo mount /dev/nvme1n1 /data
```

有关如何在重新启动后自动装载已连接的卷的说明，请参阅重启后自动挂载附加的卷 (p. 1350)。

SSD 实例存储卷

为确保 Linux 上的您的 SSD 实例存储卷实现最佳 IOPS 性能，我们建议您使用 Amazon Linux 的最新版本，或者内核版本为 3.8 或更高版本的其他 Linux AMI。如果您使用的 Linux AMI 的内核版本不是 3.8 或更高版本，则您的实例将无法实现这些实例类型可获得的最大 IOPS 性能。

像其他实例存储卷一样，您必须在启动实例时为其映射 SSD 实例存储卷。SSD 实例卷上的数据仅在其关联实例的生命周期内保留。有关更多信息，请参阅将实例存储卷添加到您的 EC2 实例 (p. 1592)。

NVMe SSD 卷

有些实例提供符合非易失性存储器规范 (NVMe) 的固态硬盘 (SSD) 实例存储卷。有关每种实例类型支持的实例存储卷类型的更多信息，请参阅实例存储卷 (p. 1581)。

要访问 NVMe 卷，必须安装 NVMe 驱动程序 (p. 1518)。以下 AMI 满足此要求：

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 或更高版本（采用 `linux-aws` 内核）

  Note

  Amazon 基于 Graviton 的实例类型需要 Ubuntu 18.04 或更高版本（采用 `linux-aws` 内核）
- Red Hat Enterprise Linux 7.4 或更高版本
- SUSE Linux Enterprise Server 12 SP2 或更高版本
- CentOS 7.4.1708 或更高版本
- FreeBSD 11.1 或更高版本
- Debian GNU/Linux 9 或更高版本

- Bottlerocket

连接到实例后，您可以使用 lspci 命令列出 NVMe 设备。以下是支持 4 台 NVMe 设备的 `i3.8xlarge` 实例的示例输出。

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

如果您使用了受支持的操作系统但未看到 NVMe 设备，请使用以下命令验证是否已加载 NVMe 模块。

- Amazon Linux、Amazon Linux 2、Ubuntu 14/16、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、CentOS 7

```
$ lsmod | grep nvme
```

```
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmem/nvmem_core.ko
```

NVMe 卷符合 NVMe 1.0e 规范。您可以对 NVMe 卷使用 NVMe 命令。利用 Amazon Linux，您可以使用 `nvme-cli` 命令从存储库安装 yum install 程序包。利用其他受支持的 Linux 版本，您可以下载 `nvme-cli` 包 (如果包在映像中不可用)。

NVMe 实例存储上的数据是使用在实例上的硬件模块中实施的 XTS-AES-256 数据块密码加密的。加密密钥是使用硬件模块生成的，并且对每台 NVMe 实例存储设备都是唯一的。当实例停止或终止并且无法恢复时，将销毁所有加密密钥。无法禁用此加密，并且无法提供自己的加密密钥。

非 NVMe SSD 卷

以下实例支持使用非 NVMe SSD 来提供高随机 /O 性能的实例存储卷：C3、G2、I2、I3、M3、R3 和 X1。有关每种实例类型支持的实例存储卷的更多信息，请参阅实例存储卷 (p. 1581)。

实例存储卷 TRIM 支持

某些实例类型支持带有 TRIM 的 SSD 卷。有关更多信息，请参阅实例存储卷 (p. 1581)。

支持 TRIM 的实例存储卷先经全面删减，然后再分配到您的实例。这些卷在实例启动时未经过文件系统的格式化处理，因此，您必须先进行格式化，而后才能挂载和使用。为了更快地访问这些卷，您在格式化它们时应跳过 TRIM 操作。

利用支持 TRIM 的实例存储卷，您可在不再需要已写入的数据时使用 TRIM 命令告知 SSD 控制器此情况。这将为控制器提供更多可用空间，从而可以减少写入放大的影响并提高性能。在 Linux 上，使用 `fstrim` 命令启用定期 TRIM。

实例存储交换卷

当系统所需内存超过实际分配内存时，可以在 Linux 中使用交换空间。启用交换空间后，Linux 系统可以将很少使用的内存页面从物理内存交换至交换空间 (现有文件系统中的专用分区或交换文件)，并为需要高速访问的内存页面释放空间。

> **Note**
>
> 使用交换空间进行内存分页并不像使用 RAM 那样快速高效。如果您的工作负载定期将内存分页为交换空间，您应考虑迁移到具有更多 RAM 的较大实例类型。有关更多信息，请参阅更改实例类型 (p. 399)。

`c1.medium` 和 `m1.small` 实例类型的可用物理内存数量有限，且启动时作为 Linux AMIs 虚拟内存的是 900 MiB 交换卷。尽管 Linux 内核将此交换空间看作根设备的一部分，但是它实际上是一个独立的实例存储卷，与根设备的类型无关。

Amazon Linux 可以自动启用和使用此交换空间，但是您的 AMI 可能需要一些额外的步骤来识别和使用此交换空间。要查看您的实例是否正在使用交换空间，可以使用 swapon -s 命令。

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
```

```
/dev/xvda3                              partition       917500  0       -1
```

上述实例拥有一个已附加并启用的 900 MiB 交换卷。如果您没有通过该命令看到列出的交换卷，则可能需要启用该设备的交换空间。使用 lsblk 命令检查您的可用磁盘。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

在这里，交换卷 xvda3 对该实例可用，但是尚未启用 (请注意 MOUNTPOINT 字段为空)。您可以使用 swapon 命令启用交换卷。

> **Note**
>
> 您必须在 /dev/ 列出的设备名称前加上 lsblk。设备的命名可以不同，例如 sda3、sde3 或 xvde3。在以下命令中使用系统的设备名称。

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

现在交换空间应该显示在 lsblk 和 swapon -s 输出中。

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

您还需要编辑您的 /etc/fstab 文件，以便在每次系统启动时自动启用此交换空间。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

将以下行附加到您的 /etc/fstab 文件中 (使用系统的交换设备名称)：

```
/dev/xvda3       none    swap    sw  0       0
```

使用实例存储卷作为交换空间

所有实例存储卷都可用作交换空间。例如，m3.medium 实例类型包含一个适用于交换空间的 4 GB SSD 实例存储卷。如果您的实例存储卷大很多 (例如 350GB)，则可以考虑将卷分区为一个较小的 4-8GB 交换分区，其余部分用作数据卷。

> **Note**
>
> 此过程仅适用于支持实例存储的实例类型。有关受支持实例类型的列表，请参阅实例存储卷 (p. 1581)。

1. 列出附加到您的实例的块储存设备以获取实例存储卷的设备名称。

   ```
   [ec2-user ~]$ lsblk -p
   NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   /dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
   /dev/xvda1 202:1    0   8G  0 disk /
   ```

在此示例中，实例存储卷为 /dev/xdvb。因为这是 Amazon Linux 实例，所以实例存储卷在 /media/ephemeral0 处格式化并挂载；并不是所有 Linux 操作系统都自动执行这一操作。

2. （可选）如果您挂载了实例存储卷（它将在 MOUNTPOINT 命令输出中列出 lsblk），您需要使用以下命令卸载它。

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. 使用 mkswap 命令在设备上设置一个 Linux 交换区域。

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. 启用新的交换空间。

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. 验证所使用的新交换空间。

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. 编辑您的 /etc/fstab 文件，以在每次系统启动时自动启用此交换空间。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

如果您的 /etc/fstab 文件拥有 /dev/xvdb (或 /dev/sdb) 条目，请将其更改为与下面的行匹配；如果没有针对此设备的条目，请将以下行附加到您的 /etc/fstab 文件 (使用您系统的交换设备名称)：

```
/dev/xvdb       none    swap    sw  0       0
```

Important

当实例停止或休眠后，实例存储卷数据将丢失；这包括在Step 3 (p. 1599)中创建的实例存储交换空间格式设置。如果您停止并重新启动已配置为使用实例存储交换空间的实例，则必须在新的实例存储卷上重复 Step 1 (p. 1598) 到 Step 5 (p. 1599)。

优化实例存储卷的磁盘性能

由于 Amazon EC2 采用特殊方式将磁盘虚拟化，所以第一次在部分实例存储卷上执行写入操作的速度会比之后的写入操作慢。对于大部分应用程序，可将此成本分摊到实例的整个使用期限。然而，如果您需要较高的磁盘性能，我们建议您在生产使用之前对每个磁盘位置执行一次性写入操作，以此来实现硬盘初始化。

Note

某些实例类型使用直接附加的固态硬盘 (SSD) 并支持 TRIM，可以在启动时提供最大性能，且无需初始化。有关每种实例类型的实例存储的信息，请参阅实例存储卷 (p. 1581)。

如果您需要在延迟或吞吐量方面具有更大灵活性，我们建议您使用 Amazon EBS。

要初始化实例存储卷，请使用以下 dd 命令，具体取决于要初始化的存储 (如 /dev/sdb 或 /dev/nvme1n1)。

Note

请确保先卸载硬盘，然后再执行该命令。
初始化可能需要很长一段时间 (对于超大型实例，约为 8 小时)。

要将实例存储卷初始化，可使用 m1.large、m1.xlarge、c1.xlarge、m2.xlarge、m2.2xlarge 和 m2.4xlarge 实例类型上的以下命令：

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

要同时对所有实例存储卷执行初始化，可使用以下命令：

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

配置硬盘以便通过对每个硬盘位置执行写入操作对其执行 RAID 初始化。当配置基于软件的 RAID 时，请务必更改最低重建速度：

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

文件存储

云文件存储是一种在云中存储数据的方法，允许服务器和应用程序通过共享文件系统访问数据。这种兼容性使得云文件存储非常适合依赖共享文件系统的工作负载，并且实现了无需更改代码的简单集成。

现在有许多文件存储解决方案，从使用块存储作为基础的计算实例上的单节点文件服务器（没有扩展性或冗余来保护数据），到自助集群解决方案，再到完全托管的解决方案，不一而足。以下内容介绍了一些由 Amazon 提供的用于与 Linux 一起使用的存储服务。

目录

- 将 Amazon S3 与 Amazon EC2 结合使用 (p. 1600)
- 将 Amazon EFS 与 Amazon EC2 结合使用 (p. 1602)
- 将 Amazon FSx 与 Amazon EC2 结合使用 (p. 1603)

将 Amazon S3 与 Amazon EC2 结合使用

Amazon S3 是一个面向互联网数据的存储库。Amazon S3 为您提供了可靠、快捷的廉价数据存储基础设施。它的设计理念是通过支持您随时从 Amazon EC2 内部或从网络上的任何地方存储和检索任何数量的数据，从而简化整个网络计算。Amazon S3 以冗余方式跨多个设施在多个设备上存储数据对象，允许很多不同的客户端或应用程序线程同时对这些数据对象进行读或写操作。您可以使用存储在 Amazon S3 中的冗余数据快速、可靠地恢复实例或应用程序故障。

Amazon EC2 使用 Amazon S3 来存储 Amazon Machine Image (AMI)。您可以使用 AMI 启动 EC2 实例。万一实例发生故障，您可以使用已存储的 AMI 立即启动其他实例，从而实现快速故障恢复和确保业务的连续性。

Amazon EC2 还使用 Amazon S3 来存储数据卷的快照（备份副本）。在应用程序或系统发生故障的情况下，您可以使用快照来快速、可靠地恢复数据。您也可以将快照用作基准来创建多个数据卷，扩展现有数据

卷的大小，或者跨多个可用区移动数据，因此使您的数据使用具有高度的可扩展性。有关使用数据卷和快照的更多信息，请参阅 Amazon Elastic Block Store (p. 1323)。

数据元是 Amazon S3 中存储的基础实体。Amazon S3 中存储的每个对象都包含在存储桶中。存储桶在最高级别上组织管理 Amazon S3 命名空间，并指定负责该存储的账户。Amazon S3 存储桶类似于互联网域名。存储在存储桶中的对象具有唯一的密钥值，可以使用 URL 进行检索。举例来说，如果密钥值为 `/photos/mygarden.jpg` 的对象存储在 *`DOC-EXAMPLE-BUCKET1`* 存储桶中，则可使用 URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg` 对该对象进行寻址。

有关 Amazon S3 功能的更多信息，请参阅 Amazon S3 产品页。

用法示例

凭借 Amazon S3 的存储优势，您可以选择使用此服务存储文件和数据集以用于 EC2 实例。有几种方法可在 Amazon S3 和您的实例间移动数据。除下面所讨论的示例外，您还可以使用其他人编写的各种工具从您的计算机或实例访问您在 Amazon S3 中的数据。Amazon 论坛中对其中一些常见工具进行了讨论。

如果您有权限，就可以使用以下某种方法在 Amazon S3 和您的实例之间复制文件。

GET 或 wget

> **Note**
>
> 此方法仅适用于公有对象。如果对象不是公有的，您会收到 `ERROR 403: Forbidden` 消息。如果您收到此错误，您必须使用 Amazon S3 控制台、Amazon CLI、Amazon API、Amazon 开发工具包或 Amazon Tools for Windows PowerShell，并且您必须拥有所需的权限。有关更多信息，请参阅 Amazon S3 用户指南中的 Amazon S3 中的 Identity and Access Management 和下载对象。

wget 实用工具是 HTTP 和 FTP 客户端，可用于从 Amazon S3 下载公用对象。该实用工具在 Amazon Linux 和大多数其他分发版中均为默认安装，可在 Windows 上下载安装。要下载 Amazon S3 对象，请使用以下命令（替换要下载的对象的 URL）。

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

Amazon Command Line Interface

Amazon Command Line Interface (Amazon CLI) 是用于管理 Amazon 服务的统一工具。Amazon CLI 能让用户对自己进行身份验证，从 Amazon S3 下载受限制的项目和上载项目。有关更多信息（例如如何安装和配置这些工具），请参阅 Amazon Command Line Interface 详细信息页。

aws s3 cp 命令与 Unix cp 命令类似。您可以将文件从 Amazon S3 复制到您的实例，从您的实例复制到 Amazon S3，可以将文件在不同 Amazon S3 位置之间复制。

使用以下命令可将一个对象从 Amazon S3 复制到您的实例。

```
[ec2-user ~]$ aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

使用以下命令可将一个对象从您的实例重新复制到 Amazon S3。

```
[ec2-user ~]$ aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

aws s3 sync 命令可以将整个 Amazon S3 存储桶同步到本地目录位置。这可以用于下载数据集并使本地副本随远程集保持更新。如果您对 Amazon S3 存储桶拥有合适权限，则当您最后在命令中将源与目标位置反转时，可以将本地目录备份推送到云。

使用以下命令可将整个 Amazon S3 存储桶下载到实例上的本地目录。

```
[ec2-user ~]$ aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

如果您是一名开发人员，则可以使用 API 访问 Amazon S3 中的数据。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南。您可以使用此 API 及其示例帮助开发应用程序，可将其与其他 API 和 SDK (如 boto Python 接口) 集成。

将 Amazon EFS 与 Amazon EC2 结合使用

Amazon EFS 提供可扩展文件存储以供和 Amazon EC2 一起使用。您可以使用 EFS 文件系统作为在多个实例上运行的工作负载和应用程序的通用数据源。有关更多信息，请参阅Amazon Elastic File System产品页。

有关如何使用 Amazon EFS 控制台创建文件系统的教程，请参阅 Amazon Elastic File System User Guide（《Amazon File System 用户指南》）中的 Getting started with Amazon Elastic File System（Amazon Elastic File System 入门）。

> **Important**
>
> Amazon EFS 在 Windows 实例上不受支持。

主题

- 测试 EFS 文件系统 (p. 1602)
- 删除 EFS 文件系统 (p. 1603)

测试 EFS 文件系统

您可以连接到实例并验证文件系统是否已挂载到您指定的目录（例如，/mnt/efs）。

验证文件系统是否已装载

1. 连接到您的实例。有关更多信息，请参阅连接到您的 Linux 实例 (p. 644)。
2. 从每个实例的终端窗口，运行 df -T 命令以验证是否已挂载 EFS 文件系统。

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

请注意，文件系统的名称（在示例输出中显示为 *efs-dns*）具有以下格式。

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. （可选）在该实例的文件系统中创建文件，然后验证您是否可以从另一实例查看该文件。

   a. 在该实例中，运行以下命令来创建文件。

   ```
   $ sudo touch /mnt/efs/test-file.txt
   ```

   b. 在另一个实例中，运行以下命令来查看文件。

   ```
   $ ls /mnt/efs
   test-file.txt
   ```

删除 EFS 文件系统

如果您不再需要文件系统，可将其删除。

删除文件系统

1. 访问 https://console.aws.amazon.com/efs/，打开 Amazon Elastic File System 控制台。
2. 选择要删除的文件系统。
3. 选择 Actions、Delete file system。
4. 当系统提示您确认时，输入文件系统 ID 并选择删除文件系统。

将 Amazon FSx 与 Amazon EC2 结合使用

借助 Amazon FSx 系列服务，可以轻松启动、运行和扩缩由常见的商业和开源文件系统提供支持的共享存储。您可以使用新的启动实例向导在启动时自动将以下类型的 Amazon FSx 文件系统附加到您的 Amazon EC2 实例：

- Amazon FSx for NetApp ONTAP 使用 NetApp ONTAP 的常见数据访问和管理功能在 Amazon 云中提供完全托管式共享存储。
- Amazon FSx for OpenZFS 提供了由常见 OpenZFS 文件系统提供支持的完全托管的、经济高效的共享存储。

> Note
>
> - 此功能仅在新启动实例向导中可用。有关更多信息，请参阅 使用新启动实例向导启动实例 (p. 575)
> - 启动时无法挂载 Amazon FSx for Windows File Server 和 Amazon FSx for Lustre 文件系统。启动后必须手动挂载这些文件系统。

您可以选择挂载先前创建的现有文件系统，也可以创建一个新的文件系统以在启动时挂载到实例。

主题

- 安全组和用户数据脚本 (p. 1603)
- 在启动时挂载 Amazon FSx 文件系统 (p. 1606)

安全组和用户数据脚本

当您使用启动实例向导将 Amazon FSx 文件系统挂载到实例时，您可以选择是否自动创建和附加启用对文件系统的访问所需的安全组，以及是否自动包含挂载文件系统和使其可用所需的用户数据脚本。

主题

- 安全组 (p. 1603)
- 用户数据脚本 (p. 1605)

安全组

如果您选择自动创建启用对文件系统的访问所需的安全组，启动实例向导将创建并附加两个安全组 - 一个安全组附加到实例，另一个安全组附加到文件系统。有关安全组要求的更多信息，请参阅使用 Amazon VPC 进行 FSx for ONTAP 文件系统访问控制和使用 Amazon VPC 进行 FSx for OpenZFS 文件系统访问控制。

已创建并附加到实例的安全组被标记为 `Name=instance-sg-1`，它包括以下入站和出站规则：

Note

Name 标签中的值在启动实例向导每次为 Amazon FSx 文件系统创建新的安全组时都会自动递增。

入站规则		
No inbound rules		
出站规则		
协议类型	端口号	目的地
UDP	111	File system security group (fsx-sg-*1*)
UDP	20001 - 20003	File system security group (fsx-sg-*1*)
UDP	4049	File system security group (fsx-sg-*1*)
UDP	2049	File system security group (fsx-sg-*1*)
UDP	635	File system security group (fsx-sg-*1*)
UDP	4045 - 4046	File system security group (fsx-sg-*1*)
TCP	4049	File system security group (fsx-sg-*1*)
TCP	635	File system security group (fsx-sg-*1*)
TCP	2049	File system security group (fsx-sg-*1*)
TCP	111	File system security group (fsx-sg-*1*)
TCP	4045 - 4046	File system security group (fsx-sg-*1*)
TCP	20001 - 20003	File system security group (fsx-sg-*1*)
All	All	File system security group (fsx-sg-*1*)

已创建并附加到文件系统的安全组被标记为 Name=fsx-sg-*1*，它包括以下入站和出站规则：

Note

Name 标签中的值在启动实例向导每次为 Amazon FSx 文件系统创建新的安全组时都会自动递增。

入站规则		
协议类型	端口号	源

UDP	2049	Instance security group (`instance-sg-1`)
UDP	20001 - 20003	Instance security group (`instance-sg-1`)
UDP	4049	Instance security group (`instance-sg-1`)
UDP	111	Instance security group (`instance-sg-1`)
UDP	635	Instance security group (`instance-sg-1`)
UDP	4045 - 4046	Instance security group (`instance-sg-1`)
TCP	4045 - 4046	Instance security group (`instance-sg-1`)
TCP	635	Instance security group (`instance-sg-1`)
TCP	2049	Instance security group (`instance-sg-1`)
TCP	4049	Instance security group (`instance-sg-1`)
TCP	20001 - 20003	Instance security group (`instance-sg-1`)
TCP	111	Instance security group (`instance-sg-1`)
出站规则		
协议类型	端口号	目的地
All	All	0.0.0.0/0

用户数据脚本

如果您选择自动附加用户数据脚本，启动实例向导会将以下用户数据添加到实例。此脚本安装必要的软件包、挂载文件系统并更新您的实例设置，以便在实例重新启动时，文件系统将自动重新挂载。

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
```

```
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0 0\n"
 >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

在启动时挂载 Amazon FSx 文件系统

要在启动时挂载新的或现有的 Amazon FSx 文件系统

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，请选择 Instances（实例），然后选择 Launch instance（启动实例）以打开启动实例向导。
3. 在 Application and OS Images（应用程序和操作系统映像）部分中，请选择要使用的 AMI。
4. 在 Instance type（实例类型）部分中，选择实例类型。
5. 在 Key pair（密钥对）部分中，选择现有密钥对或创建新密钥对。
6. 在 Network settings（网络设置）部分，执行以下操作：

   a. 选择编辑。

   b. 如果您想挂载现有文件系统，对于 Subnet（子网），请选择文件系统的首选子网。我们建议您将实例作为文件系统的首选子网启动到同一可用区中，以优化性能。

      如果您想创建新的文件系统以挂载到实例，对于 Subnet（子网），请选择要在其中启动实例的子网。

      Important

      您必须选择一个子网才能在新启动实例向导中启用 Amazon FSx 功能。如果不选择子网，将无法挂载现有文件系统或创建新的文件系统。

7. 在 Storage（存储）部分中，执行以下操作：

   a. 根据需要配置卷。

   b. 展开 File systems（文件系统）部分，然后选择 FSx。

   c. 请选择 Add shared file system（添加共享文件系统）。

   d. 对于 File system（文件系统），请选择要挂载的文件系统。

      Note

      该列表显示所选区域内您账户中的所有 Amazon FSx for NetApp ONTAP 和 Amazon FSx for OpenZFS 文件系统。

   e. 要自动创建并附加启用对文件系统的访问所需的安全组，请选择 Automatically create and attach security groups（自动创建和附加安全组）。如果您更喜欢手动创建安全组，请清除该复选框。有关更多信息，请参阅安全组 (p. 1603)。

   f. 要自动附加挂载文件系统所需的用户数据脚本，请选择 Automatically mount shared file system by attaching required user data script（通过附加所需的数据用户数据脚本自动挂载共享文件系统）。如果更喜欢手动提供用户数据脚本，请清除该复选框。有关更多信息，请参阅用户数据脚本 (p. 1605)。

8. 在 Advanced（高级）部分中，根据需要配置其他实例设置。
9. 选择启动。

实例卷限制

您的实例可以具有的卷的最大数量取决于操作系统和实例类型。考虑应将多少个卷添加到实例时，应考虑是否需要增加 I/O 带宽或存储容量。

目录

- Nitro 系统卷限制 (p. 1607)
- 特定于 Linux 的卷限制 (p. 1607)
- 带宽与容量 (p. 1607)

Nitro 系统卷限制

在 Nitro 系统 (p. 246)上构建的实例支持最大数量的附加项，这些附加项在网络接口、EBS 卷和 NVMe 实例存储卷之间共享。每个实例至少附加 1 个网络接口。NVMe 实例存储卷将自动附加。有关更多信息，请参阅弹性网络接口 (p. 1104)和实例存储卷 (p. 1581)。

其中大多数实例最多支持 28 个附加项。例如，如果在仅限 EBS 的实例上没有附加其他网络接口，您可以将多达 27 个 EBS 卷附加到该实例。如果带有 2 个 NVMe 实例存储卷的实例上还有一个网络接口，您可以将 24 个 EBS 卷附加到该实例。

对于其他实例，以下限制适用：

- 大多数裸机实例最多支持 31 个 EBS 卷。
- 内存增强型虚拟化实例最多支持 27 个 EBS 卷。
- 高内存裸机实例最多支持 19 个 EBS 卷。
- `inf1.xlarge` 和 `inf1.2xlarge` 实例最多支持 26 个 EBS 卷。
- `inf1.6xlarge` 实例最多支持 23 个 EBS 卷。
- `mac1.metal` 实例最多支持 16 个 EBS 卷。
- `inf1.24xlarge` 实例最多支持 11 个 EBS 卷。
- `g5.48xlarge` 实例最多支持 9 个 EBS 卷。
- `d3.8xlarge` 和 `d3en.12xlarge` 实例最多支持 3 个 EBS 卷。

特定于 Linux 的卷限制

附加的卷数超出 40 会导致启动失败。此数字包括根卷以及所有附加的实例存储卷和 EBS 卷。如果连接了大量卷的实例出现启动问题，请停止该实例，分离所有在启动过程中不必要的卷，然后在实例运行之后重新附加这些卷。

> **Important**
>
> 如果将 40 个以上的卷附加到 Linux 实例，系统只会尽力支持，不对此进行保证。

带宽与容量

为获得一致且可预测的带宽使用案例，请使用 EBS 优化或 10 GiB 网络连接实例并预置通用型 SSD 或 Provisioned IOPS SSD 卷。按照 Amazon EBS 优化的实例 (p. 1522)中的指导，使您为卷预配置的 IOPS 与实例提供的带宽匹配，以获得最大性能。对于 RAID 配置，许多管理员发现大于 8 个卷的阵列由于 I/O 开销提高而降低了性能回报。测试您的各个应用程序性能并根据需要优化。

Amazon EC2 实例根设备卷

当您启动一个实例时，根设备卷 包含用于启动该实例的映像。在我们推出 Amazon EC2 时，所有 AMI 都由 Amazon EC2 实例存储提供支持，也就是说，从 AMI 启动的实例的根设备，是根据一个存储在 Amazon S3 中的模板创建而来的实例存储卷。推出 Amazon EBS 之后，我们又推出了由 Amazon EBS 提供支持的 AMI。这意味着从 AMI 启动的实例的根设备是一个从 Amazon EBS 快照创建的 Amazon EBS 卷。

您可以在 Amazon EC2 实例存储支持的 AMI 和 Amazon EBS 支持的 AMI 之间进行选择。我们建议您使用由 Amazon EBS 提供支持的 AMI，因为它们启动速度更快，而且采用了持久性存储。

> **Important**
>
> 只有以下实例类型支持将实例存储卷作为根设备：C3、D2、G2、I2、M3 和 R3。

有关 Amazon EC2 为您的根卷使用的设备名称的更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。

目录

- 根设备存储概念 (p. 1608)
- 按根设备类型选择 AMI (p. 1609)
- 确定实例的根设备类型 (p. 1610)
- 将根卷更改为保留 (p. 1611)
- 更改根卷的初始大小 (p. 1613)

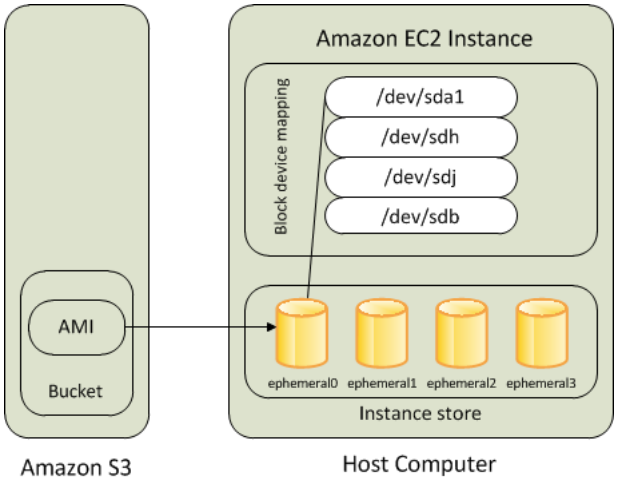
根设备存储概念

您可以从实例存储支持的 AMI 或 Amazon EBS-backed AMI 启动实例。AMI 的说明中包括 AMI 的类型；您会看到根设备在一些地方被称为 `ebs`（表示由 Amazon EBS 提供支持）或 `instance store`（表示由实例存储提供支持）。这很重要，因为您可以使用这两种 AMI 进行的操作有很大区别。有关这些区别的更多信息，请参阅 根设备存储 (p. 103)。

实例存储支持的实例

使用实例存储作为根设备的实例自带可用的一个或多个实例存储卷，其中一个卷充当根设备卷。启动实例时，用于启动该实例的映像被复制到根卷。请注意，您可以根据实例类型选择使用更多实例存储卷。

只要实例正在运行，实例存储卷上的所有数据便会存在，但是在实例终止时（实例存储支持的实例不支持 Stop (停止) 操作）或是实例失败时（例如底层硬盘有问题时），会删除这些数据。

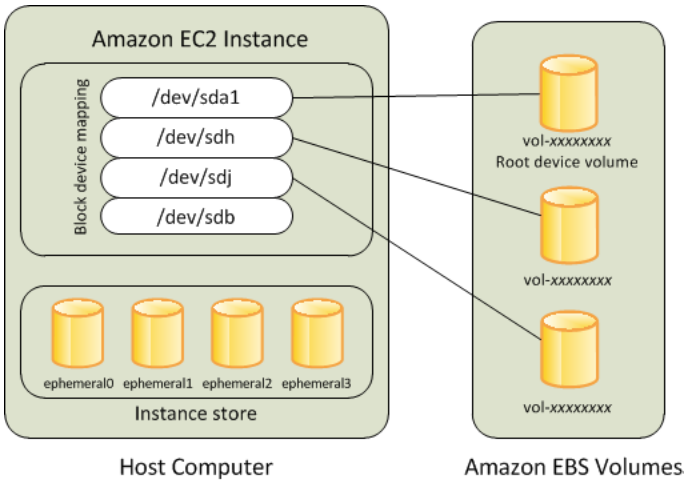


由实例存储支持的实例失败或终止后，该实例不能被恢复。如果您打算使用由 Amazon EC2 实例存储支持的实例，我们强烈建议您将数据跨多个可用区分散到不同实例存储中。您还应该定期将您的实例存储卷上的关键数据备份至持久性存储。

有关更多信息，请参阅Amazon EC2 实例存储 (p. 1579)。

由 Amazon EBS 提供支持的实例

使用 Amazon EBS 作为根设备的实例自动附加 Amazon EBS 卷。当您启动由 Amazon EBS 提供支持的实例时，系统会为您使用的 AMI 所引用的每一个 Amazon EBS 快照创建 Amazon EBS 卷。您可以根据实例类型选择使用其他Amazon EBS卷或实例存储卷。



由 Amazon EBS 提供支持的实例可以停止然后再重新启动，附加的卷中存储的数据不会受影响。当由 Amazon EBS 支持的实例处于停止状态时，您可以执行各种与该实例和卷有关的任务。例如，您可以修改实例的属性、更改其大小或更新其使用的内核，或者您可以将您的根卷附加到另一个正在运行的实例，以进行调试或实现任何其他目的。

如果由 Amazon EBS 提供支持的实例失败，您可以通过以下方法之一恢复您的会话：

- 停止，然后再次启动 (先尝试此方法)。
- 自动为相关卷拍摄快照并创建新的 AMI。有关更多信息，请参阅创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。
- 通过以下步骤将卷附加到新实例：
  1. 创建根卷的快照。
  2. 使用快照注册一个新的 AMI。
  3. 从新的 AMI 启动一个新实例。
  4. 将其余 Amazon EBS 卷与旧实例分离。
  5. 将这些 Amazon EBS 卷重新附加到新实例。

有关更多信息，请参阅Amazon EBS 卷 (p. 1324)。

按根设备类型选择 AMI

您在启动实例时指定的 AMI 决定着实例的根设备卷类型。您可以使用以下方法之一按根设备类型查看 AMI。

Console

使用控制台选择 Amazon EBS-backed AMI

1. 打开 Amazon EC2 控制台。

2. 在导航窗格中，选择 AMIs。
3. 从筛选条件列表中，选择映像类型（例如 Public images (公有映像)）。在“Search (搜索)”栏中选择 Platform (平台) 以选择操作系统（例如 Amazon Linux），然后选择 Root Device Type (根设备类型) 以选择 EBS images (EBS 映像)。
4. （可选）为了获取其他信息以帮助您进行选择，请选择 Show/Hide Columns (显示/隐藏列) 图标，更新要显示的列，然后选择 Close (关闭)。
5. 选择一个 AMI 并记下其 AMI ID。

使用控制台选择由实例存储支持的 AMI

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从筛选条件列表中，选择映像类型（例如 Public images (公有映像)）。在“Search (搜索)”栏中选择 Platform (平台) 以选择操作系统（例如 Amazon Linux），然后选择 Root Device Type (根设备类型) 以选择 Instance store (实例存储)。
4. （可选）为了获取其他信息以帮助您进行选择，请选择 Show/Hide Columns (显示/隐藏列) 图标，更新要显示的列，然后选择 Close (关闭)。
5. 选择一个 AMI 并记下其 AMI ID。

Amazon CLI

使用命令行验证 AMI 的根设备卷的类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-images (Amazon CLI)
- Get-EC2Image (Amazon Tools for Windows PowerShell)

确定实例的根设备类型

Console

使用控制台确定实例的根设备类型

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 在存储选项卡的根设备详细信息下，检查根设备类型的值，如下所示：
   - 如果值为 `EBS`，则表示这是一个由 Amazon EBS 支持的实例。
   - 如果值为 `INSTANCE-STORE`，则表示这是由实例存储支持的实例。

Amazon CLI

使用命令行确定实例的根设备类型

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- describe-instances (Amazon CLI)
- Get-EC2InstanceAmazon Tools for Windows PowerShell

将根卷更改为保留

默认情况下，当实例终止时，由 Amazon EBS 提供支持的 AMI 的根卷会被删除。您可以更改默认行为来确保卷在实例终止后保留。要更改默认行为，请使用块储存设备映射将 `DeleteOnTermination` 属性设置为 `false`。

任务

- 将根卷配置为在实例启动期间保留 (p. 1611)
- 配置根卷以便为现有实例保留 (p. 1612)
- 确认已将根卷配置为保留 (p. 1612)

将根卷配置为在实例启动期间保留

可以使用 Amazon EC2 控制台或命令行工具将根卷配置为在启动实例时保留。

Console

使用控制台将根卷配置为在启动实例时保留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例，然后选择启动实例。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面上，取消选中根卷的 Delete On Termination (终止时删除)。
6. 完成其余向导页面上的操作，然后选择 Launch。

Amazon CLI

使用 Amazon CLI 将根卷配置为在启动实例时保留

使用 run-instances 命令，并包含将 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射。

```
$ aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

在 `mapping.json` 中指定以下内容。

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

使用 Tools for Windows PowerShell 将根卷配置为在启动实例时保留

使用 New-EC2Instance 命令，并包含将 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射。

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping $bdm ...other
 parameters...
```

配置根卷以便为现有实例保留

可以只使用命令行工具，配置根卷以便为正在运行的实例保留。

Amazon CLI

使用 Amazon CLI 配置根卷以便为现有实例保留

使用 modify-instance-attribute 命令以及将 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射。

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-
mappings file://mapping.json
```

在 `mapping.json` 中指定以下内容。

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

使用 Amazon Tools for Windows PowerShell 配置根卷以便为现有实例保留

使用 Edit-EC2InstanceAttribute 命令以及将 `DeleteOnTermination` 属性设置为 `false` 的块储存设备映射。

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping $bdm
```

确认已将根卷配置为保留

可以使用 Amazon EC2 控制台或命令行工具确认已将根卷配置为保留。

Console

使用 Amazon EC2 控制台确认已将根卷配置为保留

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Instances (实例)，然后选择实例。
3. 在存储选项卡的块储存设备下，找到根卷的条目。如果终止时删除为 No，则表示卷已配置为保留。

Amazon CLI

使用 Amazon CLI 确认已将根卷配置为保留

使用 describe-instances 命令，并确认 DeleteOnTermination 响应元素中的 BlockDeviceMappings 属性设置为 false。

```
$ aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
        }
    }
...
```

Tools for Windows PowerShell

使用 Amazon Tools for Windows PowerShell 确认已将根卷配置为保留

使用 Get-EC2Instance 命令，并确认 DeleteOnTermination 响应元素中的 BlockDeviceMappings 属性设置为 false。

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

更改根卷的初始大小

默认情况下，根卷的大小取决于快照的大小。您可以按下述方式使用实例的块储存设备映射增加根卷的初始大小。

1. 确定 AMI 中指定的根卷的设备名称，如 查看 AMI 块储存设备映射中的 EBS 卷 (p. 1619) 中所述。
2. 确认 AMI 块储存设备映射中指定的快照的大小，如 查看 Amazon EBS 快照信息 (p. 1402) 中所述。
3. 如 在启动实例时更新块储存设备映射 (p. 1620) 中所述，使用实例块储存设备映射覆盖根卷的大小，请指定大于快照大小的卷大小。

例如，实例块储存设备映射的以下条目将根卷的大小 /dev/xvda 增加到 100 GiB。您可以在实例块储存设备映射中省略快照 ID，因为快照 ID 已在 AMI 块储存设备映射中指定。

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

有关更多信息，请参阅块设备映射 (p. 1615)。

Linux 实例上的设备名称

当您将卷附加到实例时，需要为卷提供设备名称。该设备名称由 Amazon EC2 使用。实例的块储存设备驱动程序会在装载卷时分配实际的卷名称，指定的名称可以与 Amazon EC2 使用的名称不同。

您的实例可支持的卷的数量取决于操作系统。有关更多信息，请参阅实例卷限制 (p. 1607)。

目录

- 可用设备名称 (p. 1614)
- 设备名称注意事项 (p. 1615)

有关 Windows 实例上的设备名称的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的 Windows 实例上的设备命名。

可用设备名称

对 Linux 实例提供两种类型的虚拟化：半虚拟化 (PV) 和硬件虚拟机 (HVM)。实例的虚拟化类型由用于启动实例的 AMI 确定。支持 HVM AMI 的所有实例类型。上一代的某些实例类型支持半虚拟化 AMI。请务必注意您的 AMI 的虚拟化类型，因为推荐的和您可以使用的可用设备名称取决于您的实例的虚拟化类型。有关更多信息，请参阅Linux AMI 虚拟化类型 (p. 106)。

下表列出了在块储存设备映射中或附加 EBS 卷时您可指定的可用设备名称。

虚拟化类型	Available	为根卷预留	建议用于 EBS 卷	实例存储卷
半虚拟化	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
全虚拟化	/dev/sd[a-z] /dev/xvd[b-c][a-z]	不同的 AMI /dev/sda1 或 /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

* 您在块储存设备映射中为 NVMe EBS 卷指定的设备名称将使用 NVMe 设备名称 (`/dev/nvme[0-26]n1`) 进行重命名。块储存设备驱动程序可以使用不同于您在块储存设备映射中为卷指定的顺序来分配 NVMe 设备名称。

** 将自动枚举 NVMe 实例存储卷并为其分配 NVMe 设备名称。

有关实例存储卷的更多信息，请参阅 Amazon EC2 实例存储 (p. 1579)。有关 NVMe EBS 卷（基于 Nitro 的实例）的更多信息，包括如何识别 EBS 设备，请参阅 Linux 实例上的 Amazon EBS 和 NVMe (p. 1518)。

设备名称注意事项

在选择设备名称时请记住以下原则：

- 尽管您可以使用用于附加实例存储卷的设备名附加 EBS 卷，我们还是强烈建议您不要这样做，因为这种操作具有不可预测性。
- 实例的 NVMe 实例存储卷数取决于该实例的大小。将自动枚举 NVMe 实例存储卷并为其分配 NVMe 设备名称 (`/dev/nvme[0-26]n1`)。
- 根据内核的块储存设备驱动程序，附加的设备所采用的名称可能与您指定的名称不同。例如，如果您指定 `/dev/sdh` 的设备名称，则设备可能命名为 `/dev/xvdh` 或`/dev/hdh`。在大多数情况下，尾部字母保持不变。在某些版本的 Red Hat Enterprise Linux（及其变体，例如，CentOS）中，尾部字母可能发生变化（`/dev/sda` 可能变为 `/dev/xvde`）。在这些情况下，每个设备名称的尾部字母都会递增相同次数。例如，如果 `/dev/sdb` 重命名为 `/dev/xvdf`，则 `/dev/sdc` 重命名为 `/dev/xvdg`。Amazon Linux 为您对重命名设备指定的名称创建符号链接。其他操作系统的行为方式可能有所不同。
- HVM AMI 不支持在设备名称中使用尾部数字，除为根设备保留的 `/dev/sda1` 和 `/dev/sda2` 以外。尽管可以使用 `/dev/sda2`，但我们不建议将此设备映射与 HVM 实例结合使用。
- 使用 PV AMI 时，您不能连接共享相同设备字母的卷，无论是否带有尾部数字都是如此。例如，如果您将一个卷附加为 `/dev/sdc`，另一个卷附加为 `/dev/sdc1`，则只有 `/dev/sdc` 将对实例可见。要在设备名称中使用尾部数字，您必须对所有基础字母相同的设备名称使用尾部数字 (例如 `/dev/sdc1`、`/dev/sdc2`、`/dev/sdc3`)。
- 一些自定义内核可能会包含限制，限制使用 `/dev/sd[f-p]` 或 `/dev/sd[f-p][1-6]`。如果您在使用 `/dev/sd[q-z]` 或 `/dev/sd[q-z][1-6]` 时遇到问题，请尝试切换为 `/dev/sd[f-p]` 或 `/dev/sd[f-p][1-6]`。

块设备映射

您启动的每个实例都有一个关联根设备卷，它是 Amazon EBS 卷或实例存储卷。您可以使用块储存设备映射来指定实例启动时要连接的其他 EBS 卷或实例存储卷。您还可以将其他 EBS 卷附加到运行中的实例，请参阅 将 Amazon EBS 卷挂载到实例 (p. 1347)。然而，将实例存储卷附加到实例的唯一办法是，在实例启动时，使用块储存设备映射来附加这些卷。

有关根设备卷的更多信息，请参阅 将根卷更改为保留 (p. 1611)。

目录

- 块储存设备映射的概念 (p. 1615)
- AMI 块储存设备映射 (p. 1618)
- 实例块储存设备映射 (p. 1620)

块储存设备映射的概念

块储存设备是一种以字节或位（块）为单位移动数据的存储设备。这些设备支持随机访问并广泛使用缓存 I/O，例如，包括硬盘、CD-ROM 驱动和闪存盘。块设备可以实际连接到计算机，或者就像实际连接到计算机一样对进行远程访问。

Amazon EC2 支持两种类型的块储存设备：

- 实例存储卷 (虚拟设备，其底层硬件实际附加到该实例的主机)
- EBS 卷 (远程存储设备)

块储存设备映射 定义了挂载到某个实例的块储存设备（实例存储卷和 EBS 卷）。您可以指定块储存设备映射作为创建 AMI 的一部分，以便使从该 AMI 启动的所有实例均可使用该映射。或者，您还可以在启动实例时指定块储存设备映射，这样该映射会覆盖您在启动实例的 AMI 中指定的块储存设备映射。请注意，某个实例类型支持的所有 NVMe 实例存储卷将在实例启动时自动枚举并为其分配设备名称；将这些卷包含在您的块储存设备映射中不起作用。

目录

- 块储存设备映射条目 (p. 1616)
- 块储存设备映射实例存储注意事项 (p. 1616)
- 块储存设备映射示例 (p. 1617)
- 如何使设备在操作系统可用 (p. 1617)

块储存设备映射条目

当您创建块储存设备映射时，可以为需要附加到该实例的每个块储存设备指定以下信息：

- 在 Amazon EC2 内使用的设备名称。在装载卷时，实例的块储存设备驱动程序将分配实际卷名称。分配的名称可以与 Amazon EC2 建议的名称不同。有关更多信息，请参阅Linux 实例上的设备名称 (p. 1614)。

对于实例存储卷，您还可以指定以下信息：

- 虚拟设备：`ephemeral[0-23]`。请注意，对您的实例可用的实例存储卷的数量和大小因实例类型而异。

对于 NVMe 实例存储卷，以下信息也适用：

- 这些卷将自动枚举并分配设备名称；将这些卷包含在块储存设备映射中将不起作用。

对于 EBS 卷，您还可以指定以下信息：

- 用于创建块储存设备的快照的 ID (snap-xxxxxxxx)。只要您指定卷大小，此值为可选。
- 卷的大小（以 GiB 计算）。所指定的大小必须大于等于指定快照的大小。
- 是否在实例终止时删除卷（`true` 或 `false`）。根设备卷的默认值为 `true`，附加的卷的默认值为 `false`。当您创建 AMI 时，其块储存设备映射会从该实例继承此设置。当您启动某个实例时，该实例会从 AMI 继承此设置。
- 卷类型：`gp2` 和（`gp3`适用于通用型 SSD）、`io1` 和（`io2`适用于预置 IOPS SSD）、`st1`（适用于吞吐量优化型 HDD）、`sc1`（适用于 Cold HDD）或（`standard`适用于磁介质卷）。默认值为 `gp2`。
- 该卷支持的每秒进行读写操作的次数 (IOPS)。（仅与 `io1` 和 `io2` 卷一起使用。）

块储存设备映射实例存储注意事项

使用在其块储存设备映射中具有实例存储卷的 AMIs 启动实例时，要考虑一些注意事项。

- 有些实例类型包含的实例存储卷多于其他类型，而有些实例类型根本不包含实例存储卷。如果实例类型支持一个实例存储卷，而且 AMI 具有用于两个实例存储卷的映射，则实例会在启动时带有一个实例存储卷。
- 实例存储卷只能在启动时进行映射。不能停止没有实例存储卷的实例 (如 `t2.micro`)，将实例更改为支持实例存储卷的类型，然后重新启动带有实例存储卷的实例。但是，您可以从实例创建 AMI 并以支持实例存储卷的实例类型启动它，然后将这些实例存储卷映射到实例。
- 如果您启动映射了实例存储卷的实例，然后停止实例，将它更改为具有较少实例存储卷的实例类型并重新启动它，则来自初始启动的实例存储卷映射会出现在实例元数据中。但是，实例使用的实例存储卷不能超出该实例类型支持的最大数量。

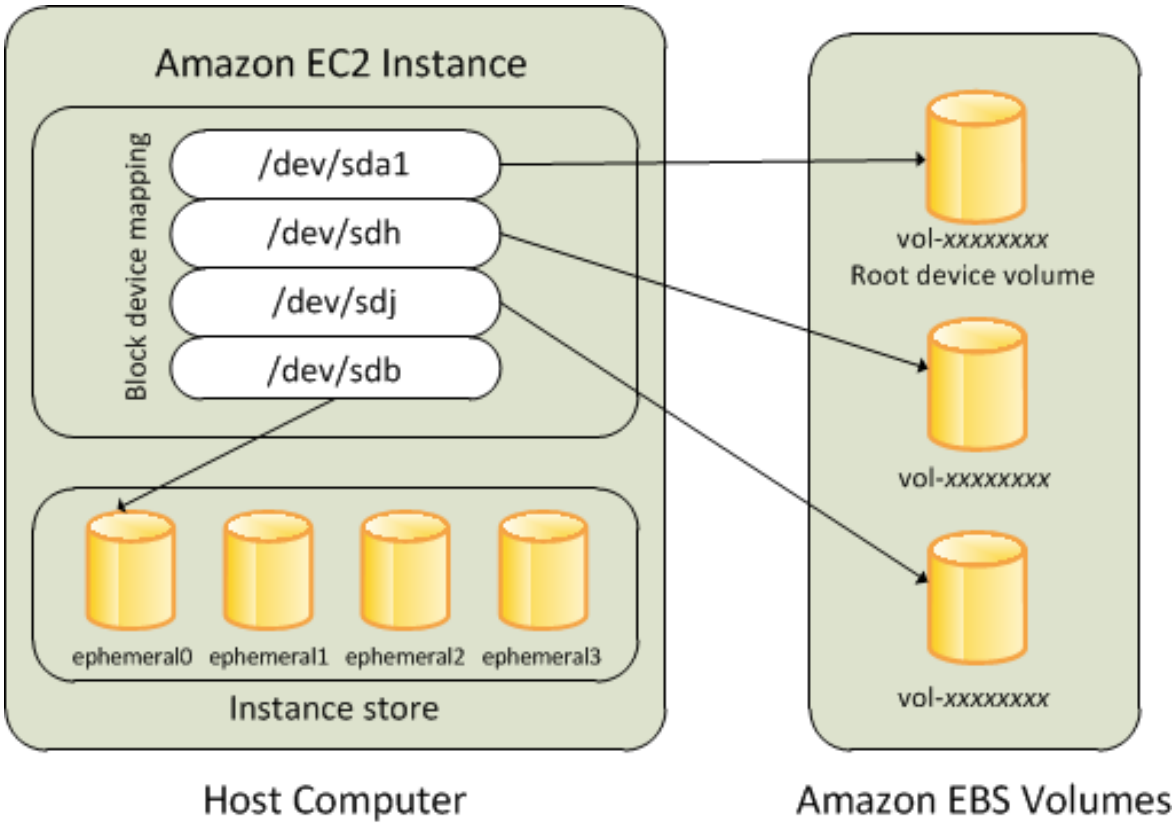
Note

实例停止时，实例存储卷上的所有数据都会丢失。

- 根据启动时的实例存储容量，M3 实例可能会在启动时忽略 AMI 实例存储块储存设备映射 (除非在启动时指定它们)。您应在启动时指定实例存储块储存设备映射（即使启动的 AMI 在 AMI 中映射了实例存储卷），以确保实例存储卷在实例启动时可用。

块储存设备映射示例

此图显示了 EBS 支持的实例的块储存设备映射示例。它将 /dev/sdb 映射到 ephemeral0 并映射两个 EBS 卷，一个映射到 /dev/sdh，另一个映射到 /dev/sdj。它还显示了作为根设备卷的 EBS 卷，即 /dev/sda1。



请注意，此块储存设备映射示例是在本主题中的示命令和 API 中例使用的。您可以在为 AMI 指定块储存设备映射 (p. 1618)和在启动实例时更新块储存设备映射 (p. 1620)中找到创建块储存设备映射的示例命令和 API。

如何使设备在操作系统可用

Amazon EC2 使用设备名称（如 /dev/sdh 和 xvdh）来描述块储存设备。Amazon EC2 使用块储存设备映射来指定要附加到 EC2 实例的块储存设备。当块储存设备附加到实例后，您必须先将其装载到操作系统，然后才可以访问此存储设备。当块储存设备从实例分离后，就被操作系统卸载下来，而您也不能再访问该存储设备。

通过 Linux 实例，当实例第一次启动时，在块储存设备映射中指定的设备名称会被映射到相应的块储存设备。默认情况下，实例类型决定要格式化并装载哪个实例存储卷。您可以在启动时装载额外的实例存储卷，前提是不得超过您的实例类型所允许的实例存储卷数量。有关更多信息，请参阅Amazon EC2 实例存

储 (p. 1579)。实例的块储存设备驱动程序决定在格式化和装载卷时要使用哪些设备。有关更多信息，请参阅将 Amazon EBS 卷挂载到实例 (p. 1347)。

AMI 块储存设备映射

各个 AMI 都拥有块储存设备映射，指定实例启动时要附加的块储存设备。Amazon 提供的 AMI 仅包含根设备。要向 AMI 添加更多块储存设备，必须创建自己的 AMI。

目录

- 为 AMI 指定块储存设备映射 (p. 1618)
- 查看 AMI 块储存设备映射中的 EBS 卷 (p. 1619)

为 AMI 指定块储存设备映射

创建 AMI 时，您可以使用两种方法来指定除根卷以外的卷。如果您在从该实例创建 AMI 前已将卷附加到运行中的实例，则 AMI 的块储存设备映射将包括这些相同的卷。对于 EBS 卷，这些现存的数据会保存在一个新的快照中，而且是块储存设备映射指定的新快照。而实例存储卷的数据无法保存。

对于 EBS 支持的 AMI，您可以使用块储存设备映射来添加 EBS 卷和实例存储卷。对于实例存储支持的 AMI，您只能添加实例存储卷，方法是在注册镜像时修改镜像清单文件中的块储存设备映射条目。

> **Note**
>
> 对于 M3 实例，您必须在启动实例时，在块储存设备映射中指定适用于实例的实例存储卷。当您启动 M3 实例时，如果在块储存设备映射中为 AMI 指定的实例存储卷未指定为块储存设备映射的一部分，则该卷可能会被忽略。

使用控制台向 AMI 添加卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择实例。
3. 选择一个实例，再依次选择 Actions（操作）Image and templates（映像和模板）、Create image（创建映像）。
4. 输入映像的名称和描述。
5. 实例卷将显示在 Instance volumes（实例卷）下。要添加另一个卷，请选择 Add volume（添加卷）。
6. 对于 Volume Type（卷类型），选择卷类型。对于 Device（设备），请选择设备名称。对于 EBS 卷，您可以指定其他详细信息，例如快照、卷大小、卷类型、IOPS 和加密状态。
7. 选择创建映像。

使用命令行向 AMI 添加卷

使用 create-image Amazon CLI 命令可为由 EBS 支持的 AMI 指定块储存设备映射。使用 register-image Amazon CLI 命令可为由实例存储支持的 AMI 指定块储存设备映射。

使用 `--block-device-mappings` 参数指定块储存设备映射。以 JSON 编码的参数可以直接在命令行上提供，也可以通过引用文件提供：

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

要添加实例存储卷，请使用以下映射。

```
{
```

```
    "DeviceName": "/dev/sdf",
    "VirtualName": "ephemeral0"
}
```

要添加空的 100 GiB gp2 卷，请使用以下映射。

```
{
    "DeviceName": "/dev/sdg",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

要添加基于快照的 EBS 卷，请使用以下映射。

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

要对设备省略映射，请使用以下映射。

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

或者，您可以将 `-BlockDeviceMapping` 参数与以下命令 (Amazon Tools for Windows PowerShell) 结合使用：

- New-EC2Image
- Register-EC2Image

查看 AMI 块储存设备映射中的 EBS 卷

您可以轻松列举块储存设备映射中适用于 AMI 的 EBS 卷。

使用控制台查看 AMI 的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择 AMIs。
3. 从 Filter 列表中选择 EBS images 以获取 EBS 支持的 AMI 的列表。
4. 选择所需的 AMI，然后查看 Details (详细信息) 选项卡。至少，以下信息适用于根设备：
   - Root Device Type (根设备类型)`ebs` ()
   - Root Device Name (例如，`/dev/sda1`)
   - Block Devices (数据块储存设备) (例如，`/dev/sda1=snap-1234567890abcdef0:8:true`)

   如果使用块储存设备映射创建的 AMI 带有额外 卷，则 Block Devices (块储存设备) 字段会显示针对这些额外 EBS 卷的映射。（此屏幕不显示实例存储卷。）

使用命令行查看 AMI 的 EBS 卷

使用 describe-images (Amazon CLI) 命令或 Get-EC2Image (Amazon Tools for Windows PowerShell) 命令来枚举 AMI 块储存设备映射中的 EBS 卷。

实例块储存设备映射

默认情况下，您启动的实例包含所有在 AMI 的块储存设备映射中指定的存储设备 (您是从该 AMI 启动实例的)。您可以在启动实例时，为实例指定要对块储存设备映射执行的更改，而这些更新会覆盖 AMI 的块储存设备映射或与其合并。

限制

- 对于根卷，您只能修改下列内容：卷大小、卷类型和 Delete on Termination 标志。
- 修改 EBS 卷时，无法减小其大小。因此，您必须指定大小等于或大于 AMI 的块储存设备映射中指定的快照大小的快照。

目录

- 在启动实例时更新块储存设备映射 (p. 1620)
- 更新正在运行的实例的块储存设备映射 (p. 1621)
- 查看实例块储存设备映射中的 EBS 卷 (p. 1622)
- 查看实例存储卷的实例块储存设备映射 (p. 1622)

在启动实例时更新块储存设备映射

您可以在启动实例时向其添加 EBS 卷和实例存储卷。请注意，针对实例更新块储存设备映射不会对启动实例的 AMI 的块储存设备映射造成永久性更改。

使用控制台向实例添加卷

1. 打开 Amazon EC2 控制台。
2. 在控制面板中，选择 Launch Instance。
3. 在 Choose an Amazon Machine Image (AMI) 页面上，选择要使用的 AMI 并选择 Select。
4. 遵循向导完成 Choose an Instance Type (选择一个实例类型) 和 Configure Instance Details (配置实例详细信息) 页面。
5. 在 Add Storage (添加存储) 页面中，您可以按以下方法修改根卷、EBS 卷和实例存储卷：
   - 若要更改根卷的大小，请查找 Type (类型) 列下的 Root (根) 卷，然后更改其 Size (大小) 字段。
   - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的 EBS 卷，请找到该卷并单击其对应的 Delete (删除) 图标。
   - 要添加 EBS 卷，请选择 Add New Volume（添加新卷），从 Type（类型）列表中选择 EBS，并填写 [Device（设备）、Snapshot（快照）等] 字段。
   - 要隐藏用于启动实例的 AMI 块储存设备映射所指定的实例存储卷，请找到该卷并选择其对应的 Delete 图标。
   - 要添加实例存储卷，请选择 Add New Volume，从 Type 列表中选择 Instance Store，然后从 Device 中选择设备名称。
6. 完成其余向导页面，然后选择 Launch。

使用 Amazon CLI 将卷添加到实例中

使用带 Amazon CLI 选项的 run-instances `--block-device-mappings` 命令可在启动时为实例指定块储存设备映射。

例如，假定 EBS 支持的 AMI 指定了以下块储存设备映射：

- /dev/sdb=ephemeral0
- /dev/sdh=snap-1234567890abcdef0
- /dev/sdj=:100

要防止 /dev/sdj 连接到从该 AMI 启动的实例，请使用以下映射。

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

要将 /dev/sdh 的大小增加到 300 GiB，请指定以下映射。请注意，您不必为 /dev/sdh 指定快照 ID，因为指定设备名称就足以识别卷。

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

要在实例启动时增加根卷的大小，请先调用带有 AMI ID 的 describe-images 以验证根卷的设备名称。例如，"RootDeviceName": "/dev/xvda"。要覆盖根卷的大小，请指定 AMI 所使用的根设备的设备名称和新的卷大小。

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

要附加额外的实例存储卷 /dev/sdc，请指定以下映射。如果实例类型不支持多个实例存储卷，此映射将无效。如果实例支持 NVMe 实例存储卷，则将自动枚举这些卷并为其分配 NVMe 设备名称。

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

使用 Amazon Tools for Windows PowerShell 将卷添加到实例中

将 -BlockDeviceMapping 参数与 New-EC2Instance 命令 (Amazon Tools for Windows PowerShell) 结合使用。

更新正在运行的实例的块储存设备映射

您可以使用 modify-instance-attribute Amazon CLI 命令更新正在运行的实例的块储存设备映射。在更改此属性之前，您不需要停止该实例。

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings file://
mapping.json
```

例如，要在实例终止时保留根卷，请在 mapping.json 中指定以下内容。

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

或者，您可以将 -BlockDeviceMapping 参数与 Edit-EC2InstanceAttribute 命令 (Amazon Tools for Windows PowerShell) 结合使用。

查看实例块储存设备映射中的 EBS 卷

您可以轻松枚举映射到实例的 EBS 卷。

Note

对于在 2009-10-31 API 发行之前启动的实例，Amazon 不会显示块储存设备映射。您必须先分离并重新附加卷，Amazon 才能显示块储存设备映射。

使用控制台查看实例的 EBS 卷

1. 打开 Amazon EC2 控制台。
2. 在导航窗格中，选择实例。
3. 在搜索栏中，输入 Root device type（根设备类型），然后选择 EBS。此操作会显示 EBS 支持的实例列表。
4. 选择所需的实例，然后查看 Storage（存储）选项卡中显示的详细信息。至少，以下信息适用于根设备：

   - Root device type（例如 EBS ）
   - Root Device Name（例如，/dev/xvda）
   - Block devices（例如，/dev/xvda、/dev/sdf 和 /dev/sdj）

   如果使用块储存设备映射启动了带有其他 EBS 卷的实例，则它们将显示在 Block devices（块储存设备）下。此选项卡上不会显示任何实例存储卷。
5. 要显示有关 EBS 卷的其他信息，请选择其卷 ID 以转到卷页面。有关更多信息，请参阅查看关于 Amazon EBS 卷的信息 (p. 1351)。

使用命令行查看实例的 EBS 卷

使用 describe-instances (Amazon CLI) 命令或 Get-EC2Instance (Amazon Tools for Windows PowerShell) 命令来枚举实例的块储存设备映射中的 EBS 卷。

查看实例存储卷的实例块储存设备映射

当您查看实例的块储存设备映射时，可以只查看 EBS 卷，但是不能查看实例存储卷。您用于查看实例的实例存储卷的方法取决于卷类型。

NVMe 实例存储卷

您可以使用 NVMe 命令行程序包 nvme-cli 来查询块储存设备映射中的 NVMe 实例存储卷。运行以下命令，下载程序包，并在实例上安装该程序包。

```
[ec2-user ~]$ sudo nvme list
```

以下是实例的示例输出。Model (模型) 列中的文本表示卷是 EBS 卷还是实例存储卷。在这个例子中，/dev/nvme1n1 和 /dev/nvme2n1 均为实例存储卷。

```
Node             SN                   Model                                    Namespace
---------------- -------------------- ---------------------------------------- ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store               1
/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage         1
/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage         1
  ...
```

HDD 或 SSD 实例存储卷

您可以使用实例元数据在块储存设备映射中查询 HDD 或 SSD 实例存储卷。未包含 NVMe 实例储存卷。

所有针对实例元数据的请求的基本 URI 均为 http://169.254.169.254/latest/。有关更多信息，请参阅实例元数据和用户数据 (p. 754)。

首先，连接到运行中的实例。从该实例中，使用此查询获取其块储存设备映射。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

该响应包含实例的块储存设备名称。举例来说，由实例存储支持的 m1.small 实例的输出如下所示。

```
ami
ephemeral0
root
swap
```

ami 设备是实例所看到的根设备。实例存储卷命名为 ephemeral[0-23]。swap 设备用于存储页面文件。如果您还映射了一些 EBS 卷，它们会依次显示为 ebs1、ebs2 等。

要了解块储存设备映射中的单个块储存设备的详细信息，可将其名称添加到上述查询，如下所示。

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-
data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
ephemeral0
```

实例类型将决定对实例可用的实例存储卷的数量。如果块储存设备映射中的实例存储卷数超过了对实例可用的实例存储卷数，则其他卷将被忽略。要查看实例的实例存储卷，请运行 lsblk 命令。要了解每种实例类型支持的实例存储卷数，请参阅实例存储卷 (p. 1581)。

撕裂写防护

撕裂写防护是由 Amazon 设计的块存储功能，可提高 I/O 密集型关系数据库工作负载的性能并减少延迟，而不会对数据弹性产生负面影响。使用 InnoDB 或 XtraDB 作为数据库引擎的关系数据库，例如 MySQL 和 MariaDB，将受益于撕裂写防护这一功能。

通常，使用大于存储设备断电原子性的页面的关系数据库使用数据记录机制来防止撕裂写。MariaDB 和 MySQL 在将数据写入数据表之前使用双写缓冲区文件来记录数据。如果写入事务期间由于操作系统崩溃或断电导致写入不完整或撕裂，数据库可以从双写缓冲区恢复数据。与写入双写缓冲区相关的 I/O 额外开销会影响数据库性能和应用程序延迟，并减少每秒可处理的事务数量。有关双写缓冲区的更多信息，请参阅 MariaDB 和 MySQL 文档。

借助撕裂写防护功能，可以在全有或全无的写入事务中将数据写入存储，这样就无需使用双写缓冲区。这样可以防止在写入事务期间因操作系统崩溃或断电将部分或撕裂的数据写入存储。在不影响工作负载弹性的情况下，每秒处理的事务数量最多可增加 30%，写入延迟最多可减少 50%。

定价

使用撕裂写防护功能不会产生额外费用。

支持的块大小和块边界对齐

撕裂写防护支持 4 KiB、8 KiB 和 16 KiB 数据块的写入操作。数据块起始逻辑块地址（LBA）必须与 4 KiB、8 KiB 或 16 KiB 的相应块的边界大小对齐。例如，对于 16 KiB 写入操作，数据块起始 LBA 必须与 16 KiB 的块边界大小对齐。

下表显示了跨存储和实例类型的支持。

	4 KiB 块	8 KiB 块	16 KiB 块
实例存储卷	所有 NVMe 实例存储卷都附加到当前 I 代新系列实例 (p. 239)。	Amazon Nitro SSD 支持 I4i、Im4GN 和 Is4Gen 实例。	
Amazon EBS 卷	所有 Amazon EBS 卷都附加到基于 nitro 的实例 (p. 246)。		

要确认您的实例和卷是否支持撕裂写防护，请查询以检查该实例是否支持撕裂写防护以及其他详细信息，例如支持的块和边界大小。有关更多信息，请参阅检查撕裂写防护支持和配置 (p. 1625)。

要求

要使撕裂防护功能正常运行，I/O 操作必须符合 NTWPU、NTWGU、NTWBU 字段中指定的大小、对齐方式和边界要求。在提交到设备之前，必须配置操作系统，确保特定的存储子系统（文件系统、LVM、RAID 等）不会修改存储堆栈中的 I/O 属性，包括块合并、拆分或块地址重新定位。

已使用以下配置测试了撕裂写防护功能：

- 支持所需块大小的实例类型和存储类型。
- Amazon Linux 2 或更高版本（内核版本为 5.10）。

- 已启用 bigalloc 的 ext4，集群大小为 16 KiB，还有最新的 ext4 实用程序（e2fsprogs 1.46.5 或更高版本）。
- O_DIRECT 文件访问模式可绕过 Linux 内核缓冲区缓存。

Note

您无需禁用 MySQL 和 MariaDB 工作负载的 I/O 合并。

检查撕裂写防护支持和配置

要确认您的实例和卷是否支持撕裂写防护，并查看包含撕裂写防护信息的 NVMe 命名空间供应商的特定数据，请使用以下命令。

```
$ sudo nvme id-ns -v device_name
```

Note

该命令以带有 ASCII 解释的十六进制形式返回供应商特定信息。您可能需要在应用程序中构建类似 ebsnvme-id 的工具，以读取和解析输出。

例如，以下命令返回 NVMe 命名空间供应商特定数据，其中包含 /dev/nvme1n1 的撕裂写防护信息。

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

如果您的实例和卷支持撕裂写防护功能，其会在 NVMe 命名空间供应商特定数据中返回以下 Amazon 撕裂写防护信息。

Note

下表中的字节表示从 NVMe 命名空间供应商特定数据开头的偏移量（以字节为单位）。

字节	描述
0:31	设备附件挂载点的名称，例如 /dev/xvda。您在卷附件请求期间提供此信息，Amazon EC2 实例可用其来创建指向 NVMe 区块设备的符号链接（nvmeXn1）。
32:63	卷 ID。例如，vol01234567890abcdef。此字段可用于将 NVMe 设备映射到附加的卷。
64:255	留待将来使用。
256:257	命名空间撕裂写防护单元大小（NTWPU）。此字段表示在断电或发生错误时，保证以原子方式写入 NVM 的写入操作的命名空间特定大小。此字段在逻辑块中指定，从以零开始的值表示。
258:259	命名空间撕裂写防护粒度大小（NTWPG）。此字段表示在断电或发生错误时，保证以原子方式写入 NVM 的写入操作的 NTWPU 下的命名空间特定大小增量。也就是说，大小应为 NTWPG * n <= NTWPU，其中 n 为正整数。写入操作 LBA 偏移量也必须与该字段对齐。此字段在逻辑块中指定，从以零开始的值表示。
260:263	命名空间撕裂写防护边界大小（NTWPB）。此字段表示该 NTWPU 值的此命名空间的原子边界大小。在断电或发生错误时，无法将保证跨原子边界写入此命名空间的操作以原子方式写入 NVM。值为 0h 表示断电或发生错误时没有原子边界。所有其他值使用与 NTWPU 字段相同的编码以逻辑块形式指定大小。

配置您的软件堆栈以防止撕裂写

具有支持卷的受支持的实例类型 (p. 1624)上默认启用撕裂写防护功能。您无需启用任何其他设置即可启用卷或实例的撕裂写防护功能。

Note

对不支持撕裂写防护的工作负载不会产生性能影响。您无需对这些工作负载进行任何更改。
支持撕裂写防护但未配置使用该功能的工作负载会继续使用双写缓冲区，不会获得任何性能优势。

要将 MySQL 或 MariaDB 软件堆栈配置为禁用双写缓冲区并使用撕裂写防护功能，请完成以下步骤：

1. 将您的卷配置为使用带有 BigAlloc 选项的 ext4 文件系统，并将集群大小设置为 4 KiB、8 KiB 或 16 KiB。使用集群大小为 4 KiB、8 KiB 或 16 KiB 的 BigAlloc，可确保文件系统分配与各自边界对齐的文件。

```
$  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
```

   Note

   对于 MySQL 和 MariaDB，必须使用 `-C 16384` 来匹配数据库页面大小。将分配粒度设置为页面大小倍数以外的值可能会导致分配与存储设备撕裂写防护边界不匹配。

   例如：

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. 将 InnoDB 配置为使用 `O_DIRECT` 刷新方法并关闭 InnoDB 双写模式。使用首选文本编辑器打开 `/etc/my.cnf`，更新 `innodb_flush_method` 和 `innodb_doublewrite` 参数，如下所示：

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

   Important

   如果您使用的是逻辑卷管理器（LVM）或其他存储虚拟化层，请确保卷的起始偏移量以 16 KiB 倍数对齐。这是相对于底层 NVMe 存储而言，用以考虑存储虚拟化层使用的元数据标头和超级块。如果您向 LVM 物理卷添加偏移量，则可能引起文件系统分配与 NVMe 设备的偏移量有偏差，从而导致撕裂写防护失效。有关更多信息，请参阅 Linux manual page（Linux 手册页面）中的 `--dataalignmentoffset`。

资源和标签

Amazon EC2 提供您可创建和使用的不同资源。这些资源中的一部分资源包括映像、实例、卷和快照。在您创建某个资源时，我们会为该资源分配一个唯一资源 ID。

可以用您定义的值标记某些资源，来帮助您组织和识别它们。

以下主题介绍了资源和标签，以及如何使用它们。

目录

- 回收站 (p. 1627)
- 资源位置 (p. 1656)
- 资源 ID (p. 1656)
- 列出并筛选您的资源 (p. 1657)
- 标记 Amazon EC2 资源 (p. 1664)
- Amazon EC2 Service Quotas (p. 1678)

回收站

回收站是一项数据恢复功能，支持您还原意外删除的 Amazon EBS 快照和 EBS 支持的 AMI。使用回收站时，如果资源被删除，回收站功能将在您指定的时间段内保留快照，而后永久删除资源。

在资源保留期到期之前，您可以随时从回收站还原资源。从回收站还原资源后，资源将从回收站中删除，您可以像使用账户中任何该类型的其他资源的一样使用此资源。如果保留期过期且资源未还原，则资源将从回收站中永久删除，并且不再可用于恢复。

使用回收站可以保护业务关键型数据免遭意外删除，从而确保业务连续性。

主题

- 如何工作？ (p. 1627)
- 支持的资源 (p. 1628)
- 注意事项 (p. 1628)
- 配额 (p. 1630)
- 相关服务 (p. 1630)
- 定价 (p. 1630)
- 所需的 IAM 权限 (p. 1631)
- 使用保留规则 (p. 1634)
- 使用回收站中的资源 (p. 1643)
- 监控回收站 (p. 1643)

如何工作？

要启用和使用回收站，您必须在要保护资源的 Amazon 区域中创建保留规则。保留规则指定以下内容：

- 要保护的资源的类型。

- 删除后要保留在回收站中的资源。
- 永久删除之前保留资源在回收站中的保留期。

使用回收站，可创建两种类型的保留规则：

- 标签级保留规则：标签级保留规则使用资源标签来标记要保留在回收站中的资源。对于每个保留规则，您可以指定一个或多个标签键和值对。使用保留规则中至少一个指定标签键值对标记的指定类型的资源，将在删除后自动保留在回收站中。如果要根据标签保护账户中的特定资源，请使用这种类型的保留规则。
- 区域级保留规则：区域级保留规则未指定任何资源标签。其适用于创建规则的区域中指定类型的所有资源，即使这些资源未被标记。如果要保护特定区域内特定类型的所有资源，请使用这种类型的保留规则。

如果资源在回收站中，您可以随时将其还原以供使用。

资源会保留在回收站中，直到发生以下情况之一：

- 您手动还原它以供使用。从回收站还原资源时，该资源将从回收站中删除，并立即可供使用。您可以像使用账户中该类型的任何其他资源一样，使用还原的资源。
- 保留期到期。如果保留期过期且资源未从回收站中还原，则资源将从回收站中永久删除，并且不再可查看或还原。

支持的资源

回收站支持以下资源类型：

- Amazon EBS 快照

  Important

  回收站保留规则也适用于归档存储层中的已归档快照。如果删除与回收站保留规则匹配的已归档快照，则该快照将在保留规则定义的保留期内保留在回收站中。归档的快照在回收站中时，按归档快照的费率计费。
- 由 Amazon EBS 支持的 Amazon Machine Image (AMI)

注意事项

使用回收站和保留规则时，需要考虑以下注意事项。

一般注意事项

- Important

  创建首个保留规则时，规则最多需要 30 分就能生效并开始保留资源。创建首个保留规则后，后续保留规则几乎立即会生效并开始保留资源。
- 如果资源在删除时与多个保留规则匹配，则保留期最长的保留规则优先。
- 您无法手动从回收站中删除资源。资源会在其保留期过期时自动删除。
- 如果资源在回收站中，您只能查看、还原或修改其标签。要以任何方式使用资源，您必须首先将其还原。
- 如果任何 Amazon Web Service（如 Amazon Backup 或 Amazon Data Lifecycle Manager）删除与留存规则匹配的资源，则该资源将由回收站自动保留。
- 将资源发送到回收站时，将为该资源分配以下系统生成标签：
  - 标签键：`aws:recycle-bin:resource-in-bin`
  - 标签值：`true`

您无法手动编辑或删除此标签。从回收站还原资源时，标签将自动删除。

快照注意事项

- Important

  如果为 AMI 及其关联快照设置了保留规则，则让快照的保留期不短于 AMI 的保留期。这可确保回收站在删除 AMI 之前不会删除与 AMI 关联的快照，避免 AMI 无法恢复。
- 如果在删除快照时启用了快速快照还原功能，则在快照发送到回收站后不久将自动禁用快照还原。
  - 如果您在快速快照还原被禁用前还原快照，则该快照将保持启用状态。
  - 如果您在快速快照还原被禁用后还原快照，则该快照将保持禁用状态。如果有需要，您必须手动重新启用快速快照还原。
- 如果在删除时共享快照，则将在发送到回收站时自动取消共享。如果还原快照，则会自动恢复以前的所有共享权限。
- 如果将其他 Amazon 服务（例如 Amazon Backup）创建的快照发送到回收站，而后从回收站还原该快照，则其不再由创建它的 Amazon 服务管理。如果不再需要快照，则必须手动删除该快照。

AMI 的注意事项

- 仅支持 Amazon EBS-backed AMIs。
- Important

  如果为 AMI 及其关联快照设置了保留规则，则让快照的保留期不短于 AMI 的保留期。这可确保回收站在删除 AMI 之前不会删除与 AMI 关联的快照，避免 AMI 无法恢复。
- 如果在删除时共享 AMI，则将在发送到回收站时自动取消共享。如果还原 AMI，则会自动恢复以前的所有共享权限。
- 您必须首先从回收站还原所有与 AMI 关联的快照，并确保其处于 `available` 状态，然后才可以从回收站还原 AMI。
- 如果将与 AMI 关联的快照从回收站中删除，则 AMI 将无法恢复。保留期到期后，AMI 将被删除。
- 如果将其他 Amazon 服务（例如 Amazon 备份）创建的 AMI 发送到回收站，而后您从回收站还原该 AMI，则其不再由创建它的 Amazon 服务管理。如果不再需要 AMI，则必须手动将其删除。

Amazon Data Lifecycle Manager 快照策略注意事项

- 如果 Amazon Data Lifecycle Manager 删除与保留规则匹配的快照，则该快照将由回收站自动保留。
- 如果 Amazon Data Lifecycle Manager 删除快照并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原快照，则必须在不再需要该快照时手动删除它。Amazon Data Lifecycle Manager 将不再管理该快照。
- 如果您手动删除由策略创建的快照，并且该快照在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在回收站中时，Amazon Data Lifecycle Manager 不管理快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，那么当达到策略的保留阈值时，Amazon Data Lifecycle Manager 将删除快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，则 Amazon Data Lifecycle Manager 将不再删除快照。如果不再需要快照，则必须手动删除该快照。

Amazon Backup 的注意事项

- 如果 Amazon Backup 删除与留存规则匹配的快照，则该快照将由回收站自动保留。

已归档快照的注意事项

- 回收站保留规则也适用于归档存储层中的已归档快照。如果删除与回收站保留规则匹配的已归档快照，则该快照将在保留规则定义的保留期内保留在回收站中。

  归档的快照在回收站中时，按归档快照的费率计费。

  如果按照某保留规则，在最短期限 90 天之前从回收站中删除了归档的快照，则需要为剩余天数付费。有关更多信息，请参阅定价和计费 (p. 1382)。

  若要使用回收站中的已归档快照，您必须首先从回收站中恢复快照，然后将其从归档层中还原到标准层。

配额

以下配额适用于回收站。

配额	默认配额			
每个区域的保留规则	250			
为每个保留规则标记密钥和值对	50			

相关服务

回收站适用于以下服务。

- Amazon CloudTrail – 使您能够记录回收站中发生的事件。有关更多信息，请参阅使用 Amazon CloudTrail 监控回收站 (p. 1646)。

定价

回收站中的资源按其标准费率计费。使用回收站和保留规则不会产生额外费用。有关更多信息，请参阅 Amazon EBS 定价。

> **Note**
>
> 在保留期过期并被永久删除后的短时间内，某些资源可能仍会在回收站控制台或 Amazon CLI 和 API 输出中显示。您无需为这些资源付费。保留期到期后，账单立即停止。

您可以使用以下 Amazon 生成的成本分配标签，以在使用 Amazon Billing and Cost Management 时实现成本跟踪和分配目的。

- 键：`aws:recycle-bin:resource-in-bin`
- 值：`true`

有关更多信息，请参阅《Amazon Billing and Cost Management 用户指南》中的 Amazon 生成的成本分配标签。

所需的 IAM 权限

默认情况下，用户没有权限使用回收站、保留规则或回收站中的资源。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

主题

- 使用回收站和保留规则的权限 (p. 1631)
- 使用回收站中的资源的权限 (p. 1632)
- 回收站的条件键 (p. 1632)

使用回收站和保留规则的权限

要使用回收站和保留规则，用户需要以下权限。

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

要使用回收站控制台，用户需要 `tag:GetResources` 权限。

以下是包含控制台用户 `tag:GetResources` 权限的示例 IAM policy。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
        ],
        "Resource": "*"
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

使用回收站中的资源的权限

有关使用回收站中的资源所需的 IAM 权限的更多信息，请参阅以下内容：

- 使用回收站中的快照的权限 (p. 1407)
- 使用回收站中的 AMI 的权限 (p. 193)

回收站的条件键

回收站定义以下条件键，您可在 IAM policy 的 Condition 元素中将其用于控制适用策略语句的条件。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

主题

- rbin:Request/ResourceType 条件键 (p. 1632)
- rbin:Attribute/ResourceType 条件键 (p. 1633)

rbin:Request/ResourceType 条件键

rbin:Request/ResourceType 条件键可以用于根据为 ResourceType 请求参数指定的值过滤对 CreateRule 和 ListRules 请求的访问。

示例 1 - CreateRule

以下示例 IAM policy 允许 IAM 主体仅在为 ResourceType 请求参数指定的值为 EBS_SNAPSHOT 或 EC2_IMAGE 时发出 CreateRule 请求。这使主体能够仅为快照和 AMI 创建新的保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

示例 2 - ListRules

以下示例 IAM policy 允许 IAM 主体仅在为 ResourceType 请求参数指定的值为 EBS_SNAPSHOT 时发出 ListRules 请求。这使主体仅列出快照的保留规则，并防止它们列出任何其他资源类型的保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

rbin:Attribute/ResourceType 条件键

rbin:Attribute/ResourceType 条件键可用于根据保留规则的 ResourceType 属性的值过滤对 DeleteRule、GetRule、UpdateRule、LockRule、UnlockRule、TagResource、UntagResource 和 ListTagsForResource 的访问。

示例 1 - UpdateRule

以下示例 IAM policy 允许 IAM 主体仅在请求的保留规则的 ResourceType 属性为 EBS_SNAPSHOT 或 EC2_IMAGE 时发出 UpdateRule 请求。这使主体能够仅为快照和 AMI 更新规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

示例 2 - DeleteRule

以下示例 IAM policy 允许 IAM 主体仅在请求的保留规则的 ResourceType 属性为 EBS_SNAPSHOT 时发出 DeleteRule 请求。这使主体能够仅为快照删除保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
```

```
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

使用保留规则

要启用和使用回收站，您必须在要保护资源的 Amazon 区域中创建保留规则。保留规则指定以下内容：

- 要保护的资源的类型。
- 删除后要保留在回收站中的资源。
- 永久删除之前保留资源在回收站中的保留期。

使用回收站，可创建两种类型的保留规则：

- 标签级保留规则：标签级保留规则使用资源标签来标记要保留在回收站中的资源。对于每个保留规则，您可以指定一个或多个标签键和值对。使用保留规则中至少一个指定标签键值对标记的指定类型的资源，将在删除后自动保留在回收站中。如果要根据标签保护账户中的特定资源，请使用这种类型的保留规则。
- 区域级保留规则：区域级保留规则未指定任何资源标签。其适用于创建规则的区域中指定类型的所有资源，即使这些资源未被标记。如果要保护特定区域内特定类型的所有资源，请使用这种类型的保留规则。

创建保留规则后，符合其条件的资源将在删除后的指定保留期内自动保留在回收站中。

主题

- 创建保留规则 (p. 1634)
- 查看回收站保留规则 (p. 1636)
- 更新保留规则 (p. 1637)
- 锁定保留规则 (p. 1638)
- 解锁保留规则 (p. 1639)
- 标签保留规则 (p. 1640)
- 查看保留规则标签 (p. 1641)
- 从保留规则中删除标签 (p. 1641)
- 查看回收站保留规则 (p. 1642)

创建保留规则

创建保留规则时，必须指定以下必要参数：

- 将受保留规则保护的资源类型。
- 将受保留规则保护的资源。您可以在标签级别和区域级别创建保留规则。
  - 若要创建标签级别保留规则，请指定识别要保护的资源的资源标签。您可为每个规则指定最多 50 个标签，将相同的标签键和值对添加到最多 5 个保留规则中。

  - 若要创建区域级别的保留规则，请勿指定任何标签键和值对。在这种情况下，指定类型的所有资源都将受到保护。
- 资源删除后要保留在回收站中的时间。期限可以长达 1 年（365 天）。

您还可以指定以下可选参数：

- 保留规则的可选名称。名称最多可以有 255 个字符。
- 保留规则的可选描述。描述长度最多为 255 个字符。

  Note

  我们建议您不要将个人身份识别、机密或敏感信息包括在留存规则描述中。
- 可选的保留规则标签，以帮助识别和组织保留规则。您最多可以为每个规则分配 50 个标签。

您也可以选择在创建时锁定保留规则。如果您在创建时锁定保留规则，则还必须指定解锁延迟时间期，可以是 7 到 30 天。保留规则默认保持解锁状态，除非您明确将其锁定。

保留规则仅在创建它们的区域中有效。如果您打算在其它区域中使用回收站，则必须在这些区域中创建其它保留规则。

您可以使用以下方法创建回收站保留规则。

Recycle Bin console

创建保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则），然后选择 Create retention rule（创建保留规则）。
3. 在 Basic details（基本详细信息）部分中，执行以下操作：

   a. （可选）在 Retention rule name（保留规则名称）中，输入保留规则的描述性名称。

   b. （可选）在 Retention rule description（保留规则描述）中，输入保留规则的简单描述。
4. 在 Rule settings（规则设置）部分，执行以下操作：

   a. 对于 Resource type（资源类型），选择要保护的保留规则的资源类型。保留规则将仅在回收站中保留此类资源。

   b. 请执行下列操作之一：

      - 要创建与区域中所有已删除的指定类型资源匹配的区域级保留规则，请选择 Apply to all resources（应用于所有资源）。保留规则将在删除资源后将所有已删除的指定资源保留在回收站中，即使资源没有任何标签也是如此。
      - 要创建标签级保留规则，请在 Resource tags to match（要匹配的资源标签）中输入标签键值对，以便标记要保留在回收站中的指定类型资源。至少具有指定标签键值对之一的指定类型资源才会根据保留规则保留。

   c. 对于 Retention period（保留期），输入保留规则在回收站中保留资源的天数。
5. （可选）若要锁定保留规则，对于 Rule lock settings（规则锁定设置），选择 Lock（锁定），然后对于 Unlock delay period（解锁延迟期），指定解锁延迟时间（以天为单位）。无法修改或删除锁定的保留规则。若要修改或删除规则，必须先将其解锁，然后等待解锁延迟期到期。有关更多信息，请参阅锁定保留规则 (p. 1638)。

   若要使保留规则保持解锁状态，对于 Rule lock settings（规则锁定设置），请保持 Unlock（解锁）处于选中状态。可以随时修改或删除已解锁的保留规则。有关更多信息，请参阅解锁保留规则 (p. 1639)。
6. （可选）在 Tags（标签）部分，执行以下操作：

- 要使用自定义标签标记规则，请选择 Add tag（添加标签），然后输入标签键值对。

7. 选择 Create retention rule（创建保留规则）。

Amazon CLI

创建保留规则

使用 create-rule Amazon CLI 命令。对于 `--retention-period`，请指定在回收站中保留已删除快照的天数。对于 `--resource-type`，为快照指定 `EBS_SNAPSHOT`，或者为 AMI 指定 `EC2_IMAGE`。要创建标签级别保留规则，请在 `--resource-tags` 中指定用于标记要保留快照的标签。若要创建区域级别的保留规则，请省略 `--resource-tags`。若要锁定保留规则，请包含 `--lock-configuration` 并指定解锁延迟期（以天为单位）。

```
$ aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

示例 1

以下示例命令创建已解锁的区域级保留规则，该规则将所有已删除的快照保留 7 天。

```
$ aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

示例 2

以下示例命令创建标签级保留规则，该规则将被 `purpose=production` 标记的所有已删除的快照保留 7 天。

```
$ aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

示例 3

以下示例命令创建锁定的区域级保留规则，该规则将所有已删除的快照保留 7 天。保留规则已锁定，解锁延迟期为 7 天。

```
$ aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

查看回收站保留规则

您可以使用以下方法之一查看回收站保留规则。

Recycle Bin console

查看保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 网格列出了所选区域的所有保留规则。要查看有关特定保留规则的更多信息，请在网格中选择该规则。

Amazon CLI

查看所有保留规则

使用 list-rules Amazon CLI 命令；对于 `--resource-type`，为快照指定 `EBS_SNAPSHOT`，或者为 AMI 指定 `EC2_IMAGE`。

```
$ aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

示例

以下示例命令列出了所有保留快照的保留规则。

```
$ aws rbin list-rules --resource-type EBS_SNAPSHOT
```

查看特定保留规则的信息

使用 get-rule Amazon CLI 命令。

```
$ aws rbin get-rule --identifier rule_ID
```

示例

以下示例命令提供了有关保留规则 `pwxIkFcvge4` 的信息。

```
$ aws rbin get-rule --identifier pwxIkFcvge4
```

更新保留规则

创建后，您可以随时更新已解锁保留规则的说明、资源标签和保留期。您无法更新保留规则的资源类型或解锁延迟期，即使保留规则已解锁也是如此。

您无法以任何方式更新锁定的保留规则。如果您需要修改锁定的保留规则，则必须先将其解锁，然后等待解锁延迟期到期。

如果您需要修改锁定保留规则的解锁延迟期，则必须解锁保留规则 (p. 1639)，然后等待当前的解锁延迟期到期。解锁延迟期到期后，必须重新锁定保留规则 (p. 1638)并指定新的解锁延迟期。

Note

我们建议您不要将个人身份识别、机密或敏感信息包括在留存规则描述中。

更新保留规则后，这些更改仅适用于其保留的新资源。这些更改不会影响之前发送到回收站的资源。例如，如果您更新了保留规则的保留期，则在新的保留期内只会保留更新后删除的快照。在更新之前发送到回收站的快照仍会在上一个（旧）保留期内保留。

您可以使用以下方法之一更新保留规则。

Recycle Bin console

更新保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 在网格中，选择要更新的保留规则，然后选择 Actions（操作）、Edit retention rule（编辑保留规则）。
4. 在 Rule details（规则详细信息）部分中，根据需要更新 Retention rule name（保留规则名称）和 Retention rule description（保留规则描述）。
5. 在 Rule settings（规则设置）部分中，根据需要更新 Resource type（资源类型）、Resource tags to match（要匹配的资源标签）和 Retention period（保留期）。
6. 在 Tags（标签）部分，根据需要添加或删除保留规则标签。
7. 选择 Save retention rule（保存保留规则）。

Amazon CLI

更新保留规则

使用 update-rule Amazon CLI 命令。对于 `--identifier`，指定要更新的保留规则的 ID。对于 `--resource-types`，为快照指定 `EBS_SNAPSHOT`，或者为 AMI 指定 `EC2_IMAGE`。

```
$ aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

示例

以下示例命令更新了保留规则 `6lsJ2Fa9nh9`，以将所有快照保留 7 天，并更新其描述。

```
$ aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

锁定保留规则

回收站允许您随时锁定区域级别的保留规则。

Note

您无法锁定标签级别的保留规则。

即使拥有所需 IAM 权限的用户，也无法修改或删除锁定的保留规则。锁定保留规则以保护其免遭意外或恶意修改和删除。

锁定保留规则时，必须指定解锁延迟期。这是解锁保留规则后必须等待的时间，然后才能修改或删除该规则。在解锁延迟期内，您无法修改或删除保留规则。只有在解锁延迟期到期后，您才可修改或删除保留规则。

保留规则锁定后，您无法更改解锁延迟期。如果您的账户权限已外泄，则解锁延迟期会让您有更多时间检测和应对安全威胁。此期限的长度应长于您识别和应对安全漏洞所花费的时间。若要设置正确的持续时间，您可以查看以前的安全事件以及识别和修复账户漏洞所需的时间。

我们建议您使用 Amazon EventBridge 规则来通知您保留规则锁定状态的变化。有关更多信息，请参阅使用 Amazon EventBridge 监控回收站 (p. 1643)。

注意事项

- 您只能锁定区域级别的保留规则。
- 您可以随时锁定已解锁的保留规则。
- 解锁延迟期必须为 7 到 30 天。
- 您可以在解锁延迟期内重新锁定保留规则。重新锁定保留规则会重置解锁延迟期。

您可以使用以下方法之一锁定区域级别的保留规则。

Recycle Bin console

锁定保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航面板中，选择 Retention rules（保留规则）。
3. 在网格中，选择要锁定的已解锁保留规则，然后选择 Actions（操作）、Edit retention rule lock（编辑保留规则锁定）。
4. 在编辑保留规则锁定屏幕上，选择 Lock（锁定），然后对于 Unlock delay period（解锁延迟期），指定解锁延迟期（以天为单位）。
5. 选择 I acknowledge that locking the retention rule will prevent it from being modified or deleted（我确认锁定保留规则将阻止其被修改或删除）复选框，然后选择 Save（保存）。

Amazon CLI

锁定已解锁的保留规则

使用 lock-rule Amazon CLI 命令。对于 `--identifier`，指定要锁定的保留规则 ID。对于 `--lock-configuration`，以天为单位指定解锁延迟期。

```
$ aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

示例

以下示例命令锁定保留规则 `6lsJ2Fa9nh9` 并将解锁延迟期设置为 15 天。

```
$ aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

解锁保留规则

您无法修改或删除锁定的保留规则。如果您需要修改锁定的保留规则，则必须先将其解锁。解锁保留规则后，必须等待解锁延迟期到期，然后才能修改或删除该规则。在解锁延迟期内，您无法修改或删除保留规则。

拥有所需 IAM 权限的用户可以随时修改和删除已解锁的保留规则。让保留规则处于解锁状态，会使其遭受意外或恶意修改和删除的风险。

注意事项

- 您可以在解锁延迟期内重新锁定保留规则。
- 您可以在解锁延迟期到期后重新锁定保留规则。
- 您无法绕过解锁延迟期。
- 初始锁定后，您无法更改解锁延迟期。

我们建议您使用 Amazon EventBridge 规则来通知您保留规则锁定状态的变化。有关更多信息，请参阅使用 Amazon EventBridge 监控回收站 (p. 1643)。

您可以使用以下方法之一解锁已锁定的区域级别保留规则。

Recycle Bin console

解锁保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航面板中，选择 Retention rules（保留规则）。
3. 在网格中，选择要解锁的已锁定保留规则，然后选择 Actions（操作）、Edit retention rule lock（编辑保留规则锁定）。
4. 在编辑保留规则锁定屏幕上，选择 Unlock（解锁），然后选择 Save（保存）。

Amazon CLI

解锁已锁定的保留规则

使用 unlock-rule Amazon CLI 命令。对于 `--identifier`，指定要解锁的保留规则 ID。

```
$ aws rbin unlock-rule \
--identifier rule_ID
```

示例

以下示例命令解锁保留规则 `6lsJ2Fa9nh9`。

```
$ aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

标签保留规则

可以给保留规则分配自定义标签，以便按不同的方式将它们分类，例如按用途、拥有者或环境分类。这有助于根据所分配的自定义标签高效查找特定保留规则。

您可以使用以下方法之一为保留规则分配标签。

Recycle Bin console

标记保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要标记的保留规则，选择 Tags（标签）选项卡，然后选择 Manage tags（管理标签）。
4. 选择 Add tag (添加标签)。对于 Key（键），输入标签建。对于 Value（值），输入键值。

5. 选择 Save（保存）。

Amazon CLI

标记保留规则

使用 tag-resource Amazon CLI 命令。对于 `--resource-arn`，请指定要标记的保留规则的 Amazon Resource Name (ARN)，并为 `--tags` 指定标签键值对。

```
$ aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

示例

以下示例命令使用标签 `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` 来标记保留规则 `purpose=production`。

```
$ aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tags key=purpose,value=production
```

查看保留规则标签

您可以使用以下方法之一查看分配给保留规则的标签。

Recycle Bin console

查看保留规则的标签

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要查看标签的保留规则，然后选择 Tags（标签）选项卡。

Amazon CLI

查看分配给保留规则的标签

使用 list-tags-for-resource Amazon CLI 命令。对于 `--resource-arn`，请指定保留规则的 ARN。

```
$ aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

示例

以下示例命令列举保留规则 `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` 的标签。

```
$ aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

从保留规则中删除标签

您可以使用以下方法之一从保留规则中删除标签。

Recycle Bin console

从保留规则中删除标签

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要从中删除标签的保留规则，选择 Tags（标签）选项卡，然后选择 Manage tags（管理标签）。
4. 在标签旁选择 Remove（移除），以移除标签。
5. 选择 Save（保存）。

Amazon CLI

从保留规则中删除标签

使用 untag-resource Amazon CLI 命令。对于 `--resource-arn`，请指定保留规则的 ARN。对于 `--tagkeys`，请指定要删除标签的标签键。

```
$ aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

示例

以下示例命令删除保留规则 `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` 的标签键为 `purpose` 的标签。

```
$ aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

查看回收站保留规则

您可以随时删除保留规则。删除保留规则时，回收站内在删除完成后将不再保留删除的新资源。根据保留规则中定义的保留期限，在删除保留规则之前发送到回收站的资源将继续保留在回收站中。期限到期后，资源将从回收站中永久删除。

您可以使用以下方法之一删除保留规则。

Recycle Bin console

删除保留规则

1. 在以下位置打开回收站控制台 https://console.aws.amazon.com/rbin/home/
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 在表格中选择要删除的保留规则，然后选择 Actions（操作）、Delete retention rule（删除保留规则）。
4. 在系统提示时，输入确认消息并选择 Delete retention rule（删除保留规则）。

Amazon CLI

删除保留规则

使用 delete-rule Amazon CLI 命令。对于 `--identifier`，请指定要删除的保留规则的 ID。

```
$ aws rbin delete-rule --identifier rule_ID
```

示例

以下示例命令删除保留规则 `6lsJ2Fa9nh9`。

```
$ aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

使用回收站中的资源

回收站支持以下资源类型：

- Amazon EBS 快照
- 由 Amazon EBS 支持的 Amazon Machine Image (AMI)

主题

- 在回收站中处理快照 (p. 1643)
- 使用回收站中的 AMI (p. 1643)

此部分包含了主题链接，可供了解如何使用受支持的资源类型。

在回收站中处理快照

有关使用回收站中的快照的更多信息，请参阅 从回收站中还原快照 (p. 1407)。

使用回收站中的 AMI

有关使用回收站中的 AMI 的更多信息，请参阅 从回收站恢复 AMI (p. 193)。

监控回收站

您可以使用以下功能来监控回收站。

主题

- 使用 Amazon EventBridge 监控回收站 (p. 1643)
- 使用 Amazon CloudTrail 监控回收站 (p. 1646)

使用 Amazon EventBridge 监控回收站

回收站将事件发送到 Amazon EventBridge，以根据保留规则执行操作。使用 EventBridge，您可以创建规则以发起编程操作，从而响应这些事件。例如，您可以创建 EventBridge 规则，当保留规则解锁并进入其解锁延迟期时，该规则会向您的电子邮件发送通知。有关更多信息，请参阅 Creating Amazon EventBridge rules that react to events（创建对事件作出反应的 Amazon EventBridge 规则）。

EventBridge 中的事件表示为 JSON 对象。事件独有的字段包含在 JSON 对象的 `detail` 部分。`event` 字段包含事件名称。`result` 字段包含启动事件的操作的已完成状态。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 事件模式。

有关 EventBridge 的更多信息，请参阅 Amazon EventBridge User Guide（《Amazon EventBridge 用户指南》）中的 What Is Amazon EventBridge?（什么是 Amazon EventBridge？）。

事件

- RuleLocked (p. 1644)
- RuleChangeAttempted (p. 1644)
- RuleUnlockScheduled (p. 1645)
- RuleUnlockingNotice (p. 1645)
- RuleUnlocked (p. 1645)

RuleLocked

以下是成功锁定保留规则时回收站生成的事件示例。该事件可以由 CreateRule 和 LockRule 请求生成。api-name 字段中注明了生成事件的 API。

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
}
```

RuleChangeAttempted

以下是回收站针对尝试修改或删除锁定规则失败生成的事件示例。该事件可以由 DeleteRule 和 UpdateRule 请求生成。api-name 字段中注明了生成事件的 API。

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "DeleteRule"
```

```
  }
}
```

RuleUnlockScheduled

以下是在解锁保留规则并且其解锁延迟期开始时回收站生成的事件示例。

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
}
```

RuleUnlockingNotice

以下是保留规则处于解锁延迟期，直到解锁延迟期到期前一天，回收站每天生成的事件示例。

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012,
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

以下是保留规则的解锁延迟期到期且可对保留规则进行修改或删除时，回收站生成的事件示例。

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
```

```
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

使用 Amazon CloudTrail 监控回收站

回收站服务与 Amazon CloudTrail 集成。CloudTrail 是提供用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 将回收站中执行的所有 API 调用作为事件捕获。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新管理事件。您可以使用 CloudTrail 收集的信息来确定向回收站发出的请求、发出请求的 IP 地址、何人发出请求、何时发出请求，以及其它详细信息。

有关 CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》。

CloudTrail 中的回收站信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。当受支持的事件活动在回收站中发生时，该活动将记录在 CloudTrail 事件中，并与其它 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 Amazon 账户中的事件（包括回收站事件），请创建跟踪记录。通过跟踪，CloudTrail 可将日志文件传送至 S3 存储桶。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 S3 存储桶。此外，可以配置其他 Amazon 服务，进一步分析和应对 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的创建跟踪记录概述部分。

支持的 API 操作

对于回收站，您可以使用 CloudTrail 将以下 API 操作记录为管理活动。

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

有关日志记录管理事件的更多信息，请参阅 CloudTrail 用户指南中的记录跟踪记录的管理事件。

身份信息

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentityElement。

了解回收站日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下是示例 CloudTrail 日志条目。

CreateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "CreateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": {
    "identifier": "jkrnexample"
```

```
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


GetRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListRules


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "resourceTags": [
      {
        "resourceTagKey": "test",
        "resourceTagValue": "test"
      }
    ]
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


UpdateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
```

```
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


DeleteRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
```

```
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:25Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "DeleteRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


TagResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
```

```
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


UntagResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tagKeys": [
      "purpose"
    ]
  },
  "responseElements": null,
  "requestID": "example7-6c1e-4f09-9e46-bb957example",
  "eventID": "example6-75ff-4c94-a1cd-4d5f5example",
  "readOnly": false,
```

```
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


ListTagsForResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


LockRule


```
{
```

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "123456789012",
  "arn": "arn:aws:iam::123456789012:root",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::123456789012:role/Admin",
      "accountId": "123456789012",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2022-10-25T00:45:11Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2022-10-25T00:45:19Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "LockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
  "identifier": "jkrnexample",
  "lockConfiguration": {
    "unlockDelay": {
      "unlockDelayValue": 7,
      "unlockDelayUnit": "DAYS"
    }
  }
},
"responseElements": {
  "identifier": "jkrnexample",
  "description": "",
  "resourceType": "EBS_SNAPSHOT",
  "retentionPeriod": {
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "resourceTags": [],
  "status": "available",
  "lockConfiguration": {
    "unlockDelay": {
      "unlockDelayValue": 7,
      "unlockDelayUnit": "DAYS"
    }
  },
  "lockState": "locked"
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
```

```
  }
}
```

UnlockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UnlockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EC2_IMAGE",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "pending_unlock",
    "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
```

```
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

资源位置

Amazon EC2 资源特定于它们所在的 Amazon 区域或可用区。

资源	类型	描述
Amazon EC2 资源标识符	区域性的	每个资源标识符（例如 AMI ID、实例 ID、EBS 卷 ID 或 EBS 快照 ID）都与其区域相关联，并且只能在创建资源的区域中使用。
用户提供的资源名称	区域性的	每个资源名称（例如，安全组名称或密钥对名称）都与其区域相关联，并且只能在创建资源的区域中使用。尽管您可以在多个区域创建名称相同的资源，但是它们之间并无关联。
AMI	区域性的	AMI 与文件位于 Amazon S3 中的区域相关联。您可以将 AMI 从一个区域复制到另一个区域。有关更多信息，请参阅复制 AMI (p. 172)。
EBS 快照	区域性的	EBS 快照与其区域相关联，并且只能用于在同一区域中创建卷。您可以将快照从一个区域复制到另一个区域。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。
EBS 卷	可用区	Amazon EBS 卷与其可用区相关联，只能附加到同一可用区内的实例。
弹性 IP 地址	区域性的	弹性 IP 地址与区域相关联，并且只能与同一区域中的实例相关联。
实例	可用区	实例与您在其中启动实例的可用区相关联。但它的实例 ID 与区域相关联。
密钥对	全球性或区域性	您使用 Amazon EC2 创建的密钥对与您在其中创建它们的区域相关联。您可以创建您自己的 RSA 密钥对并将其上传到您打算在其中使用它的区域；因此，您可以通过将密钥对上传到每个区域来使其在全球范围内可用。 有关更多信息，请参阅Amazon EC2 密钥对和 Linux 实例 (p. 1289)。
安全组	区域性的	安全组与区域相关联，并且只能分配给同一区域中的实例。您不能使用安全组规则让一个实例与其所在区域外的实例通信。另一个区域中实例的流量被视为 WAN 带宽。

资源 ID

创建资源时，我们会为每个资源分配一个唯一资源 ID。资源 ID 采用以下格式：资源标识符 (例如，快照的 snap) 后接连字符以及字母与数字的唯一组合。

每个资源标识符（例如 AMI ID、实例 ID、EBS 卷 ID 或 EBS 快照 ID）都与其区域相关联，并且只能在创建资源的区域中使用。

您可以使用资源 ID 在 Amazon EC2 控制台中查找您的资源。如果您正在通过命令行工具或 Amazon EC2 API 使用 Amazon EC2，则某些命令需要资源 ID。例如，如果您正在使用 stop-instances Amazon CLI 命令来停止实例，则必须在该命令中指定实例 ID。

资源 ID 长度

在 2016 年 1 月之前，分配给某些资源类型的新创建资源的 ID 在连字符之后使用了 8 个字符（例如 i-1a2b3c4d）。2016 年 1 月至 2018 年 6 月，我们将这些资源类型的 ID 更改为在连字符后使用 17 个字符（例如 `i-1234567890abcdef0`）。根据您的帐户创建时间，您可能有一些带有短 ID 的现有资源，但是，任何新资源的 ID 都会比较长。

列出并筛选您的资源

您可以使用 Amazon EC2 控制台获取某些类型的资源的列表。您可以使用相应命令或 API 操作获取每种类型的资源的列表。如果您拥有许多资源，可以筛选结果以仅包含或排除符合特定标准的资源。

目录

- 使用控制台列出并筛选资源 (p. 1657)
- 使用 CLI 和 API 列出并筛选 (p. 1661)
- 使用 Amazon EC2 全局视图列出和筛选跨区域的资源 (p. 1663)

使用控制台列出并筛选资源

目录

- 使用控制台列出资源 (p. 1657)
- 使用控制台筛选资源 (p. 1657)

使用控制台列出资源

您可以使用控制台查看最常用的 Amazon EC2 资源类型。要查看其他资源，请使用命令行界面或 API 操作。

要使用控制台列出 EC2 资源

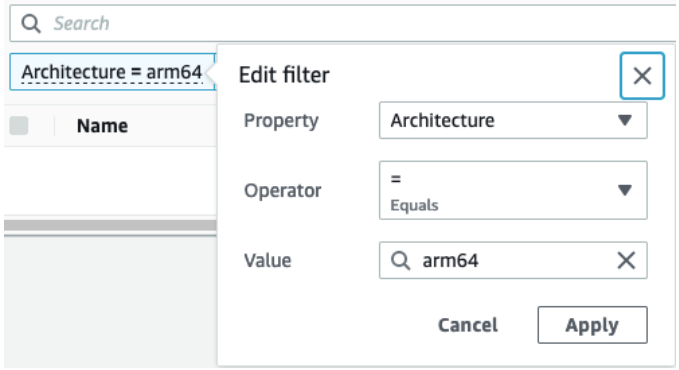
1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择与资源类型对应的选项。例如，要列出实例，请选择实例。

   该页面显示所选资源类型的所有资源。

使用控制台筛选资源

筛选资源列表

1. 在导航窗格中，选择资源类型 (例如，Instances)。
2. 选择搜索字段。
3. 从列表中选择筛选条件。
4. 选择运算符，例如 =（等于）。某些属性具有更多可供选择的运算符。请注意，并非所有页面都支持选择运算符。
5. 选择筛选条件值。
6. 要编辑选定的筛选条件，请选择过滤条件令牌（蓝色框），进行所需的编辑，然后选择 Apply（应用）。请注意，并非所有页面都支持编辑选定的筛选条件。



7. 完成后，删除筛选条件。

旧和新 Amazon EC2 控制台之间的搜索和筛选功能略有不同。

新控制台

新控制台支持两种类型的筛选。

- API 筛选发生在服务器端。该筛选应用于 API 调用，可减少服务器返回的资源数量。它可以对大型资源集进行快速筛选，并可降低服务器和浏览器之间的数据传输时间和成本。API 筛选支持 =（等于）和 :（包含）运算符，并且始终区分大小写。
- 客户端筛选发生在客户端。它可以对浏览器中现有的数据（也就是 API 已返回的数据）进行筛选。客户端筛选与 API 筛选结合使用，可以在浏览器中筛选出较小的数据集。除 =（等于）和 :（包含）运算符外，客户端筛选还可以支持范围运算符 [例如 >=（大于等于）] 和否定（反向）运算符 [例如 !=（不等于）]。

新 Amazon EC2 控制台支持以下类型的搜索：

按关键字搜索

按关键词搜索是一种自由文本搜索，可让您在所有资源属性或标签中搜索特定的值，而无需指定要搜索的属性或标签键。

> **Note**
>
> 所有关键字搜索都使用客户端筛选。

要按关键字进行搜索，请在搜索框中输入或粘贴要查找的内容，然后按 Enter。例如，搜索 123 时将会比对任何属性（例如 IP 地址、实例 ID、VPC ID 或 AMI ID）或任何标签（例如 Name）中包含 123 的所有实例。如果自由文本搜索返回不需要的匹配项，请再应用其他筛选条件。

按属性搜索

按属性搜索可让您在所有资源中搜索特定属性。

> **Note**
>
> 属性搜索可以使用 API 筛选或客户端筛选，具体取决于所选的属性。执行属性搜索时，会相应地对属性进行分组。

例如，您可以搜索所有实例的 Instance state 属性，以便仅返回处于 `stopped` 状态的实例。要实现此目的，应按照以下步骤进行：

1. 在实例屏幕上的搜索字段中，开始输入 `Instance state`。输入字符时，实例状态将显示两种类型的筛选条件：API 筛选条件和客户端筛选条件。
2. 要在服务器端进行搜索，请在 API 筛选条件下选择 实例状态。要在客户端进行搜索，请在客户端筛选条件下选择实例状态（客户端）。

这时会显示所选属性的可能运算符列表。

3. 选择 =（等于）运算符。

   这时会显示所选属性和运算符的可能值列表。

4. 从列表中选择已停止。

按标签搜索

借助按标签搜索功能，您可以按标签键或标签值来筛选当前显示的表中的资源。

标签搜索使用 API 筛选或客户端筛选方式，具体取决于 Preferences（首选项）窗口中的设置。

确保对标签执行 API 筛选

1. 打开 Preferences（首选项）窗口。
2. 清除 Use regular expression matching（使用正则表达式匹配）复选框。如果选中此复选框，则将执行客户端筛选。
3. 选择 Use case sensitive matching（使用区分大小写的匹配）复选框。如果清除了此复选框，则将执行客户端筛选。
4. 选择 Confirm（确认）。

按标签搜索时，您可以使用以下值：

- （空）– 查找具有指定标签键，但必须不具有标签值的所有资源。
- All values（所有值）– 查找具有指定标签键和任何标签值的所有资源。
- Not tagged（未添加标签）– 搜索不具有指定标签键的所有资源。
- 显示的值 – 查找具有指定标签键和指定标签值的所有资源。

您可以使用以下技术来增强或优化搜索：

逆向搜索

反向搜索可让您搜索与指定的值不匹配的资源。在 Instances（实例）和 AMI 屏幕中，反向搜索的方法是首先选择 != （不等于）或 !: （不包含）运算符，然后选择一个值。在其他屏幕中，反向搜索可通过在搜索关键词前加上感叹号（!）字符来执行。

> **Note**
>
> 只有客户端筛选条件上的关键字搜索和属性搜索支持反向搜索。API 筛选条件上的属性搜索不支持它。

例如，您可以搜索所有实例的实例状态属性，以便包含处于 `terminated` 状态的所有实例。要实现此目的，应按照以下步骤进行：

1. 在实例屏幕上的搜索字段中，开始输入 `Instance state`。输入字符时，实例状态将显示两种类型的筛选条件：API 筛选条件和客户端筛选条件。
2. 在 Client filters（客户端筛选条件）下，选择 Instance state (client) [实例状态（客户端）]。只有客户端筛选条件支持反向搜索。

   这时会显示所选属性的可能运算符列表。

3. 选择 !=（不等于），然后选择 terminated（已终止）。

要根据实例状态属性筛选实例，您还可以使用实例状态列中的搜索图标 ()。带加号 (+) 的搜索图标将显示与该属性匹配的所有实例。带减号 (-) 的搜索图标将排除与该属性匹配的所有实例。

以下是使用反向搜索的另一个示例：要列出未分配名为 `launch-wizard-1` 的安全组的所有实例，则在 Client filters（客户端筛选条件）下，按 Security group name（安全组名称）属性进行搜索，然后选择 != 并在搜索栏中输入 `launch-wizard-1`。

部分搜索

使用部分搜索，可以搜索部分字符串值。要执行部分搜索，请仅输入要搜索的关键字的一部分。在 Instances（实例）和 AMI 屏幕中，部分搜索只能通过 :（包含）运算符来执行。在其他屏幕中，您可以选择该客户端筛选条件属性，然后立即仅输入要搜索的关键词的一部分。例如，在 Instance type（实例类型）屏幕上，要搜索所有 `t2.micro`、`t2.small` 和 `t2.medium` 实例，则按 Instance Type（实例类型）属性进行搜索，然后输入关键词 `t2`。

正则表达式搜索

要使用正则表达式搜索，必须在 Preferences（首选项）中选中 Use regular expression matching（使用正则表达式匹配）复选框。

当需要匹配字段中具有特定模式的值时，可以使用正则表达式。例如，要搜索以 s 开头的值，请搜索 `^s`。要搜索以 `xyz` 结尾的值，请搜索 `xyz$`。或者要搜索以数字开头，后跟一个或多个字符的值，请搜索 `[0-9]+.*`。

> **Note**
>
> 只有客户端筛选条件上的关键字搜索和属性搜索支持正则表达式搜索。API 筛选条件上的属性搜索不支持它。

区分大小写搜索

要使用区分大小写搜索功能，必须在 Preferences（首选项）窗口中选择 Use case sensitive matching（使用区分大小写的匹配）复选框。区分大小写的首选项仅适用于客户端筛选条件和标签筛选条件。

> **Note**
>
> API 筛选条件始终区分大小写。

通配符搜索

使用 * 通配符匹配零个或多个字符。使用 ? 通配符匹配零个或一个字符。例如，假设您有一个包含值 `prod`、`prods`、和 `production` 的数据集，搜索 `prod*` 将会匹配所有值，而 `prod?` 只匹配 `prod` 和 `prods`。要使用文字值，请使用反斜杠 (\ ) 进行转义。例如，“`prod\*`”将匹配 `prod*`。

> **Note**
>
> 仅 API 筛选条件上的属性和标签搜索支持通配符搜索。客户端筛选条件上的关键词搜索以及属性和标签搜索不支持通配符。

合并搜索

通常，具有相同属性的多个筛选条件会自动以 OR 连接。例如，搜索 `Instance State : Running` 和 `Instance State : Stopped` 会返回正在运行或已停止的所有实例。要使用 AND 连接搜索，请跨不同的属性进行搜索。例如，搜索 `Instance State : Running` 和 `Instance Type : c4.large` 只会返回为类型为 `c4.large` 且处于运行状态的实例。

Old console

旧 Amazon EC2 控制台支持以下类型的搜索：

按关键字搜索

按关键字搜索是一种自由文本搜索，可让您在所有资源属性中搜索特定的值。要按关键字进行搜索，请在搜索框中输入或粘贴要查找的内容，然后按 Enter。例如，搜索 123 会匹配其任何属性（例如 IP 地址、实例 ID、VPC ID 或 AMI ID）中包含 123 的所有实例。如果自由文本搜索返回不需要的匹配项，请再应用其他筛选条件。

按属性搜索

按属性搜索可让您在所有资源中搜索特定属性。例如，您可以搜索所有实例的 State 属性，以便仅返回处于 stopped 状态的实例。要实现此目的，应按照以下步骤进行：

1. 在“实例”屏幕上的搜索字段中，开始输入 Instance State。随着您的输入，页面上会显示匹配属性的列表。
2. 从列表中选择 Instance State (实例状态)。此时页面上会显示所选属性的可能值列表。
3. 从列表中选择 Stopped。

您可以使用以下技术来增强或优化搜索：

反向搜索

反向搜索可让您搜索与指定的值不匹配的资源。反向搜索是通过在搜索关键字前面加上感叹号 (!) 字符来执行的。例如，如果要列出所有未终止的实例，请按 Instance State 属性进行搜索，然后输入关键字 !Terminated。

部分搜索

使用部分搜索，可以搜索部分字符串值。要执行部分搜索，请仅输入要搜索的关键字的一部分。例如，要搜索所有 t2.micro、t2.small 和 t2.medium 实例，请按 Instance Type 属性进行搜索，然后输入关键字 t2。

正则表达式搜索

当需要匹配字段中具有特定模式的值时，可以使用正则表达式。例如，如果要搜索具有以 s 开头的属性值的所有实例，请搜索 ^s。或者要搜索具有以 xyz 结尾的属性值的所有实例，请搜索 xyz$。正则表达式搜索不区分大小写。

合并搜索

通常，具有相同属性的多个筛选条件会自动以 OR 连接。例如，搜索 Instance State : Running 和 Instance State : Stopped 会返回正在运行或已停止的所有实例。要使用 AND 连接搜索，请跨不同的属性进行搜索。例如，搜索 Instance State : Running 和 Instance Type : c4.large 只会返回为 c4.large 且处于停止状态的实例。

使用 CLI 和 API 列出并筛选

每个资源类型都有相应的 CLI 命令和 API 操作，您可用来列出该类型的资源。生成的资源列表可能很长，因此筛选结果以仅包括符合特定条件的资源可能会更快、更有用。

筛选注意事项

- 您可以在单一请求中指定多个筛选条件和多个筛选条件值。
- 您可以将通配符与筛选值一同使用。星号 (*) 匹配零个或多个字符，而问号 (?) 匹配零个或一个字符。
- 筛选值区分大小写。
- 您的搜索中可包含通配符的字面值；您只需要在字符前用反斜线隔开字符。例如，用 *amazon\?\\ 值搜索文字字符串 *amazon?\。

支持的筛选条件

要查看每个 Amazon EC2 资源支持的筛选条件，请参阅以下文档：

- Amazon CLI：Amazon CLI Command Reference-Amazon EC2 中的 describe 命令。
- Tools for Windows PowerShell：Amazon Tools for PowerShell Cmdlet Reference-Amazon EC2 中的 Get 命令。

- 查询 API：Amazon EC2 API Reference 中的 Describe API 操作。

Example 示例：指定单个筛选条件

您可以使用 describe-instances 列出 Amazon EC2 实例。如果没有筛选条件，响应将包含您的所有资源的信息。您可以使用以下命令在输出中仅包含正在运行的实例。

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

要仅列出正在运行的实例的实例 ID，请按如下方式添加 --query 参数。

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

下面是示例输出。

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example 示例：指定多个筛选条件或筛选条件值

如果指定多个筛选条件或多个筛选条件值，则资源必须与所有筛选条件匹配才能包括在结果中。

您可以使用以下命令列出类型为 m5.large 或 m5d.large 的所有实例。

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

您可以使用以下命令列出类型为 t2.micro 的所有已停止实例。

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped Name=instance-
type,Values=t2.micro
```

Example 示例：在筛选条件值中使用通配符

如果在使用 describe-snapshots 描述 EBS 快照时将 database 指定为 description 筛选条件的筛选条件值，则该命令将仅返回描述为“database”的快照。

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

* 通配符可与零个或多个字符匹配。如果将 *database* 指定为筛选条件值，则该命令将仅返回其描述包含“database”一词的快照。

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

? 通配符完全匹配 1 个字符。如果指定 database? 作为筛选条件值，该命令将仅返回描述为“database”或“database”后跟一个字符的快照。

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

如果指定 database????，该命令将仅返回其描述为“数据库”后跟最多四个字符的快照。它不包括带有“数据库”后跟五个或更多字符的说明。

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example 示例：基于日期进行筛选

使用 Amazon CLI，您可以使用 JMESPath 通过表达式来筛选结果。例如，以下 describe-snapshots 命令会显示 Amazon Web Services 账户 在指定日期（由 *2020-03-31* 表示）之前创建的所有快照的 ID（由 *123456789012* 表示）。如果未指定所有者，则结果将包括所有公有快照。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?
(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

以下命令显示在指定日期范围内创建的所有快照的 ID。

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?
(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --output text
```

基于标签进行筛选

有关如何根据资源标签筛选资源列表的示例，请参阅通过命令行使用标签 (p. 1672)。

使用 Amazon EC2 全局视图列出和筛选跨区域的资源

通过 Amazon EC2 全局视图，您可以在单个控制台中跨单个 Amazon 区域或跨多个区域查看一些 Amazon EC2 和 Amazon VPC 资源。使用 Amazon EC2 全局视图，可以查看已启用 Amazon Web Services 账户 的所有区域中所有 VPC、子网、实例、安全组、卷和自动扩缩组的摘要。Amazon EC2 全局视图还提供 global search（全局搜索）功能，让您能同时搜索多个区域中的特定资源或特定资源类型。

Amazon EC2 全局视图不允许您以任何方式修改资源。

所需的权限

用户必须具有以下权限才能使用 Amazon EC2 全局视图。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs",
    "ec2:DescribeRegions",
    "ec2:DescribeVolumes",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "autoscaling:DescribeAutoScalingGroups"
  ],
  "Resource": "*"
  }]
}
```

使用 Amazon EC2 全局视图

通过以下网址打开 Amazon EC2 全局视图控制台：https://console.aws.amazon.com/ec2globalview/home。

> **Important**
>
> 您不能在 Firefox 中使用私密窗口来访问 Amazon EC2 全局视图。

控制台由两个选项卡组成：

- Region explorer（区域资源管理器）— 此选项卡包括以下各节：

- Resource summary（资源摘要）— 高度概述了所有区域资源的情况。

  已启用区域表示已启用 Amazon Web Services 账户 的区域数。剩余字段表示您当前在这些区域中拥有的资源数量。选择任何链接以查看所有区域该类型的资源。例如，如果 Instances（实例）标签以下的链接是 29 in 10 Regions（10 个区域中的 29 个），它表示您当前在 10 个区域有 29 个实例。选择该链接以查看所有 29 个实例的列表。
- 每个区域的资源数 – 列出所有 Amazon Web Services 区域（包括未启用账户的区域），并提供每个区域每种资源类型的总计。

  选择区域名称，以查看该特定区域所有类型的所有资源。例如，选择 Africa (Cape Town) af-south-1（非洲（开普敦）af-south-1）可查看该区域中的所有 VPC、子网、实例、安全组、卷和自动扩缩组。或者，选择一个区域，然后选择 View resources for selected Region（查看所选区域的资源）。

  选择特定区域中特定资源类型的值，以便仅查看该区域中该类型的资源。例如，选择 Africa (Cape Town) af-south-1（非洲（开普敦）af-south-1）实例的值，以仅查看该区域中的实例。
- Global search（全局搜索）— 使用此选项卡，您可以在单个区域或跨多个区域搜索特定资源或特定资源类型。它还使您能够查看特定资源的详细信息。

  要搜索资源，请在网格前面的字段中输入搜索条件。您可以按区域、按资源类型以及按分配给资源的标签进行搜索。

  要查看特定资源的详细信息，请在网格中选中。您也可以选择资源的资源 ID，以在各自的控制台中打开该资源。例如，选择实例 ID 以在 Amazon EC2 控制台中打开实例，或选择子网 ID 以在 Amazon VPC 控制台中打开子网。

标记 Amazon EC2 资源

为了方便您管理实例、映像以及其他 Amazon EC2 资源，您可通过标签 的形式为每个资源分配元数据。标签可让您按各种标准（例如用途、所有者或环境）对 Amazon 资源进行分类。这在您具有相同类型的很多资源时会很有用—您可以根据分配给特定资源的标签快速识别该资源。本主题介绍标签并说明如何创建标签。

> Warning
>
> 很多不同的 API 调用返回标签键及其值。拒绝访问 `DescribeTags` 不会自动拒绝访问其他 API 返回的标签。作为最佳实践，我们建议您不要在标签中包含敏感数据。

目录

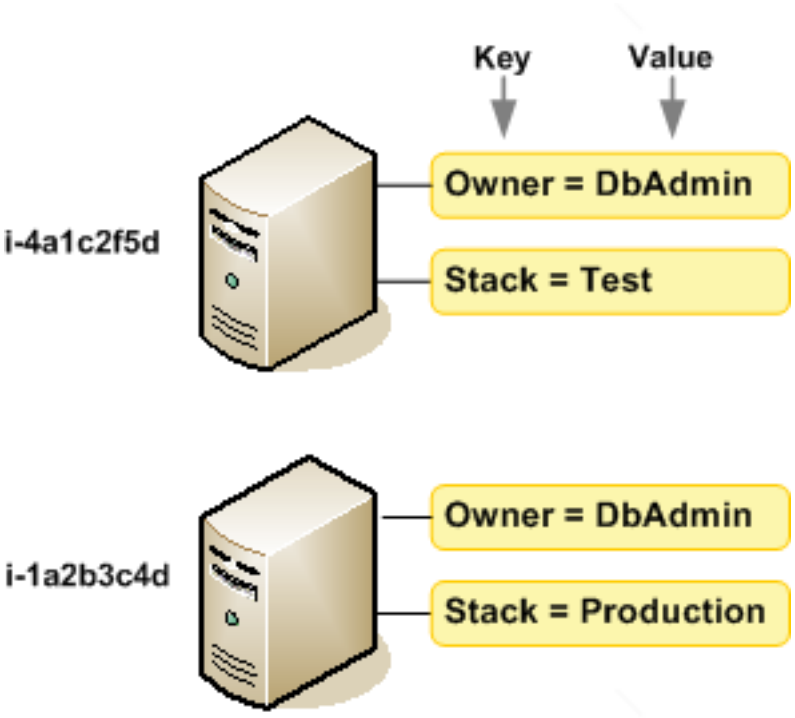
- 有关标签的基本知识 (p. 1664)
- 标记 资源 (p. 1665)
- 标签限制 (p. 1668)
- 标签和访问管理 (p. 1668)
- 为资源添加标签以便于进行计费 (p. 1669)
- 通过控制台使用标签 (p. 1669)
- 通过命令行使用标签 (p. 1672)
- 使用实例元数据中的实例标签 (p. 1675)
- 使用 CloudFormation 为资源添加标签 (p. 1677)

有关标签的基本知识

标签是为 Amazon 资源分配的标记。每个标签都包含您定义的一个键 和一个可选值。

标签可让您按各种标准（例如用途、所有者或环境）对 Amazon 资源进行分类。例如，您可以为账户中的 Amazon EC2 实例定义一组标签，以跟踪每个实例的所有者和堆栈级别。

下图说明了标签的工作方式。在此示例中，您为每个实例分配了两个标签 — 一个标签使用键 Owner，另一个使用键 Stack。每个标签都拥有相关的值。



我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理资源时会更加轻松。您可以根据添加的标签搜索和筛选资源。有关如何实施有效资源标记策略的更多信息，请参阅 标记最佳实践 Amazon 白皮书。

标签对 Amazon EC2 没有任何语义意义，应严格按字符串进行解析。同时，标签不会自动分配至您的资源。您可以修改标签的密钥和值，还可以随时删除资源的标签。您可以将标签的值设为空的字符串，但是不能将其设为空值。如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。如果删除资源，资源的所有标签也会被删除。

Note

删除资源后，其标签可能会在短时间内在控制台、API 和 CLI 输出中仍保持可见。这些标签将逐步解除与资源的关联，并永久删除。

标记 资源

您可以标记您的账户中已存在的大多数 Amazon EC2 资源。下面的表 (p. 1666)列出了支持标记的资源。

如果使用的是 Amazon EC2 控制台，则您可以使用相关资源屏幕上的 Tags (标签) 选项卡或使用 Tags (标签) 屏幕向资源应用标签。在您创建资源时，某些资源屏幕能让您为资源指定标签；例如，具有 Name 键并且具有您指定的值的标签。在大多数情况下，控制台会在资源创建后 (而不是在资源创建期间) 立即应用标签。控制台可能根据 Name 标签对资源进行组织，但此标签对于 Amazon EC2 服务没有任何语义意义。

如果使用的是 Amazon EC2 API、Amazon CLI 或 Amazon 软件开发工具包，则您可以使用 CreateTags EC2 API 操作向现有资源应用标签。此外，某些资源创建操作允许您在创建资源时为其指定标签。如果无法在资源创建期间应用标签，系统会回滚资源创建过程。这样可确保要么创建带有标签的资源，要么根本不创建资源，即任何时候都不会创建出未标记的资源。通过在创建时标记资源，您不需要在资源创建后运行自定义标记脚本。有关允许用户在创建时标记资源的更多信息，请参阅 在创建过程中授予标记资源的权限 (p. 1231)。

下表描述了可以标记的 Amazon EC2 资源以及可在创建时使用 Amazon EC2 API、Amazon CLI 或 Amazon 软件开发工具包标记的资源。

Amazon EC2 资源标记支持

资源	支持标签	支持在创建时标记
AFI	是	是
AMI	是	是
捆绑任务	否	否
Capacity Reservation	是	是
运营商网关	是	是
客户端 VPN 终端节点	是	是
客户端 VPN 路由	否	否
客户网关	是	是
Dedicated Host	是	是
专用主机 预留	是	是
DHCP 选项	是	是
EBS 快照	是	是
EBS 卷	是	是
EC2 Fleet	是	是
仅出口 Internet 网关	是	是
弹性 IP 地址	是	是
Elastic Graphics 加速器	是	否
实例	是	是
实例事件窗口	是	是
实例存储卷	不适用	不适用
Internet 网关	是	是
IP 地址池 (BYOIP)	是	是
密钥对	是	是
启动模板	是	是
启动模板版本	否	否
本地网关	是	否
本地网关路由表	是	否
本地网关虚拟接口	是	否
本地网关虚拟接口组	是	否

资源	支持标签	支持在创建时标记
本地网关路由表 VPC 关联	是	是
本地网关路由表虚拟接口组关联	是	否
NAT 网关	是	是
网络 ACL	是	是
网络接口	是	是
置放群组	是	是
前缀列表	是	是
Reserved Instance	是	否
Reserved Instance清单	否	否
路由表	是	是
竞价型实例集请求	是	是
竞价型实例请求	是	是
安全组	是	是
安全组规则	是	否
子网	是	是
流量镜像筛选	是	是
流量镜像会话	是	是
流量镜像目标	是	是
转换网关	是	是
Transit Gateway 多播域	是	是
中转网关路由表	是	是
转换网关 VPC 连接	是	是
虚拟专用网关	是	是
VPC	是	是
VPC 终端节点	是	是
VPC 终端节点服务	是	是
VPC 终端节点服务配置	是	是
VPC 流日志	是	是
VPC 对等连接	是	是
VPN 连接	是	是

您可以在创建时使用 Amazon EC2 控制台中的 Amazon EC2 启动实例向导 (p. 577)为实例、卷、Elastic Graphics、网络接口和竞价型实例请求添加标签。您可以在创建时使用卷屏幕为 EBS 卷添加标签，使用快照屏幕为 EBS 快照添加标签。或者，也可以使用资源创建 Amazon EC2 API（例如 RunInstances）在创建资源时应用标签。

对于支持在创建时进行标记的 Amazon EC2 API 操作，您可以在 IAM policies 中应用基于标签的资源级权限，以对可在创建时标记资源的用户和组实施精细控制。您的资源从创建开始会受到适当的保护 — 标签会立即用于您的资源，因此控制资源使用的任何基于标签的资源级权限都会立即生效。可以更准确地对您的资源进行跟踪和报告。您可以强制对新资源使用标记，可以控制对资源设置哪些标签键和值。

此外，您还可以在 IAM policies 中对 `CreateTags` 和 `DeleteTags` Amazon EC2 API 操作应用资源级权限，从而控制对现有资源设置哪些标签键和值。有关更多信息，请参阅示例：标记资源 (p. 1261)。

有关标记资源以便于计费的更多信息，请参阅 Amazon Billing 用户指南中的使用成本分配标签。

标签限制

下面是适用于标签的基本限制：

- 每个资源的标签数上限 – 50
- 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值。
- 最大键长度 – 128 个 Unicode 字符（采用 UTF-8 格式）
- 最大值长度 – 256 个 Unicode 字符 (采用 UTF-8 格式)
- 允许使用的字符
  - 虽然 EC2 允许在其标签中使用任何字符，但其他服务具有更严格的限制。允许在不同的服务中使用的字符包括：可以使用 UTF-8 表示的字母（`a-z`、`A-Z`）、数字（`0-9`）和空格以及以下字符：`+ - = . _ : / @`。
  - 如果在实例元数据中启用实例标签，实例标签键只能使用字母 (`a-z`、`A-Z`)、数字 (`0-9`) 及以下字符：`+ - = . , _ : @`。实例标签 keys 不能包含空格或 `/`，也不能只包含 `.`（一个句号）、`..`（两个句号）或 `_index`。有关更多信息，请参阅使用实例元数据中的实例标签 (p. 1675)。
- 标签键和值区分大小写。
- `aws:` 前缀专门预留供 Amazon 使用。如果某个标签具有带有此标签键，则您无法编辑该标签的键或值。具有 `aws:` 前缀的标签不计入每个资源的标签数限制。

您不能仅依据标签终止或删除资源，而必须指定资源的标识符。例如，要删除您使用名为 `DeleteMe` 的标签键标记的快照，您必须将 `DeleteSnapshots` 操作与快照的资源标识符 (如 `snap-1234567890abcdef0`) 结合使用。

当您为公有或共享资源添加标签时，您分配的标签仅对您的 Amazon 账户可用；其他 Amazon 账户无权访问这些标签。为了对共享资源进行基于标签的访问控制，每个 Amazon 账户必须分配自己的一组标签来控制对资源的访问。

您无法标记所有资源。有关更多信息，请参阅Amazon EC2 资源标记支持 (p. 1666)。

标签和访问管理

如果您使用的是 Amazon Identity and Access Management (IAM)，则可以控制Amazon账户中的哪些用户拥有创建、编辑或删除标签的权限。有关更多信息，请参阅在创建过程中授予标记资源的权限 (p. 1231)。

您还可以使用资源标签来实现基于属性的控制 (ABAC)。您可以创建 IAM policies，基于资源标签允许操作。有关更多信息，请参阅使用资源标签控制对 EC2 资源的访问 (p. 1233)。

为资源添加标签以便于进行计费

您也可以使用标签来组织您的 Amazon 账单，使其反映您的成本结构。要执行此操作，请注册以获取包含标签键值的 Amazon 账户账单。有关设置带有标签的成本分配报告的更多信息，请参阅 Amazon Billing 用户指南中的月度成本分配报告。如需查看组合资源的成本，请按具有相同标签键值的资源组织您的账单信息。例如，您可以将特定的应用程序名称用作几个资源的标签，然后组织账单信息，以查看在数个服务中的使用该应用程序的总成本。有关更多信息，请参阅 Amazon Billing 用户指南中的使用成本分配标签。

Note

如果您已启用报告，则可以在 24 小时后查看当月的数据。

成本分配标签可指示哪些资源导致产生成本，而删除或停用资源并不总是能降低成本。例如，即使删除包含原始数据的快照，其他快照引用的快照数据也将保留。有关更多信息，请参阅 Amazon Billing 用户指南中的 Amazon Elastic Block Store 卷和快照。

Note

标记的弹性 IP 地址不会显示在成本分配报告中。

通过控制台使用标签

通过使用 Amazon EC2 控制台，您可以查看在同一区域的所有 Amazon EC2 资源中使用了哪些标签。您可以按资源和资源类型来查看资源，也可以查看与指定标签相关的每种资源类型的项目数量。您还可以通过 Amazon EC2 控制台同时在一个或多个资源中应用或删除标签。

要了解有关使用筛选条件列出资源的更多信息，请参阅 列出并筛选您的资源 (p. 1657)。

为便于使用并取得最佳结果，请使用 Amazon Web Services Management Console中的标签编辑器，此编辑器提供了一种用于创建和管理标签的集中而统一的方法。有关更多信息，请参阅 Amazon Web Services Management Console 入门中的标签编辑器。

任务

- 显示标签 (p. 1669)
- 在单个资源上添加和删除标签 (p. 1670)
- 向一组资源添加和删除标签 (p. 1671)
- 在启动实例时添加标签 (p. 1671)
- 按标签筛选资源列表 (p. 1672)

显示标签

您可以在 Amazon EC2 控制台中以两种不同的方式显示标签。您可以显示单个资源或所有资源的标签。

显示单个资源的标签

当您在 Amazon EC2 控制台中选择特定资源页面时，它会显示这些资源列表。例如，如果您从导航窗格中选择实例，则控制台会显示您的 Amazon EC2 实例。当您从其中一个列表中选择一种资源时 (例如，实例)，如果该资源支持标签，则您可以查看和管理标签。在大多数资源页面上，您可以通过选择 Tags（标签）选项卡来查看标签。

您可以在资源列表中添加列，以显示密钥相同的标签的所有值。您可以使用该列按照标签对资源列表进行分类和筛选。

New console

- 选择屏幕右上角齿轮形状的 Preferences（首选项）图标。在 Preferences（首选项）对话框中，在 Tag columns（标签列）下，选择其中一个标签键，然后选择 Confirm（确认）。

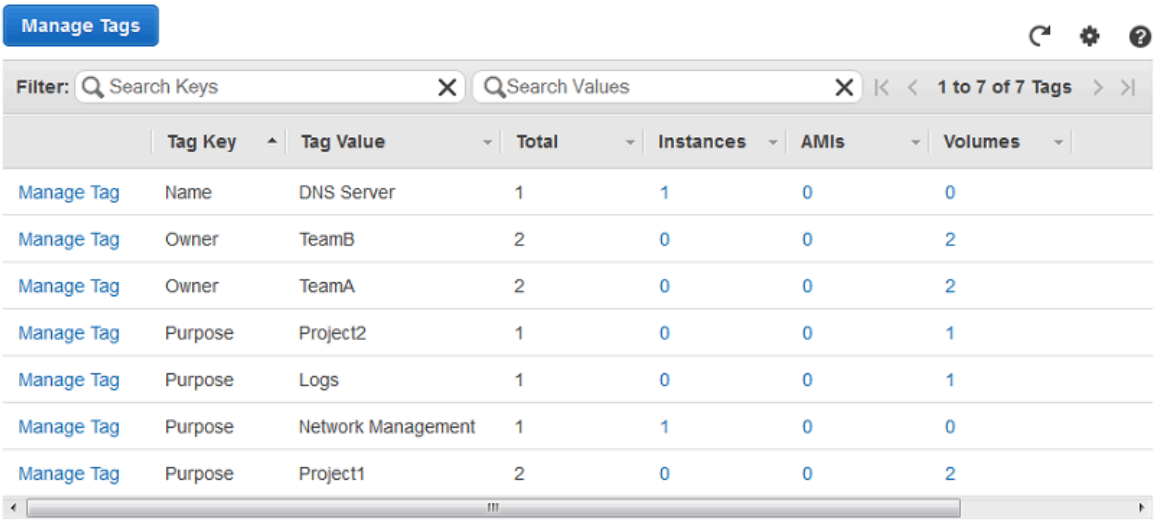
Old console

资源列表中添加新列以显示标签的方法有两种：

- 在 Tags 选项卡上，选择 Show Column。控制台中添加了一个新列。
- 选择 Show/Hide Columns 齿轮状图标，然后在 Show/Hide Columns 对话框中的 Your Tag Keys 下选择标签键。

显示所有资源的标签

您可以通过选择 Amazon EC2 控制台导航窗格中的 Tags (标签)，显示所有资源的标签。下图显示了 Tags (标签) 窗格，其中按资源类型列出了所有正在使用的标签。



在单个资源上添加和删除标签

您可以直接在资源页面管理单个资源的标签。

向单个资源添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中，选择要标记的资源所在区域。有关更多信息，请参阅资源位置 (p. 1656)。
3. 在导航窗格中，选择资源类型 (例如，Instances)。
4. 从资源列表中选择资源，然后选择标签选项卡。
5. 依次选择管理标签、添加标签。输入标签的键和值。完成添加标签后，选择保存。

删除单个资源的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中，选择要取消标记的资源所在区域。有关更多信息，请参阅资源位置 (p. 1656)。
3. 在导航窗格中，选择资源类型 (例如，Instances)。
4. 从资源列表中选择资源，然后选择标签选项卡。
5. 选择 Manage tags (管理标签)。对于每个标签，选择删除。完成删除标签后，选择保存。

向一组资源添加和删除标签

为一组资源添加标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中，选择要标记的资源所在区域。有关更多信息，请参阅资源位置 (p. 1656)。
3. 在导航窗格中，选择 Tags。
4. 在内容窗格的顶部，选择 Manage Tags。
5. 对于筛选条件，选择资源类型（例如，实例）。
6. 在资源列表中，选中每个资源旁边的复选框。
7. 在添加标签下，输入标签的键和值，然后选择添加标签。

   Note

   如果您添加的新标签的标签键与现有标签的相同，则新标签将覆盖现有标签。

删除一组资源的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中，选择要取消标记的资源所在区域。有关更多信息，请参阅资源位置 (p. 1656)。
3. 在导航窗格中，依次选择 Tags、Manage Tags。
4. 要查看正在使用的标签，请选择 Show/Hide Columns 齿轮状图标，然后在 Show/Hide Columns 对话框中，选择要查看的标签键，然后选择 Close。
5. 对于筛选条件，选择资源类型（例如，实例）。
6. 在资源列表中，选中每个资源旁边的复选框。
7. 在删除标签下，输入标签键，然后选择删除标签。

在启动实例时添加标签

New console

使用启动实例向导添加标签

1. 在导航栏中，选择的实例的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。选择满足您的需求的区域。有关更多信息，请参阅资源位置 (p. 1656)。
2. 选择 Launch instance (启动实例)。
3. 在 Name and tags（名称和标签）下，您可以为实例输入描述性名称并指定标签。

   实例名称是一个标签，其中密钥为 Name（名称），而值为您指定的名称。您可以标记实例、卷、弹性图形和网络接口。对于竞价型实例，您只能标记竞价型实例请求。

   指定实例名称和其它标签为可选项。

   - 对于 Name（名称），为实例输入一个描述性名称。如果您没有指定名称，则可以通过其 ID 标识实例，该 ID 将在您启动实例时自动生成。
   - 要添加其它标签，请选择 Add additional tags（添加其它标签）。选择 Add tag（添加标签），然后输入密钥和值，然后选择要标记的资源类型。为每个要添加的其它标签选择 Add tag（添加标签）。
4. 在 Application and OS Images (Amazon Machine Image) [应用程序和操作系统镜像（Amazon Machine Image）] 下，为您的实例选择操作系统（OS），然后选择 AMI。有关更多信息，请参阅应用程序和操作系统镜像 (Amazon Machine Image) (p. 577)。

5. （可选）在 Key pair (login)（密钥对（登录））下，为 Key pair name（密钥对名称）选择一个现有密钥对或新建一个密钥对。
6. 将所有其他字段保持为其默认值，或为所需的实例配置选择特定值。有关字段的信息，请参阅 使用定义的参数启动实例 (p. 577)。
7. 在 Summary（摘要）面板中，查看配置，然后选择 Launch instance（启动实例）。

Old console

使用启动实例向导添加标签

1. 在导航栏中，选择的实例的区域。选择该内容是非常重要的，因为可以在区域之间共享某些 Amazon EC2 资源，而无法共享其他资源。选择满足您的需求的区域。有关更多信息，请参阅资源位置 (p. 1656)。
2. 选择 Launch Instance（启动实例）。
3. Choose an Amazon Machine Image (AMI) (选择 Amazon Machine Image (AMI)) 页面会显示称为“Amazon Machine Image (AMI)”的基本配置的列表。选择要使用的 AMI，然后选择 Select。有关更多信息，请参阅查找 Linux AMI (p. 116)。
4. 在 Configure Instance Details 页面上，根据需要配置实例设置，然后选择 Next: Add Storage。
5. 在 Add Storage (添加存储) 页面上，您可以为实例指定额外的存储卷。完成后，选择 Next: Add Tags。
6. 在 Add Tags 页面上，为实例、卷或两者指定标签。选择 Add another tag 以向您的实例添加多个标签。完成时选择 Next: Configure Security Group（下一步：配置安全组）。
7. 在 Configure Security Group (配置安全组) 页面上，您可以从您所拥有的现有安全组中进行选择，或根据向导的指示创建新的安全组。完成操作后，选择 Review and Launch。
8. 检视您的设置。在您确认选择无误之后，选择 Launch。选择现有密钥对或创建新的密钥对，选中确认复选框，然后选择 Launch Instances。

按标签筛选资源列表

您可以基于一个或多个标签键和标签值来筛选资源列表。

按标签筛选资源列表

1. 在导航窗格中，选择资源类型 (例如，Instances)。
2. 选择搜索字段。
3. 从列表中选择标签键。
4. 从列表中选择相应的标签值。
5. 完成后，删除筛选条件。

有关筛选条件的更多信息，请参阅列出并筛选您的资源 (p. 1657)。

通过命令行使用标签

您可以在创建许多 EC2 资源时，使用创建命令的标签规范参数将标签添加到这些资源。您可以使用资源的描述命令查看资源的标签。您还可以使用以下命令为现有资源添加、更新或删除标签。

任务	Amazon CLI	Amazon Tools for Windows PowerShell
添加或覆盖一个或多个标签	create-tags	New-EC2Tag

任务	Amazon CLI	Amazon Tools for Windows PowerShell
删除一个或多个标签	delete-tags	Remove-EC2Tag
描述一个或多个标签	describe-tags	Get-EC2Tag

任务

- 在创建资源时添加标签 (p. 1673)
- 向现有资源添加标签 (p. 1674)
- 描述标记的资源 (p. 1675)

在创建资源时添加标签

以下示例说明如何在创建资源时应用标签。

Note

在命令行中输入 JSON 格式参数的方式因操作系统而异。

- Linux、macOS 或 Unix 和 Windows PowerShell – 使用单引号（'）括住 JSON 数据结构。
- Windows – 在 Windows 命令行中使用命令时，不使用单引号。

有关更多信息，请参阅为 Amazon CLI 指定参数值。

Example 示例：启动实例并向实例和卷应用标签

以下 run-instances 命令启动实例，并将键为 **webserver** 和值为 **production** 的标签应用于实例。该命令还向创建的任何 EBS 卷（此示例中为根卷）应用键为 **cost-center** 且值为 **cc123** 的标签。

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

您可以在启动时向实例和卷应用相同的标签键和值。下面的命令启动一个实例并向此实例和创建的任何 EBS 卷应用键为 **cost-center**、值为 **cc123** 的标签。

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example 示例：创建卷并应用标签

下面的 create-volume 命令创建一个卷并应用两个标签：**purpose=production** 和 **cost-center=cc123**。

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

向现有资源添加标签

以下示例演示如何使用 create-tags 命令向现有资源添加标签。

Example 示例：将标签添加到资源

以下示例将标签 **Stack=production** 添加到指定的映像，或者覆盖该 AMI 的现有标签（其中标签键为 **Stack**）。如果命令成功，则不返回任何输出。

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example 示例：将标签添加到多个资源

此示例为 AMI 和实例添加（或覆盖）两个标签。其中一个标签仅包含键 (**webserver**)，不包含值（我们将值设置为空字符串）。另一个标签则包含键 (**stack**) 和值 (**Production**)。如果命令成功，则不返回任何输出。

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example 示例：使用特殊字符添加标签

此示例将标签 **[Group]=test** 添加到实例。方括号（**[** 和 **]**）是特殊字符，必须对其进行转义。

如果您使用的是 Linux 或 OS X，要转义特殊字符，请用双引号 (**"**) 将具有特殊字符的元素引起来，然后用单引号 (**'**) 将整个键和值结构引起来。

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

如果您使用的是 Windows，要转义特殊字符，请用双引号 (") 将具有特殊字符的元素引起来，然后在每个双引号字符前面添加反斜杠 (****)，如下所示：

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

如果您使用的是 Windows PowerShell，要转义特殊字符，请用双引号 (**"**) 将具有特殊字符的值引起来，在每个双引号字符前面添加反斜杠 (****)，然后用单引号 (**'**) 将整个键和值结构引起来，如下所示：

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

描述标记的资源

以下示例展示如何将筛选条件与 describe-instances 结合使用，以查看具有特定标签的实例。所有 EC2 描述命令都使用此语法跨单个资源类型按标签进行筛选。或者，您可以使用 describe-tags 命令按标签跨 EC2 资源类型进行筛选。

Example 示例：描述具有指定标签键的实例

以下命令描述了具有 **Stack** 标签（无论标签的值如何）的实例。

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example 示例：描述具有指定标签的实例

以下命令描述具有标签 **Stack=production** 的实例。

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example 示例：描述具有指定标签值的实例

以下命令描述了具有值为 **production** 的标签（无论标签键如何）的实例。

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example 示例：描述具有指定标签的所有 EC2 资源

以下命令描述带有标签 **Stack=Test** 的所有 EC2 资源。

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

使用实例元数据中的实例标签

您可以从实例元数据访问实例的标签。通过从实例元数据访问标签，您无需再使用 DescribeInstances 或 DescribeTags API 调用来检索标签信息，这可以减少每秒的 API 事务量，并允许您的标签检索随您控制的实例数量扩展。此外，在实例上运行的本地进程可以直接从实例元数据中查看实例的标签信息。

默认情况下，实例元数据中不提供标签；您必须明确允许访问。您可以在实例启动时或启动后在正在运行或停止的实例上允许访问。您还可以通过在启动模板中指定标签来允许访问标签。使用模板启动的实例允许访问实例元数据中的标签。

如果您添加或删除实例标签，对于基于 Nitro 系统构建的实例 (p. 246)，实例元数据将在实例运行时更新，无需停止后再启动实例。对于所有其他实例，要更新实例元数据中的标签，您必须停止后再启动实例。

主题

- 允许访问实例元数据中的标签 (p. 1676)
- 关闭对实例元数据中的标签的访问 (p. 1676)
- 查看是否允许访问实例元数据中的标签 (p. 1677)
- 从实例元数据中检索标签 (p. 1677)

允许访问实例元数据中的标签

默认情况下，无法访问实例元数据中的实例标签。对于每个实例，您必须使用以下方法之一明确允许访问。

要允许使用控制台访问实例元数据中的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions（操作）、Instance settings（实例设置）、Allow tags in instance metadata（允许实例元数据中的标签）。
4. 要允许访问实例元数据中的标签，请选择 Allow（允许）复选框。
5. 选择 Save（保存）。

要允许使用 Amazon CLI 在启动时访问实例元数据中的标签

使用 run-instances 命令并将 `InstanceMetadataTags` 设置为 `enabled`。

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

要允许使用 Amazon CLI 访问正在运行或已停止的实例上的实例元数据中的标签

请使用 modify-instance-metadata-options 命令，并将 `--instance-metadata-tags` 设置为 `enabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

关闭对实例元数据中的标签的访问

要关闭对实例元数据中的实例标签的访问，请使用以下方法之一。您无需在启动时关闭对实例元数据上的实例标签的访问，因它处于关闭状态。

要使用控制台关闭对实例元数据中的标签的访问

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择实例，然后依次选择 Actions（操作）、Instance settings（实例设置）、Allow tags in instance metadata（允许实例元数据中的标签）。
4. 要关闭对实例元数据中的标签的访问，请清除 Allow（允许）复选框。
5. 选择 Save（保存）。

要使用 Amazon CLI 关闭对实例元数据中的标签的访问

请使用 modify-instance-metadata-options 命令，并将 `--instance-metadata-tags` 设置为 `disabled`。

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
```

```
    --instance-metadata-tags disabled
```

查看是否允许访问实例元数据中的标签

对于每个实例，您可以使用 Amazon EC2 控制台或 Amazon CLI 查看是否允许从实例元数据对实例标签进行访问。

查看是否允许使用控制台访问实例元数据中的标签

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances（实例），然后选择实例。
3. 在 Details（详细信息）选项卡上，选中 Allow tags in instance metadata（允许实例元数据中的标签）字段。如果该值为 Enabled（已启用），则允许实例元数据中的标签。如果该值为 Disabled（禁用），则不允许实例元数据中的标签。

查看是否允许使用 Amazon CLI 访问实例元数据中的标签

使用 describe-instances 命令并指定实例 ID。

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

以下示例输出已由于空间问题被截断。"InstanceMetadataTags" 参数表明是否允许实例元数据中的标签。如果该值为 enabled，则允许实例元数据中的标签。如果该值为 disabled，则不允许实例元数据中的标签。

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
   ...

   "MetadataOptions": {
   "State": "applied",
   "HttpTokens": "optional",
   "HttpPutResponseHopLimit": 1,
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "disabled",
   "InstanceMetadataTags": "enabled"
   },
   ...
```

从实例元数据中检索标签

如果实例元数据中允许使用实例标签，则可以从实例元数据访问 tags/instance 类别。有关如何从实例元数据中检索标签的示例，请参阅 获取实例的实例标签 (p. 773)。

使用 CloudFormation 为资源添加标签

对于 Amazon EC2 资源类型，您可以使用 Tags 或 TagSpecifications 属性指定标签。

以下示例使用其 Tags 属性将标签 **Stack=Production** 添加到 AWS::EC2::Instance。

Example 示例：YAML 中的 Tags

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example 示例：JSON 中的 Tags

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

以下示例使用其 TagSpecifications 属性将标签 **Stack=Production** 添加到 AWS::EC2::LaunchTemplate LaunchTemplateData。

Example 示例：YAML 中的 TagSpecifications

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example 示例：JSON 中的 TagSpecifications

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Amazon EC2 Service Quotas

Amazon EC2 提供您可使用的不同资源。这些资源包括映像、实例、卷和快照。在创建 Amazon 账户时，我们根据区域设置对这些资源的默认配额（也称为限制）。举例来说，对于您可以在某一区域中启动的实例，存在一个最大数量限制。因此，举个例子，当您在 美国西部（俄勒冈） 区域中启动实例时，请求一定不能导致您的用量超出您在该区域中的最大实例数限制。

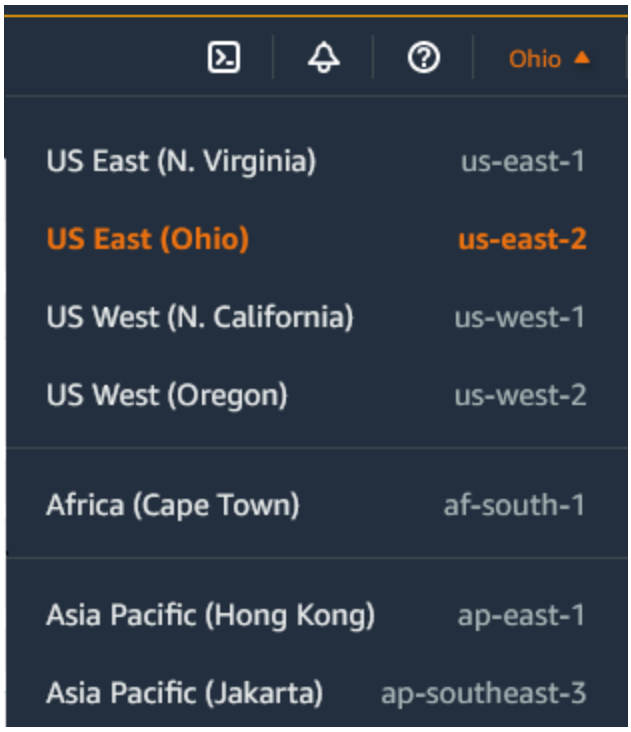
Amazon EC2 控制台提供了对 Amazon EC2 和 Amazon VPC 控制台管理的资源的限制信息。您可以请求提高这些限制的值。使用我们提供的限制信息可管理您的 Amazon 基础设施。需要时请提前计划请求提高限制。

查看您的当前限制

您可以使用 Amazon EC2 控制台或服务限额控制台来查看和管理每个区域的限制。

使用 Amazon EC2 控制台查看当前限制

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择一个区域。



3. 从导航窗格中，选择 Limits。
4. 在列表中找到资源。您可以使用搜索字段按资源名称或资源组筛选列表。当前限制列显示您的账户对该资源的当前最大限制。

使用服务限额控制台查看当前限制

1. 访问 https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/，打开 Service Quotas 控制台。
2. 从导航栏中选择一个区域。
3. 使用搜索栏按资源名称筛选列表。例如，输入 **`On-Demand`** 即可查找按需型实例的限制。
4. 要查看更多信息，请选择限额名称以打开限额的详细信息页面。

请求提高

您可以查看和管理每个区域的限制。

使用 Amazon EC2 控制台请求提高限制

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择一个区域。
3. 从导航窗格中，选择 Limits。
4. 在列表中选择资源，然后选择请求提高限制。
5. 填写提高限制表格中的必填字段，然后选择提交。我们将通过您指定的联系方式进行响应。

对使用端口 25 发送的电子邮件的限制

在所有实例上，Amazon EC2 默认会限制通过端口 25 对公有 IP 地址的出站流量。您可以请求删除此限制。有关更多信息，请参阅 Amazon 知识中心中的如何从 Amazon EC2 实例或 Amazon Lambda 函数删除端口 25 上的限制？。

Note

此限制不适用于通过端口 25 向以下地点发送的出站流量：

- 存在原始网络接口的 VPC 主 CIDR 块中的 IP 地址。
- RFC 1918、RFC 6598 和 RFC 4193 中定义的 CIDR 中的 IP 地址。

排除 EC2 实例的故障

以下文档可帮助您排查实例存在的问题。

目录

- 排查实例启动问题 (p. 1681)
- 排查实例的连接问题。 (p. 1684)
- 排查实例的停止问题 (p. 1700)
- 排查实例终止（关闭） (p. 1703)
- 通过故障状态检查来排查实例问题 (p. 1704)
- 排查无法访问的实例的问题 (p. 1723)
- 从错误的卷启动 (p. 1726)
- 使用 EC2Rescue for Linux (p. 1727)
- 适用于 Linux 实例的 EC2 Serial Console (p. 1736)
- 发送诊断中断（适用于高级用户） (p. 1752)

有关 Windows 实例的更多帮助信息，请参阅Amazon EC2 用户指南（适用于 Windows 实例）中的排除 Windows 实例的故障。

排查实例启动问题

以下问题将阻止您启动实例。

启动问题

- 设备名称无效 (p. 1681)
- 超出实例限制 (p. 1682)
- 实例容量不足 (p. 1682)
- 当前不支持请求的配置。请查看文档以了解支持的配置。 (p. 1683)
- 实例立即终止 (p. 1683)

设备名称无效

描述

在尝试启动新实例时，您将收到 `Invalid device name` *`device_name`* 错误。

原因

如果您在尝试启动实例时遇到此错误，则请求中为一个或多个卷指定的设备名称无效。可能的原因包括：

- 所选 AMI 目前可能在使用该设备名称。

- 该设备名称可能是为根卷保留的。
- 该设备名称可能用于请求中的另一个卷。
- 该设备名称可能对操作系统无效。

解决方案

要解决问题，请执行以下操作：

- 确保所选 AMI 未使用该设备名称。运行以下命令，查看 AMI 使用的设备名称。

```
$ aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- 确保没有使用为根卷保留的设备名称。有关更多信息，请参阅可用设备名称 (p. 1614)。
- 确保在请求中指定的每个卷都有唯一的设备名称。
- 确保指定的设备名称采用正确格式。有关更多信息，请参阅可用设备名称 (p. 1614)。

超出实例限制

描述

在尝试启动新实例或重新启动已停止的实例时，您将收到 `InstanceLimitExceeded` 错误。

原因

在尝试启动新实例或重新启动已停止的实例时，如果您已达到可在区域中启动的实例的数目限制，则将收到 `InstanceLimitExceeded` 错误。在创建 Amazon 账户时，我们根据区域设置可运行的实例数的默认限制。

解决方案

您可以根据区域请求提高实例限制。有关更多信息，请参阅 Amazon EC2 Service Quotas (p. 1678)。

实例容量不足

描述

在尝试启动新实例或重新启动已停止的实例时，您将收到 `InsufficientInstanceCapacity` 错误。

原因

如果您在尝试启动实例或重新启动已停止的实例时收到此错误，则表示 Amazon 当前没有足够的可用按需容量来服务您的请求。

解决方案

要解决该问题，请尝试以下操作：

- 等待几分钟，然后再次提交您的请求；容量可能经常转移。

- 提交减少了实例数的新请求。例如，如果您要提交 1 个启动包含 15 个实例的请求，请改为尝试提交 3 个包含 5 个实例的请求或 15 个包含 1 个实例的请求。
- 如果您要启动实例，请提交新请求，无需指定可用区。
- 如果您要启动实例，请使用其他实例类型 (可在后期调整大小) 提交新请求。有关更多信息，请参阅更改实例类型 (p. 399)。
- 如果您将实例启动到集群置放群组中，则会获得容量不足错误。有关更多信息，请参阅使用置放群组 (p. 1180)。

当前不支持请求的配置。请查看文档以了解支持的配置。

描述

当您尝试启动新实例时会出现 `Unsupported` 错误，因为不支持实例配置。

原因

错误消息提供了更多详细信息。例如，指定的区域或可用区可能不支持实例类型或实例购买选项。

解决方案

尝试其他实例配置。要搜索符合您要求的实例类型，请参阅 查找 Amazon EC2 实例类型 (p. 396)。

实例立即终止

描述

您的实例会从 `pending` 状态变为 `terminated` 状态。

原因

下面是实例可能立即终止的一些原因：

- 您已超出 EBS 卷限制。有关更多信息，请参阅实例卷限制 (p. 1607)。
- EBS 快照损坏。
- 根 EBS 卷已加密，但您无权访问用于解密的 KMS 密钥。
- 在块储存设备映射中为 AMI 指定的快照已加密，但您无权访问用于解密的 KMS 密钥，或者您无权访问 KMS 密钥 来加密还原的卷。
- 您用来启动实例的由实例存储支持的 AMI 缺少必需部分（一个 image.part.xx 文件）

有关更多信息，请通过以下某种方法了解终止原因。

使用 Amazon EC2 控制台了解终止原因

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择实例。
3. 在第一个选项卡上，在状态转换原因旁边查看原因。

使用 Amazon Command Line Interface 控制台了解终止原因

1. 使用 describe-instances 命令并指定实例 ID。

```
aws ec2 describe-instances --instance-id instance_id
```

2. 检查命令返回的 JSON 响应，并记下 StateReason 响应元素中的值。

   下面的代码块显示了 StateReason 响应元素的示例。

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

使用 Amazon CloudTrail 了解终止原因

有关更多信息，请参阅 Amazon CloudTrail 用户指南中的使用 CloudTrail 事件历史记录查看事件。

解决方案

根据找到的终止原因，执行以下某项操作：

- **Client.VolumeLimitExceeded: Volume limit exceeded** - 删除未使用的卷。您可以提交请求，要求提高卷限制。
- **Client.InternalError: Client error on launch** – 确保您具有访问用于解密和加密卷的 Amazon KMS keys 所需的权限。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的在 Amazon KMS 中使用密钥策略。

排查实例的连接问题。

以下信息和常见错误可以帮助您排查连接到实例时出现的问题。

要排查连接到 Windows 实例时出现的问题，请参阅《Amazon EC2 用户指南（适用于 Windows 实例）》中的排查 Windows 实例的问题。

连接问题和错误

- 连接问题的常见原因 (p. 1685)
- 连接到您的实例时出错：连接超时 (p. 1686)
- Error: unable to load key ...(错误：无法加载密钥...) Expecting: ANY PRIVATE KEY(需要：任何私有密钥) (p. 1689)
- 错误：服务器无法识别用户密钥 (p. 1689)
- 错误：权限被拒绝或 [实例] 端口 22 关闭了连接 (p. 1690)
- 错误：未保护的私有密钥文件 (p. 1692)
- 错误：私有密钥的格式必须以“-----BEGIN RSA PRIVATE KEY-----”开头，以“-----END RSA PRIVATE KEY-----”结尾 (p. 1693)
- 错误：服务器拒绝我们的密钥或 没有支持的身份验证方法 (p. 1693)
- 无法对实例执行 Ping 操作 (p. 1694)
- 错误：服务器意外关闭了网络连接 (p. 1694)
- 错误：EC2 Instance Connect 的主机密钥验证失败 (p. 1694)

- 无法使用 EC2 Instance Connect 连接到 Ubuntu 实例 (p. 1696)
- 我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)

连接问题的常见原因

建议您通过验证是否正确执行了以下任务，开始排查实例连接问题。

验证实例的用户名

您可以使用用户账户的用户名或用于启动实例的 AMI 的默认用户名连接到实例。

- 获取用户账户的用户名。

  有关如何创建用户账户的更多信息，请参阅管理 Linux 实例上的用户 (p. 705)。
- 获取用于启动实例的 AMI 的默认用户名：

用于启动实例的 AMI	默认用户名
Amazon Linux 2022 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` 或者 `ec2-user`
Debian	`admin`
Fedora	`fedora` 或者 `ec2-user`
RHEL	`ec2-user` 或者 `root`
SUSE	`ec2-user` 或者 `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
其他	检查 AMI 提供程序

验证安全组规则是否允许流量

确保与您的实例关联的安全组允许来自您的 IP 地址的入站 SSH 流量。默认情况下，VPC 的默认安全组不允许传入 SSH 流量。默认情况下，由启动实例向导创建的安全组允许传入的 SSH 流量。有关向 Linux 实例添加入站 SSH 流量规则的步骤，请参阅 为您的 Linux 实例授权入站流量 (p. 1287)。有关验证步骤，请参阅 连接到您的实例时出错：连接超时 (p. 1686)。

验证实例是否准备就绪

启动实例后，需要几分钟准备好实例，以便您能连接到实例。检查实例以确保它正在运行并通过了状态检查。

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 请验证以下内容：

   a. 在Instance state (实例状态) 列中，验证您的实例是否处于 `running` 状态。

b. 在 Status check (状态检查) 列中，验证您的实例是否已通过两项状态检查。

验证您是否执行了设置任务和先决条件以连接到实例

有关常规设置任务，请参阅 设置以连接到实例 (p. 645)。

有关特定于连接类型（例如 SSH、EC2 Instance Connect、OpenSSH、PuTTY）的先决条件，请参阅以下选项。

Linux 或 macOS X

如果您的本地计算机操作系统是 Linux 或 macOS X，请检查以下连接选项的特定先决条件：

- SSH 客户端 (p. 649)
- EC2 Instance Connect (p. 652)
- Amazon Systems Manager 会话管理器

Windows

如果您的本地计算机操作系统是 Window，请检查以下连接选项的特定先决条件：

- OpenSSH (p. 661)
- PuTTY (p. 663)
- Amazon Systems Manager 会话管理器
- 适用于 Linux 的 Windows 子系统 (p. 669)

连接到您的实例时出错：连接超时

如果连接到实例时显示错误消息 `Network error: Connection timed out` 或 `Error connecting to [instance], reason: -> Connection timed out: connect`，请尝试以下选项：

检查您的安全组规则。

您需要一条安全组规则，它允许在适当端口上传输来自您的本地计算机公有 IPv4 地址的入站流量。

New console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在控制台页面底部的 Security (安全) 选项卡上的 Inbound rules (入站规则) 下，检查对所选实例生效的规则列表。

   - 对于 Linux 实例：验证是否有允许流量从您的本地计算机到端口 22 (SSH) 的规则。
   - 对于 Windows 实例：验证是否有允许流量从您的本地计算机到端口 3389 (RDP) 的规则。

   如果您的安全组没有允许来自您的本地计算机的入站流量的规则，请向您的安全组添加一条规则。有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
4. 对于允许入站流量的规则，请检查 Source（源）字段。如果该值是单个 IP 地址，并且如果该 IP 地址不是静态的，则每次重新启动计算机时都会分配一个新的 IP 地址。这将导致该规则不包括您计算机的 IP 地址流量。如果您的计算机位于企业网络上，或者当您通过互联网服务提供商 (ISP) 进行连接时，抑或您的计算机的 IP 地址是动态的，则该 IP 地址可能不是静态的，并且每次重新启动计算机时都会更改。为了确保您的安全组规则允许来自您的本地计算机的入站流量，应该指定您的客户端计算机使用的 IP 地址的范围，而不是为 Source（源）指定单个 IP 地址。

有关安全组规则的更多信息，请参阅Amazon VPC 用户指南中的安全组规则。

Old console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在屏幕底部的 Description (描述) 选项卡中，在 Security groups (安全组) 旁，选择 view inbound rules (查看入站规则) 以显示对所选实例生效的规则列表。

   - 对于 Linux 实例：当您选择 view inbound rules (查看入站规则) 时，将会出现一个窗口，其中显示了允许流量到哪些端口。验证是否有允许流量从您的计算机到端口 22 (SSH) 的规则。
   - 对于 Windows 实例：当您选择 view inbound rules (查看入站规则) 时，将会出现一个窗口，其中显示了允许流量到哪些端口。验证是否有允许流量从您的计算机到端口 3389 (RDP) 的规则。

   如果您的安全组没有允许入站流量的规则，请向您的安全组添加一条规则。有关更多信息，请参阅为您的 Linux 实例授权入站流量 (p. 1287)。
4. 每次重新启动本地计算机时，均可分配一个新的 IP 地址（和主机名）。如果您的安全组具有允许来自单个 IP 地址的入站流量的规则，则当您的计算机在企业网络上，或当您通过 Internet 服务提供商 (ISP) 进行连接时，此地址可能不是静态的。请改为指定客户端计算机使用的 IP 地址的范围。

   有关安全组规则的更多信息，请参阅Amazon VPC 用户指南中的安全组规则。

查看子网的路由表。

您需要使用某个路由，以将发往 VPC 外部的所有流量发送到 VPC 的 Internet 网关。

New console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在 Networking (联网) 选项卡上，记下 VPC ID 和 Subnet ID (子网 ID) 的值。
4. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
5. 在导航窗格中，选择 Internet Gateways。验证是否有 Internet 网关附加到您的 VPC。否则，请选择 Create internet gateway (创建 Internet 网关)，为 Internet 网关输入名称，然后选择 Create internet gateway (创建 Internet 网关)。然后，对于您创建的 Internet 网关，依次选择 Actions (操作)、Attach to VPC (附加到 VPC)，选择您的 VPC，然后选择 Attach internet gateway (附加 Internet 网关) 将其附加到您的 VPC。
6. 在导航窗格中，选择 Subnets，然后选择您的子网。
7. 在 Route Table (路由表) 选项卡上，验证 `0.0.0.0/0` 的路由是否为目的地以及您的 VPC 的 Internet 网关是否为目标。如果您使用实例的 IPv6 地址连接到实例，请检查是否有一个路由可以将所有 IPv6 流量 (`::/0`) 指向 Internet 网关。否则请执行以下操作：

   a. 选择路由表的 ID (rtb-xxxxxxxx) 以导航到路由表。
   b. 在 Routes (路由) 选项卡上，选择 Edit routes (编辑路由)。选择 Add route (添加路由)，将 `0.0.0.0/0` 用作目的地并将 Internet 网关用作目标。对于 IPv6，选择 Add route (添加路由)，将 `::/0` 用作目的地并将 Internet 网关用作目标。
   c. 选择 Save routes（保存路由）。

Old console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在 Description 选项卡中，记下 VPC ID 和 Subnet ID 的值。
4. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
5. 在导航窗格中，选择 Internet Gateways。验证是否有 Internet 网关附加到您的 VPC。否则，选择 Create Internet Gateway 以创建 Internet 网关。选择 Internet 网关，然后选择 Attach to VPC 并按照说明将其附加到您的 VPC。
6. 在导航窗格中，选择 Subnets，然后选择您的子网。
7. 在 Route Table 选项卡上，验证 `0.0.0.0/0` 的路由是否为目的地以及您的 VPC 的 Internet 网关是否为目标。如果您使用实例的 IPv6 地址连接到实例，请检查是否有一个路由可以将所有 IPv6 流量 (`::/0`) 指向 Internet 网关。否则请执行以下操作：

   a. 选择路由表的 ID (rtb-xxxxxxxx) 以导航到路由表。
   b. 在 Routes (路由) 选项卡上，选择 Edit routes (编辑路由)。选择 Add route (添加路由)，将 `0.0.0.0/0` 用作目的地并将 Internet 网关用作目标。对于 IPv6，选择 Add route (添加路由)，将 `::/0` 用作目的地并将 Internet 网关用作目标。
   c. 选择 Save routes（保存路由）。

检查子网的网络访问控制列表 (ACL)。

网络 ACL 必须允许端口 22（Linux 实例）或端口 3389（Windows 实例）上来自您的本地 IP 地址的入站流量。还须允许到临时端口 (1024-65535) 的出站流量。

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Subnets（子网）。
3. 选择您的子网。
4. 对于 Inbound rules (入站规则)，请在 Network ACL (网络 ACL) 选项卡上验证这些规则是否允许来自所需端口的计算机的入站流量。如果不允许，请删除或修改阻止该流量的规则。
5. 对于 Outbound rules (出站规则)，验证规则是否允许到您的计算机临时端口的出站流量。如果不允许，请删除或修改阻止该流量的规则。

如果您的计算机在企业网络上

请询问网络管理员内部防火墙是否允许端口 22 (对于 Linux 实例) 或端口 3389 (对于 Windows 实例) 上来自您的计算机的入站和出站流量。

如果您的计算机有防火墙，请验证其是否允许端口 22 (对于 Linux 实例) 或端口 3389 (对于 Windows 实例) 上来自您的计算机的入站和出站流量。

检查您的实例是否具有公有 IPv4 地址。

如果没有，您可以将弹性 IP 地址与您的实例关联。有关更多信息，请参阅弹性 IP 地址 (p. 1094)。

检查实例上的 CPU 负载；服务器可能已超过负载。

Amazon 自动提供数据，例如 Amazon CloudWatch 指标和实例状态，您可以使用这些数据查看实例上 CPU 的负载情况；如有必要，还可以调整负载的处理方式。有关更多信息，请参阅使用 CloudWatch 监控您的实例 (p. 1000)。

- 如果您的负载是可变的，您可以使用 Auto Scaling 和 Elastic Load Balancing 自动增加或减少实例。
- 如果您的负载呈稳定增长的态势，您可以迁移到更大的实例类型。有关更多信息，请参阅更改实例类型 (p. 399)。

要使用 IPv6 地址连接实例，请检查以下各项：

- 您的子网必须与一个路由表关联，此表中具有一个将 IPv6 流量 (`::/0`) 指向 Internet 网关的路由。
- 您的安全组规则必须允许适当端口 (Linux 的端口 22 和 Windows 的端口 3389) 传输来自本地 IPv6 地址的入站流量。
- 您的网络 ACL 规则必须允许入站和出站 IPv6 流量。
- 如果您从旧版 AMI 启动实例，则其可能未针对 DHCPv6 进行配置（IPv6 地址不会在网络接口上自动识别）。有关更多信息，请参阅Amazon VPC 用户指南中的在实例中配置 IPv6。
- 您的本地计算机必须拥有 IPv6 地址，且必须配置为使用 IPv6。

Error: unable to load key ...(错误：无法加载密钥...) Expecting: ANY PRIVATE KEY(需要：任何私有密钥)

如果您尝试连接到您的实例并收到错误消息 `unable to load key ... Expecting: ANY PRIVATE KEY`，则说明未正确配置用于存储私有密钥的文件。如果私有密钥文件以 `.pem` 为结尾，则它可能仍未正确配置。未正确配置私有密钥文件的一个可能原因是缺少证书。

如果未正确配置私有密钥文件，请按照下列步骤解决该错误

1. 创建新的密钥对。有关更多信息，请参阅使用 Amazon EC2 创建密钥对 (p. 1290)。

   Note

   另外，您也可以使用第三方工具创建新的密钥对。有关更多信息，请参阅使用第三方工具创建密钥对，并将公有密钥导入 Amazon EC2 (p. 1293)。
2. 将新密钥对添加到您的实例。有关更多信息，请参阅我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)。
3. 使用新的密钥对连接到实例。

错误：服务器无法识别用户密钥

如果您使用 SSH 连接到实例

- 请在连接时使用 `ssh -vvv` 获得三倍的详细调试信息：

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

下列样本输出演示了如果您尝试使用服务器无法识别的密钥连接实例时您可能会看到的信息：

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
```

```
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

如果您使用 PuTTY 连接到实例

- 验证私有密钥 (.pem) 文件是否已转换为 PuTTY 可识别的格式 (.ppk)。有关转换您的私有密钥的更多信息，请参阅 使用 PuTTY 从 Windows 连接到 Linux 实例 (p. 663)。

  Note

  在 PuTTYgen 中，加载私有密钥文件并选择 Save Private Key (保存私有密钥) 而不是 Generate (生成)。
- 验证您在连接时是否对为 AMI 使用了正确的用户名称。在 PuTTY Configuration (PuTTY 配置) 窗口的 Host name (主机名) 框中输入用户名。

用于启动实例的 AMI	默认用户名
Amazon Linux 2022 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` 或者 `ec2-user`
Debian	`admin`
Fedora	`fedora` 或者 `ec2-user`
RHEL	`ec2-user` 或者 `root`
SUSE	`ec2-user` 或者 `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
其他	检查 AMI 提供程序

- 验证您的入站安全组规则允许入站流量进入合适的端口。有关更多信息，请参阅授权网络访问您的实例 (p. 1287)。

错误：权限被拒绝或 [实例] 端口 22 关闭了连接

如果您使用 SSH 连接到实例并出现任何以下错误：`Host key not found in [directory]`、`Permission denied (publickey)``Authentication failed, permission`

`denied` 或 `Connection closed by [instance] port 22`，请确认您使用的是 AMI 对应的用户名进行连接并且为实例指定了正确的私有密钥（`.pem`）文件）。

正确的用户名如下所示：

用于启动实例的 AMI	默认用户名
Amazon Linux 2022 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` 或者 `ec2-user`
Debian	`admin`
Fedora	`fedora` 或者 `ec2-user`
RHEL	`ec2-user` 或者 `root`
SUSE	`ec2-user` 或者 `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
其他	检查 AMI 提供程序

例如，要使用 SSH 客户端连接到从 Amazon Linux 实例，请使用以下命令：

```
ssh -i /path/key-pair-name.pem instance-user-name@ec2-203-0-113-25.compute-1.amazonaws.com
```

请确认您使用的私有密钥文件对应于您启动实例时选择的密钥对。

New console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在 Details（详细信息）选项卡的 Instance details (实例详细信息) 下，验证 Key pair name (密钥对名称) 的值。
4. 如果您启动实例时没有指定密钥对，则可以终止实例并启动新实例，从而确保指定密钥对。如果这是您一直使用的实例，但您不再有密钥对的 `.pem` 文件，则可以使用新的密钥对取代该密钥对。有关更多信息，请参阅我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)。

Old console

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在 Description 选项卡上，验证 Key pair name 的值。
4. 如果您启动实例时没有指定密钥对，则可以终止实例并启动新实例，从而确保指定密钥对。如果这是您一直使用的实例，但您不再有密钥对的 `.pem` 文件，则可以使用新的密钥对取代该密钥对。有关更多信息，请参阅我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？ (p. 1696)。

如果您已经生成了您自己的密钥对，请确保您的密钥生成器被设置为创建 RSA 密钥。不接受 DSA 密钥。

如果您遇到 Permission denied (publickey) 错误但以上情况都不适用 (例如，您之前能够连接)，则可能是实例主目录的权限发生了更改。/home/*instance-user-name*/.ssh/authorized_keys 的权限必须限制为仅限所有者。

在您的实例上验证权限

1. 停止您的实例并分离根卷。有关更多信息，请参阅停止和启动您的实例 (p. 610)和从 Linux 实例分离 Amazon EBS 卷 (p. 1364)。
2. 在当前实例所在的可用区中启动一个临时实例 (使用与您用于当前实例的 AMI 类似或相同的 AMI)，并将根卷附加到此临时实例。有关更多信息，请参阅将 Amazon EBS 卷挂载到实例 (p. 1347)。
3. 连接临时实例，创建一个挂载点并挂载您附加的卷。有关更多信息，请参阅使 Amazon EBS 卷可在 Linux 上使用 (p. 1348)。
4. 在临时实例中，检查附加的卷的 /home/*instance-user-name*/ 目录的权限。如有必要，按如下方式调整权限：

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. 卸载该卷，将其与临时实例分离，然后将其重新附加到原来的实例。确保为根卷指定正确的设备名称；例如，/dev/xvda。
6. 启动您的实例。如果不再需要临时实例，可以终止它。

错误：未保护的私有密钥文件

必须保护您的私钥文件，防止其他任何用户对其进行读写操作。如果除您外其他任何人都能够读取或写入您的私钥，则 SSH 会忽略您的密钥，并且您会看到以下警告消息。

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

如果在尝试登录到您的实例时看到类似的消息，请检查此错误消息的第一行，验证您为实例使用的公钥是否正确。上述示例利用 .ssh/my_private_key.pem 文件权限使用私钥 0777，这可使任何人都能读取或写入此文件。此权限级别非常不安全，因此 SSH 会忽略此密钥。

如果从 MacOS 或 Linux 连接，请运行以下命令以修复此错误，替入您的私有密钥文件的路径。

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

如果要从 Windows 连接，请在您的本地计算机上执行以下步骤。

1. 导航到您的 .pem 文件。
2. 右键单击 .pem 文件并选择 Properties (属性)。
3. 选择安全性选项卡。

4. 选择 Advanced (高级)。
5. 验证您是否是文件的所有者。如果不是，请将所有者更改为您的用户名。
6. 选择 Disable inheritance (禁用继承) 和 Remove all inherited permissions from this object (从此对象中删除所有继承的权限)。
7. 选择 Add (添加)、Select a principal (选择委托人)，输入您的用户名，然后选择 OK (确定)。
8. 从 Permission Entry (权限条目) 窗口，授予 Read (读取) 权限，然后选择 OK (确定)。
9. 单击 Apply（应用）以确保所有设置都已保存。
10. 选择 OK (确定) 关闭 Advanced Security Settings (高级安全设置) 窗口。
11. 选择 OK (确定) 关闭 Properties (属性) 窗口。
12. 您应该能够通过 SSH 从 Windows 连接到 Linux 实例。

从 Windows 命令提示符处运行以下命令。

1. 在命令提示符下，导航到 .pem 文件的文件路径位置。
2. 运行以下命令以重置和删除显式权限：

```
icacls.exe $path /reset
```

3. 运行以下命令以向当前用户授予读取权限：

```
icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
```

4. 运行以下命令以禁用继承并删除继承的权限。

```
icacls.exe $path /inheritance:r
```

5. 您应该能够通过 SSH 从 Windows 连接到 Linux 实例。

错误：私有密钥的格式必须以“-----BEGIN RSA PRIVATE KEY-----”开头，以“-----END RSA PRIVATE KEY-----”结尾

如果您使用第三方工具（如 ssh-keygen）创建 RSA 密钥对，则它会生成 OpenSSH 密钥格式的私有密钥。当您连接到实例时，如果使用 OpenSSH 格式的私有密钥来解密密码，您将收到错误 `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`。

要解决该错误，私有密钥必须采用 PEM 格式。使用以下命令创建 PEM 格式的私有密钥：

```
ssh-keygen -m PEM
```

错误：服务器拒绝我们的密钥或 没有支持的身份验证方法

如果您使用 PuTTY 连接到实例并出现以下任一错误：错误：服务器拒绝了我们的密钥或错误：没有支持的身份验证方法，请确认您使用 AMI 的相应用户名进行连接。在 PuTTY Configuration (PuTTY 配置) 窗口的 User name (用户名) 中键入用户名。

正确的用户名如下所示：

用于启动实例的 AMI	默认用户名
Amazon Linux 2022 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` 或者 `ec2-user`
Debian	`admin`
Fedora	`fedora` 或者 `ec2-user`
RHEL	`ec2-user` 或者 `root`
SUSE	`ec2-user` 或者 `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
其他	检查 AMI 提供程序

您还应该验证：

- 您使用的是否是最新版本的 PuTTY？有关更多信息，请参阅 PuTTY 网页。
- 已将您的私有密钥 (.pem) 文件正确转换为 PuTTY 可识别的格式 (.ppk)。有关转换您的私有密钥的更多信息，请参阅 使用 PuTTY 从 Windows 连接到 Linux 实例 (p. 663)。

无法对实例执行 Ping 操作

`ping` 命令是一种 ICMP 流量 — 如果您无法对实例执行 ping 操作，请确保您的入站安全组规则允许的 `Echo Request` 消息的 ICMP 流量来自所有资源，或来自从中发出命令的计算机或实例。

如果您无法从实例发出 `ping` 命令，请确保您的出站安全组规则允许的 `Echo Request` 消息的 ICMP 流量发送到所有目标，或发送到您正在尝试对其执行 ping 操作的主机。

`Ping`由于网络延迟或硬件问题， 命令还可能被防火墙阻止或超时。您应咨询本地网络或系统管理员，以帮助进行进一步的故障排除。

错误：服务器意外关闭了网络连接

如果您使用 PuTTY 连接到实例并出现“服务器意外关闭了网络连接”错误，请确认您已在 PuTTY Configuration (PuTTY 配置) 的 Connection (连接) 页面上启用 keepalives 以避免断开连接。有些服务器如果在指定的时间内未接收到任何数据，将会断开与客户端的连接。将“Seconds between keepalives”(keepalives 之间的秒数) 设置为 59 秒。

如果在启用 keepalives 后仍出现问题，请尝试在 PuTTY Configuration (PuTTY 配置) 的 Connection (连接) 页面上禁用 Nagle 的算法。

错误：EC2 Instance Connect 的主机密钥验证失败

如果您轮换实例主机密钥，则新主机密钥不会自动上传到 Amazon 可信主机密钥数据库。当您尝试使用 EC2 Instance Connect 基于浏览器的客户端连接到实例时，会导致主机密钥验证失败，并且无法连接到实例。

要解决此错误，您必须在实例上运行 `eic_harvest_hostkeys` 脚本，该脚本会将新主机密钥上传到 EC2 Instance Connect。脚本位于 Amazon Linux 2 实例上的 `/opt/aws/bin/` 和 Ubuntu 实例上的 `/usr/share/ec2-instance-connect/`。

Amazon Linux 2

解决 Amazon Linux 2 实例上的主机密钥验证失败错误

1. 使用 SSH 连接到您的实例。

   您可以使用 EC2 Instance Connect CLI 或使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名进行连接。对于 Amazon Linux 2，默认用户名是 `ec2-user`。

   例如，如果实例是使用 Amazon Linux 2 启动的，实例的公有 DNS 名称是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
   ```

   有关连接到实例的更多信息，请参阅使用 SSH 连接到 Linux 实例 (p. 649)。
2. 导航到以下文件夹。

   ```
   [ec2-user ~]$ cd /opt/aws/bin/
   ```
3. 在您的实例上运行以下命令。

   ```
   [ec2-user ~]$ ./eic_harvest_hostkeys
   ```

   请注意，调用成功导致没有输出。

   现在，您可以使用 EC2 Instance Connect 基于浏览器的客户端连接到您的实例。

Ubuntu

解决 Ubuntu 实例上的主机密钥验证失败错误

1. 使用 SSH 连接到您的实例。

   您可以使用 EC2 Instance Connect CLI 或使用在启动实例时为其分配的 SSH 密钥对以及用于启动实例的 AMI 的默认用户名进行连接。对于 Ubuntu，默认用户名是ubuntu。

   例如，如果实例是使用 Ubuntu 启动的，实例的公有 DNS 名称是 `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`，并且密钥对是 `my_ec2_private_key.pem`，请使用以下命令通过 SSH 连接到实例：

   ```
   $ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
   ```

   有关连接到实例的更多信息，请参阅使用 SSH 连接到 Linux 实例 (p. 649)。
2. 导航到以下文件夹。

   ```
   [ec2-user ~]$ cd /usr/share/ec2-instance-connect/
   ```
3. 在您的实例上运行以下命令。

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

请注意，调用成功导致没有输出。

现在，您可以使用 EC2 Instance Connect 基于浏览器的客户端连接到您的实例。

无法使用 EC2 Instance Connect 连接到 Ubuntu 实例

如果您使用 EC2 Instance Connect 连接到 Ubuntu 实例，并且尝试连接时出错，则可以使用以下信息尝试修复此问题。

可能的原因

实例上的 `ec2-instance-connect` 软件包不是最新版本。

解决方案

将实例上的 `ec2-instance-connect` 软件包更新到最新版本，如下所示：

1. 使用 EC2 Instance Connect 以外的方法连接 (p. 644)到实例。
2. 在您的实例上使用以下命令将 `ec2-instance-connect` 软件包更新到最新版本。

```
apt update && apt upgrade
```

我丢失了私有密钥。我怎样才能连接到我的 Linux 实例？

如果丢失由 EBS 支持的实例的私有密钥，您可以重新获取对您的实例的访问权限。您必须停止实例，分离卷并将其作为数据卷附加到另一个实例，然后使用新的公有密钥修改 `authorized_keys` 文件，将卷移回原始实例，并重启实例。有关启动、连接和停止实例的更多信息，请参阅 实例生命周期 (p. 570)。

此过程仅支持具有 EBS 根卷的实例。如果根设备是实例存储卷，则无法使用此过程重新获得对实例的访问权限；您必须拥有私有密钥才能连接到实例。要确定实例的根设备类型，请打开 Amazon EC2 控制台，选择实例，选择相应实例，然后选择存储选项卡，检查根设备详细信息部分中的根设备类型的值。

该值为 `EBS` 或 `INSTANCE-STORE`。

如果丢失私有密钥，除以下步骤外，还有其他方法可以连接到 Linux 实例。有关更多信息，请参阅如果我在 SSH 密钥对初始启动后丢失，该如何连接到 Amazon EC2 实例？

使用不同的密钥对连接由 EBS 支持的实例的步骤

- 步骤 1：创建新的密钥对 (p. 1697)
- 步骤 2：获取有关原始实例及其根卷的信息 (p. 1697)
- 步骤 3：停止原始实例 (p. 1697)
- 步骤 4：启动临时实例 (p. 1697)
- 步骤 5：从原始实例中分离根卷并将其附加到临时实例 (p. 1698)
- 步骤 6：将新的公钥添加到已安装到临时实例的原始卷上的 authorized_keys (p. 1698)
- 步骤 7：从临时实例中卸载并分离原始卷，然后将其重新附加到原始实例 (p. 1699)
- 步骤 8：使用新密钥对连接到原始实例 (p. 1700)
- 步骤 9：清除 (p. 1700)

步骤 1：创建新的密钥对

使用 Amazon EC2 控制台或第三方工具创建新的密钥对。如果您要将新密钥对的名称设置为与丢失的私有密钥相同的名称，则必须先删除现有密钥对。有关创建新密钥对的信息，请参阅使用 Amazon EC2 创建密钥对 (p. 1290)或使用第三方工具创建密钥对，并将公有密钥导入 Amazon EC2 (p. 1293)。

步骤 2：获取有关原始实例及其根卷的信息

请记下以下信息，因为您需要它来完成此过程。

获取有关原始实例的信息

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中选择 Instances (实例)，然后选择要连接到的实例。（我们将此称为原始实例。）
3. 在 Details（详细信息）选项卡上，记下实例 ID 和 AMI ID。
4. 在 Networking（网络）选项卡上，记下可用区。
5. 在 Storage（存储）选项卡的 Root device name（根设备名称）下，记下根卷的设备名称（例如 `/dev/xvda`）。然后，在 Block devices（块存储设备）下，查找此设备的名称并记下卷 ID（例如 vol-0a1234b5678c910de）。

步骤 3：停止原始实例

依次选择实例状态、停止实例。如果此选项处于禁用状态，则表示实例已停止，或者其根设备是实例存储卷。

> Warning
>
> 当您停止某个实例时，任何实例存储卷上的数据都将被擦除。要保留实例存储卷中的数据，请确保将其备份到持久性存储中。

步骤 4：启动临时实例

New console

启动临时实例

1. 在导航窗格中，选择 Instances（实例），然后选择 Launch instances（启动实例）。
2. 在 Name and tags（名称和标签）部分，对于 Name（名称），输入 Temporary（临时）。
3. 在 Application and OS Images（应用程序和操作系统映像）部分中，选择您启动原始实例时所用的 AMI。如果此 AMI 不可用，您可以创建一个可在已停止的实例中使用的 AMI。有关更多信息，请参阅 创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。
4. 在 Instance type（实例类型）部分中，保留默认的实例类型。
5. 在 Key pair（密钥对）部分中，对于 Key pair name（密钥对名称），选择现有密钥对进行使用或创建新密钥对。
6. 在 Network settings（网络设置）部分，选择 Edit（编辑），然后为 Subnet（子网），选择与原始实例位于同一可用区的子网。
7. 在 Summary（摘要）面板中，选择 Launch（启动）。

Old console

选择 Launch instances（启动实例），然后使用启动向导通过以下选项启动一个临时实例：

- 在 Choose an AMI (选择一个 AMI) 页面上，选择您启动原始实例时所用的 AMI。如果此 AMI 不可用，您可以创建一个可在已停止的实例中使用的 AMI。有关更多信息，请参阅创建一个由 Amazon EBS 支持的 Linux AMI (p. 137)。

- 在 Choose an Instance Type (选择一个实例类型) 页上，保留向导为您选择的默认实例类型。
- 在 Configure Instance Details (配置实例详细信息) 页面上，请指定与原始实例相同的可用区。如果您在 VPC 中启动实例，请选择此可用区中的一个子网。
- 在 Add Tags 页面上，向实例添加标签 `Name=Temporary` 以指示这是一个临时实例。
- 在 Review 页面上，选择 Launch。选择您在步骤 1 中创建的密钥对，然后选择 Launch Instances（启动实例）。

步骤 5：从原始实例中分离根卷并将其附加到临时实例

1. 在导航窗格中，选择 Volumes（卷），并选择原始实例的根设备卷（您已在上一步骤中记下它的卷 ID）。依次选择 Actions（操作）、Detach Volume（分离卷），然后选择 Detach（分离）。等待卷的状态变为 `available`。（您可能需要选择 Refresh (刷新) 图标。）
2. 如果卷仍保持选中状态，则选择 Actions（操作），然后选择 Attach Volume（附加卷）。选择临时实例的实例 ID，记下在 Device name（设备名称）下指定的设备名称（例如 `/dev/sdf`），然后选择 Attach volume（附加卷）。

   Note

   如果已从 Amazon Web Services Marketplace AMI 启动原始实例，并且卷包含 Amazon Web Services Marketplace 代码，则必须先停止临时实例，然后才能附加卷。

步骤 6：将新的公钥添加到已安装到临时实例的原始卷上的 authorized_keys

1. 连接到临时实例。
2. 在临时实例中，挂载附加到实例的卷以访问其文件系统。例如，如果设备名称为 `/dev/sdf`，请使用以下命令将卷挂载为 `/mnt/tempvol`。

   Note

   您的实例上显示的设备名称可能不同。例如，作为 `/dev/sdf` 挂载的设备可能在实例上显示为 `/dev/xvdf`。某些版本的 Red Hat（或其变体，如 CentOS）甚至可能将尾部字母增加 4 个字符，其中 `/dev/sd`*f* 成为 `/dev/xvd`*k*。

   a. 使用 lsblk 命令确定卷是否已分区。

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   ##xvda1 202:1    0    8G  0 part /
   xvdf    202:80   0  101G  0 disk
   ##xvdf1 202:81   0  101G  0 part
   xvdg    202:96   0   30G  0 disk
   ```

   在前一个示例中，`/dev/xvda` 和 `/dev/xvdf` 是分区卷，而 `/dev/xvdg` 不是。如果您的卷已分区，则应在后续步骤中挂载分区 (`/dev/xvdf1`)，而不是原始设备 (`/dev/xvdf`)。

   b. 创建临时目录以挂载卷。

   ```
   [ec2-user ~]$ sudo mkdir /mnt/tempvol
   ```

   c. 使用之前确定的卷名称或设备名称在临时挂载点挂载卷（或分区）。所需命令取决于操作系统的文件系统。请注意，您的实例上显示的设备名称可能不同。有关更多信息，请参阅步骤 6 中的 note。

   - Amazon Linux、Ubuntu 和 Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2、CentOS、SUSE Linux 12 和 RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

Note

如果您收到说明文件系统受损的错误，请运行以下命令以使用 fsck 实用程序检查文件系统并修复任何问题：

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. 在临时实例中，借助临时实例 authorized_keys 中的新公有密钥，在已挂载卷上使用以下命令更新 authorized_keys。

   Important

   以下示例使用 Amazon Linux 用户名 ec2-user。您可能需要使用其他用户名来替换，例如对于 Ubuntu 实例为 ubuntu。

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

如果复制成功，则可以转到下一步骤。

（可选）如果您没有权限编辑 /mnt/tempvol 中的文件，您必须使用 sudo 更新文件，然后检查文件的权限，以验证您是否能够登录原始实例。请使用以下命令检查文件权限。

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

在这个输出示例中，*222* 是用户 ID；*500* 是组 ID。接下来，请使用 sudo 重新运行失败的复制命令。

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

再次运行以下命令以确定权限是否已更改。

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

如果用户 ID 和组 ID 已经更改，请使用以下命令进行恢复。

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

步骤 7：从临时实例中卸载并分离原始卷，然后将其重新附加到原始实例

1. 在临时实例中，卸载已附加的卷，以将其重新附加到原始实例。例如，使用以下命令卸载 /mnt/tempvol 处的卷。

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. 从临时实例中分离卷（您在上一步中卸载了该卷）：从 Amazon EC2 控制台，在导航窗格中选择 Volumes（卷），为原始实例选择根设备卷（您在上一步中记下了卷 ID），依次选择 Actions（操作）、Detach volume（分离卷），然后选择 Detach（分离）。等待卷的状态变为 `available`。（您可能需要选择 Refresh (刷新) 图标。）
3. 将卷重新附加到原始实例：在卷仍保持选中状态时，选择 Actions（操作），然后选择 Attach Volume（附加卷）。选择原始实例的实例 ID，请指定您以前在步骤 2 (p. 1697) 中记下的原始根设备附加的设备名称（`/dev/sda1` 或 `/dev/xvda`），然后选择 Attach volume（附加卷）。

   Important

   如果您不指定与原始附加相同的设备名称，则无法启动原始实例。Amazon EC2 要求根设备卷位于 `sda1` 或者 `/dev/xvda`。

步骤 8：使用新密钥对连接到原始实例

选择原始实例，然后依次选择实例状态、启动实例。在实例进入 `running` 状态后，您可以使用新密钥对的私有密钥文件连接到该实例。

Note

如果您的新密钥对和相应私有密钥文件的名称不同于原始密钥对的名称，请确保在连接到实例时指定新私有密钥文件的名称。

步骤 9：清除

(可选) 如果您将不再使用临时实例，可以将其终止。选择临时实例，然后依次选择 Instance State（实例状态）和 Terminate instance（终止实例）。

排查实例的停止问题

如果您已停止由 Amazon EBS 支持的实例，并且它卡在 `stopping` 状态，这说明底层主机可能存在问题。

当实例处于 `stopping` 状态或处于除 `running` 外的任何其他状态时，不会收取任何实例使用费用。只有当实例处于 `running` 状态时，您使用实例时才需要付费。

强制停止实例

通过控制台或 Amazon CLI 强制停止实例。

Note

当实例处于 `stopping` 状态时，您只能强制实例停止使用控制台。当实例处于除 `shutting-down` 和 `terminated` 之外的任何状态时，您只能强制实例停止使用 Amazon CLI。

New console

使用控制台强制停止实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择卡住实例。

3. 选择 Instance state（实例状态）、Force stop（强制停止实例）、Stop（停止）。

   请注意，只有当您的实例处于 `stopping` 状态时，Force stop instance（强制停止实例）才可用。如果您的实例处于另一状态（除 `shutting-down` 和 `terminated` 之外的状态），您可以使用 Amazon CLI 强制停止您的实例。

Old console

使用控制台强制停止实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择卡住实例。
3. 依次选择 Instance State（实例状态）、Stop（停止）、Yes, Forcefully Stop（是，强制停止）。

Amazon CLI

使用 Amazon CLI 强制停止实例

使用 stop-instances 命令和 `--force` 选项，如下所示：

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

如果在 10 分钟后，实例未停止，请在 Amazon Web Services re:Post 上寻求帮助。为了帮助加快解决问题，请提供实例 ID 并描述已采取的步骤。此外，如果您有支持计划，则可在支持中心创建技术支持案例。

创建替代实例

要在等待 Amazon Web Services re:Post 或支持中心的帮助时尝试解决此问题，请创建替代实例。创建卡住实例的 AMI，并使用新的 AMI 启动一个新实例。

Important

如果仅注册系统状态检查 (p. 974)，则建议创建替换实例，因为实例状态检查将导致 AMI 复制损坏操作系统的精确副本。确认状态消息后，创建 AMI 并使用新 AMI 启动新实例。

New console

使用控制台创建替代实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择卡住实例。
3. 依次选择 Actions (操作)、Image and templates (映像和模板) 和 Create Image (创建映像)。
4. 在 Create image (创建映像) 页面上，执行以下操作：

   a. 输入 AMI 的名称和说明。
   b. 选择 No reboot。
   c. 选择创建映像。

   有关更多信息，请参阅 从实例创建 Linux AMI (p. 139)。
5. 从 AMI 启动新实例，验证新实例是否正常运行。
6. 选择卡住的实例，然后依次选择 Actions（操作）、Instance State（实例状态）、Terminate（终止）。如果该实例也因卡住而终止，则 Amazon EC2 会自动强制其在几个小时内终止。

Old console

使用控制台创建替代实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择卡住实例。
3. 依次选择 Actions、Image 和 Create Image。
4. 在 Create Image 对话框中，填写以下字段，然后选择 Create Image：
   a. 为 AMI 指定名称和描述。
   b. 选择 No reboot。

   有关更多信息，请参阅 从实例创建 Linux AMI (p. 139)。
5. 从 AMI 启动新实例，验证新实例是否正常运行。
6. 选择卡住的实例，然后依次选择 Actions、Instance State、Terminate。如果该实例也因卡住而终止，则 Amazon EC2 会自动强制其在几个小时内终止。

Amazon CLI

使用 CLI 创建替代实例

1. 使用 create-image (Amazon CLI) 命令和 `--no-reboot` 选项从卡住实例创建 AMI，如下所示：

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. 使用 run-instances (Amazon CLI) 命令从 AMI 启动新实例，如下所示：

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large --
key-name MyKeyPair --security-groups MySecurityGroup
```

3. 验证新实例是否正常运行。
4. 使用 terminate-instances (Amazon CLI) 命令终止卡住实例，如下所示：

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

如果无法按上一步骤所述从该实例创建 AMI，则可以设置替代实例，如下所示：

(替代) 使用控制台创建替代实例

1. 选择实例并选择 Description、Block devices。选择每个卷并记下其卷 ID。请务必注意哪个卷是根卷。
2. 在导航窗格中，选择 Volumes。选择该实例的各个卷，然后依次选择 Actions、Create Snapshot。
3. 在导航窗格中，选择快照。选择您刚刚创建的快照，然后依次选择 Actions、Create Volume。
4. 使用与粘滞的实例相同的操作系统启动实例。注意其根卷的卷 ID 和设备名称。
5. 在导航窗格中，选择Instances（实例），选择刚才启动的实例，然后依次选择 Instance state（实例状态）、Stop Instance（停止实例）。
6. 在导航窗格中，选择 Volumes，选择已停止实例的根卷，然后依次选择 Actions、Detach Volume。
7. 选择您从卡住的实例创建的根卷，依次选择 Actions、Attach Volume，然后将其附加到新实例以作为其根卷（使用记下的设备名称）。将任何其他非根卷附加到该实例。
8. 在导航窗格中，选择 Instances，然后选择替代实例。依次选择实例状态、启动实例。验证该实例是否正常运行。

9. 选择卡住的实例，然后依次选择实例状态、终止实例。如果该实例也因卡住而终止，则 Amazon EC2 会自动强制其在几个小时内终止。

排查实例终止（关闭）

当实例未处于 `running` 状态时，不会向您收取任何实例使用费用。换言之，当您终止实例时，一旦实例的状态变为 `shutting-down`，就不再产生与该实例相关的费用。

实例立即终止

有多个问题可能会导致您的实例在启动后立即终止。参阅 实例立即终止 (p. 1683) 了解更多信息。

延迟的实例终止

如果您的实例处于 `shutting-down` 状态超过数分钟，这可能是因为实例运行的关闭脚本造成了延迟。

另一个可能的原因是底层主机有问题。如果您的实例处于 `shutting-down` 状态已有数小时，Amazon EC2 会视之为卡住的实例，并会强制终止它。

如果您的实例看起来卡在正在终止状态已有数小时，请在 Amazon EC2 论坛发帖请求帮助。为了帮助加快解决问题，请提供实例 ID 并描述已采取的步骤。此外，如果您有支持计划，则可在支持中心创建技术支持案例。

已终止实例仍然显示

在您终止某个实例之后，它会在删除之前的短时间内保持可见。状态显示为 `terminated`。如果该条目在几小时之后未删除，请联系 Support。

错误：此实例可能无法终止。修改其“disableApiTermination”实例属性

如果您尝试终止实例并收到 `The instance instance_id may not be terminated. Modify its 'disableApiTermination' instance attribute` 错误消息，则表明此实例已启用终止保护。终止保护可防止实例意外终止。有关更多信息，请参阅启用终止保护 (p. 637)。

终止实例前，必须先禁用终止保护。

要使用 Amazon EC2 控制台禁用终止保护，请选择实例，然后依次选择操作、实例设置、更改终止保护。

要使用 Amazon CLI 禁用终止保护，请使用以下命令。

```
$ aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-termination
```

自动启动或终止的实例

通常，以下行为意味着您已使用 Amazon EC2 Auto Scaling、EC2 队列或 Spot 队列，根据已定义的条件自动扩展计算资源：

- 您终止实例，新实例将自动启动。
- 您启动一个实例，并且其中一个实例将自动终止。
- 您停止实例且此实例终止，新实例会自动启动。

要停止弹性伸缩，请参阅 Amazon EC2 Auto Scaling 用户指南、EC2 Fleet (p. 814) 或 创建 Spot 队列请求 (p. 900)。

通过故障状态检查来排查实例问题

如果您的实例未能通过状态检查，以下信息可帮助您解决问题。请首先确定您的应用程序是否存在任何问题。如果您验证的结果是实例没有按照预期运行应用程序，请查看状态检查信息和系统日志。

有关导致状态检查出现故障的问题示例，请参阅 实例的状态检查 (p. 975)。

目录

- 查看状态检查信息 (p. 1704)
- 检索系统日志 (p. 1705)
- 诊断基于 Linux 的实例的系统日志错误 (p. 1705)
- 内存不足：终止进程 (p. 1706)
- 错误：mmu_update 失败 (内存管理更新失败) (p. 1706)
- I/O 错误（块储存设备故障） (p. 1707)
- I/O 错误：既不是本地磁盘也不是远程磁盘（破损的分布式块储存设备） (p. 1708)
- request_module：runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) (p. 1709)
- “严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配) (p. 1710)
- “FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) (p. 1710)
- ERROR：无效内核 (EC2 不兼容内核) (p. 1711)
- fsck：尝试打开时没有找到此文件或目录... (未找到文件系统) (p. 1712)
- 挂载文件系统时出现一般性错误（挂载失败） (p. 1714)
- VFS：无法在未知块上挂载根 fs (根文件系统不匹配) (p. 1715)
- 错误：无法确定根设备的主/次编号…（根文件系统/设备不匹配） (p. 1716)
- XENBUS：设备没有驱动程序… (p. 1717)
- … 没有检查时，已强制执行检查的工作日 (文件系统检查要求) (p. 1718)
- fsck 卡在退出状态...（设备缺失） (p. 1718)
- GRUB 提示 (grubdom>) (p. 1719)
- 提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。(硬编码的 MAC 地址)。 (p. 1721)
- 无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误) (p. 1722)
- XENBUS：连接设备时超时 (Xenbus 超时) (p. 1723)

查看状态检查信息

使用 Amazon EC2 控制台调查受损实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)，然后选择您的实例。
3. 在详细信息窗格中，选择 Status Checks，查看所有 System Status Checks 和 Instance Status Checks 的各项结果。

如果系统状态检查失败，您可以尝试以下一种选项：

- 创建实例恢复警报。有关更多信息，请参阅创建停止、终止、重启或恢复实例的警报 (p. 1021)。
- 如果您将实例类型更改为了基于 Nitro 系统 (p. 246)构建的实例，则当您在从没有所需的 ENA 和 NVMe 驱动程序的实例中迁移时，状态检查将失败。有关更多信息，请参阅更改实例类型的兼容性 (p. 402)。

- 对于使用由 Amazon EBS 支持的 AMI 的实例，停止并重启该实例。
- 对于使用实例存储支持的 AMI 的实例，可终止实例并启动替换实例。
- 等待 Amazon EC2 解决问题。
- 将您的问题发布到 Amazon EC2 论坛。
- 如果您的实例位于 Auto Scaling 组中，则 Amazon EC2 Auto Scaling 服务会自动启动替换实例。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的 Auto Scaling 实例的运行状况检查。
- 检索系统日志并查找错误。

检索系统日志

如果实例状态检查失败，则您可以重启实例并检索系统日志。日志能够显示错误之处，从而帮助您诊断问题。重启可清除日志中不必要的信息。

重启实例并检索系统日志

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances，然后选择您的实例。
3. 依次选择 Instance state (实例状态)、Reboot instance (启动实例)。实例重启可能需要几分钟时间。
4. 验证问题是否依然存在；在一些情况下，重启可以解决此问题。
5. 如果实例位于 `running` 状态中，选择实例，依次选择 Actions (操作)、Monitor and troubleshoot (监控和故障排除)、Get system log (获取系统日志)。
6. 查看屏幕上显示的日志，使用下面的已知系统日志错误语句列表来诊断问题。
7. 如果您的情况与我们的检查结果不同，或者，如果您的实例存在问题而我们的检查没有发现，请选择 Status Checks 选项卡上的 Submit feedback 帮助我们改进检测试验。
8. 如果您的问题没有得到解决，您可以将问题发布到 Amazon EC2 论坛。

诊断基于 Linux 的实例的系统日志错误

对于无法通过实例状态检查的 Linux 实例，例如实例可到达性检查，请验证您是否按照上述步骤检索了系统日志。以下列表中包含一些常见的系统日志错误，还有一些建议您采取以解决此问题的针对性操作。

内存错误

- 内存不足：终止进程 (p. 1706)
- 错误：mmu_update 失败 (内存管理更新失败) (p. 1706)

设备错误

- I/O 错误（块储存设备故障） (p. 1707)
- I/O 错误：既不是本地磁盘也不是远程磁盘（破损的分布式块储存设备） (p. 1708)

内核错误

- request_module：runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe) (p. 1709)
- “严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配) (p. 1710)
- “FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失) (p. 1710)
- ERROR：无效内核 (EC2 不兼容内核) (p. 1711)

文件系统错误

- fsck：尝试打开时没有找到此文件或目录... (未找到文件系统) (p. 1712)
- 挂载文件系统时出现一般性错误（挂载失败）(p. 1714)
- VFS：无法在未知块上挂载根 fs (根文件系统不匹配) (p. 1715)
- 错误：无法确定根设备的主/次编号...（根文件系统/设备不匹配）(p. 1716)
- XENBUS：设备没有驱动程序... (p. 1717)
- ... 没有检查时，已强制执行检查的工作日 (文件系统检查要求) (p. 1718)
- fsck 卡在退出状态...（设备缺失）(p. 1718)

操作系统错误

- GRUB 提示 (grubdom>) (p. 1719)
- 提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。(硬编码的 MAC 地址)。 (p. 1721)
- 无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误) (p. 1722)
- XENBUS：连接设备时超时 (Xenbus 超时) (p. 1723)

内存不足：终止进程

指示内存不足错误的系统日志条目与下方显示的内容类似。

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

潜在原因

内存耗尽

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	请执行下列操作之一： • 停止并修改实例以使用不同的实例类型，然后再次启动实例。例如，一个更大或内存优化型实例类型。 • 重启实例以使其恢复未受损状态。除非您更改实例类型，否则该问题可能还会出现。
实例存储支持的	请执行下列操作之一： • 终止实例并启动新实例，指定一个不同的实例类型。例如，一个更大或内存优化型实例类型。 • 重启实例以使其恢复未受损状态。除非您更改实例类型，否则该问题可能还会出现。

错误：mmu_update 失败 (内存管理更新失败)

表示内存管理更新故障的系统日志条目与以下示例类似：

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

潜在原因

Amazon Linux 的问题

建议采取的措施

将您的问题发布到开发人员论坛，或联系 Amazon Web Services Support。

I/O 错误（块储存设备故障）

表示输入/输出错误的系统日志条目类似于以下示例：

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

潜在原因

实例类型	潜在原因
由 Amazon EBS 支持	发生故障的 Amazon EBS 卷
实例存储支持的	发生故障的物理驱动器

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。 2. 分离该卷。 3. 尝试恢复该卷。 Note 最好的做法是经常拍摄 Amazon EBS 卷的快照。这样能大幅降低因故障而导致数据丢失的风险。 4. 重新将卷附加到实例。 5. 启动实例。
实例存储支持的	终止实例并启动新的实例。 Note 无法恢复数据。从备份恢复。 Note 比较好的做法是使用 Amazon S3 或 Amazon EBS 进行备份。实例存储卷是直接与单个主机和磁盘故障相关的。

I/O 错误：既不是本地磁盘也不是远程磁盘（破损的分布式块储存设备）

表示设备的输入/输出错误的系统日志条目类似于以下示例：

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

潜在原因

实例类型	潜在原因
由 Amazon EBS 支持	发生故障的 Amazon EBS 卷

实例类型	潜在原因
实例存储支持的	发生故障的物理驱动器

建议采取的措施

终止实例并启动新的实例。

对于由 Amazon EBS 支持的实例，您可以从最近拍摄的快照恢复数据，方法是从该快照创建映像。快照之后添加的任何数据都无法恢复。

request_module：runaway loop modprobe (在较旧的 Linux 版本上循环旧内核 modprobe)

表示此条件的系统日志类似于下方显示的示例。使用不稳定或陈旧的 Linux 内核 (如 2.6.16-xenU) 可能会在启动时导致无法终止的循环环境。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	使用以下其中一个选项可使用较新的内核 (基于 GRUB 的内核或静态内核)。 选项 1：终止实例并启动新实例，指定 `-kernel` 和 `-ramdisk` 参数。 选项 2： 1. 停止实例。 2. 修改内核和虚拟磁盘的属性以使用较新的内核。 3. 启动实例。
实例存储支持的	终止实例并启动新实例，指定 `-kernel` 和 `-ramdisk` 参数。

“严重错误：内核太旧”和“fsck：在尝试打开 /dev 时没有此文件或目录”(内核与 AMI 不匹配)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

潜在原因

不可兼容的内核和用户空间

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。 2. 修改配置以使用较新的内核。 3. 启动实例。
实例存储支持的	执行以下步骤： 1. 创建使用较新内核的 AMI。 2. 终止实例。 3. 从您创建的 AMI 中启动新实例。

“FATAL: Could not load /lib/modules”或者“BusyBox”(内核模块缺失)

表示此条件的系统日志类似于下方显示的示例。

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No such
 file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
```

```
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

潜在原因

以下一个或多个条件可能会导致此问题：

- 虚拟磁盘缺失
- 缺少正确的虚拟磁盘模块
- Amazon EBS 根卷没有正确附加为 `/dev/sda1`

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 为 Amazon EBS 卷选择经过纠正的虚拟磁盘。 2. 停止实例。 3. 分离并修复该卷。 4. 将卷附加到实例。 5. 启动实例。 6. 修改 AMI 以使用经过纠正的虚拟磁盘。
实例存储支持的	执行以下步骤： 1. 终止此实例，然后启动包含正确虚拟磁盘的新实例。 2. 创建包含正确虚拟磁盘的新 AMI。

ERROR：无效内核 (EC2 不兼容内核)

表示此条件的系统日志类似于下方显示的示例。

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro
```

```
initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

潜在原因

以下一个或两个条件都可能会导致此问题：

- GRUB 不支持所提供的内核
- 后备内核不存在

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。 2. 替换为正在工作的内核。 3. 安装后备内核。 4. 通过纠正内核修改 AMI。
实例存储支持的	执行以下步骤： 1. 终止此实例，然后启动包含正确内核的新实例。 2. 创建包含正确内核的 AMI。 3. （可选）通过 Amazon Web Services Support 寻求技术支持以便恢复数据。

fsck：尝试打开时没有找到此文件或目录... (未找到文件系统)

表示此条件的系统日志类似于下方显示的示例。

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]
```

```
Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

潜在原因

- 虚拟磁盘文件系统定义 /etc/fstab 中存在错误
- /etc/fstab 中存在配置错误的文件系统定义
- 硬盘丢失/故障

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例，分离根卷，修补/修改 /etc/fstab 该卷，将其附加到实例，然后启动该实例。 2. 修改虚拟磁盘以使其包含经过修改的 /etc/fstab（如果适用）。 3. 修改 AMI 以使用较新的虚拟磁盘。 fstab 中的第 6 个字段定义此安装的可用性要求，非零值暗示将在该卷上执行文件系统检查并且必须 成功完成。能否在 Amazon EC2 中使用此字段还不确定，因为故障一般会导致交互性控制台提示信息，但是目前此功能在 Amazon EC2 中尚不可用。请谨慎使用此功能，并阅读 Linux man 页面了解有关 fstab 的信息。
实例存储支持的	执行以下步骤：

对于此实例类型	请执行该操作
	1. 终止实例并启动新的实例。 2. 将所有不正确 Amazon EBS 卷与重启的实例分离。 3. （可选）通过 Amazon Web Services Support 寻求技术支持以便恢复数据。

挂载文件系统时出现一般性错误（挂载失败）

表示此条件的系统日志类似于下方显示的示例。

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

潜在原因

实例类型	潜在原因
由 Amazon EBS 支持	• 分离或出故障的 Amazon EBS 卷。 • 文件系统损坏。 • 匹配错误的内存虚拟磁盘与 AMI 组合 (如 Debian 内存虚拟磁盘和 SUSE AMI)。
实例存储支持的	

实例类型	潜在原因
	• 发生故障的驱动器。 • 损坏的文件系统。 • 匹配错误的虚拟磁盘和组合 (例如，Debian 虚拟磁盘和 SUSE AMI)。

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。 2. 分离根卷。 3. 将根卷附加到已知正在工作的实例。 4. 运行文件系统检查 (fsck –a /dev/…)。 5. 修正所有错误。 6. 从已知正在工作的实例分离卷。 7. 将卷附加到已停止的实例。 8. 启动实例。 9. 重新检查实例的状态。
实例存储支持的	请尝试以下任一操作： • 启动新实例。 • （可选）通过 Amazon Web Services Support 寻求技术支持以便恢复数据。

VFS：无法在未知块上挂载根 fs (根文件系统不匹配)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

潜在原因

实例类型	潜在原因
由 Amazon EBS 支持	• 设备附加错误。 • 根设备没有附加到正确的设备点。 • 文件系统不是预期的格式。

实例类型	潜在原因
	• 使用旧内核 (如 2.6.16-XenU)。 • 实例上的近期更新内核 (错误更新或更新错误)
实例存储支持的	硬件设备故障。

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	请执行下列操作之一： • 停止实例，然后再重启。 • 修改根卷以附加到正确的设备点，可能是 /dev/sda1，而不是 /dev/sda。 • 停止并修改新内核。 • 请参阅您的 Linux 发行版的文档以检查是否有已知更新错误。更改或重新安装内核。
实例存储支持的	终止实例并使用新内核启动新实例。

错误：无法确定根设备的主/次编号...（根文件系统/设备不匹配）

表示此条件的系统日志类似于下方显示的示例。

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

潜在原因

- 虚拟块储存设备驱动程序缺失或配置错误
- 设备枚举冲突 (sda 与 xvda，或是 sda 而不是 sda1)
- 实例内核选择错误

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。 2. 分离该卷。 3. 修正设备映射问题。 4. 启动实例。 5. 修改 AMI 以解决设备映射问题。
实例存储支持的	执行以下步骤： 1. 创建附有适当补丁程序的新 AMI (正确映射块储存设备)。 2. 终止实例并从您创建的 AMI 中启动新实例。

XENBUS：设备没有驱动程序...

表示此条件的系统日志类似于下方显示的示例。

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

潜在原因

- 虚拟块储存设备驱动程序缺失或配置错误
- 设备枚举冲突 (sda 与 xvda)
- 实例内核选择错误

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止实例。

对于此实例类型	请执行该操作
	2. 分离该卷。 3. 修正设备映射问题。 4. 启动实例。 5. 修改 AMI 以解决设备映射问题。
实例存储支持的	执行以下步骤： 1. 创建附有适当补丁程序的 AMI (正确映射块储存设备)。 2. 终止实例并使用您创建的 AMI 启动新实例。

… 没有检查时，已强制执行检查的工作日 (文件系统检查要求)

表示此条件的系统日志类似于下方显示的示例。

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

潜在原因

文件系统检查时间已过；正在强制执行文件系统检查。

建议采取的措施

- 耐心等候文件系统检查的完成。文件系统检查可能需要很长一段时间，具体取决于根文件系统的大小。
- 使用 tune2fs 或适合您的文件系统的工具修改文件系统，以去除强制执行文件系统检查 (fsck) 的功能。

fsck 卡在退出状态…（设备缺失）

表示此条件的系统日志类似于下方显示的示例。

```
Cleaning up ifupdown....
Loading kernel modules...done.
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

潜在原因

- 为缺失的磁盘查找虚拟磁盘
- 强制执行文件系统一致性检查

- 磁盘故障或者已分离

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	尝试以下一个或多个措施以解决此问题： • 停止实例，将该卷附加到正在运行的实例。 • 手动运行一致性检查。 • 修正虚拟磁盘以使其包含相关实用程序。 • 修改文件系统调整参数以删除一致性要求 (不推荐)。
实例存储支持的	尝试以下一个或多个措施以解决此问题： • 通过正确的工具作业重新绑定虚拟磁盘。 • 修改文件系统调整参数以删除一致性要求 (不推荐)。 • 终止实例并启动新的实例。 • （可选）通过 Amazon Web Services Support 寻求技术支持以便恢复数据。

GRUB 提示 (grubdom>)

表示此条件的系统日志类似于下方显示的示例。

```
   GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

      [ Minimal BASH-like line editing is supported.   For

        the   first   word,  TAB  lists  possible  command

        completions.  Anywhere else TAB lists the possible

        completions of a device/filename. ]

grubdom>
```

潜在原因

实例类型	潜在原因
由 Amazon EBS 支持	• 缺少 GRUB 配置文件。 • 使用了错误的 GRUB 映像，应使用不同位置的 GRUB 配置文件。 • 使用了不受支持的文件系统存储您的 GRUB 配置文件 (例如，将您的根文件系统转换为 GRUB 早期版本不支持的类型)。
实例存储支持的	• 缺少 GRUB 配置文件。

实例类型	潜在原因
	• 使用了错误的 GRUB 映像，应使用不同位置的 GRUB 配置文件。 • 使用了不受支持的文件系统存储您的 GRUB 配置文件 (例如，将您的根文件系统转换为 GRUB 早期版本不支持的类型)。

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	选项 1：修改 AMI 并重启实例： 1. 修改源 AMI 以便在标准位置 (/boot/grub/menu.lst) 创建 GRUB 配置文件。 2. 验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。 3. 选择合适的 GRUB 映像 (hd0 – 第一个磁盘或 hd00 – 第一个磁盘，第一个分区)。 4. 终止实例并使用您创建的 AMI 启动一个新实例。 选项 2：修复现有实例： 1. 停止实例。 2. 分离根卷文件系统。 3. 将根卷文件系统附加到已知正在工作的实例。 4. 挂载文件系统。 5. 创建 GRUB 配置文件。 6. 验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。 7. 分离文件系统。 8. 附加到原始实例。 9. 修改内核属性以便使用正确的 GRUB 映像 (第 1 个磁盘或其上的第 1 个分区)。 10启动实例。
实例存储支持的	选项 1：修改 AMI 并重启实例： 1. 使用位于标准位置 (/boot/grub/menu.lst) 的 GRUB 配置文件创建新 AMI。 2. 选择合适的 GRUB 映像 (hd0 – 第一个磁盘或 hd00 – 第一个磁盘，第一个分区)。 3. 验证您的 GRUB 版本支持基础文件系统类型，并根据需要升级 GRUB。 4. 终止实例并使用您创建的 AMI 启动新实例。 选项 2：终止此实例并启动新实例，指定正确的内核。

对于此实例类型	请执行该操作
	Note 要从现有实例恢复数据，请联系 Amazon Web Services Support。

提起接口 eth0：设备 eth0 的 MAC 地址与预期不同，驳回。(硬编码的 MAC 地址)。

表示此条件的系统日志类似于下方显示的示例。

```
...
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected, ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

潜在原因

AMI 配置中存在硬编码接口 MAC

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	请执行下列操作之一： • 修改 AMI 以删除硬编码并重启实例。 • 修改实例以删除硬编码 MAC 地址。 OR 执行以下步骤： 1. 停止实例。 2. 分离根卷。 3. 将卷附加到另一个实例并修改卷以删除硬编码 MAC 地址。 4. 将卷附加到原始实例。 5. 启动实例。
实例存储支持的	请执行下列操作之一： • 修改实例以删除硬编码 MAC 地址。 • 终止实例并启动新的实例。

无法加载 SELinux 策略。计算机处于强制执行模式。正在中断。(SELinux 配置错误)

表示此条件的系统日志类似于下方显示的示例。

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

潜在原因

SELinux 已在错误的情况下启动：

- GRUB 不支持所提供的内核
- 后备内核不存在

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	执行以下步骤： 1. 停止失败的实例。 2. 分离失败的实例的根卷。 3. 将根卷附加到另一个 Linux 的运行实例 (之后称为“恢复实例”)。 4. 连接到恢复实例并挂载失败的实例的根卷。 5. 在挂载的根卷上禁用 SELinux。此过程因 Linux 分配而异；有关更多信息，请参阅特定于操作系统的文档。 Note 在某些系统上，可通过在 `SELINUX=disabled` 文件中设置 `/mount_point/etc/sysconfig/selinux` 来禁用 SELinux (其中，*mount_point* 是您在恢复实例上安装卷的位置)。 6. 从恢复实例卸载和分离根卷并将该根卷重新附加到原始实例。 7. 启动实例。
实例存储支持的	执行以下步骤： 1. 终止实例并启动新的实例。 2. （可选）通过 Amazon Web Services Support 寻求技术支持以便恢复数据。

XENBUS：连接设备时超时 (Xenbus 超时)

表示此条件的系统日志类似于下方显示的示例。

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

潜在原因

- 块储存设备未连接到实例
- 此实例使用的是旧实例内核

建议采取的措施

对于此实例类型	请执行该操作
由 Amazon EBS 支持	请执行下列操作之一： • 修改 AMI 和实例以便使用新内核并重启实例。 • 重启实例。
实例存储支持的	请执行下列操作之一： • 终止实例。 • 修改 AMI 以使用新实例，使用此 AMI 启动新实例。

排查无法访问的实例的问题

您可以使用以下方法对无法访问的 Linux 实例进行故障排除。有关对无法访问的 Windows 实例进行问题排查的信息，请参阅排查无法访问的实例的问题。

目录

- 实例重启 (p. 1723)
- 实例控制台输出 (p. 1724)
- 捕获无法访问的实例的屏幕截图 (p. 1724)
- 主机发生故障时的实例恢复 (p. 1725)

实例重启

能够重启无法访问的实例对于故障排除和一般实例管理都非常有用。

就像可以通过按下重置按钮来重置计算机一样，您可以使用 Amazon EC2 控制台、CLI 或 API 来重置 EC2 实例。有关更多信息，请参阅重启实例 (p. 631)。

实例控制台输出

控制台输出对于问题诊断是非常有价值的工具。它尤其适合用于排查内核问题和服务配置问题，它们可能会导致实例在 SSH 后台程序启动前终止或变得不可达到。

对于 Linux/Unix，实例控制台输出显示了确切的控制台输出，在正常情况下，它们会显示在连接到计算机的物理显示器上。控制台输出返回缓冲的信息，该信息在实例转变状态 (启动、停止、重新引导和终止) 之后很快发布。发布的输出不会持续更新；仅当它可能是最大值时。

对于 Windows 实例，实例控制台输出包括最后三个系统事件日志错误。

您可以选择在实例生命周期中随时检索最新的串行控制台输出。仅在 基于 Nitro 系统构建的实例 (p. 246) 上支持该选项。它不是通过 Amazon EC2 控制台受支持的。

Note

仅保存最新发布的 64 KB 输出，可在最近一次发布后至少 1 小时都可以访问。

只有实例的所有人可以访问控制台输出。您可以使用控制台或命令行检索您的实例的控制台输出。

使用以下方法之一获取控制台输出。

New console

获取控制台输出

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions (操作)、Monitor and troubleshoot (监控和问题排查)、Get system log (获取系统日志)。

Old console

获取控制台输出

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances，然后选择实例。
3. 依次选择 Actions、Instance Settings、Get System Log。

Command line

获取控制台输出

您可以使用以下任一命令。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- get-console-output (Amazon CLI)
- Get-EC2ConsoleOutput (Amazon Tools for Windows PowerShell)

有关常见的系统日志错误的更多信息，请参阅 诊断基于 Linux 的实例的系统日志错误 (p. 1705)。

捕获无法访问的实例的屏幕截图

如果您无法通过 SSH 或 RDP 访问您的实例，您可以捕获实例的屏幕截图并将其作为图像查看。该图像可以让您查看实例的状态，更快地处理问题。您可在实例运行时或在其崩溃后生成屏幕截图。此屏幕截图不会

产生数据传输费用。生成的图像为 JPG 格式，大小不超过 100 kb。当实例存在以下情况时，将不支持此功能：使用 NVIDIA GRID 驱动程序、在裸机实例（类型为 `*.metal` 的实例）上或由基于 ARM 的 Graviton 或 Graviton 2 处理器支持。以下区域提供此功能：

- US East (N. Virginia) Region
- 美国东部（俄亥俄）区域
- US West (Oregon) Region
- US West (N. California) Region
- Europe (Ireland) Region
- 欧洲（法兰克福）区域
- Asia Pacific (Tokyo) Region
- 亚太区域（首尔）
- Asia Pacific (Singapore) Region
- Asia Pacific (Sydney) Region)
- South America (São Paulo) Region)
- 亚太地区 (孟买) 区域
- Canada (Central) Region)
- 欧洲（伦敦）区域
- 欧洲（巴黎）区域

访问实例控制台

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 选择要捕获的实例。
4. 选择 Actions (操作)、Monitor and troubleshoot (监控和问题排查)。
5. 选择 Get Instance Screenshot (获取屏幕实例截图)。

右键单击图像以下载并保存该图像。

使用命令行捕获屏幕截图

您可以使用以下任一命令。返回的内容采用 base64 编码。有关这些命令行界面的更多信息，请参阅 访问 Amazon EC2 (p. 3)。

- get-console-screenshot (Amazon CLI)
- GetConsoleScreenshot（Amazon EC2 查询 API）

主机发生故障时的实例恢复

如果底层主机上的硬件出现不可恢复性问题，Amazon 可能会预定实例停止事件。我们会通过电子邮件提前通知您这类事件。

恢复发生故障的主机上运行的 Amazon EBS 支持的实例

1. 将您实例存储卷上的所有关键数据 Amazon EBS 或 Amazon S3。
2. 停止实例。
3. 启动实例。
4. 恢复所有重要数据。

有关更多信息，请参阅停止和启动您的实例 (p. 610)。

恢复发生故障的主机上运行的实例存储支持的实例

1. 从该实例创建 AMI。
2. 将映像上传到 Amazon S3。
3. 将重要数据备份到 Amazon EBS 或 Amazon S3。
4. 终止实例。
5. 从 AMI 启动新实例。
6. 将所有重要数据恢复到新实例。

有关更多信息，请参阅创建由实例存储支持的 Linux AMI (p. 142)。

从错误的卷启动

在某些情况下，您可能会发现某个并非附加到 /dev/xvda 或 /dev/sda 的卷成为了您的实例的根卷。当您将另一个实例的根卷或从某个根卷的快照中创建的卷附加到带有现有根卷的实例时，可能会发生这种情况。

这是由于 Linux 中的初始虚拟磁盘的工作方式导致的。它将选择在 / 中定义为 /etc/fstab 的卷，在某些发行版中，这是由附加到卷分区的标签决定的。具体来说，您将发现您的 /etc/fstab 与下面类似：

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

如果您检查两个卷的标签，您将看到它们都包含 / 标签：

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

在此示例中，您最终可以让 /dev/xvdf1 (而不是您打算从中启动实例的 /dev/xvda1 卷) 成为您的实例在初始虚拟磁盘运行后从中启动的根设备。要解决此问题，请使用相同的 e2label 命令更改您不想从中启动实例的附加卷的标签。

某些情况下，在 /etc/fstab 中指定 UUID 可以解决此问题。但是，如果两个卷来自同一快照，或者辅助卷是通过主卷的快照创建的，则它们将共享 UUID。

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

更改已附加 ext4 卷的标签

1. 使用 e2label 命令将卷的标签更改为 / 之外的其他标签。

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. 验证卷是否有新标签。

```
[ec2-user ~]$ sudo e2label /dev/xvdf1
old/
```

更改已附加 xfs 卷的标签

- 使用 xfs_admin 命令将卷的标签更改为 / 之外的其他标签。

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

如上所示更改卷标签后，您应该能够重新引导实例并在实例引导时让初始虚拟磁盘选择适当的卷。

Important

如果您要分离使用新标签的卷并将它返回到另一实例以用作根卷，则必须再次执行上述过程并将卷标签更改回其原始值。否则，其他实例将不会启动，因为内存虚拟磁盘无法找到标签为 / 的卷。

使用 EC2Rescue for Linux

EC2Rescue for Linux 是一种易于使用的开源工具，可在 Amazon EC2 Linux 实例上运行此工具以通过其包含 100 多个模块的库来诊断和排查常见问题。适用于 EC2Rescue for Linux 的几个常见使用案例包括：收集 syslog 和程序包管理器日志，收集资源利用率数据以及诊断/修复已知的有问题的内核参数和常见的 OpenSSH 问题。

AWSSupport-TroubleshootSSH 运行手册安装了 EC2Rescue for Linux，使用该工具检查或尝试修复阻止通过 SSH 远程连接到 Linux 计算机的常见问题。有关详细信息以及要运行此自动化，请参阅 Amazon Web Services Support-TroubleshootSSH。

如果您使用的是 Windows 实例，请参阅 EC2Rescue for Windows Server。

目录

- 安装 EC2Rescue for Linux (p. 1727)
- 使用 EC2Rescue for Linux (p. 1730)
- 开发 EC2Rescue 模块 (p. 1732)

安装 EC2Rescue for Linux

EC2Rescue for Linux 工具可以安装在满足以下先决条件的 Amazon EC2 Linux 实例上。

先决条件

- 支持的操作系统：
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- 软件要求：

- Python 2.7.9+ 或 3.2+

AWSSupport-TroubleshootSSH 运行手册安装了 EC2Rescue for Linux，使用该工具检查或尝试修复阻止通过 SSH 远程连接到 Linux 计算机的常见问题。有关详细信息以及要运行此自动化，请参阅 Amazon Web Services Support-TroubleshootSSH。

如果您的系统具有所需的 Python 版本，可以安装标准构建过程。否则，您可以安装捆绑构建过程，其中包括 Python 的最小副本。

安装标准构建过程

1. 从正常工作的 Linux 实例下载 EC2Rescue for Linux 工具：
2. （可选）在继续操作之前，您可以选择性地验证 EC2Rescue for Linux 安装文件的签名。有关更多信息，请参阅（可选）验证 EC2Rescue for Linux 的签名 (p. 1728)。
3. 下载 sha256 哈希文件：
4. 验证 tarball 的完整性：

```
sha256sum -c ec2rl.tgz.sha256
```

5. 解压缩 tarball：

```
tar -xzvf ec2rl.tgz
```

6. 通过列出帮助文件来验证安装：

```
cd ec2rl-<version_number>
./ec2rl help
```

安装捆绑构建过程

有关指向下载和限制列表的链接，请参阅 github 上的 EC2Rescue for Linux。

（可选）验证 EC2Rescue for Linux 的签名

下面是验证基于 Linux 的操作系统的 EC2Rescue for Linux 软件包是否有效的推荐过程。

当您从 Internet 下载应用程序时，我们建议您验证软件发行商的身份，并检查应用程序在发行后是否已遭更改或损坏。这会保护您免于安装含有病毒或其他恶意代码的应用程序版本。

如果您在执行本主题中的步骤后确定适用于 EC2Rescue for Linux 的软件已遭更改或损坏，请不要运行安装文件。否则，可联系 Amazon Web Services。

适用于基于 Linux 的操作系统的 EC2Rescue for Linux 文件是使用 GnuPG（安全数字签名的 Pretty Good Privacy 的开源式执行 (OpenPGP) 标准）进行签名的。GnuPG（也称为 GPG）通过数字签名进行身份验证和完整性检查。Amazon 发布了公有密钥和签名，可供您用于验证下载的 EC2Rescue for Linux 程序包。有关 PGP 和 GnuPG (GPG) 的更多信息，请访问 http://www.gnupg.org。

第一步是与软件发行商建立信任。下载软件发行商的公有密钥，检查公有密钥的所有人是否真为其人，然后将该公有密钥添加到您的密钥环。密钥环是已知公有密钥的集合。验证公有密钥的真实性后，您可以使用它来验证应用程序的签名。

任务

- 安装 GPG 工具 (p. 1729)
- 验证并导入公有密钥 (p. 1729)
- 验证软件包的签名 (p. 1729)

安装 GPG 工具

如果您的操作系统是 Linux 或 Unix，GPG 工具可能已经安装。要测试系统上是否已安装这些工具，请在命令提示符处输入 gpg2。如果已安装 GPG 工具，您会看到 GPG 命令提示。如果没有安装 GPG 工具，您会看到错误信息，告诉您无法找到命令。您可以从存储库安装 GnuPG 包。

在基于 Debian 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：

```
apt-get install gnupg2
```

在基于 Red Hat 的 Linux 上安装 GPG 工具

- 从终端设备运行以下命令：

```
yum install gnupg2
```

验证并导入公有密钥

本流程的下一步是验证 EC2Rescue for Linux 公有密钥，并在 GPG 密钥环中将其添加为可信任密钥。

验证并导入 EC2Rescue for Linux 公有密钥

1. 在命令提示符处，使用以下命令获取我们的公共 GPG 生成密钥的副本：
2. 在保存 `ec2rl.key` 的目录中的命令提示符处，使用以下命令将 EC2Rescue for Linux 公有密钥导入密钥环：

```
gpg2 --import ec2rl.key
```

该命令返回的结果类似于下方内容：

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
```

验证软件包的签名

在安装 GPG 工具、验证并导入 EC2Rescue for Linux 公有密钥以及确认 EC2Rescue for Linux 公有密钥可信后，便可以验证 EC2Rescue for Linux 安装脚本的签名。

验证 EC2Rescue for Linux 安装脚本签名

1. 在命令提示符处，运行以下命令以下载安装脚本的签名文件：
2. 通过在保存 `ec2rl.tgz.sig` 和 EC2Rescue for Linux 安装文件的目录中的命令提示符处运行以下命令来验证签名。这两个文件都必须存在。

```
gpg2 --verify ./ec2rl.tgz.sig
```

输出应与以下内容类似：

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
     Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
```

如果输出包含短语 `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`，则意味着已成功验证签名，您可以继续运行 EC2Rescue for Linux 安装脚本。

如果输出包含短语 `BAD signature`，则检查是否正确执行了此过程。如果您持续获得此响应，请联系 Amazon Web Services，而不要运行之前下载的安装文件。

下面是有关您可能看到的警告的详细信息：

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.这表示您坚信自己拥有 EC2Rescue for Linux 的可信公有密钥的个人信任级别。理想情况下，您将前往 Amazon Web Services 办公室并亲自接收此密钥。但更常见的情况是，从网站下载此密钥。在这种情况下，该网站是 Amazon Web Services 网站。
- gpg2: no ultimately trusted keys found. 这意味着您 (或您信任的其他人) 对特定密钥不是“绝对信任”。

有关更多信息，请参阅 http://www.gnupg.org。

使用 EC2Rescue for Linux

下面是您可以执行以便开始使用此工具的常见任务。

任务

- 运行 EC2Rescue for Linux (p. 1730)
- 上传结果 (p. 1731)
- 创建备份 (p. 1731)
- 获取帮助 (p. 1731)

运行 EC2Rescue for Linux

您可以运行 EC2Rescue for Linux，如以下示例所示。

Example 示例：运行所有模块

要运行所有模块，请运行 EC2Rescue for Linux（不带任何选项）：

```
./ec2rl run
```

有些模块需要根访问权限。如果您不是根用户，请使用 sudo 运行这些模块，如下所示：

```
sudo ./ec2rl run
```

Example 示例：运行特定模块

要仅运行特定模块，请使用 --only-modules 参数：

```
./ec2rl run --only-modules=module_name --arguments
```

例如，此命令运行 dig 模块以查询 amazon.com 域：

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example 示例：查看结果

您可以在 /var/tmp/ec2rl 中查看结果：

```
cat /var/tmp/ec2rl/logfile_location
```

例如，查看 dig 模块的日志文件：

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

上传结果

如果 Amazon Web Services Support 需要您提供结果或者需要您从 S3 存储桶分享结果，请使用 EC2Rescue for Linux CLI 工具上传结果。EC2Rescue for Linux 命令的输出应提供您需要使用的命令。

Example 示例：将结果上传到 Amazon Web Services Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example 示例：将结果上传到 S3 存储桶

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

有关为 Amazon S3 生成预签名 URL 的更多信息，请参阅使用预签名 URL 上传对象。

创建备份

使用以下命令为实例、一个或多个卷或者特定设备 ID 创建备份。

Example 示例：使用 Amazon 系统映像 (AMI) 备份实例

```
./ec2rl run --backup=ami
```

Example 示例：备份与实例关联的所有卷

```
./ec2rl run --backup=allvolumes
```

Example 示例：备份特定卷

```
./ec2rl run --backup=volumeID
```

获取帮助

EC2Rescue for Linux 包括帮助文件，为您提供各可用命令的信息和语法。

Example 示例：显示常规帮助

```
./ec2rl help
```

Example 示例：列出可用模块

```
./ec2rl list
```

Example 示例：显示特定模块的帮助

```
./ec2rl help module_name
```

例如，使用以下命令显示 dig 模块的帮助文件：

```
./ec2rl help dig
```

开发 EC2Rescue 模块

模块使用 YAML 编写，这是一种数据序列化标准。模块的 YAML 文件包括一个文档，用于表示模块及其属性。

添加模块属性

下表列出了可用的模块属性。

属性	描述
name	模块的名称。该名称长度应少于或等于 18 个字符。
version	模块的版本号。
标题	模块的简短说明性标题。此值的长度应少于或等于 50 个字符。

helptext	模块的详细说明。每一行的长度应少于或等于 75 个字符。如果模块使用必需或可选参数，请在 helptext 值中包括这些参数。
	例如：
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	运行模块的阶段。支持的值： • prediagnostic • run • postdiagnostic
language	编写模块代码使用的语言。支持的值： • bash • python

属性	描述
	Note Python 代码必须同时兼容 Python 2.7.9+ 和 Python 3.2+。
remediation	指示模块是否支持修正。支持的值为 `True` 或 `False`。 模块默认为 `False`（如果不存在），这使其成为那些不支持修正的模块的可选属性。
content	整个脚本代码。
constraint	包含限制值的对象的名称。
domain	说明如何分组或分类模块的描述符。所包括的模块组使用以下域： • application • net • os • performance
class	由模块执行的任务类型的描述符。所包括的模块组使用以下类： • collect (从程序收集输出) • diagnose (基于一组标准确定通过/失败) • gather (复制文件并写入特定文件)
distro	此模块支持的 Linux 发行版的列表。所包含的模块组使用以下发行版： • alami (Amazon Linux) • rhel • ubuntu • suse
必需	模块从 CLI 选项使用的必需参数。
可选	模块可使用的可选参数。
software	模块中使用的软件可执行文件。此属性用于指定默认情况下未安装的软件。EC2Rescue for Linux 逻辑在运行模块之前确保这些程序存在并且可执行。
程序包	可执行文件的源软件包。此属性用于随软件提供软件包的详细信息，包括用于下载或者获取更多信息的 URL。
sudo	指示运行模块是否需要根访问权限。 您无需在模块脚本中实施 sudo 检查。如果值为 true，则 EC2Rescue for Linux 逻辑仅在执行用户具有根访问权限时才运行模块。

属性	描述
perfimpact	指示模块对其运行环境是否会产生重大性能影响。如果值为 true 并且没有 `--perfimpact=true` 参数，则跳过模块。
parallelexclusive	指定需要互斥的程序。例如，所有指定“bpf”的模块以串行方式运行。

设置环境变量

下表列出了可用的环境变量。

环境变量	描述
EC2RL_CALLPATH	`ec2rl.py` 的路径。此路径可用于定位 lib 目录和使用分发的 Python 模块。
EC2RL_WORKDIR	诊断工具的主 tmp 目录。 默认值：`/var/tmp/ec2rl`。
EC2RL_RUNDIR	用于存储所有输出的目录。 默认值：`/var/tmp/ec2rl/<date&timestamp>`。
EC2RL_GATHEREDDIR	用于放置收集的模块数据的根目录。 默认值:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/`.
EC2RL_NET_DRIVER	为实例上第一个 (按照字母顺序排序) 非虚拟网络接口使用的驱动程序。 示例： • xen_netfront • ixgbevf • ena
EC2RL_SUDO	如果 EC2Rescue for Linux 以根身份运行，则为 true；否则为 false。
EC2RL_VIRT_TYPE	由实例元数据提供的虚拟化类型。 示例： • default-hvm • default-paravirtual
EC2RL_INTERFACES	系统上的接口枚举列表。该值为包含名称的字符串，例如 `eth0`、`eth1` 等。这通过 `functions.bash` 生成，仅对其来源模块可用。

使用 YAML 语法

在您构建模块 YAML 文件时，应注意以下事项：

- 三个连字符 (---) 表示文档的明确开始位置。
- `!ec2rlcore.module.Module` 标签指示 YAML 分析器在从数据流创建对象时调用哪个构造函数。您可在 `module.py` 文件内部查找构造函数。
- `!!str` 标签告知 YAML 解析器不尝试确定数据的类型，而是将内容解释为字符串文本。
- 竖线字符 (|) 告知 YAML 解析器该值为文字类型的标量。在这种情况下，解析器包括所有空格。对于模块而言这非常重要，因为保留了缩进和换行字符。
- YAML 标准缩进为两个空格，在下例中可以看到。请确保您为脚本保留了标准缩进 (例如，对于 Python 为四个空格)，然后在模块文件中将全部内容缩进两个空格。

模块示例

示例 1 (`mod.d/ps.yaml`)：

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every $period
 seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
  sudo: !!str False
  perfimpact: !!str False
```

```
parallelexclusive: !!str
```

适用于 Linux 实例的 EC2 Serial Console

使用 EC2 Serial Console，您可以访问 Amazon EC2 实例的串行端口，通过该端口可以排查启动、网络配置和其他方面的问题。串行控制台不要求您的实例拥有任何联网功能。使用串行控制台，您可以向实例输入命令，就像键盘和显示器直接连接到实例的串行端口一样。串行控制台会话在实例重启和停止期间持续存在。在重新启动过程中，您可以从一开始就查看所有引导消息。

默认情况下，对串行控制台的访问权限不可用。您的组织必须授予账户对串行控制台的访问权限，并配置 IAM policy 以授予用户对串行控制台的访问权限。通过使用实例 ID、资源标签和其他 IAM 操作，可以精细地控制串行控制台访问。有关更多信息，请参阅配置对 EC2 Serial Console 的访问 (p. 1736)。

串行控制台可使用 EC2 控制台或 Amazon CLI 访问。

串行控制台不会产生额外的成本。

如果您使用的是 Windows 实例，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的适用于 Windows 实例的 EC2 Serial Console。

主题

- 配置对 EC2 Serial Console 的访问 (p. 1736)
- 连接到 EC2 Serial Console (p. 1742)
- 终止 EC2 Serial Console 会话 (p. 1746)
- 使用 EC2 Serial Console 对 Linux 实例进行故障故障 (p. 1747)

配置对 EC2 Serial Console 的访问

要配置对串行控制台的访问权限，您必须在账户级别授予串行控制台访问权限，然后配置 IAM policy 以向用户授予访问权限。您还必须在每个实例上配置基于密码的用户，以使您的用户能够使用串行控制台进行故障排查。

主题

- EC2 Serial Console 的访问级别 (p. 1736)
- 管理账户对 EC2 Serial Console 的访问权限 (p. 1737)
- 为 EC2 Serial Console 访问配置 IAM policy (p. 1739)
- 设置 OS 用户密码 (p. 1741)

EC2 Serial Console 的访问级别

默认情况下，在账户级别无法访问串行控制台。您需要在账户级别明确授予对串行控制台的访问权限。有关更多信息，请参阅管理账户对 EC2 Serial Console 的访问权限 (p. 1737)。

您可以使用服务控制策略 (SCP) 来允许在组织内访问串行控制台。然后，您可以使用 IAM policy 控制访问，从而在用户级别实现精确的访问控制。通过使用 SCP 和 IAM policy 的组合，您可以对串行控制台进行不同级别的访问控制。

组织级别

您可以使用服务控制策略 (SCP) 来允许组织内的成员账户访问串行控制台。有关 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的服务控制策略。

实例级别

您可以通过使用 IAM PrincipalTag 和 ResourceTag 构造以及通过其 ID 指定实例，来配置串行控制台访问策略。有关更多信息，请参阅为 EC2 Serial Console 访问配置 IAM policy (p. 1739)。

用户级别

您可以通过配置 IAM policy 以允许或拒绝指定用户将 SSH 公钥推送到特定实例的串行控制台服务的权限，来配置用户级别的访问权限。有关更多信息，请参阅为 EC2 Serial Console 访问配置 IAM policy (p. 1739)。

操作系统级别

您可以在访客操作系统级别设置用户密码。这为某些使用案例提供了对串行控制台的访问权限。但是，要监控日志，您不需要基于密码的用户。有关更多信息，请参阅设置 OS 用户密码 (p. 1741)。

管理账户对 EC2 Serial Console 的访问权限

默认情况下，在账户级别无法访问串行控制台。您需要在账户级别明确授予对串行控制台的访问权限。

主题

- 授予用户账户访问管理权限 (p. 1737)
- 查看账户对串行控制台的访问权限状态 (p. 1737)
- 授予账户访问串行控制台的权限。 (p. 1738)
- 拒绝账户访问串行控制台 (p. 1739)

授予用户账户访问管理权限

要允许用户管理对 EC2 Serial Console 的账户访问权限，您需要授予其所需的 IAM 权限。

以下策略授予查看账户状态以及允许和阻止账户访问 EC2 Serial Console 的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

有关更多信息，请参阅 IAM 用户指南 中的创建 IAM 策略。

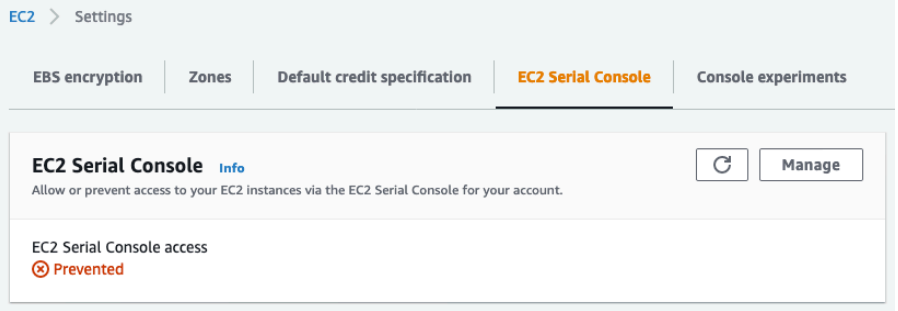
查看账户对串行控制台的访问权限状态

查看账户对串行控制台的访问权限状态（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格上，选择 EC2 Dashboard (EC2 控制面板)。
3. 从 Account attributes（账户属性）中，选择 EC2 Serial Console。

EC2 Serial Console access（EC2 Serial Console 访问）字段指示账户访问权限为 Allowed（允许）还是 Prevented（阻止）。

以下屏幕截图显示，阻止了该账户使用 EC2 Serial Console。



查看账户对串行控制台的访问权限状态 (Amazon CLI)

使用 get-serial-console-access-status 命令查看串行控制台的账户访问状态。

```
aws ec2 get-serial-console-access-status --region us-east-1
```

在以下输出中，true 表示允许该账户访问串行控制台。

```
{
    "SerialConsoleAccessEnabled": true
}
```

授予账户访问串行控制台的权限。

授予账户访问串行控制台的权限（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格上，选择 EC2 Dashboard (EC2 控制面板)。
3. 从 Account attributes（账户属性）中，选择 EC2 Serial Console。
4. 选择管理。
5. 要允许访问账户中所有实例的 EC2 Serial Console，请选中 Allow（允许）复选框。
6. 选择更新。

授予账户访问串行控制台的权限 (Amazon CLI)

使用 enable-serial-console-access 命令允许账户访问串行控制台。

```
aws ec2 enable-serial-console-access --region us-east-1
```

在以下输出中，true 表示允许该账户访问串行控制台。

```
{
    "SerialConsoleAccessEnabled": true
}
```

拒绝账户访问串行控制台

拒绝账户访问串行控制台（控制台）

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格上，选择 EC2 Dashboard (EC2 控制面板)。
3. 从 Account attributes（账户属性）中，选择 EC2 Serial Console。
4. 选择管理。
5. 要阻止访问账户中所有实例的 EC2 Serial Console，请清除 Allow（允许）复选框。
6. 选择更新。

拒绝账户访问串行控制台 (Amazon CLI)

使用 disable-serial-console-access 命令阻止账户访问串行控制台。

```
aws ec2 disable-serial-console-access --region us-east-1
```

在以下输出中，false 表示拒绝该账户访问串行控制台。

```
{
    "SerialConsoleAccessEnabled": false
}
```

为 EC2 Serial Console 访问配置 IAM policy

默认情况下，用户无权访问串行控制台。您的组织必须配置 IAM policy 以授予用户所需的访问权限。有关更多信息，请参阅 IAM 用户指南 中的创建 IAM 策略。

对于串行控制台访问，请创建包含 ec2-instance-connect:SendSerialConsoleSSHPublicKey 操作的 JSON 策略文档。此操作会授予用户将公钥推送到串行控制台服务的权限，该服务将启动串行控制台会话。我们建议限制对特定 EC2 实例的访问。否则，具有此权限的所有用户都可以连接到所有 EC2 实例的串行控制台。

示例 IAM policy

- 明确允许访问串行控制台 (p. 1739)
- 明确拒绝访问串行控制台 (p. 1740)
- 使用资源标签控制对串行控制台的访问 (p. 1740)

明确允许访问串行控制台

默认情况下，没有人可以访问串行控制台。要授予对串行控制台的访问权限，您需要将策略配置为明确允许访问。我们建议配置一个策略以限制对特定实例的访问。

以下策略允许访问由实例 ID 标识的特定实例的串行控制台。

请注意，DescribeInstances、DescribeInstanceTypes 和 GetSerialConsoleAccessStatus 操作不支持资源级权限，因此必须为这些操作指定以 *（星号）表示的所有资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

明确拒绝访问串行控制台

以下 IAM policy 允许访问标有 *（星号）的所有实例的串行控制台，并明确拒绝访问由 ID 标识的特定实例的串行控制台。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

使用资源标签控制对串行控制台的访问

您可以使用资源标签来控制对实例的串行控制台的访问。

基于属性的访问控制是一种授权策略，它根据可附加到用户和 Amazon 资源的标签来定义权限。例如，只有当实例的资源标签和委托人标签具有相同的标签键 `SerialConsole` 值时，以下策略才会允许用户启动该实例的串行控制台连接。

有关使用标签控制对Amazon资源的访问的更多信息，请参阅 IAM 用户指南中的控制对Amazon资源的访问。

请注意，DescribeInstances、DescribeInstanceTypes 和 GetSerialConsoleAccessStatus 操作不支持资源级权限，因此必须为这些操作指定以 *（星号）表示的所有资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole": "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

设置 OS 用户密码

您可以在没有密码的情况下连接到串行控制台。但是，要使用串行控制台对实例进行故障排查，实例必须拥有基于密码的 OS 用户。

您可以为任何 OS 用户（包括根用户）设置密码。请注意，根用户可以修改所有文件，而每个 OS 用户可能只有有限权限。

您必须为要使用串行控制台的每个实例设置用户密码。这是每个实例的一次性要求。

> **Note**
>
> 以下说明仅在使用 Amazon 提供的 AMI 启动实例时才适用，因为默认情况下，Amazon 提供的 AMI 不通过基于密码的用户配置。如果您使用已配置了根用户密码的 AMI 启动实例，则可以跳过这些说明。

设置 OS 用户密码

1. 连接 (p. 644)到您的实例。除 EC2 Serial Console 连接方法外，您还可以使用任何方法连接到自己的实例。
2. 要为用户设置密码，请使用 passwd 命令。在以下示例中，用户是 root。

```
[ec2-user ~]$ sudo passwd root
```

下面是示例输出。

```
Changing password for user root.
New password:
```

3. 出现提 `New password` 示时，输入新密码。
4. 出现提示时，重新输入密码。

连接到 EC2 Serial Console

您可以使用 Amazon EC2 控制台或通过 SSH 连接到 EC2 实例的串行控制台。连接到串行控制台后，您可以使用它来排除引导、网络配置和其他方面的问题。有关排查故障的更多信息，请参阅 使用 EC2 Serial Console 对 Linux 实例进行故障故障 (p. 1747)。

主题

- 注意事项 (p. 1742)
- 先决条件 (p. 1742)
- 连接到 EC2 Serial Console (p. 1743)
- EC2 Serial Console 指纹 (p. 1745)

注意事项

- 每个实例仅支持一个活动串行控制台连接。
- 串行控制台连接通常会持续一小时，除非您将其终止。但是，在系统维护期间，Amazon EC2 将终止串行控制台会话。
- 在断开与串行控制台的连接后，需要 30 秒钟来停用会话，然后才能允许新会话。
- Linux 支持的串行控制台端口：ttyS0
- 连接到串行控制台时，您可能会观察到实例的吞吐量略有下降。

先决条件

- 以下 Amazon Web Services 区域 支持：美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）、加拿大（中部）、欧洲地区（法兰克福）、欧洲地区（爱尔兰）、欧洲地区（伦敦）、欧洲地区（巴黎）、欧洲地区（斯德哥尔摩）、南美洲（圣保罗）、Amazon GovCloud（美国东部）和 Amazon GovCloud（美国西部）。
- 在 Wavelength Zone 或 Amazon Outposts 中不支持。
- 仅在以下 Local Zone 中支持：
  - 美国达拉斯

    Local Zone 名称：`us-east-1-dfw-1a`

    父区域：美国东部（弗吉尼亚州北部）
  - 美国洛杉矶

    Local Zone 名称：`us-west-2-lax-1a`、`us-west-2-lax-1b`

    父区域：美国西部（俄勒冈州）
- 支持基于 Nitro 系统 (p. 246)构建的所有虚拟化实例。
- 不支持裸机实例。
- 配置对 EC2 Serial Console 的访问如下所述：
  - 管理账户对 EC2 Serial Console 的访问权限 (p. 1737).
  - 为 EC2 Serial Console 访问配置 IAM policy (p. 1739)。所有将使用串行控制台的用户都必须拥有所需的权限。

  - 设置 OS 用户密码 (p. 1741).
- 如需使用基于浏览器的客户端 (p. 1743)连接至串行控制台，您的浏览器必须支持 WebSocket。如果您的浏览器不支持 WebSocket，请使用您自己的密钥和 SSH 客户端 (p. 1744)连接至串行控制台。
- 该实例必须处于 `running` 状态。如果实例处于 `pending`、`stopping`、`stopped`、`shutting-down` 或 `terminated` 状态，则无法连接到串行控制台。有关实例状态的更多信息，请参阅 实例生命周期 (p. 570)。
- 如果实例使用 Amazon EC2 Systems Manager，则必须在实例上安装 SSM Agent 3.0.854.0 版或更高版本。有关 SSM Agent 的更多信息，请参阅《Amazon Systems Manager 用户指南》中的使用 SSM Agent。

您不需要在实例上安装或运行 sshd 服务器。

连接到 EC2 Serial Console

连接选项

- 使用基于浏览器的客户端进行连接 (p. 1743)
- 使用您自己的密钥和 SSH 客户端进行连接 (p. 1744)

使用基于浏览器的客户端进行连接

您可以使用基于浏览器的客户端连接到 EC2 实例的串行控制台。您可以通过在 Amazon EC2 控制台中选择实例并选择连接到串行控制台来完成此操作。基于浏览器的客户端处理权限并可提供成功连接。

EC2 Serial Console 适用于大多数浏览器，并支持键盘和鼠标输入。

使用基于浏览器的客户端（Amazon EC2 控制台）连接到实例的串行端口

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 您可以选择相应实例，然后选择 Actions（操作）、Monitor and troubleshoot（监控和问题排查）、EC2 Serial Console、Connect（连接）。

   您也可以选择相应实例，然后选择 Connect（连接）、EC2 Serial Console、Connect（连接）。

   浏览器内终端窗口随即打开。
4. 按 Enter。如果返回登录提示，则表示您已连接到串行控制台。

   如果保持黑屏，则可以使用以下信息来帮助解决连接到串行控制台的问题：

   - 检查您是否已配置了串行控制台的访问权限。有关更多信息，请参阅配置对 EC2 Serial Console 的访问 (p. 1736)。
   - 使用 SysRq 连接到串行控制台。SysRq 不要求您通过基于浏览器的客户端进行连接。有关更多信息，请参阅使用 SysRq 对 Linux 实例进行故障排查 (p. 1750)。
   - 重新启动 getty。如果您对实例拥有 SSH 访问权限，则使用 SSH 连接到实例，然后使用以下命令重新启动 getty。

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - 重启实例。您可以使用 SysRq、EC2 控制台 或 Amazon CLI 重启实例 。有关更多信息，请参阅 使用 SysRq 对 Linux 实例进行故障排查 (p. 1750) 或 重启实例 (p. 631)。
5. 在 `login` 提示符下，输入您之前设置 (p. 1741)的基于密码的用户的用户名，然后按 Enter 键。
6. 在 `Password` 提示符下，输入密码，然后按 Enter 键。

您现在已登录实例，可以使用串行控制台进行故障排查。

使用您自己的密钥和 SSH 客户端进行连接

您可以使用自己的 SSH 密钥，并在使用 串行控制台 API 时从您选择的 SSH 客户端连接到您的实例。这使您能够从将公有密钥推送到实例的串行控制台功能中受益。

使用 SSH 连接到实例的串行控制台

1. 将 SSH 公钥推送到实例以启动串行控制台会话

   使用 send-serial-console-ssh-public-key 命令可将 SSH 公有密钥推送到实例。这将启动串行控制台会话。

   如果已为此实例启动串行控制台会话，则该命令将失败，因为您每次只能打开一个会话。在断开与串行控制台的连接后，需要 30 秒钟来停用会话，然后才能允许新会话。

   ```
   $ aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. 使用私钥连接到串行控制台

   在从串行控制台服务删除公钥之前，使用 ssh 命令连接到串行控制台。在移除之前，您有 60 秒钟的时间。

   使用与公钥对应的私钥。

   用户名格式为 `instance-id.port0`，其中包括实例 ID 和端口 0。在以下示例中，用户名为 `i-001234a4bf70dec41EXAMPLE.port0`。

   对于除 Amazon GovCloud (US) 区域外，所有支持的 Amazon 区域：

   串行控制台服务的公有 DNS 名称的格式为 `serial-console.ec2-instance-connect.region.aws`。在以下示例中，串行控制台服务位于 *us-east-1* 区域。

   ```
   $ ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
   connect.us-east-1.aws
   ```

   仅对于 Amazon GovCloud (US) 区域：

   Amazon GovCloud (US) 区域中串行控制台服务的公有 DNS 名称的格式为 `serial-console.ec2-instance-connect.GovCloud-region.amazonaws.com`。在以下示例中，串行控制台服务位于 *us-gov-east-1* 区域。

   ```
   $ ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
   connect.us-gov-east-1.amazonaws.com
   ```

3. （可选）验证指纹

   首次连接到串行控制台时，系统会提示您验证指纹。您可以比较串行控制台指纹与为了进行验证而显示的指纹。如果这些指纹不匹配，则表示有人可能在试图实施“中间人”攻击。如果它们匹配，您可以放心地连接到串行控制台。

   以下指纹用于 us-east-1 区域中的串行控制台服务。有关每个区域的指纹，请参阅 EC2 Serial Console 指纹 (p. 1745)。

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
```

Note

该指纹仅在您第一次连接到串行控制台时出现。

4. 按 Enter。如果返回提示，则表示您已连接到串行控制台。

   如果保持黑屏，则可以使用以下信息来帮助解决连接到串行控制台的问题：

   - 检查您是否已配置了串行控制台的访问权限。有关更多信息，请参阅配置对 EC2 Serial Console 的访问 (p. 1736)。
   - 使用 SysRq 连接到串行控制台。SysRq 不要求您通过 SSH 进行连接。有关更多信息，请参阅使用 SysRq 对 Linux 实例进行故障排查 (p. 1750)。
   - 重新启动 getty。如果您对实例拥有 SSH 访问权限，则使用 SSH 连接到实例，然后使用以下命令重新启动 getty。

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - 重启实例。您可以使用 SysRq、EC2 控制台 或 Amazon CLI 重启实例 。有关更多信息，请参阅 使用 SysRq 对 Linux 实例进行故障排查 (p. 1750) 或 重启实例 (p. 631)。

5. 在 `login` 提示符下，输入您之前设置 (p. 1741)的基于密码的用户的用户名，然后按 Enter 键。
6. 在 `Password` 提示符下，输入密码，然后按 Enter 键。

   您现在已登录实例，可以使用串行控制台进行故障排查。

EC2 Serial Console 指纹

EC2 Serial Console 指纹对每个 Amazon 区域都是唯一的。

- us-east-1 – 美国东部（弗吉尼亚北部）

  ```
  SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
  ```

- us-east-2 – 美国东部（俄亥俄）

  ```
  SHA256:EhwPkTzRtTY7TRSzz26XbB0/HvV9jRM7mCZN0xw/d/0
  ```

- us-west-1 – 美国西部（加利福尼亚北部）

  ```
  SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
  ```

- us-west-2 – 美国西部（俄勒冈）

  ```
  SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
  ```

- ap-south-1 – 亚太地区（孟买）

  ```
  SHA256:oBLXcYmklqHHEbliARxEgH8IsO51rezTPiSM35BsU40
  ```

- ap-northeast-2 – 亚太地区（首尔）

  ```
  SHA256:FoqWXNX+DZ++GuNTztg9PK49WYMqBX+FrcZM2dSrqrI
  ```

- ap-southeast-1 – 亚太地区（新加坡）

```
SHA256:PLFNn7WnCQDHx3qmwLu1Gy/O8TUX7LQgZuaC6L45CoY
```

- ap-southeast-2 – 亚太地区（悉尼）

```
SHA256:yFvMwUK9lEUQjQTRoXXzuN+cW9/VSe9W984Cf5Tgzo4
```

- ap-northeast-1 – 亚太地区（东京）

```
SHA256:RQfsDCZTOfQawewTRDV1t9Em/HMrFQe+CRlIOT5um4k
```

- ca-central-1 – 加拿大（中部）

```
SHA256:P2O2jOZwmpMwkpO6YW738FIOTHdUTyEv2gczYMMO7s4
```

- eu-central-1 –欧洲（法兰克福）

```
SHA256:aCMFS/yIcOdOlkXvOl8AmZ1Toe+bBnrJJ3Fy0k0De2c
```

- eu-west-1 –欧洲（爱尔兰）

```
SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E
```

- eu-west-2 – 欧洲（伦敦）

```
SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
```

- eu-west-3 – 欧洲（巴黎）

```
SHA256:q8ldnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeEWs
```

- eu-north-1 – 欧洲（斯德哥尔摩）

```
SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
```

- sa-east-1 – 南美洲（圣保罗）

```
SHA256:rd2+/32Ognjew1yVIemENaQzC+Botbih62OqAPDq1dI
```

- us-gov-east-1 – Amazon GovCloud（美国东部）

```
SHA256:tIwe19GWsoyLClrtvu38YEEh+DHIkqnDcZnmtebvF28
```

- us-gov-west-1 – Amazon GovCloud（美国西部）

```
SHA256:kfOFRWLaOZfB+utbd3bRf8OlPf8nGO2YZLqXZiIw5DQ
```

终止 EC2 Serial Console 会话

终止串行控制台会话的方式取决于客户端。

基于浏览器的客户端

要终止串行控制台会话，请关闭串行控制台浏览器内终端窗口。

标准 OpenSSH 客户端

要终止串行控制台会话，请使用以下命令关闭 SSH 连接。此命令必须在换行之后立即运行。

```
$ ~.
```

Note

您用于关闭 SSH 连接的命令可能会有所不同，取决于您正在使用的 SSH 客户端。

使用 EC2 Serial Console 对 Linux 实例进行故障故障

通过使用 EC2 Serial Console，您可以通过连接到实例的串行端口来排查启动、网络配置和其他方面的问题。

主题

- 使用 GRUB 对 Linux 实例进行故障排查 (p. 1747)
- 使用 SysRq 对 Linux 实例进行故障排查 (p. 1750)

有关对 Windows 实例进行故障排查的信息，请参阅 Amazon EC2 用户指南（适用于 Windows 实例）中的使用 EC2 Serial Console 对 Windows 实例进行故障排查。

使用 GRUB 对 Linux 实例进行故障排查

GNU GRUB（GNU GRand Unified Bootloader [统一引导加载程序] 的缩写，通常称为 GRUB）是大多数 Linux 操作系统的默认引导加载程序。从 GRUB 菜单中，您可以选择要引导到哪个内核，或修改菜单项以更改内核的启动方式。这在对失败的实例进行故障排查时非常有用。

在引导流程中将显示 GRUB 菜单。该菜单无法通过普通 SSH 访问，但您可以通过 EC2 Serial Console 访问。

主题

- 先决条件 (p. 1747)
- 配置 GRUB (p. 1747)
- 使用 GRUB (p. 1749)

先决条件

您必须先授予串行控制台访问权限，然后才能配置和使用 GRUB。有关更多信息，请参阅配置对 EC2 Serial Console 的访问 (p. 1736)。

配置 GRUB

在通过串行控制台使用 GRUB 之前，您必须将实例配置为通过串行控制台使用 GRUB。

要配置 GRUB，请根据用于启动实例的 AMI 选择以下程序之一。

Amazon Linux 2

在 Amazon Linux 2 实例上配置 GRUB

1. 连接到您的实例 (p. 644)。
2. 在 `/etc/default/grub` 中添加或更改以下选项：

- 设置 GRUB_TIMEOUT=1。
- 添加 GRUB_TERMINAL="console serial".
- 添加 GRUB_SERIAL_COMMAND="serial --speed=115200".

以下是 /etc/default/grub 的示例。您可能需要根据系统设置更改配置。

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
GRUB_TIMEOUT=1
GRUB_DISABLE_RECOVERY="true"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. 运行以下命令以应用更新后的配置。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

Ubuntu

在 Ubuntu 实例上配置 GRUB

1. 连接到您的实例 (p. 644)。
2. 在 /etc/default/grub.d/50-cloudimg-settings.cfg 中添加或更改以下选项：
   - 设置 GRUB_TIMEOUT=1。
   - 添加 GRUB_TIMEOUT_STYLE=menu.
   - 添加 GRUB_TERMINAL="console serial".
   - 删除 GRUB_HIDDEN_TIMEOUT.
   - 添加 GRUB_SERIAL_COMMAND="serial --speed=115200".

   以下是 /etc/default/grub.d/50-cloudimg-settings.cfg 的示例。您可能需要根据系统设置更改配置。

```
# Cloud Image specific Grub settings for Generic Cloud Images
# CLOUD_IMG: This file was created/modified by the Cloud Image build process

# Set the recordfail timeout
GRUB_RECORDFAIL_TIMEOUT=0

# Do not wait on grub prompt
GRUB_TIMEOUT=1
GRUB_TIMEOUT_STYLE=menu

# Set the default commandline
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295"

# Set the grub console type
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. 运行以下命令以应用更新后的配置。

```
[ec2-user ~]$ sudo update-grub
```

RHEL

在 RHEL 实例上配置 GRUB

1. 连接到您的实例 (p. 644)。
2. 在 /etc/default/grub 中添加或更改以下选项：
   - 删除 GRUB_TERMINAL_OUTPUT.
   - 添加 GRUB_TERMINAL="console serial".
   - 添加 GRUB_SERIAL_COMMAND="serial --speed=115200".

   以下是 /etc/default/grub 的示例。您可能需要根据系统设置更改配置。

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
 rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. 运行以下命令以应用更新后的配置。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

对于使用 CentOS AMI 启动的实例，默认情况下为串行控制台配置了 GRUB。

以下是 /etc/default/grub 的示例。根据您的系统设置，您的配置可能会有所不同。

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

使用 GRUB

配置 GRUB 后，连接到串行控制台并使用重启命令重启实例。在重新启动过程中，您会看到 GRUB 菜单。出现 GRUB 菜单时按任意键可停止启动流程，从而使您可以与 GRUB 菜单进行交互。

主题

- 单用户模式 (p. 1750)
- 紧急模式 (p. 1750)

单用户模式

单用户模式将在较低的运行级别启动内核。例如，它可能会挂载文件系统，但不会激活网络，从而使您有机会执行修复实例所需的维护。

启动到单用户模式

1. 连接到 (p. 1743)实例的串行控制台。
2. 使用以下命令重新引导实例。

```
[ec2-user ~]$ sudo reboot
```

3. 在重新启动期间，当 GRUB 菜单出现时，按任意键停止引导流程。
4. 在 GRUB 菜单中，使用箭头键选择要引导的内核，然后按键盘上的 e。
5. 使用箭头键将光标定位在包含内核的行上。该行以 `linux` 或 `linux16` 开头，取决于启动实例所使用的 AMI。对于 Ubuntu，有两行开头为 `linux`，必须在下一步中修改。
6. 在行末添加 `single` 一词。

   以下是 Amazon Linux 2 的示例。

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. 按 Ctrl+X 可启动到单用户模式。
8. 在 `login` 提示符下，输入您之前设置 (p. 1741)的基于密码的用户的用户名，然后按 Enter 键。
9. 在 `Password` 提示符下，输入密码，然后按 Enter 键。

紧急模式

紧急模式与单用户模式类似，只是内核在可达到的最低运行级别运行。

要启动到紧急模式，请按照上一节的 单用户模式 (p. 1750) 中的步骤操作，但在第 6 步中添加的词是 `emergency` 而非 `single`。

使用 SysRq 对 Linux 实例进行故障排查

系统请求 (SysRq) 键（有时称为“magic SysRq”）可用于在 Shell 外直接向内核发送命令，无论内核正在执行什么操作，内核都会响应。例如，如果实例已停止响应，则可以使用 SysRq 密钥告诉内核崩溃或重新启动。有关更多信息，请参阅 Wikipedia 中的 Magic SysRq 键。

主题

- 先决条件 (p. 1750)
- 配置 SysRq (p. 1750)
- 使用 SysRq (p. 1751)

先决条件

您必须先授予串行控制台访问权限，然后才能配置和使用 SysRq。有关更多信息，请参阅配置对 EC2 Serial Console 的访问 (p. 1736)。

配置 SysRq

要配置 SysRq，请在当前引导周期中启用 SysRq 命令。要使配置永久化，您还可以为后续引导启用 SysRq 命令。

为当前引导周期启用所有 SysRq 命令

1. 连接到您的实例 (p. 644)。
2. 运行以下命令。

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

Note

下次重新启动时将会清除此设置。

为后续引导启用所有 SysRq 命令

1. 创建文件 /etc/sysctl.d/99-sysrq.conf 并在您收藏的编辑器中打开。

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. 添加以下行。

```
kernel.sysrq=1
```

3. 重启实例以应用更改。

```
[ec2-user ~]$ sudo reboot
```

4. 在 login 提示符下，输入您之前设置 (p. 1741)的基于密码的用户的用户名，然后按 Enter 键。
5. 在 Password 提示符下，输入密码，然后按 Enter 键。

使用 SysRq

您可以在基于 EC2 Serial Console 浏览器的客户端中或 SSH 客户端中使用 SysRq 命令。每个客户端发送中断请求的命令都不同。

要使用 SysRq，请根据您正在使用的客户端选择以下程序之一。

Browser-based client

在串行控制台基于浏览器的客户端中使用 SysRq

1. 连接到 (p. 1743)实例的串行控制台。
2. 要发送中断请求，请按 CTRL+0（零）。如果您的键盘支持，还可以使用暂停或中断键发送中断请求。

```
[ec2-user ~]$ CTRL+0
```

3. 要发出 SysRq 命令，请按键盘上与所需命令对应的键。例如，要显示 SysRq 命令列表，请按 h。

```
[ec2-user ~]$ h
```

h 命令的输出类似于以下内容。

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
```

```
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

在 SSH 客户端中使用 SysRq

1. 连接到 (p. 1743)实例的串行控制台。
2. 要发送中断请求，请按 ~B（波浪号后跟大写 B）。

```
[ec2-user ~]$ ~B
```

3. 要发出 SysRq 命令，请按键盘上与所需命令对应的键。例如，要显示 SysRq 命令列表，请按 h。

```
[ec2-user ~]$ h
```

h 命令的输出类似于以下内容。

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

Note

您用于发送中断请求的命令可能会有所不同，取决于您正在使用的 SSH 客户端。

发送诊断中断（适用于高级用户）

Warning

诊断中断供高级用户使用。使用不当会对您的实例产生负面影响。向实例发送诊断中断可能会触发实例崩溃和重新启动，从而导致数据丢失。

您可以将诊断中断发送到无法访问或无响应的 Linux 实例以手动触发内核错误。

在出现内核错误时，Linux 操作系统通常会发生崩溃并重启。操作系统的具体行为取决于其配置。内核错误也可用于使实例的操作系统内核执行任务，例如生成崩溃转储文件。然后，您可以使用崩溃转储文件中的信息进行根本原因分析并调试实例。

崩溃转储数据由操作系统在实例本身上本地生成。

在向您的实例发送诊断中断之前，我们建议您查阅适合您操作系统的文档，然后进行必要的配置更改。

目录

- 支持的实例类型 (p. 1753)
- 先决条件 (p. 1753)
- 发送诊断中断 (p. 1755)

支持的实例类型

除 Amazon Graviton 处理器支持的实例类型外的所有基于 Nitro 的实例类型均支持诊断中断。有关更多信息，请参阅 基于 Nitro 系统构建的实例 (p. 246) 和 Amazon Graviton。

先决条件

在使用诊断中断之前，必须配置实例的操作系统。这可确保它在发生内核错误时执行所需的操作。

将 Amazon Linux 2 配置为在发生内核错误时生成崩溃转储

1. 连接到您的 实例。
2. 安装 kexec 和 kdump。

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. 配置内核以便为辅助内核预留适当的内存量。要预留的内存量取决于实例的总可用内存。使用首选文本编辑器打开 /etc/default/grub 文件，找到以 GRUB_CMDLINE_LINUX_DEFAULT 开始的行，然后按以下格式添加 crashkernel 参数：crashkernel=*memory_to_reserve*。例如，要预留 160MB，请修改 grub 文件，如下所示：

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. 保存更改并关闭 grub 文件。
5. 重新构建 GRUB2 配置文件。

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. 在基于 Intel 和 AMD 处理器的实例上，send-diagnostic-interrupt 命令将未知的非屏蔽中断 (NMI) 发送到实例。您必须将内核配置为在收到未知 NMI 时发生崩溃。使用首选文本编辑器打开 /etc/sysctl.conf 文件，并添加以下内容。

```
kernel.unknown_nmi_panic=1
```

7. 重启实例并重新连接到它。
8. 使用正确的 crashkernel 参数验证是否已启动内核。

```
$ grep crashkernel /proc/cmdline
```

以下示例输出指示成功的配置。

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. 确认 kdump 服务正在运行。

```
[ec2-user ~]$ systemctl status kdump.service
```

以下示例输出显示在 kdump 服务正在运行的情况下的结果。

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

Note

默认情况下，崩溃转储文件将保存到 /var/crash/。要更改位置，请使用首选文本编辑器修改 /etc/kdump.conf 文件。

将 Amazon Linux 配置为在发生内核错误时生成崩溃转储

1. 连接到您的 实例。
2. 安装 kexec 和 kdump。

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. 配置内核以便为辅助内核预留适当的内存量。要预留的内存量取决于实例的总可用内存。

```
$ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
```

例如，要为崩溃内核预留 160MB，请使用以下命令。

```
$ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
```

4. 在基于 Intel 和 AMD 处理器的实例上，send-diagnostic-interrupt 命令将未知的非屏蔽中断 (NMI) 发送到实例。您必须将内核配置为在收到未知 NMI 时发生崩溃。使用首选文本编辑器打开 /etc/sysctl.conf 文件，并添加以下内容。

```
kernel.unknown_nmi_panic=1
```

5. 重启实例并重新连接到它。
6. 使用正确的 crashkernel 参数验证是否已启动内核。

```
$ grep crashkernel /proc/cmdline
```

以下示例输出指示成功的配置。

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
 LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. 确认 kdump 服务正在运行。

```
[ec2-user ~]$ sudo service kdump status
```

如果该服务正在运行，则命令将返回 Kdump is operational 响应。

Note

默认情况下，崩溃转储文件将保存到 /var/crash/。要更改位置，请使用首选文本编辑器修改 /etc/kdump.conf 文件。

配置 SUSE Linux Enterprise、Ubuntu 或 Red Hat Enterprise Linux

请参阅以下网站：

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

> **Note**
>
> 在基于 Intel 和 AMD 处理器的实例上，`send-diagnostic-interrupt` 命令将未知的非屏蔽中断 (NMI) 发送到实例。您必须将内核配置为在收到未知 NMI 时发生崩溃。将以下内容添加到配置文件。

```
kernel.unknown_nmi_panic=1
```

发送诊断中断

在完成必要的配置更改后，您可以使用 Amazon CLI 或 Amazon EC2 API 将诊断中断发送到实例。

将诊断中断发送到实例 (Amazon CLI)

使用 send-diagnostic-interrupt 命令并指定实例 ID。

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

相关信息

下列相关资源在您使用此服务的过程中会有所帮助。

Amazon 上的 Linux

- 来自 Amazon 的 Linux – 来自 Amazon 的基于 Linux 的现代操作系统组合。
- EC2 Image Builder – 自动创建、管理和部署自定义、安全且最新的服务器映像，这些映像是预先安装的，并预置了软件设置以符合特定 IT 标准。

Amazon Web Services re:Post

Amazon Web Services re:Post – Amazon 托管式问答（Q & A）服务，为您的技术问题提供众包、经专家审查的答案。

定价

Amazon EC2 定价 – Amazon EC2 的定价信息。

一般Amazon资源

以下一般资源在您使用 Amazon 的过程中会有所帮助。

- 入门资源中心 – 了解如何设置 Amazon Web Services 账户、加入 Amazon 社区和启动您的第一个应用程序。
- Amazon Web Services Support 中心 – 用于创建和管理 Amazon Web Services Support 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及Amazon Trusted Advisor。
- Amazon Web Services Support – 提供有关 Amazon Web Services Support 的信息的主要网页，这是一个一对一的快速响应支持渠道，可以帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关Amazon账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon 网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

文档历史记录

下表描述 Amazon EC2 文档集的重要补充部分（2019 年开始）。我们还经常更新文档来处理您发送给我们的反馈意见。

变更	说明	日期
新裸机实例 (p. 1757)	C6in、M6idn、M6in、R6idn 和 R6in 的裸机实例。	2023 年 3 月 21 日
修改实例元数据选项	现在，您可以使用 Amazon EC2 控制台修改实例元数据选项。	2023 年 3 月 20 日
就地 macOS 操作系统更新	现在，您可以在 M1 Mac 实例上执行就地 Apple macOS 操作系统更新。	2023 年 3 月 14 日
UEFI Preferred	现在，您可以创建同时支持统一可扩展固件接口（UEFI）和传统 BIOS 启动模式的单个 AMI。	2023 年 3 月 3 日
修改 IMDSv2 的 AMI	修改现有 AMI，以确保从此 AMI 启动的实例默认要求使用 IMDSv2。	2023 年 2 月 28 日
为 ENA Express 添加支持的实例	添加了一个表，其中包含 ENA Express 支持的新实例和现有实例类型。	2023 年 2 月 13 日
在 Amazon EBS 上进行故障测试	使用 Amazon FIS 暂时停止 EBS 卷与其附加实例之间的 I/O，以测试工作负载如何处理 I/O 中断。	2023 年 1 月 27 日
启动模板中的 AMI 别名	您可以在启动模板中指定 Amazon Systems Manager 参数而不是 AMI ID，从而无需每次 AMI ID 发生更改时都更新模板。	2023 年 1 月 19 日
对 C6i、I3en 和 M6i 的休眠支持	使 C6i、I3en 和 M6i 实例类型上运行的新启动实例休眠。	2022 年 12 月 19 日
撕裂写防护	借助撕裂写防护这一数据块存储功能，可提高 I/O 密集型关系数据库工作负载的性能并减少延迟，而不会影响数据弹性。	2022 年 11 月 29 日
Hpc6id 实例 (p. 1757)	采用第 3 代英特尔至强可扩展处理器（Ice Lake）的新内存优化型实例。	2022 年 11 月 29 日
R6in 和 R6idn 实例 (p. 1757)	适用于网络密集型工作负载的全新内存优化型实例。	2022 年 11 月 28 日
M6in 和 M6idn 实例 (p. 1757)	新的通用计算实例类型。	2022 年 11 月 28 日
ENA Express	使用 ENA Express 提高吞吐量并最大限度减少 EC2 实例之间网络流量的尾部延迟。	2022 年 11 月 28 日

C6in 实例 (p. 1757)	新的计算优化型实例非常适合运行高性能计算。	2022 年 11 月 28 日
回收站保留规则锁定	您可以锁定保留规则，以保护其免遭意外或恶意修改和删除。	2022 年 11 月 23 日
复制 AMI 标签	复制 AMI 时，可以同时复制用户定义的 AMI 标签。	2022 年 11 月 18 日
用于存储和还原的 AMI 大小	可在 Amazon S3 存储桶之间存储和还原的 AMI 大小（压缩前）现可高达 5000 GB。	2022 年 11 月 16 日
适用于竞价型实例的 priceCapacityOptimized 分配策略	使用 `priceCapacityOptimized` 分配策略的竞价型实例集需同时考虑价格和容量，以选择中断可能性最小、价格尽可能最低的竞价型实例池。	2022 年 11 月 10 日
适用于竞价型实例的价格容量优化分配策略	使用 `price-capacity-optimized` 分配策略的 EC2 实例集需同时考虑价格和容量，以选择中断可能性最小、价格尽可能最低的竞价型实例池。	2022 年 11 月 10 日
取消与您的账户共享 AMI	如果已与您的 Amazon Web Services 账户 共享 AMI，而您不想再与您的账户共享该 AMI，则可以将您的账户从 AMI 的启动权限中移除。	2022 年 11 月 4 日
转移弹性 IP 地址	您现在可以将弹性 IP 地址从一个 Amazon 账户转移到另一个账户。	2022 年 10 月 31 日
替换根卷	您可以使用 AMI 替换正在运行的实例的根 Amazon EBS 卷。	2022 年 10 月 27 日
Trn1 实例 (p. 1757)	新的加速型计算实例针对由 Amazon Trainium 芯片支持的深度学习进行了优化。	2022 年 10 月 10 日
自动将实例连接到数据库	使用自动连接功能将一个或多个 EC2 实例快速连接到一个 RDS 数据库，以允许它们之间的流量。	2022 年 10 月 10 日
AMI 限额	限额现在适用于创建和共享 AMI。	2022 年 10 月 10 日
为 AMI 配置 IMDSv2	配置您的 AMI，以确保从此 AMI 启动的实例默认要求使用 IMDSv2。	2022 年 10 月 3 日
启动竞价型实例中断	您可以在 Amazon EC2 控制台中选择一个竞价型实例并启动中断，从而测试竞价型实例上的应用程序将如何处理中断。	2022 年 9 月 26 日

经过验证的 AMI 提供商	在 Amazon EC2 控制台中，将 Amazon 或经过验证的 Amazon 合作伙伴拥有的公有 AMI 标记为经过验证的提供商。	2022 年 7 月 22 日
R6a 实例 (p. 1757)	采用第三代 AMD EPYC 处理器的新内存优化型实例。	2022 年 7 月 19 日
Amazon Outposts 上的置放群组	增加了适用于 Outpost 上的置放群组的主机分布策略。	2022 年 6 月 30 日
回收站的条件键	您可以使用 `rbin:Request/ResourceType` 和 `rbin:Attribute/ResourceType` 条件键来筛选回收站访问权限请求。	2022 年 6 月 14 日
R6id 实例 (p. 1757)	采用第 3 代英特尔至强可扩展处理器（Ice Lake）的新内存优化型实例。	2022 年 6 月 9 日
io2 Block Express 卷	您可以修改 io2 Block Express 卷的大小和预调配 IOPS，并为其启用快速快照还原。	2022 年 5 月 31 日
Amazon Outposts 上的专属主机	您可以在 Amazon Outposts 上分配专属主机。	2022 年 5 月 31 日
M6id 实例 (p. 1757)	采用第 3 代英特尔至强可扩展处理器（Ice Lake）的新通用实例。	2022 年 5 月 26 日
C6id 实例 (p. 1757)	采用第 3 代英特尔至强可扩展处理器（Ice Lake）的新计算优化型实例。	2022 年 5 月 26 日
实例停止保护	要防止实例意外停止，可以为实例启用停止保护。	2022 年 5 月 24 日
C7g 实例 (p. 1757)	采用最新 Amazon Graviton3 处理器的新计算优化型实例。	2022 年 5 月 23 日
UEFI 安全引导	UEFI 安全引导构建在 Amazon EC2 长期以来的安全启动过程之上，并提供了额外的深度防御功能，可以帮助客户保护软件免受重新引导过程中持续存在的威胁。	2022 年 5 月 10 日
NitroTPM	Nitro 可信平台模块 (NitroTPM) 是一种虚拟设备，由 Amazon Nitro 系统提供，并符合 TPM 2.0 规范。	2022 年 5 月 10 日
AMI 状态更改事件	现在，当 AMI 更改状态时，Amazon EC2 会生成一个事件。您可以使用 Amazon EventBridge 检测并响应这些事件。	2022 年 5 月 9 日
描述公有密钥	您可以查询 Amazon EC2 密钥对的公有密钥和创建日期。	2022 年 4 月 28 日

创建密钥对	您可以在创建新密钥对时指定密钥格式（PEM 或 PPK）。	2022 年 4 月 28 日
I4i 实例 (p. 1757)	采用第 3 代英特尔至强可扩展处理器 (Ice Lake) 的新存储优化型实例。	2022 年 4 月 27 日
在启动时挂载 Amazon FSx 文件系统	您可以使用新的启动实例向导在启动时挂载新的或现有的 Amazon FSx for NetApp ONTAP 或 Amazon FSx for OpenZFS 文件系统。	2022 年 4 月 12 日
新启动实例向导	Amazon EC2 控制台中全新改进后的启动体验，提供了更快、更简单的 EC2 实例启动方法。	2022 年 4 月 5 日
自动弃用公用 AMI	默认情况下，所有公用 AMI 的弃用日期设置为自 AMI 创建日期起的两年。	2022 年 3 月 31 日
实例元数据类别：autoscaling/target-lifecycle-state	使用 Auto Scaling 组时，您可以从实例元数据访问实例的目标生命周期状态。	2022 年 3 月 24 日
竞价放置分数	根据您的 Spot 容量要求，获取 Amazon区域或可用区的建议。	2022 年 3 月 16 日
X2idn 和 X2iedn 实例 (p. 1757)	采用英特尔至强可扩展处理器 (Ice Lake) 的新内存优化型实例。	2022 年 3 月 10 日
AMI 的上次启动时间	`lastLaunchedTime` 指示您上次使用 AMI 启动实例时的时间戳。	2022 年 2 月 28 日
C6a 实例 (p. 1757)	新的计算优化型实例，采用第三代 AMD EPYC 处理器（米兰）。	2022 年 2 月 14 日
AMI 回收站	回收站能够让您还原意外删除的 AMI。	2022 年 2 月 3 日
X2iezn 实例 (p. 1757)	采用英特尔 Xeon Platinum 处理器（Cascade Lake）的新内存优化型实例。	2022 年 1 月 26 日
ED25519 密钥	EC2 Instance Connect 和 EC2 Serial Console 现在支持 ED25519 密钥。	2022 年 1 月 20 日
新增 Local Zones	在亚特兰大、菲尼克斯和西雅图添加 Local Zones。	2022 年 1 月 11 日
竞价型实例集的基于属性的实例类型选择	指定实例必须具有的属性，Amazon EC2 将使用这些属性标识所有实例类型。	2022 年 1 月 11 日
EC2 机群的基于属性的实例类型选择	指定实例必须具有的属性，Amazon EC2 将使用这些属性标识所有实例类型。	2022 年 1 月 11 日
用于容量预留的其他 RHEL 平台	用于按需容量预留的其他 Red Hat Enterprise Linux 平台。	2022 年 1 月 11 日

Hpc6a 实例 (p. 1757)	新的计算优化型实例，采用第二代 AMD EPYC 处理器。	2022 年 1 月 10 日
实例元数据中的实例标签	您可以从实例元数据访问实例的标签。	2022 年 1 月 6 日
集群置放群组中的容量预留	您可以在集群置放群组中创建容量预留。	2022 年 1 月 6 日
Im4gn 和 Is4gen 实例 (p. 1757)	新存储优化型实例。	2021 年 11 月 30 日
Amazon EBS 快照回收站	Amazon EBS 快照回收站是一项快照还原功能，能够使您还原意外删除的快照。	2021 年 11 月 29 日
M6a 实例 (p. 1757)	由 AMD 第三代 EPYC 处理器提供支持的新通用型实例。	2021 年 11 月 29 日
G5g 实例 (p. 1757)	新加速计算实例配备基于 64 位 Arm 架构的 Amazon Graviton2 处理器。	2021 年 11 月 29 日
R6i 实例 (p. 1757)	新内存优化型实例。	2021 年 11 月 22 日
G5 实例 (p. 1757)	新加速计算实例具有多达 8 个 NVIDIA A10G GPU 和第二代 AMD EPY 处理器。	2021 年 11 月 11 日
竞价型实例集 launch-before-terminate	竞价型实例集可以在新的替换竞价型实例启动后终止接收再平衡通知的竞价型实例。	2021 年 11 月 4 日
EC2 机群 launch-before-terminate	EC2 机群可以在新的替换竞价型实例启动后终止接收再平衡通知的竞价型实例。	2021 年 11 月 4 日
比较时间戳	您可以通过将 Amazon EC2 Linux 实例的时间戳与 ClockBound 进行比较来确定事件的真实时间。	2021 年 11 月 2 日
与企业和 OU 共享 AMI	您现在可以与以下 Amazon 资源共享 AMI：企业和企业部门 (OU)。	2021 年 10 月 29 日
C6i 实例 (p. 1757)	采用英特尔至强可扩展处理器 (Ice Lake) 的新计算优化型实例。	2021 年 10 月 28 日
新增 Local Zones	在拉斯维加斯、纽约市和波特兰添加 Local Zones。	2021 年 10 月 26 日
DL1 实例 (p. 1757)	新的加速计算实例采用 Habana Gaudi 加速器和 Intel Xeon Platinum 处理器 (Cascade Lake)。	2021 年 10 月 26 日
按需容量预留机群	您可以使用容量预留机群启动容量预留的组或机群。	2021 年 10 月 5 日
Ubuntu 20.04 LTS - Focal 的休眠支持	休眠从 Ubuntu 20.04 LTS - Focal AMI 启动的新推出的实例。	2021 年 10 月 4 日

专属主机上的 T3 实例	Amazon EC2 专用主机上的 T3 实例支持。	2021 年 9 月 14 日
VT1 实例 (p. 1757)	使用 Xilinx Alveo U30 媒体加速器且专为实时视频转码工作负载设计的全新加速计算实例。	2021 年 9 月 13 日
对 RHEL、Fedora 和 CentOS 的休眠支持	使从 RHEL、Fedora 和 CentOS AMI 启动的新启动实例休眠。	2021 年 9 月 9 日
新增 Local Zones	添加芝加哥、明尼阿波利斯和堪萨斯城的 Local Zones。	2021 年 9 月 8 日
Amazon EC2 全局视图	通过 Amazon EC2 全局视图，您可以在单个控制台中查看跨多个 Amazon 区域的 VPC、子网、实例、安全组和卷。	2021 年 9 月 1 日
Amazon Data Lifecycle Manager 的 AMI 弃用支持	Amazon Data Lifecycle Manager EBS 支持的 AMI 策略可以弃用 AMI。AWSDataLifecycleManagerServiceRoleForAMIManagement Amazon 托管式策略已进行更新以支持此功能。	2021 年 8 月 23 日
C5d、M5d 和 M5d 和 M5d 的休眠支持	使 C5d、M5d 和 R5d 实例类型上运行的新启动实例休眠。	2021 年 8 月 19 日
Amazon EC2 密钥对	Amazon EC2 现在支持 Linux 和 Mac 实例上的 ED25519 密钥。	2021 年 8 月 17 日
M6i 实例 (p. 1757)	采用第三代英特尔至强可扩展处理器 (Ice Lake) 的新通用型实例。	2021 年 8 月 16 日
Amazon Data Lifecycle Manager 的 CloudWatch 指标	您可以使用 Amazon CloudWatch 监控您的 Amazon Data Lifecycle Manager 策略。	2021 年 7 月 28 日
新增本地区域	在丹佛添加本地区域。	2021 年 7 月 27 日
针对 EBS 直接 API 的 CloudTrail 数据事件	ListSnapshotBlocks、ListChangedBlocks、GetSnapshotBlock 和 PutSnapshotBlock API 都可以记录为 CloudTrail 中的数据事件。	2021 年 7 月 27 日
网络接口前缀	您可以自动或手动为网络接口分配私有 IPv4 或 IPv6 CIDR 范围。	2021 年 7 月 22 日
io2 Block Express 卷	io2 Block Express 卷现在已在支持 R5b 实例的所有区域和可用区域中正式发布。	2021 年 7 月 19 日
事件窗口	您可以为重新启动、停止或终止 Amazon EC2 实例的计划事件定义每周重复运行的自定义事件窗口。	2021 年 7 月 15 日
针对安全组规则的资源 ID 和标记支持 (p. 1757)	您可以按资源 ID 引用安全组规则。您还可以为安全组规则添加标签。	2021 年 7 月 7 日

新增 Local Zones	在达拉斯和费城添加 Local Zones。	2021 年 7 月 7 日
弃用 AMI	现在，您可以指定何时弃用 AMI。	2021 年 6 月 11 日
Windows 按秒计费 (p. 1757)	Amazon EC2 按秒对基于 Windows 和 SQL 服务器的使用收费，最低收取一分钟的费用。	2021 年 6 月 10 日
内存增强型虚拟化实例 (p. 1757)	专门针对运行大型内存数据库构建的虚拟化内存增强型实例。新类型是 u-6tb1.56xlarge、u-6tb1.112xlarge、u-9tb1.112xlarge 和 u-12tb1.112xlarge。	2021 年 5 月 11 日
根卷替换	现在，您可以使用根卷替换任务来替换正在运行的实例的根 EBS 卷。	2021 年 4 月 22 日
使用 S3 存储和还原 AMI	将 EBS 支持的 AMI 存储在 S3 中，然后从 S3 还原它们，以启用 AMI 跨分区复制。	2021 年 4 月 6 日
EC2 Serial Console	通过建立面向实例串行端口的连接来排除引导和网络连接问题。	2021 年 3 月 30 日
启动模式	Amazon EC2 现在在选定的基于 AMD 和 Intel 的 EC2 实例上支持 UEFI 启动。	2021 年 3 月 22 日
X2gd 实例 (p. 1757)	新内存优化型实例配备基于 64 位 Arm 架构的 Amazon Graviton2 处理器。	2021 年 3 月 16 日
创建反向 DNS 记录	您现在可以为弹性 IP 地址设置反向 DNS 查找。	2021 年 2 月 3 日
对 io2 卷的多重挂载支持	您现在可以为 Amazon EBS 多重挂载启用预置 IOPS SSD（io2）卷。	2020 年 12 月 18 日
C6gn 实例 (p. 1757)	新计算优化型实例配备基于 64 位 Arm 架构的 Amazon Graviton2 处理器。这些实例可以使用高达 100 Gbps 的网络带宽。	2020 年 12 月 18 日
Amazon Data Lifecycle Manager	使用 Amazon Data Lifecycle Manager 自动执行跨 Amazon 账户共享快照和复制快照的过程。	2020 年 12 月 17 日
G4ad 实例 (p. 1757)	由 AMD Radeon Pro V520 GPU 和 AMD 第 2 代 EPYC 处理器提供支持的新实例。	2020 年 12 月 9 日
在创建 AMI 时标记 AMI 和快照	创建 AMI 时，您可以使用相同的标签来标记 AMI 和快照，也可以使用不同的标签来标记它们。	2020 年 12 月 4 日

io2 Block Express 预览	您可以选择加入 io2 Block Express 卷预览。io2Block Express 卷预览提供亚毫秒级延迟，并支持比 io2 卷更高的 IOPS、更高的吞吐量和更大的容量。	2020 年 12 月 1 日
gp3 卷 (p. 1757)	一种新 Amazon EBS 通用型 SSD 卷类型。您可以在创建或修改卷时指定预置 IOPS 和吞吐量。	2020 年 12 月 1 日
D3、D3en、M5zn 和 R5b 实例 (p. 1757)	在 Nitro 系统上构建的新实例类型。	2020 年 12 月 1 日
吞吐量优化型 HDD h 和 Cold HDD 卷大小	吞吐量优化 HDD (st1) 和冷 HDD (sc1) 卷的大小范围可为 125 GiB 到 16 TiB。	2020 年 11 月 30 日
Mac1 实例	在 Apple Mac mini 计算机上构建的新实例，支持在 Amazon EC2 上运行 macOS 工作负载。	2020 年 11 月 30 日
使用 Amazon EventBridge 监控竞价型实例集事件	创建触发编程操作以响应 Spot 队列状态更改和错误的 EventBridge 规则。	2020 年 11 月 20 日
使用 Amazon EventBridge 监控 EC2 机群事件	创建触发编程操作以响应 EC2 队列 状态更改和错误的 EventBridge 规则。	2020 年 11 月 20 日
删除 instant 机群	在单个 API 调用中删除类型 instant 的 EC2 队列 并终止队列中的所有实例。	2020 年 11 月 18 日
对 T3 和 T3a 的休眠支持	使 T3 和 T3a 实例类型上运行的新启动实例休眠。	2020 年 11 月 17 日
Amazon EFS 快速创建	您可以使用 Amazon EFS 快速创建在启动时创建 Amazon Elastic File System (Amazon EFS) 文件系统并将其挂载到实例。	2020 年 11 月 9 日
Amazon Data Lifecycle Manager	您可以使用 Amazon Data Lifecycle Manager 来自动创建、保留和删除 EBS 支持的 AMI。	2020 年 11 月 9 日
Wavelength 区域中的容量预留	现在可以在Wavelength 区中创建和使用 容量预留。	2020 年 11 月 4 日
P4d 实例 (p. 1757)	为机器学习和 HPC 工作负载提供高性能平台的新加速计算实例。	2020 年 11 月 2 日
对 I3、M5ad 和 R5ad 的休眠支持	使 I3、M5ad 和 R5ad 实例类型上运行的新启动实例休眠。	2020 年 10 月 21 日
竞价型实例 vCPU 限制	竞价型实例限制现在根据您为完成未处理的请求而正在使用或将使用的运行中竞价型实例所用的 vCPU 数量进行管理。	2020 年 10 月 1 日

Local Zones 中的容量预留	现在可以在 Local Zones 中创建和使用容量预留。	2020 年 9 月 30 日
Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager 策略最多可配置四个计划。	2020 年 9 月 17 日
T4g 实例 (p. 1757)	Amazon Graviton2 处理器支持的新一般用途实例，它们基于 64 位 Arm Neoverse 内核和由 Amazon 设计的定制硅片以优化性能和降低成本。	2020 年 9 月 14 日
对 M5a 和 R5a 的休眠支持	使 M5a 和 R5a 实例类型上运行的新启动实例休眠。	2020 年 8 月 28 日
适用于 Amazon EBS 的预置 IOPS SSD（io2）卷	预置 IOPS SSD（io2）卷旨在提供 99.999% 的容量耐用性且 AFR 不高于 0.001%。	2020 年 8 月 24 日
实例元数据提供实例位置和放置信息	placement 类别下的新实例元数据字段：区域、放置组名称、分区号、主机 ID 和可用区 ID。	2020 年 8 月 24 日
C5ad 实例 (p. 1757)	新的计算优化型实例，采用第二代 AMD EPYC 处理器。	2020 年 8 月 13 日
Wavelength 区域	Wavelength 区域是在其中部署 Wavelength 基础设施的运营商位置中的隔离区域。	2020 年 8 月 6 日
容量预留组	您可以使用 Amazon Resource Groups 创建容量预留的逻辑集合，然后将实例启动定位到这些组中。	2020 年 7 月 29 日
C6gd、M6gd 和 R6gd 实例 (p. 1757)	Amazon Graviton2 处理器支持的新一般用途实例，它们基于 64 位 Arm Neoverse 内核和由 Amazon 设计的定制硅片以优化性能和降低成本。	2020 年 7 月 27 日
快速快照还原	您可以为与您共享的快照启用快速快照还原。	2020 年 7 月 21 日
C6g 和 R6g 实例 (p. 1757)	Amazon Graviton2 处理器支持的新一般用途实例，它们基于 64 位 Arm Neoverse 内核和由 Amazon 设计的定制硅片以优化性能和降低成本。	2020 年 6 月 10 日
G4dn 的裸机实例 (p. 1757)	为应用程序提供对主机服务器物理资源的直接访问的新实例。	2020 年 6 月 5 日
C5a 实例 (p. 1757)	新的计算优化型实例，采用第二代 AMD EPYC 处理器。	2020 年 6 月 4 日
自带 IPv6 地址	您可以将部分或全部 IPv6 地址范围从本地网络引入到您的 Amazon 账户中。	2020 年 5 月 21 日

M6g 实例 (p. 1757)	Amazon Graviton2 处理器支持的新一般用途实例，它们基于 64 位 Arm Neoverse 内核和由 Amazon 设计的定制硅片以优化性能和降低成本。	2020 年 5 月 11 日
使用 Systems Manager 参数启动实例	您可以在启动实例时指定 Amazon Systems Manager 参数而不是 AMI。	2020 年 5 月 5 日
Amazon Linux 2 内核实时修补	适用于 Amazon Linux 2 的内核实时修补使您能够将安全漏洞和严重错误修补程序应用于正在运行的 Linux 内核，而无需重启或中断正在运行的应用程序。	2020 年 4 月 28 日
停止和启动竞价型实例	停止由 Amazon EBS 支持的竞价型实例并根据需要随时启动它，而不是依赖于停止中断行为。	2020 年 1 月 13 日
为资源添加标签 (p. 1757)	您可以标记仅出口互联网网关、本地网关、本地网关路由表、本地网关虚拟接口、本地网关虚拟接口组、本地网关路由表 VPC 关联以及本地网关路由表虚拟接口组关联。	2020 年 1 月 10 日
使用会话管理器连接到您的实例	您可以从 Amazon EC2 控制台使用实例来启动会话管理器会话。	2019 年 12 月 18 日
Inf1 实例 (p. 1757)	采用 Amazon Inferentia 的新实例，后者是一个机器学习推理芯片，旨在以低成本提供高性能。	2019 年 12 月 3 日
账户级别的默认积分规范	您可以在每个 Amazon 区域的账户级别设置每个可突增性能实例系列的默认积分规范。	2019 年 11 月 25 日
实例类型查找	您可以找到满足您需求的实例类型。	2019 年 11 月 22 日
专属主机 (p. 1757)	现在，您可以配置专用主机以支持实例系列中的多种实例类型。	2019 年 11 月 21 日
Amazon EBS 快速快照还原	您可以在 EBS 快照上启用快速快照还原，以确保从快照创建的 EBS 卷在创建时已完全初始化，并立即交付所有预配置性能。	2019 年 11 月 20 日
实例元数据服务版本 2	您可以使用 实例元数据服务版本 2，这是一种面向会话的方法，用于请求实例元数据。	2019 年 11 月 19 日
排队购买预留实例	您最早可以提前三年排队购买 Reserved Instance。	2019 年 10 月 4 日
G4dn 实例 (p. 1757)	具有 NVIDIA Tesla GPU 的新实例。	2019 年 9 月 19 日

诊断中断	您可以将诊断中断发送到无法访问或无响应的实例以触发内核错误。	2019 年 8 月 14 日
容量优化的分配策略	使用 EC2 实例集或竞价型实例集，您可以通过为正在启动的实例数量提供最佳容量来从 Spot 池启动竞价型实例。	2019 年 8 月 12 日
Elastic Fabric Adapter (p. 1757)	EFA 现在支持 Open MPI 3.1.4 和 Intel MPI 2019 Update 4。	2019 年 7 月 26 日
为资源添加标签 (p. 1757)	在创建时启动模板。	2019 年 7 月 24 日
EC2 Instance Connect	EC2 Instance Connect 提供了一种简单且安全的方法以使用安全 Shell (SSH) 连接到实例。	2019 年 6 月 27 日
主机恢复	如果在专用主机上发生意外硬件故障，则在新主机上自动重新启动实例。	2019 年 6 月 5 日
Amazon EBS 多卷快照	您可以跨附加到 EC2 实例的多个 EBS 卷拍摄准确时间点、数据协调和崩溃一致性快照。	2019 年 5 月 29 日
为资源添加标签 (p. 1757)	您可以标记专用主机预留。	2019 年 5 月 27 日
Amazon EBS 默认加密	在区域中启用默认加密后，将使用用于 EBS 加密的默认 KMS 密钥加密在区域中创建的所有新 EBS 卷。	2019 年 5 月 23 日
为资源添加标签 (p. 1757)	您可以标记 VPC 终端节点、终端节点服务和终端节点服务配置。	2019 年 5 月 13 日
Microsoft SQL Server 数据库从 Windows 到 Linux 的平台转换助手	将现有 Microsoft SQL Server 工作负载从 Windows 移动到 Linux 操作系统。	2019 年 5 月 8 日
I3en 实例 (p. 1757)	新的 I3en 实例可以使用高达 100 Gbps 的网络带宽。	2019 年 5 月 8 日
T3a 实例 (p. 1757)	采用 AMD EPYC 处理器的新实例。	2019 年 4 月 24 日
M5ad 和 R5ad 实例 (p. 1757)	采用 AMD EPYC 处理器的新实例。	2019 年 3 月 27 日
为资源添加标签 (p. 1757)	您可以为 专用主机 预留分配自定义标签以便按不同的方式将它们分类。	2019 年 3 月 14 日
M5、M5d、R5、R5d 和 z1d 裸机实例 (p. 1757)	为应用程序提供对主机服务器物理资源的直接访问的新实例。	2019 年 2 月 13 日

之前年份的历史

下表描述 Amazon EC2 文档集的重要补充部分（2018 年以及之前年份）。

功能	API 版本	描述	发行日期
分区置放群组	2016-11-15	分区置放群组跨逻辑分区来分配实例，以确保一个分区中的实例不会与其他分区中的实例共享基础硬件。有关更多信息，请参阅分区置放群组 (p. 1178)。	2018 年 12 月 20 日
p3dn.24xlarge 实例	2016-11-15	新的 p3dn.24xlarge 实例提供 100 Gbps 的网络带宽。	2018 年 12 月 7 日
休眠 EC2 Linux 实例	2016-11-15	如果 Linux 实例已启用休眠并且满足休眠先决条件，则可以休眠该实例。有关更多信息，请参阅休眠 Linux 按需型实例 (p. 616)。	2018 年 11 月 28 日
Amazon Elastic Inference 加速器	2016-11-15	您可以将 Amazon EI 加速器附加到实例上以添加 GPU 支持的加速，从而减少运行深度学习推理的成本。有关更多信息，请参阅Amazon Elastic Inference (p. 808)。	2018 年 11 月 28 日
实例具有 100 Gbps 网络带宽	2016-11-15	新 C5n 实例可以使用高达 100 Gbps 的网络带宽。	2018 年 11 月 26 日
实例配有基于 Arm 的处理器	2016-11-15	新 A1 实例可以显著节省成本，非常适合横向扩展和基于 Arm 的工作负载。	2018 年 11 月 26 日
Spot 控制台推荐实例队列	2016-11-15	Spot 控制台根据 Spot 最佳实践（实例多元化）推荐实例队列，以满足您应用程序所需的最低硬件规格（vCPU、内存和存储）。有关更多信息，请参阅创建 Spot 队列请求 (p. 900)。	2018 年 11 月 20 日
新 EC2 队列请求类型：`instant`	2016-11-15	EC2 队列现在支持新请求类型 `instant`，您可用它来跨实例类型和购买模式同步预配置容量。`instant` 请求在 API 响应中返回启动的实例，不采取更多操作，使您能够控制是否启动实例以及何时启动。有关更多信息，请参阅EC2 队列请求类型 (p. 815)。	2018 年 11 月 14 日
采用 AMD EYPC 处理器的实例	2016-11-15	新的通用型 (M5a) 和内存优化型实例 (R5a) 为微服务、小到中型数据库、虚拟桌面、开发和测试环境、业务应用程序等提供了更低的价格选项。	2018 年 11 月 6 日
Spot 节省信息	2016-11-15	您可以查看使用单个竞价型实例集或所有竞价型实例的竞价型实例所节省的成本。有关更多信息，请参阅通过购买竞价型实例实现节省 (p. 455)。	2018 年 11 月 5 日
用于优化 CPU 选项的控制台支持	2016-11-15	启动实例时，您可以使用 Amazon EC2 控制台优化 CPU 选项以适应特定的工作负载或业务需求。有关更多信息，请参阅优化 CPU 选项 (p. 721)。	2018 年 10 月 31 日
控制台支持从实例创建启动模板	2016-11-15	您可以通过 Amazon EC2 控制台，以实例为基础创建新的启动模板。有关更多信息，请参阅创建启动模板 (p. 590)。	2018 年 10 月 30 日
On-Demand Capacity Reservations	2016-11-15	您可在特定可用区中为 Amazon EC2 实例预留容量任意持续时间。这使您能够独立于预留实例 (RI) 提供的账单折扣来创建和管理容量预留。有关更多信息，请参阅On-Demand Capacity Reservations (p. 538)。	2018 年 10 月 25 日

功能	API 版本	描述	发行日期
自带 IP 地址 (BYOIP)	2016-11-15	您可将自己的全部或部分公有 IPv4 地址从本地网络引入到 Amazon 账户中。在将地址范围引入 Amazon 中之后，它会在您的账户中显示为地址池。您可从地址池创建弹性 IP 地址，并将其用于您的 Amazon 资源。有关更多信息，请参阅在 Amazon EC2 中使用您自己的 IP 地址 (BYOIP) (p. 1070)。	2018 年 10 月 23 日
在创建时标记专用主机和控制台支持	2016-11-15	您可在创建时标记专用主机，并可以使用 Amazon EC2 控制台管理专用主机标签。有关更多信息，请参阅分配 专用主机 (p. 509)。	2018 年 10 月 22 日
g3s.xlarge 实例	2016-11-15	引入 g3s.xlarge 实例，扩展了计算加速型 G3 实例系列的范围。	2018 年 10 月 11 日
内存增强型实例	2016-11-15	这些实例专门针对运行大型内存中数据库构建。它们通过直接访问主机硬件提供裸机性能。有关更多信息，请参阅内存优化型实例 (p. 322)。	2018 年 9 月 27 日
f1.4xlarge 实例	2016-11-15	f1.4xlarge 实例的引入扩展了计算加速型 F1 实例系列的范围。	2018 年 9 月 25 日
针对 Spot 队列计划扩展的控制台支持。	2016-11-15	根据日期和时间增加或减少队列的当前容量。有关更多信息，请参阅使用计划扩展功能扩展 Spot 队列 (p. 918)。	2018 年 9 月 20 日
T3 实例	2016-11-15	T3 实例是可突增通用实例类型，它提供基准级别的 CPU 性能，并能够根据需要随时突增 CPU 使用率。有关更多信息，请参阅可突增性能实例 (p. 274)。	2018 年 8 月 21 日
EC2 队列的分配策略	2016-11-15	您可以指定是按价格（最低价格优先）还是优先级（最高优先级优先）来满足按需容量。您可以指定在其中分配您的目标 Spot 容量的 Spot 池数量。有关更多信息，请参阅竞价型实例的分配策略 (p. 833)。	2018 年 7 月 26 日
Spot 队列的分配策略	2016-11-15	您可以指定是按价格（最低价格优先）还是优先级（最高优先级优先）来满足按需容量。您可以指定在其中分配您的目标 Spot 容量的 Spot 池数量。有关更多信息，请参阅竞价型实例的分配策略 (p. 872)。	2018 年 7 月 26 日
R5 和 R5d 实例	2016-11-15	R5 和 R5d 实例非常适合高性能数据库、分布式内存中缓存和内存中分析。R5d 实例带有 NVMe 实例存储卷。有关更多信息，请参阅内存优化型实例 (p. 322)。	2018 年 7 月 25 日
z1d 实例	2016-11-15	这些实例为需要高每核心性能和大量内存的应用设计，例如 Electronic Design Automation (EDA) 和关系数据库。这些实例带有 NVME 实例存储卷。有关更多信息，请参阅内存优化型实例 (p. 322)。	2018 年 7 月 25 日
自动化快照生命周期	2016-11-15	您可以使用 Amazon Data Lifecycle Manager 来自动创建和删除 EBS 卷的快照。有关更多信息，请参阅Amazon Data Lifecycle Manager (p. 1448)。	2018 年 7 月 12 日

功能	API 版本	描述	发行日期
启动模板 CPU 选项	2016-11-15	在使用命令行工具创建启动模板时，您可以优化 CPU 选项以适合特定工作负载或业务需求。有关更多信息，请参阅创建启动模板 (p. 590)。	2018 年 7 月 11 日
标记专用主机	2016-11-15	您可以标记专用主机。有关更多信息，请参阅标记专用主机 (p. 518)。	2018 年 7 月 5 日
`i3.metal` 实例	2016-11-15	`i3.metal` 实例为应用程序提供对主机服务器的物理资源 (如处理器和内存) 的直接访问。有关更多信息，请参阅存储优化型实例 (p. 347)。	2018 年 5 月 17 日
获取最新的控制台输出	2016-11-15	使用 get-console-output Amazon CLI 命令时，您可以检索某些实例类型的最新控制台输出。	2018 年 5 月 9 日
优化 CPU 选项	2016-11-15	启动实例时，您可以优化 CPU 选项以适应特定的工作负载或业务需求。有关更多信息，请参阅优化 CPU 选项 (p. 721)。	2018 年 5 月 8 日
EC2 Fleet	2016-11-15	您可以使用 EC2 实例集在不同的 EC2 实例类型和可用区以及按需型实例、预留实例和竞价型实例采购模型之间启动一组实例。有关更多信息，请参阅EC2 Fleet (p. 814)。	2018 年 5 月 2 日
竞价型实例集 中的按需型实例	2016-11-15	您可以在 Spot 队列请求中包含按需容量请求，以确保始终拥有实例容量。有关更多信息，请参阅Spot 队列 (p. 871)。	2018 年 5 月 2 日
创建时标记 EBS 快照	2016-11-15	在创建过程中，您可以将标签应用于快照。有关更多信息，请参阅创建 Amazon EBS 快照 (p. 1372)。	2018 年 4 月 2 日
更改置放群组	2016-11-15	您可以将实例移入或移出置放群组，也可以更改实例的置放群组。有关更多信息，请参阅更改实例的置放群组 (p. 1186)。	2018 年 3 月 1 日
较长的资源 ID	2016-11-15	您可以为更多资源类型启用较长 ID 格式。有关更多信息，请参阅资源 ID (p. 1656)。	2018 年 2 月 9 日
网络性能改进	2016-11-15	在其他实例或 Amazon S3 之间发送或接收网络通信时，集群置放群组之外的实例现在可以受益于增加的带宽。	2018 年 1 月 24 日
标记弹性 IP 地址	2016-11-15	您可以标记您的弹性 IP 地址。有关更多信息，请参阅为弹性 IP 地址添加标签 (p. 1096)。	2017 年 12 月 21 日
Amazon Linux 2	2016-11-15	Amazon Linux 2 是 Amazon Linux 的新版本。它可为您的应用程序提供稳定、安全且高性能的基础。有关更多信息，请参阅Amazon Linux (p. 208)。	2017 年 12 月 13 日
Amazon Time Sync Service	2016-11-15	您可以使用 Amazon Time Sync Service 在您的实例上保持准确的时间。有关更多信息，请参阅为 Linux 实例设置时间 (p. 714)。	2017 年 11 月 29 日
T2 无限	2016-11-15	T2 无限实例可以突增到基准以上所需的时间。有关更多信息，请参阅可突增性能实例 (p. 274)。	2017 年 11 月 29 日

功能	API 版本	描述	发行日期
启动模板	2016-11-15	启动模板可以包含用于启动实例的全部或部分参数，而无需在每次启动实例时都指定这些参数。有关更多信息，请参阅通过启动模板启动实例 (p. 588)。	2017 年 11 月 29 日
分布置放	2016-11-15	建议在具有少量应单独放置的重要实例的应用程序中使用分布置放群组。有关更多信息，请参阅分布置放群组 (p. 1178)。	2017 年 11 月 29 日
H1 实例	2016-11-15	H1 实例设计用于高性能大数据工作负载。有关更多信息，请参阅存储优化型实例 (p. 347)。	2017 年 11 月 28 日
M5 实例	2016-11-15	M5 实例是通用计算实例。这些实例兼顾了计算、内存、存储和网络资源。	2017 年 11 月 28 日
竞价型实例休眠	2016-11-15	在发生中断时，Spot 服务可以将竞价型实例休眠。有关更多信息，请参阅休眠中断的竞价型实例 (p. 486)。	2017 年 11 月 28 日
Spot 队列目标跟踪	2016-11-15	您可以为 Spot 队列设置目标跟踪扩展策略。有关更多信息，请参阅使用目标跟踪策略扩展 Spot 队列 (p. 916)。	2017 年 11 月 17 日
Spot 队列与 Elastic Load Balancing 集成	2016-11-15	您可以将一个或多个负载均衡器附加到 Spot 队列。	2017 年 11 月 10 日
X1e 实例	2016-11-15	X1e 实例非常适合高性能数据库、内存中数据库和其他内存密集型企业应用程序。有关更多信息，请参阅内存优化型实例 (p. 322)。	2017 年 11 月 28 日
C5 实例	2016-11-15	C5 实例专为计算密集型应用程序设计。有关更多信息，请参阅计算优化型实例 (p. 305)。	2017 年 11 月 6 日
合并和拆分可转换预留实例	2016-11-15	您可以合并两个或更多可转换预留实例，也可以将其与新可转换预留实例交换。您还可以使用修改过程将 可转换预留实例 拆分为较小的预留。有关更多信息，请参阅交换 可转换预留实例 (p. 441)。	2017 年 11 月 6 日
P3 实例	2016-11-15	P3 实例是计算优化型 GPU 实例。有关更多信息，请参阅Linux 加速计算实例 (p. 358)。	2017 年 10 月 25 日
修改 VPC 租赁	2016-11-15	可以将 VPC 的实例租赁属性从 `dedicated` 改为 `default`。有关更多信息，请参阅更改 VPC 的租期 (p. 538)。	2017 年 10 月 16 日
按秒计费	2016-11-15	Amazon EC2 按秒对基于 Linux 的使用收费，最低收取一分钟的费用。	2017 年 10 月 2 日
在中断时停止	2016-11-15	您可以指定在竞价型实例中断时 Amazon EC2 应将其停止还是终止。有关更多信息，请参阅中断行为 (p. 485)。	2017 年 9 月 18 日
给 NAT 网关加标签	2016-11-15	您可以给自己的 NAT 网关加标签。有关更多信息，请参阅标记 资源 (p. 1665)。	2017 年 9 月 7 日
安全组规则说明	2016-11-15	您可以向安全组规则添加说明。有关更多信息，请参阅安全组规则 (p. 1304)。	2017 年 8 月 31 日

功能	API 版本	描述	发行日期
恢复弹性 IP 地址	2016-11-15	如果您释放了一个在 VPC 中使用的弹性 IP 地址，则可能能够恢复它。有关更多信息，请参阅恢复弹性 IP 地址 (p. 1102)。	2017 年 8 月 11 日
标记 Spot 队列实例	2016-11-15	您可以将您的 Spot 队列配置为自动标记其启动的实例。	2017 年 7 月 24 日
G3 实例	2016-11-15	G3 实例为使用 DirectX 或 OpenGL 的图形应用程序提供经济高效的高性能平台。G3 实例还提供 NVIDIA GRID 虚拟工作站功能，支持 4 台分辨率高达 4096x2160 的监视器。有关更多信息，请参阅Linux 加速计算实例 (p. 358)。	2017 年 7 月 13 日
F1 实例	2016-11-15	F1 实例是加速计算实例。有关更多信息，请参阅Linux 加速计算实例 (p. 358)。	2017 年 4 月 19 日
在创建过程中，为资源添加标签	2016-11-15	在创建过程中，您可以将标签应用于实例和卷。有关更多信息，请参阅标记 资源 (p. 1665)。此外，您可以使用基于标签的资源级权限来控制应用的标签。有关更多信息，请参阅 在创建过程中授予标记资源的权限 (p. 1231)。	2017 年 3 月 28 日
I3 实例	2016-11-15	I3 实例是存储优化型实例。有关更多信息，请参阅存储优化型实例 (p. 347)。	2017 年 2 月 23 日
在附加的 EBS 卷上进行修改	2016-11-15	对于附加到大多数 EC2 实例的大多数 EBS 卷，您可以在不分离卷或不停止实例的情况下修改卷大小、类型和 IOPS。有关更多信息，请参阅Amazon EBS 弹性卷 (p. 1493)。	2017 年 2 月 13 日
附加 IAM 角色	2016-11-15	您可以为现有实例附加、分离或替换 IAM 角色。有关更多信息，请参阅适用于 Amazon EC2 的 IAM 角色 (p. 1277)。	2017 年 2 月 9 日
专用竞价型实例	2016-11-15	您可在 Virtual Private Cloud (VPC) 中的单租户硬件上运行竞价型实例。有关更多信息，请参阅指定竞价型实例的租期 (p. 458)。	2017 年 1 月 19 日
IPv6 支持	2016-11-15	您可以将一个 IPv6 CIDR 与 VPC 和子网关联，并为 VPC 中的实例分配 IPv6 地址。有关更多信息，请参阅Amazon EC2 实例 IP 寻址 (p. 1053)。	2016 年 12 月 1 日
R4 实例	2016-09-15	R4 实例是内存优化型实例。R4 实例非常适合内存密集型、延迟敏感型工作负载，例如商业智能 (BI)、数据挖掘和分析、内存中数据库、分布式 Web 级内存缓存，以及非结构化大数据的应用程序性能实时处理。有关更多信息，请参阅 内存优化型实例 (p. 322)	2016 年 11 月 30 日
新的 `t2.xlarge` 和 `t2.2xlarge` 实例类型	2016-09-15	T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅可突增性能实例 (p. 274)。	2016 年 11 月 30 日

功能	API 版本	描述	发行日期
P2 实例	2016-09-15	P2 实例使用 NVIDIA Tesla GPU K80 和适用于使用 CUDA 和 OpenCL 编程模型的通用 GPU 计算设计。有关更多信息，请参阅Linux 加速计算实例 (p. 358)。	2016 年 29 月 9 日
`m4.16xlarge` 实例	2016-04-01	引入具有 64 个 vCPU 和 256GiB RAM 的 `m4.16xlarge` 实例，扩展了通用 M4 系列的范围。	2016 年 6 月 9 日
Spot 队列的自动扩展		现在，您可以为 Spot 队列设置扩展策略。有关更多信息，请参阅Spot 队列的自动扩展 (p. 914)。	2016 年 9 月 1 日
Elastic Network Adapter (ENA)	2016-04-01	您现在可以将 ENA 用于增强网络。有关更多信息，请参阅增强联网支持 (p. 1143)。	2016 年 6 月 28 日
增强了对查看和修改较长 ID 的支持	2016-04-01	您现在可以查看和修改其他 IAM 用户、IAM 角色或根用户的较长 ID 设置。有关更多信息，请参阅资源 ID (p. 1656)。	2016 年 6 月 23 日
在 Amazon 账户之间复制加密的 Amazon EBS 快照	2016-04-01	您现在可以在 Amazon 账户之间复制加密的 EBS 快照。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。	2016 年 6 月 21 日
捕获实例控制台的屏幕截图	2015-10-01	您现在可以在调试无法访问的实例时获取其他信息。有关更多信息，请参阅捕获无法访问的实例的屏幕截图 (p. 1724)。	2016 年 24 月 5 日
X1 实例	2015-10-01	专为正在运行的内存中数据库、大数据处理引擎和高性能计算 (HPC) 应用程序设计的内存优化的实例。有关更多信息，请参阅内存优化型实例 (p. 322)。	2016 年 18 月 5 日
两种新的 EBS 卷类型	2015-10-01	您现在可以创建经过吞吐量优化的 HDD (st1) 以及冷数据 HDD (sc1) 卷。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。	2016 年 4 月 19 日
添加了针对 Amazon EC2 的新的 NetworkPacketsIn 和 NetworkPacketsOut 指标		添加了针对 Amazon EC2 的新的 NetworkPacketsIn 和 NetworkPacketsOut 指标。有关更多信息，请参阅实例指标 (p. 1003)。	2016 年 3 月 23 日
Spot 队列的 CloudWatch 指标		您现在可以获取 Spot 队列的 CloudWatch 指标。有关更多信息，请参阅Spot 队列的 CloudWatch 指标 (p. 912)。	2016 年 3 月 21 日
计划实例	2015-10-01	利用计划的预留实例 (计划实例)，您可以购买具有指定的开始时间和持续时间，并且每日、每周或每月重复一次的容量预留。有关更多信息，请参阅Scheduled Reserved Instances (p. 447)。	2016 年 1 月 13 日
较长的资源 ID	2015-10-01	我们将逐步引入某些 Amazon EC2 和 Amazon EBS 资源类型的更长 ID。在选择周期内，您可以为支持的资源类型启用较长 ID 格式。有关更多信息，请参阅资源 ID (p. 1656)。	2016 年 1 月 13 日

功能	API 版本	描述	发行日期
ClassicLink DNS 支持	2015-10-01	您可以对您的 VPC 启用 ClassicLink DNS 支持，以使定位在链接的 EC2-Classic 实例与 VPC 中的实例之间的 DNS 主机名解析为私有 IP 地址而不是公有 IP 地址。有关更多信息，请参阅启用 ClassicLink DNS 支持 (p. 1206)。	2016 年 1 月 11 日
新 t2.nano 实例类型	2015-10-01	T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅可突增性能实例 (p. 274)。	2015 年 12 月 15 日
专用主机	2015-10-01	Amazon EC2 专用主机是指实例容量供您专用的物理服务器。有关更多信息，请参阅Dedicated Hosts (p. 504)。	2015 年 11 月 23 日
竞价型实例持续时间	2015-10-01	现在，您可以为竞价型实例指定持续时间。不支持竞价型限制（2023 年 1 月）。	2015 年 10 月 6 日
Spot 队列修改请求	2015-10-01	您现在可以修改 Spot 队列请求的目标容量。有关更多信息，请参阅修改 Spot 队列请求 (p. 910)。	2015 年 9 月 29 日
Spot 队列多样化分配策略	2015-04-15	您现在可以使用单个竞价型实例集请求在多个 Spot 池中分配竞价型实例。有关更多信息，请参阅竞价型实例的分配策略 (p. 872)。	2015 年 9 月 15 日
Spot 队列实例权重	2015-04-15	您现在可以定义每个实例类型在应用程序性能中所占的容量单位，并相应地为每个 Spot 池的竞价型实例调整愿意支付的金额。有关更多信息，请参阅Spot 队列实例权重 (p. 891)。	2015 年 8 月 31 日
新的重启警报操作和用于警报操作的新 IAM 角色		增加了重启警报操作和与警报操作一起使用的新 IAM 角色。有关更多信息，请参阅创建停止、终止、重启或恢复实例的警报 (p. 1021)。	2015 年 7 月 23 日
新 t2.large 实例类型		T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅可突增性能实例 (p. 274)。	2015 年 6 月 16 日
M4 实例		实现了计算、内存和网络资源平衡的通用型实例。M4 实例由带 AVX2 的自定义 Intel 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器支持。	2015 年 6 月 11 日
Spot Fleets	2015-04-15	您可以管理竞价型实例的集合或队列，而不必管理单独的竞价型实例请求。有关更多信息，请参阅Spot 队列 (p. 871)。	2015 年 5 月 18 日
将弹性 IP 地址迁移至 EC2-Classic	2015-04-15	您无法将已分配为在 EC2-Classic 中使用的弹性 IP 地址迁移到在 VPC 中使用。有关更多信息，请参阅the section called “弹性 IP 地址” (p. 1213)。	2015 年 5 月 15 日
将具有多个磁盘的虚拟机作为 AMI 导入	2015-03-01	VM Import 过程现在支持将具有多个磁盘的虚拟机作为 AMI 导入。有关更多信息，请参阅 VM Import/Export 用户指南 中的使用 VM Import/Export 将虚拟机作为映像导入。	2015 年 4 月 23 日

功能	API 版本	描述	发行日期
新 g2.8xlarge 实例类型		新 g2.8xlarge 实例受四种高性能 NVIDIA GPU 支持，非常适合 GPU 计算工作负载，包括大规模呈现、转码、机器学习以及其他需要大规模并行处理能力的服务器端工作负载。	2015 年 4 月 7 日
D2 实例		密集存储实例，经过优化，适用于需要顺序访问直接附加的实例存储上大量数据的应用程序。D2 实例适合在密集存储系列中提供最佳性价比。由 2.4 GHz Intel® Xeon® E5 2676v3 (Haswell) 处理器提供支持，通过提供额外的计算能力、更多内存和增强联网功能，HS1 上的 D2 实例得到了极大改进。此外，D2 实例有四种实例大小可供选择，存储容量分别是 6TB、12TB、24TB 和 48TB。 有关更多信息，请参阅存储优化型实例 (p. 347)。	2015 年 3 月 24 日
EC2 实例的自动恢复		您可以创建 Amazon CloudWatch 警报用于监控 Amazon EC2 实例，并且在实例受损（由于发生底层硬件故障或需要 Amazon 参与才能修复的问题）时自动恢复实例。恢复的实例与原始实例相同，包括实例 ID、IP 地址以及所有实例元数据。 有关更多信息，请参阅恢复实例 (p. 640)。	2015 年 1 月 12 日
C4 实例		下一代计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C4 实例基于自定义 2.9 GHz Intel® Xeon® E5-2666 v3 (Haswell) 处理器。C4 实例采用睿频加速技术，单核或双核经睿频加速后，处理器时钟频率可高达 3.5Ghz。C4 实例扩展自 C3 计算优化型实例的功能，可为客户在 EC2 实例中提供最高的处理器性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体动力学。 有关更多信息，请参阅计算优化型实例 (p. 305)。	2015 年 1 月 11 日
ClassicLink	2014-10-01	您可使用 ClassicLink 将 EC2-Classic 实例链接到您账户中的 VPC。您可以将 VPC 安全组与 EC2-Classic 实例关联起来，从而允许 EC2-Classic 实例与 VPC 中使用私有 IP 地址的实例进行通信。有关更多信息，请参阅ClassicLink (p. 1201)。	2015 年 1 月 7 日
竞价型实例终止通知		防范竞价型实例中断的最佳方法是为应用程序设计容错能力。此外，您还可以利用竞价型实例中断通知，该通知可在 Amazon EC2 必须停止或终止您的竞价型实例时，提前两分钟发出警告。 有关更多信息，请参阅竞价型实例中断通知 (p. 490)。	2015 年 1 月 5 日
DescribeVolumes 分页支持	2014-09-01	DescribeVolumes API 调用现在可使用 MaxResults 和 NextToken 参数支持结果分页。有关更多信息，请参阅 Amazon EC2 API Reference 中的 DescribeVolumes。	2014 年 10 月 23 日

功能	API 版本	描述	发行日期
T2 实例	2014-06-15	T2 实例旨在提供适度的基本性能，并能够根据您工作负载的需要进行突增以显著提高性能。其专用于需要快速响应、拥有短时间高性能和低成本要求的应用程序。有关更多信息，请参阅可突增性能实例 (p. 274)。	2014 年 6 月 30 日
新 EC2 Service Limits (EC2 服务限制) 页面		使用 Amazon EC2 控制台中的 EC2 Service Limits (EC2 服务限制) 页面可按区域查看 Amazon EC2 和 Amazon VPC 提供的资源的当前限制。	2014 年 6 月 19 日
Amazon EBS 通用型 SSD 卷	2014-05-01	通用型 SSD 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷可提供不超过 10 毫秒的延迟，能突增至 3000 IOPS 很长时间，基准性能为 3 IOPS/GiB。通用型 SSD 卷的大小范围为 1 GiB 到 1 TiB。有关更多信息，请参阅通用型 SSD (gp2) 卷 (p. 1330)。	2014 年 6 月 16 日
Amazon EBS encryption	2014-05-01	Amazon EBS 加密 提供 EBS 数据卷和快照的无缝加密，无需构建和维护安全密钥管理基础设施。通过使用 Amazon 托管式密钥 加密数据，EBS 加密可保护静态数据的安全。加密还发生在托管 EC2 实例的服务器上，当数据在 EC2 实例和 EBS 存储之间移动时提供数据加密。有关更多信息，请参阅Amazon EBS 加密 (p. 1504)。	2014 年 5 月 21 日
R3 实例	2014-02-01	内存优化型实例具有最佳的每 GiB RAM 价格点和高性能。这些实例十分适合于关系数据库和 NoSQL 数据库、内存分析解决方案、科学计算以及其他可受益于 R3 实例的 vCPU 高内存、高计算性能和增强的联网功能的内存密集型应用程序。 有关更多信息，请参阅 Amazon EC2 实例类型。	2014 年 4 月 9 日
新 Amazon Linux AMI 版本		Amazon Linux AMI 2014.03 发布。	2014 年 3 月 27 日
额外 M3 实例	2013-10-15	现在支持 M3 实例大小 `m3.medium` 和 `m3.large`。有关更多信息，请参阅 Amazon EC2 实例类型。	2014 年 1 月 20 日
I2 实例	2013-10-15	这些实例提供极高的 IOPS，并在 Linux 实例上支持 TRIM，可实现更好的 SSD 连续写入性能。I2 实例还支持增强联网，从而减小实例间延迟、降低网络抖动，显著提高每秒数据包 (PPS) 性能。有关更多信息，请参阅存储优化型实例 (p. 347)。	2013 年 12 月 19 日
更新了 M3 实例	2013-10-15	M3 实例大小、`m3.xlarge` 和 `m3.2xlarge` 现在支持具有 SSD 卷的实例存储。	2013 年 12 月 19 日
导入 Linux 虚拟机	2013-10-15	VM Import 过程现在支持 Linux 实例的导入。有关更多信息，请参阅 VM Import/Export 用户指南。	2013 年 12 月 16 日
RunInstances 的资源级权限	2013-10-15	您现在可以在 Amazon Identity and Access Management 中创建策略以控制 Amazon EC2 RunInstances API 操作的资源级权限。有关更多信息以及示例策略，请参阅适用于 Amazon EC2 的 Identity and Access Management (p. 1223)。	2013 年 11 月 20 日

功能	API 版本	描述	发行日期
C3 实例	2013-10-15	计算优化型实例，可按经济的价格提供非常高的 CPU 性能。C3 实例还支持增强联网，这种联网可减小实例间延迟、降低网络抖动并显著提高每秒数据包 (PPS) 性能。这些实例十分适用于高流量 Web 应用程序、广告服务、批处理、视频编码、分布式分析、高能物理学、基因组分析和计算流体动力学。 有关更多信息，请参阅 Amazon EC2 实例类型。	2013 年 11 月 14 日
从 Amazon Web Services Marketplace 启动实例		您现在可以使用 Amazon EC2 启动向导从 Amazon Web Services Marketplace 启动实例。有关更多信息，请参阅启动 Amazon Web Services Marketplace 实例 (p. 608)。	2013 年 11 月 11 日
G2 实例	2013-10-01	这些实例十分适用于视频创建服务、3D 可视化、流式处理图形密集型应用程序以及需要大规模并行处理能力的其他服务器端工作负载。有关更多信息，请参阅Linux 加速计算实例 (p. 358)。	2013 年 11 月 4 日
新启动向导		提供一个重新设计的新的 EC2 启动向导。有关更多信息，请参阅使用旧的启动实例向导启动实例 (p. 583)。	2013 年 10 月 10 日
修改 Amazon EC2 预留实例的实例类型	2013-10-01	您现在可以修改同一系列 (例如 M1、M2、M3、C1) 中 Linux 预留实例的实例类型。有关更多信息，请参阅修改 预留实例 (p. 434)。	2013 年 10 月 09 日
新 Amazon Linux AMI 版本		Amazon Linux AMI 2013.09 发布。	2013 年 9 月 30 日
修改 Amazon EC2 预留实例	2013-08-15	您现在可以修改区域中的预留实例。有关更多信息，请参阅 修改 预留实例 (p. 434)。	2013 年 9 月 11 日
分配公有 IP 地址	2013-07-15	在 VPC 中启动实例时，现在可以分配公有 IP 地址。有关更多信息，请参阅在实例启动期间分配公有 IPv4 地址 (p. 1057)。	2013 年 8 月 20 日
授予资源级权限	2013-06-15	Amazon EC2 支持新的亚马逊资源名称 (ARN) 和条件键。有关更多信息，请参阅适用于 Amazon EC2 的 IAM policy (p. 1225)。	2013 年 7 月 8 日
增量快照副本	2013-02-01	您现在可以执行增量快照副本。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。	2013 年 6 月 11 日
新 Tags (标签) 页面		Amazon EC2 控制台中提供一个新的 Tags (标签) 页面。有关更多信息，请参阅标记 Amazon EC2 资源 (p. 1664)。	2013 年 4 月 4 日
新 Amazon Linux AMI 版本		Amazon Linux AMI 2013.03 发布。	2013 年 3 月 27 日

功能	API 版本	描述	发行日期
EBS 优化的额外实例类型	2013-02-01	以下实例类型现在可作为 EBS 优化的实例启动：`c1.xlarge`、`m2.2xlarge`、`m3.xlarge` 和 `m3.2xlarge`。 有关更多信息，请参阅Amazon EBS 优化的实例 (p. 1522)。	2013 年 3 月 19 日
将 AMI 从一个区域复制到另一个区域	2013-02-01	您可以将 AMI 从一个区域复制到另一个区域，以便快速轻松地在多个 Amazon 区域中启动一致的实例。 有关更多信息，请参阅复制 AMI (p. 172)。	2013 年 3 月 11 日
在默认 VPC 中启动实例	2013-02-01	根据各区域的情况，您的 Amazon 账户可以在 EC2-Classic 或 VPC 中启动实例，或者仅在 VPC 中启动。如果您只能在 VPC 中启动实例，我们会为您创建一个默认 VPC。当您启动实例时，我们会将其启动为默认 VPC，除非您创建了非默认 VPC 并在启动实例时对其做出指定。	2013 年 3 月 11 日
内存增强型集群 (cr1.8xlarge) 实例类型	2012-12-01	拥有大量内存以及增强的 CPU 和网络性能。这些实例非常适合用于内存分析、图形分析和科学计算应用。	2013 年 1 月 21 日
高存储 (`hs1.8xlarge`) 实例类型	2012-12-01	高存储实例为每个实例提供非常高的存储密度以及读取和写入的高连续性。他们非常适合用于数据仓库、Hadoop/MapReduce 和并行文件系统。	2012 年 12 月 20 日
EBS 快照副本	2012-12-01	您可以使用快照备份创建数据备份、创建新 Amazon EBS 卷，或创建 Amazon Machine Image (AMI)。有关更多信息，请参阅复制 Amazon EBS 快照 (p. 1377)。	2012 年 12 月 17 日
已更新 Provisioned IOPS SSD 卷的 EBS 指标和状态检查	2012 年 10 月 1 日	已更新 EBS 指标，以便包含 Provisioned IOPS SSD 卷的两项新指标。有关更多信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)。还添加了 Provisioned IOPS SSD 卷的新状态检查。有关更多信息，请参阅EBS 卷状态检查 (p. 1359)。	2012 年 11 月 20 日
Linux 内核		已更新了 AKI ID；已重组了发行版内核；已更新了 PVOps 部分。	2012 年 11 月 13 日
M3 实例	2012 年 10 月 1 日	提供新的 M3 超大型和 M3 双倍超大型实例类型。有关更多信息，请参阅 Amazon EC2 实例类型。	2012 年 10 月 31 日
竞价型实例请求状态	2012 年 10 月 1 日	竞价型实例请求状态简化了确定您的 Spot 请求状态的过程。	2012 年 10 月 14 日
新 Amazon Linux AMI 版本		Amazon Linux AMI 2012.09 发布。	2012 年 10 月 11 日

功能	API 版本	描述	发行日期
Amazon EC2 预留实例 Marketplace	2012 年 8 月 15 日	预留实例 Marketplace 将想要出售不再需要的 Amazon EC2 预留实例的卖方与正在寻找购买额外容量的买方匹配起来。通过预留实例 Marketplace 购买和出售的预留实例与其他预留实例一样工作，不同的是他们受标准条款限制更少，并能以不同价格出售。	2012 年 9 月 11 日
适用于 Amazon EBS 的 Provisioned IOPS SSD	2012 年 7 月 20 日	Provisioned IOPS SSD 卷为 I/O 密集型工作负载，如依赖于稳定和快速响应时间的数据库应用程序，提供可预测、高性能的服务。有关更多信息，请参阅Amazon EBS 卷类型 (p. 1327)。	2012 年 7 月 31 日
适用于 Amazon EC2 的高 I/O 实例	2012 年 6 月 15 日	高 I/O 实例通过使用基于 SSD 的本地实例存储提供低延时、高性能的磁盘 I/O。	2012 年 7 月 18 日
IAM 对 Amazon EC2 实例的作用	2012-06-01	适用于 Amazon EC2 实例的 IAM 角色提供： • Amazon在 Amazon EC2 实例上运行的应用程序的 访问密钥。 • Amazon EC2 实例上的 Amazon 访问密钥的自动交替。 • 为 Amazon EC2 实例上请求 Amazon 服务的运行应用程序细调权限。	2012 年 6 月 11 日
让启动和处理中断可能性变得更加容易的竞价型实例功能。		现在您可以按照以下方式管理您的竞价型实例： • 使用 Auto Scaling 启动配置指定您愿意为竞价型实例支付的金额，并设置计划来指定您愿意为竞价型实例支付的金额。有关更多信息，请参阅 Amazon EC2 Auto Scaling 用户指南 中的在 Auto Scaling 组中启动 Spot 实例。 • 实例启动或终止时获得通知。 • 在 Amazon 资源堆栈中使用 Amazon CloudFormation 模板来启动竞价型实例。	2012 年 6 月 7 日
用于 Amazon EC2 状态检查的 EC2 实例导出和时间戳	2012 年 5 月 1 日	已添加对实例状态和系统状态时间戳的支持，该戳记显示状态检查失败的日期和时间。	2012 年 5 月 25 日
Amazon VPC 实例和系统状态检查中的 EC2 实例导出和时间戳	2012 年 5 月 1 日	已添加将 EC2 实例导出至 Citrix Xen、Microsoft Hyper-V 和 VMware vSphere 的支持。 已添加多实例和系统状态检查中的时间戳的支持。	2012 年 5 月 25 日
八倍超大型集群计算	2012 年 4 月 1 日	添加了对 VPC 中的 `cc2.8xlarge` 实例的支持。	2012 年 4 月 26 日
Amazon Web Services Marketplace AMI	2012 年 4 月 1 日	增加了对 Amazon Web Services Marketplace AMI 的支持。	2012 年 4 月 19 日
新 Linux AMI 版本		Amazon Linux AMI 2012.03 发布。	2012 年 3 月 28 日
新 AKI 版本		我们发布了 AKI 版本 1.03 和适用于 Amazon GovCloud (US) 区域的 AKI。	2012 年 3 月 28 日

功能	API 版本	描述	发行日期
中型实例、所有 AMI 上 64 位的支持和基于 Java 的 SSH 客户端	2011 年 12 月 15 日	已添加一种新的实例类型和 64 位信息的支持。添加了使用基于 Java 的 SSH 客户端连接到 Linux 实例的过程。	2012 年 3 月 7 日
预留实例定价套餐	2011 年 12 月 15 日	增加了新的一节来讨论如何充分利用预留实例定价套餐自带的折扣价格。	2012 年 3 月 5 日
Amazon Virtual Private Cloud 中的适用于 EC2 实例的 Elastic Network Interfaces (ENIs)	2011 年 12 月 1 日	已添加有关 VPC 中适用于 EC2 实例的 Elastic Network Interfaces (ENIs) 的新章节。有关更多信息，请参阅弹性网络接口 (p. 1104)。	2011 年 12 月 21 日
新 GRU 区域和 AKI		已添加适用于 SA-East-1 区域的新 AKI 版本的有关信息。此版本弃用了 AKI 版本 1.01。AKI 版本 1.02 将继续向后兼容。	2011 年 12 月 14 日
Amazon EC2 预留实例的新产品类型	2011 年 11 月 1 日	您可以选择各种各样的预留实例产品，以满足您对实例的预期使用要求。	2011 年 12 月 1 日
Amazon EC2 实例状态	2011 年 11 月 1 日	您可以查看您的实例状态的其他详细信息，包括 Amazon 计划的可能会影响您的实例的事件。这些操作活动包括，执行软件更新和安全性补丁程序所要求的实例重启，和出现硬件问题时所需的实例停止。有关更多信息，请参阅监控实例状态 (p. 974)。	2011 年 11 月 16 日
Amazon EC2 集群计算实例类型		Amazon EC2 八倍超大型集群计算 (cc2.8xlarge) 的补充支持。	2011 年 11 月 14 日
新 PDX 区域和 AKI		增加了适用于新 US-West 2 区域的新 AKI 版本的有关信息。	2011 年 11 月 8 日
Amazon VPC 中的竞价型实例	2011-07-15	增加了 Amazon VPC 中的竞价型实例支持的有关信息。通过此更新，用户可以在 Virtual Private Cloud (VPC) 中启动竞价型实例。通过在 VPC 中启动竞价型实例，竞价型实例的用户可以享受到 Amazon VPC 带来的好处。	2011 年 10 月 11 日
新 Linux AMI 版本		增加了 Amazon Linux AMI 2011.09 版本的有关信息。此次更新消除了来自 Amazon Linux AMI 的 Beta 标记，支持将存储库锁定到一个特定版本的功能，并在已安装软件包可更新时（包括安全性更新），为您提供更新通知。	2011 年 9 月 26 日
适用于 CLI 工具用户的简化的 VM Import 过程	2011-07-15	`ImportInstance` 和 `ImportVolume` 的增强功能简化了 VM Import 过程；现在，创建导入任务后，系统会将映像上传到 Amazon EC2 上。此外，通过引入 `ResumeImport`，用户可以从任务停止的时间点重新开始未完成的上传。	2011 年 9 月 15 日
导入 VHD 文件格式的支持		VM Import 现在可导入 VHD 格式的虚拟机图像文件。VHD 文件格式与 Citrix Xen 和 Microsoft Hyper-V 虚拟化平台兼容。通过这种新产品，VM Import 现在支持 RAW、VHD 和 VMDK (与 VMware ESX 兼容的) 图像格式。有关更多信息，请参阅 VM Import/Export 用户指南。	2011 年 8 月 24 日

功能	API 版本	描述	发行日期
更新至适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器		适用于 VMware vCenter 虚拟设备 (连接器) 的 1.1 版本的 Amazon EC2 VM Import 连接器的有关补充信息。此次更新包括访问因特网的代理支持、更好的错误处理方法、任务进度栏准确性的提高以及一些 bug 修复。	2011 年 6 月 27 日
让 Linux AMI 运行用户提供的内核		增加了 AKI 版本从 1.01 变到 1.02 的有关信息。此版本更新了 PVGRUB，以解决与 t1.micro Linux 实例相关的启动失败问题。有关更多信息，请参阅用户提供的内核 (p. 226)。	2011 年 6 月 20 日
竞价型实例可用区定价更改	2011 年 5 月 15 日	增加了竞价型实例可用区定价功能的有关信息。在本版本中，我们增加了新的可用区定价选项，当您查询竞价型实例请求和 Spot 价格历史记录时，返回的信息中包括这些新的定价选项。通过这些新增功能，可以更方便地确定将竞价型实例启动到特定可用区所需的价格。	2011 年 5 月 26 日
Amazon Identity and Access Management		已添加 Amazon Identity and Access Management（IAM）的有关信息，使用户可以指定借助 Amazon EC2 资源一般能使用哪些 Amazon EC2 功能。有关更多信息，请参阅适用于 Amazon EC2 的 Identity and Access Management (p. 1223)。	2011 年 4 月 26 日
让 Linux AMI 运行用户提供的内核		已添加让 Linux AMI 使用 PVGRUB Amazon Kernel Image (AKI) 来运行用户提供的内核的有关信息。有关更多信息，请参阅用户提供的内核 (p. 226)。	2011 年 4 月 26 日
专用实例		专用实例是在 Amazon Virtual Private Cloud (Amazon VPC) 中启动的，是在主机硬件层次上物理隔离的实例。专用实例让您能享用 Amazon VPC 和 Amazon 云的好处，包括按需弹性配置、仅为实际用量付费等，但同时也在硬件层次上隔离您的 Amazon EC2 计算实例。有关更多信息，请参阅Dedicated Instances (p. 533)。	2011 年 3 月 27 日
预留实例更新至 Amazon 管理控制台		更新至 Amazon 管理控制台让用户查看他们的预留实例以及购买额外预留实例，包括专用预留实例，变得更加简单。有关更多信息，请参阅 Reserved Instances (p. 408)。	2011 年 3 月 27 日
新 Amazon Linux 参考 AMI		新的 Amazon Linux 参考 AMI 替代了 CentOS 参考 AMI。已删除 CentOS 参考 AMI 的有关信息，包含题为“Correcting Clock Drift for Cluster Instances on CentOS 5.4 AMI”的章节。	2011 年 3 月 15 日
元数据信息	2011 年 1 月 1 日	已添加元数据的有关信息，将反映 2011-01-01 版本中的更改。有关更多信息，请参阅实例元数据和用户数据 (p. 754)和实例元数据类别 (p. 776)。	2011 年 3 月 11 日

功能	API 版本	描述	发行日期
适用于 VMware vCenter 的 Amazon EC2 VM Import 连接器。		已添加适用于 VMware vCenter 虚拟设备 (连接器) 的 Amazon EC2 VM Import 连接器的有关信息。这个连接器是一个用于 VMware vCenter 的插件，集成了 VMware vSphere 客户端，并提供了一个图形用户界面，您可以用它来将 VMware 虚拟机导入到 Amazon EC2 中。	2011 年 3 月 3 日
实施卷分离		您现在可以使用 Amazon Web Services Management Console 强制将 Amazon EBS 卷从实例分离。有关更多信息，请参阅从 Linux 实例分离 Amazon EBS 卷 (p. 1364)。	2011 年 2 月 23 日
实例终止保护		您现在可以使用 Amazon 管理控制台来防止实例终止。有关更多信息，请参阅启用终止保护 (p. 637)。	2011 年 2 月 23 日
校正 Amazon's CentOS 5.4 AMI 上的集群实例的 Clock Drift		已添加如何为 Amazon's CentOS 5.4 AMI 上的集群实例校正 Clock Drift 的有关信息。	2011 年 1 月 25 日
VM Import	2010-11-15	已添加有关 VM Import 的信息，允许您将虚拟机或卷导入到 Amazon EC2 中。有关更多信息，请参阅 VM Import/Export 用户指南。	2010 年 12 月 15 日
实例的基本监控	2010-08-31	已添加有关 EC2 实例的基本监控的信息。	2010 年 12 月 12 日
筛选条件和标记	2010-08-31	已添加列举、筛选和标记资源的有关信息。有关更多信息，请参阅列出并筛选您的资源 (p. 1657)和标记 Amazon EC2 资源 (p. 1664)。	2010 年 9 月 19 日
幂等实例启动	2010-08-31	已添加关于确保实例运行时的幂等性的信息。有关更多信息，请参阅 Amazon EC2 API 参考中的确保幂等性。	2010 年 9 月 19 日
微型实例	2010-06-15	Amazon EC2 为特定类型的应用程序提供 `t1.micro` 实例类型。有关更多信息，请参阅可突增性能实例 (p. 274)。	2010 年 9 月 8 日
Amazon Identity and Access ManagementAmazon EC2 的		Amazon EC2 现已集成（Amazon Identity and Access ManagementIAM）。有关更多信息，请参阅适用于 Amazon EC2 的 Identity and Access Management (p. 1223)。	2010 年 9 月 2 日
集群实例	2010-06-15	Amazon EC2 为您的高性能计算 (HPC) 应用程序提供了集群计算实例。有关更多信息，请参阅 Amazon EC2 实例类型。	2010 年 7 月 12 日
Amazon VPC IP 地址指定	2010-06-15	Amazon VPC 用户现在可以指定用于分配在 VPC 中启动的实例的 IP 地址。	2010 年 7 月 12 日
对 Amazon EBS 卷进行 Amazon CloudWatch 监控		Amazon CloudWatch 监控现在可以自动用于 Amazon EBS 卷。有关更多信息，请参阅Amazon EBS 的 Amazon CloudWatch 指标 (p. 1563)。	2010 年 6 月 14 日
内存增强型超大型实例	2009-11-30	Amazon EC2 现在支持内存增强型超大型 (m2.xlarge) 实例类型。有关更多信息，请参阅 Amazon EC2 实例类型。	2010 年 2 月 22 日