
Amazon WAF、Amazon Firewall Manager 和 Amazon Shield Advanced 开发人员指南



Amazon WAF、Amazon Firewall Manager 和 Amazon Shield Advanced: 开发人员指南

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、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其它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 WAF , AmazonShield 和Amazon Firewall Manager ?	1
Amazon WAF	1
Amazon Shield	2
Amazon Firewall Manager	2
设置	3
注册一个 Amazon Web Services 账户	3
保护 IAM 用户	3
下载工具	3
Amazon WAF	5
Amazon WAF 的工作原理	6
Amazon WAF 组件	6
Amazon WAFWeb ACL 容量单位 (WCU)	6
您可以用来保护的资源Amazon WAF	7
Amazon WAF 入门	8
步骤 1 : 设置 Amazon WAF	8
步骤 2 : 创建 Web ACL	8
步骤 3 : 添加字符串匹配规则	9
步骤 4 : 添加Amazon托管规则组	10
第 5 步 : 完成您的 Web ACL 配置	10
步骤 6 : 清除资源	11
Web ACL (Web ACL)	11
Amazon资源如何处理来自的响应延迟Amazon WAF	12
Web ACL 规则和规则组评估	12
决定 Web ACL 的默认操作	16
验证码、挑战和令牌域配置	16
使用 Web ACL	17
规则组	23
托管规则组	24
管理您自己的规则组	78
来自其他服务的规则组	79
规则	80
Rule name (规则名称)	80
规则操作	81
规则语句	81
Web 请求正文、标头和 Cookie	113
IP 集和正则表达式模式集	114
创建和管理 IP 集	114
创建和管理正则表达式模式集	116
自定义的 Web 请求和响应	118
自定义请求标头插入	119
自定义响应	120
支持的状态代码	122
网络请求上的标签	123
标注分类	124
语法和命名要求	124
添加标签	126
与标签匹配	127
标注分类	127
智能威胁缓解	130
缓解码选项	131
最佳实践	135
网络请求令牌	136
机器人控制	142
账户盗用	155

客户端应用程序集成	164
CAPTCHA和Challenge行动	175
记录 Web ACL 流量	180
日志定价	180
Amazon WAF记录目的地	180
管理 Web ACL 的日志记录	187
日志字段	188
日志示例	192
列出限速的 IP 地址	199
测试和调整您的保护措施	200
测试和调整高级步骤	200
准备测试	201
监控和优化	202
在生产中启用保护	206
如何Amazon WAF使用亚马逊 CloudFront 功能	207
Amazon WAF与 CloudFront 自定义错误页面一起使用	207
Amazon WAF与 CloudFront 用于在您自己的 HTTP 服务器上运行的应用程序	208
选择 CloudFront 响应的 HTTP 方法	208
您使用Amazon WAF服务的安全性	209
数据保护	209
身份和访问管理	210
日志记录和监控	228
合规性验证	229
故障恢复能力	230
基础设施安全性	230
Amazon WAF 配额	230
将您的Amazon WAF经典资源迁移到Amazon WAF	232
为什么要迁移到 Amazon WAF ?	232
迁移的工作原理	233
迁移注意事项	233
迁移 Web ACL	234
Amazon WAF Classic	238
设置Amazon WAF经典	238
注册一个 Amazon Web Services 账户	3
保护 IAM 用户	3
Download tools	239
怎么样Amazon WAF经典作品	240
Amazon WAF经典定价	242
.....	242
入Amazon WAF入	242
步骤 1：设置Amazon WAF经典	243
步骤 2：创建 Web ACL	243
步骤 3：创建 IP 匹配条件	244
步骤 4：创建地理匹配条件	244
步骤 5：创建字符串匹配条件	245
步骤 5A：创建正则表达式条件 (可选)	246
步骤 6：创建 SQL 注入匹配条件	247
步骤 7：(可选) 创建其他条件	248
步骤 8：创建规则并添加条件	248
步骤 9：将规则添加 Web ACL	249
步骤 10：清除资源	250
创建和配置 Web 访问控制列表 (Web ACL)	252
使用条件	253
使用规则	280
使用 Web ACL	286
使用Amazon WAF与结合使用的经典规则组Amazon Firewall Manager	295
创建Amazon WAF经典规则组	295

从中添加和删除规则Amazon WAF经典规则组	296
开始使用Amazon Firewall Manager启用Amazon WAF经典规则	297
第 1 步：完成先决条件	298
第 2 步：创建规则	298
第 3 步：创建规则组	298
第 4 步：创建并应用Amazon Firewall ManagerAmazon WAF经典策略	299
教程：创建Amazon Firewall Manager具有分层规则的策略	300
第 1 步：指定 Firewall Manager 管理员账户	301
第 2 步：使用 Firewall Manager 管理员账户创建规则组	301
第 3 步：创建 Firewall Manager 策略并附加通用规则组	301
第 4 步：添加特定于账户的规则	301
结论	302
记录 Web ACL 流量信息	302
列出根据基于速率的规则而阻止的 IP 地址	306
操作方法Amazon WAFClassic CloudFront 功能	307
使用Amazon WAF经典搭配 CloudFront 自定义错误页面	307
使用Amazon WAF经典搭配 CloudFront 对于在您自己的 HTTP 服务器上运行的应用程序	307
选择 CloudFront 响应的 HTTP 方法	308
安全性	308
数据保护	309
身份和访问管理	310
日志记录和监控	324
合规性验证	325
故障恢复能力	326
基础设施安全性	326
Amazon WAF经典配额	326
Amazon Shield	329
Shield 的工作原理	330
Amazon Shield Standard 概览	330
Amazon Shield Advanced 概览	331
DDoS 攻击示例	333
Shield 如何检测事件	334
Shield 如何缓解事件	336
DDoS 弹性架构示例	339
Web 应用程序的 DDoS 弹性示例	340
TCP 和 UDP 应用程序的 DDoS 弹性示例	341
示例 Shield 高级用例	342
开始使用	343
订阅 Shield 高级版	343
添加资源以保护和配置保护	344
配置 SRT 支持	346
在中创建 DDoS 仪表板 CloudWatch 并设置 CloudWatch 警报	348
SRT 支持	348
为Shield 响应小组 (SRT) 配置访问权限	349
配置主动参与操作	350
联系 SRT	351
使用 SRT 配置自定义缓解措施	351
资源保护	351
按资源类型划分的保护	352
应用层 (第 7 层) 保护	353
使用运行状况检查配置基于健康的检测	358
管理资源保护	364
保护	368
跟踪保护更改	369
对 DDoS 事件的可见性	369
全球和账户活动	370
事件	373

指标	377
事件跨账户可见性	378
响应 DDoS 事件	380
联系应用程序层攻击的支持人员	380
手动缓解应用层攻击	381
在攻击之后申请服务抵扣金额	381
使用 Shield 服务时的安全性	382
数据保护	383
身份和访问管理	383
日志记录和监控	400
合规性验证	401
故障恢复能力	401
基础设施安全性	401
Amazon Shield Advanced 配额	401
Amazon Firewall Manager	403
Amazon Firewall Manager 定价	403
Amazon Firewall Manager 先决条件	403
第 1 步：加入和配置 Amazon Organizations	404
步骤 2：设置 Amazon Firewall Manager 管理员账户	404
步骤 3：启用 Amazon Config	404
步骤 4：对于第三方政策，请在 Amazon Marketplace 中订阅并配置第三方设置	405
步骤 5：对于 Network Firewall 和 DNS 防火墙策略，启用资源共享	406
第 5 步：Amazon Firewall Manager 在默认禁用的区域中使用	406
管理 Firewall Manager 管理员	406
更改账户时	407
取消账户变更资格	407
入门 Amazon Firewall Manager	408
入门 Amazon WAF	408
开始使用 Amazon Shield Advanced 策略	410
Amazon VPC 安全组策略入门	413
开始使用 Amazon Network Firewall 策略	415
DNS Firewall 策略入门	416
Palo Alto Networks Cloud NGFW 政策入门	418
Fortigate CNF 政策入门	420
使用 Amazon Firewall Manager 策略	422
常规设置	422
创建策略	422
删除策略	439
策略范围	440
托管列表	441
Amazon WAF 策略	444
Amazon Shield Advanced 策略	449
安全组策略	452
Network Firewall 策略	457
DNS 防火墙策略	463
帕洛阿尔托网络云 NGFW 政策	464
强化 CNF 政策	464
Network Firewall 和 DNS 防火墙策略的资源共享	465
使用资源集	466
在 Firewall Manager 中使用资源集时的注意事项	466
创建资源集	466
查看资源合规性	467
Firewall Manager 调查结果	469
Amazon WAF 策略结果	470

Shield	470
安全组通用策略结果	471
安全组内容审核策略结果	471
安全组使用情况审核策略结果	471
DNS Firewall	472
安全性	472
数据保护	473
Identity and Access Management	473
日志记录和监控	496
合规性验证	497
故障恢复能力	497
基础设施安全性	497
Amazon Firewall Manager 配额	497
软配额	498
硬配额	499
监控	500
监控工具	500
自动化工具	500
手动工具	501
使用监控 CloudWatch	501
使用 Amazon CloudTrail 记录 API 调用	509
Amazon CloudTrail 中的 Amazon WAF 信息	509
Amazon Shield Advanced中的信息 CloudTrail	516
Amazon Firewall Manager中的信息 CloudTrail	517
使用 Amazon WAF 和 Amazon Shield Advanced API	520
使用 Amazon 软件开发工具包	520
向Amazon WAF或 Shield Advanced 发出 HT	520
请求 URI	520
HTTP 标头	520
HTTP 请求正文	521
HTTP 响应	522
错误响应	522
对请求进行身份验证	523
相关信息	524
文档历史记录	525
2018 年之前的更新	538
Amazon词汇表	540
.....	dxli

什么是Amazon WAF , AmazonShield和Amazon Firewall Manager ?

您可以[Amazon Firewall Manager \(p. 403\)](#)一起使用[Amazon WAF \(p. 5\)](#)[Amazon Shield \(p. 329\)](#)、和来创建全面的安全解决方案。Amazon WAF是一个 Web 应用程序防火墙，可使用控制对您的内容进行访问。Amazon Shield在网络和传输层（第 3 层和第 4 层）以及应用层（第 7 层）提供针对Amazon资源的分布式拒绝服务 (DDoS) 攻击的保护。Amazon Firewall Manager提供跨账户和资源的保护管理Amazon WAF，例如和 Shield Advanced，即使添加了新资源也是如此。

主题

- [Amazon WAF \(p. 1\)](#)
- [Amazon Shield \(p. 2\)](#)
- [Amazon Firewall Manager \(p. 2\)](#)

Amazon WAF

Amazon WAF是一个 Web 应用程序防火墙，可以监视转发到您的内容的 Web 应用程序资源应用您的规则和 HTTPS 请求。您可以保护以下资源类型：

- 亚马逊 CloudFront 配送
- Amazon API Gateway
- Application Load Balancer
- Amazon AppSyncGraphQL
- Amazon Cognito 用户池
- Amazon App Runner 服务

Amazon WAF让您可以控制对您的内容进行的访问。根据指定的条件 (如请求源自的 IP 地址或查询字符串的值)，您的内容会使用所请求的内容或使用 HTTP 状态代码 403 (Forbidden) 来响应请求。

在最基本的情况下，Amazon WAF 允许您选择以下行为之一：

- 允许除您指定的请求之外的所有请求 — 这在您想要 Amazon CloudFront、Amazon API Gateway、Application Load Balancer、Amazon Cognito 或Amazon App Runner为公共网站提供内容，但又想阻止攻击者的请求时很有用。Amazon AppSync
- 阻止除您指定的请求之外的所有请求 — 这在您想要为受限制的网站提供内容时非常有用，该网站的用户可以通过网络请求中的属性（例如他们用来浏览网站的 IP 地址）来识别。
- 统计符合您条件的请求-您可以使用该Count操作来跟踪您的网络流量，而无需修改处理方式。您可以将其用于常规监控，也可以用于测试新的 Web 请求处理规则。当您想要允许或阻止基于 Web 请求中的新属性的请求时，可以先配置Amazon WAF为计算与这些属性匹配的请求数。这使您可以在将规则切换为允许或阻止匹配请求之前确认新的配置设置。
- 针对符合您标准的请求运行验证码或质询检查 — 您可以对请求实施验证码和静默质询控制，以帮助减少进入受保护资源的机器人流量。

使用 Amazon WAF 有几个优势：

- 使用您指定的标准进一步防范 Web 攻击。您可以使用 Web 请求的特征定义标准，例如：

- 请求源自的 IP 地址。
- 请求源自的国家/地区。
- 请求标头中的值。
- 出现在请求中的字符串，可以是特定的字符串，也可以是与正则表达式 (regex) 模式匹配的字符串。
- 请求的长度。
- 存在可能是恶意的 SQL 代码 (称为 SQL 注入)。
- 存在可能是恶意的脚本 (称为跨站点脚本)。
- 可以允许、阻止或计数的 Web 请求。或者，规则可以阻止或统计不仅满足指定条件的 Web 请求，还可以在任意 5 分钟时段内超过指定请求数量的 Web 请求。
- 可以重复用于多个 Web 应用程序的规则。
- 来自 Amazon 和 Amazon Web Services Marketplace 卖家的托管规则组。
- 实时指标和采样的 Web 请求。
- 使用 Amazon WAF API 的自动化管理。

如果你想精细控制为资源增加的保护，那么Amazon WAF单靠自己可能是正确的选择。有关 Amazon WAF 的更多信息，请参阅 [Amazon WAF \(p. 5\)](#)。

Amazon Shield

您可以使用Amazon WAF Web 访问控制列表 (Web ACL) 来帮助最大限度地减少分布式拒绝服务 (DDoS) 攻击的影响。为了进一步防御 DDoS 攻击，Amazon还提供Amazon Shield Standard和Amazon Shield Advanced。Amazon Shield Standard除了您已经支付的费用和其他Amazon服务外，还会自动包含在内 Amazon WAF，无需支付任何额外费用。

Amazon Shield Advanced为您的 Amazon EC2 实例、Elastic Load Balancing 均衡器、CloudFront 分配、Route 53 托管区域和Amazon Global Accelerator标准加速器提供扩展的 DDoS 攻击保护。Amazon Shield Advanced会产生额外费用。Shield Advanced 选项和功能包括自动应用层 DDoS 缓解、高级事件可见性以及Shield 响应小组 (SRT) 的专门支持。如果您拥有高知名度的网站或容易遭受频繁的DDoS攻击，请考虑购买Shield Advanced提供的额外保护。有关其他信息，请参阅[Amazon Shield Advanced功能和选项 \(p. 332\)](#)和[决定是否订阅Amazon Shield Advanced和应用额外保护 \(p. 333\)](#)。

Amazon Firewall Manager

Amazon Firewall Manager简化您在多个账户和资源上的管理和维护任务，以实现各种保护，包括 Amazon WAF、Amazon VPC 安全组和 Amazon Route 53 Resolver DNS 防火墙。Amazon Shield AdvancedAmazon Network Firewall您添加新账户和资源应用您的规则和保护。

有关 Firewall Manager 的更多信息，请参阅 [Amazon Firewall Manager \(p. 403\)](#)。

设置

本主题介绍了准备使用Amazon WAF、和的预备步骤，例如创建账户Amazon Shield Advanced。Amazon Firewall Manager您无需为这些初步物品付费。您只需为使用的 Amazon 服务付费。

主题

- [注册一个 Amazon Web Services 账户 \(p. 3\)](#)
- [保护 IAM 用户 \(p. 3\)](#)
- [下载工具 \(p. 3\)](#)

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 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](#)

下载工具

Amazon Web Services Management Console包括Amazon WAF、和的控制台Amazon Shield AdvancedAmazon Firewall Manager，但如果您想以编程方式访问服务，请参阅以下内容：

- API 指南记录了服务支持的操作，并提供了指向相关 SDK 和 CLI 文档的链接：
 - [Amazon WAF API 参考](#)
 - [Amazon Shield Advanced API 参考](#)
 - [Amazon Firewall Manager API 参考](#)
 - 要调用 API 而不必处理低级别详细信息（例如汇编原始 HTTP 请求），那么您可以使用 Amazon SDK。Amazon SDK 提供用于封装 Amazon 服务的功能的函数和数据类型。要下载 Amazon SDK 和访问安装说明，请参阅适用页面：
 - [Java](#)
 - [JavaScript](#)
 - [.NET](#)
 - [Node.js](#)
 - [PHP](#)
 - [Python](#)
 - [Ruby](#)
- 有关 Amazon SDK 的完整列表，请参阅[用于 Amazon Web Services 的工具](#)。
- 您可以使用 Amazon Command Line Interface (Amazon CLI) 从命令行控制多个 Amazon 服务。您还可以使用脚本自动执行命令。有关更多信息，请参阅[Amazon Command Line Interface](#)：
 - Amazon Tools for Windows PowerShell 支持这些 Amazon 服务。有关更多信息，请参阅[Amazon Tools for PowerShell Cmdlet 参考](#)。

Amazon WAF

Amazon WAF 是一种 Web 应用程序防火墙，可让您监视转发到受保护的 Web 应用程序资源的 HTTP (S) 请求。您可以保护以下资源类型：

- 亚马逊 CloudFront 配送
- Amazon API Gateway
- Application Load Balancer
- Amazon AppSync GraphQL API
- Amazon Cognito 用户池
- Amazon App Runner 服务

Amazon WAF 让您可以控制对您的的访问。根据指定的条件 (Forbidden) 或查询字符串的值)，与您的受保护资源相关的服务会使用所请求的内容、使用 HTTP 状态代码 403 (Forbidden) 或使用自定义响应来响应请求。

Note

您还可以使用 Amazon WAF 保护托管在 Amazon Elastic Container Service (Amazon ECS) 容器中的应用程序。Amazon ECS 是一项高度可扩展的快速容器管理服务，可让您轻松地在 cluster 上运行、停止和管理 Docker 容器。要使用此选项，您需要将 Amazon ECS 配置为使用已启用的 Application Load Balancer Amazon WAF 来路由和保护服务中的任务之间的 HTTP (S) 第 7 层流量。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的服务[负载均衡](#)。

主题

- [Amazon WAF 的工作原理 \(p. 6\)](#)
- [Amazon WAF 入门 \(p. 8\)](#)
- [Web ACL \(Web ACL \) \(p. 11\)](#)
- [规则组 \(p. 23\)](#)
- [规则 \(p. 80\)](#)
- [检查请求正文、标题和 Cookie \(p. 113\)](#)
- [IP 集和正则表达式模式集 \(p. 114\)](#)
- [中的自定义 Web 请求和响应 Amazon WAF \(p. 118\)](#)
- [网络请求上的标签 \(p. 123\)](#)
- [Amazon WAF 智能威胁缓解 \(p. 130\)](#)
- [记录 Web ACL 流量 \(p. 180\)](#)
- [列出受基于速率的规则进行速率限制的 IP 地址 \(p. 199\)](#)
- [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)
- [如何 Amazon WAF 使用亚马逊 CloudFront 功能 \(p. 207\)](#)
- [您使用 Amazon WAF 服务的安全性 \(p. 209\)](#)
- [Amazon WAF 配额 \(p. 230\)](#)
- [将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)

Amazon WAF 的工作原理

您可以使用 Amazon WAF 来控制您的受保护资源如何响应 HTTP (S) Web 请求。为此，您可以定义 Web 访问控制列表 (ACL)，然后将其与要保护的一个或多个 Web 应用程序资源关联起来。关联资源将传入的请求转发给 Amazon WAF 进行 Web ACL 检查。

在 Web ACL 中，您可以创建规则来定义要在请求中查找的流量模式并指定对匹配请求采取的操作。操作选择包括以下内容：

- 允许请求进入受保护的资源进行处理和响应。
- 阻止请求。
- 计算请求数。
- 对请求运行验证码或质疑检查，以验证人类用户和标准浏览器使用情况。

主题

- [Amazon WAF 组件 \(p. 6\)](#)
- [Amazon WAF Web ACL 容量单位 \(WCU \) \(p. 6\)](#)
- [您可以用来保护的资源 Amazon WAF \(p. 7\)](#)

Amazon WAF 组件

以下是以下的核心组件 Amazon WAF：

- Web ACL — 您可以使用 Web 访问控制列表 (ACL) 保护一组 Amazon 资源。您可以创建 Web ACL 并通过添加规则来定义其保护策略。规则定义了检查 Web 请求的标准，它们指定了对符合其标准的请求采取的操作。您还为 Web ACL 设置了默认操作，该操作指示是阻止还是允许通过规则尚未阻止或允许的任何请求。

网络 ACL 是一种 Amazon WAF 资源。

- 规则 — 每条规则都包含定义检查标准的声明，以及在 Web 请求符合标准时应采取的操作。当 Web 请求满足条件时，这是一个匹配。您可以配置规则来阻止匹配请求、允许它们通过、计算请求的数量，或者对使用验证码谜题或静默客户端浏览器挑战的请求运行机器人控制。

规则不是 Amazon WAF 资源。它仅存在于 Web ACL 或规则组的上下文中。

- 规则组 - 您可以直接在 Web ACL 中定义规则，也可以在可重复使用的规则组中定义规则。Amazon 托管规则，Amazon Web Services Marketplace 卖家提供托管规则组供您使用。您还可以定义自己的规则组。

规则组是一种 Amazon WAF 资源。

Amazon WAF Web ACL 容量单位 (WCU)

Amazon WAF 使用 Web ACL 容量单位 (WCU) 来计算和控制运行规则、规则组和 Web ACL 所需的操作资源。Amazon WAF 在配置规则组和 Web ACL 时强制执行 WCU 限制。WCU 不影响 Amazon WAF 检查网络流量的方式。

Amazon WAF 以不同的方式计算每种规则类型的容量，以反映每个规则的相对成本。与使用更多处理能力的更复杂规则相比，运行成本很低的简单规则使用更少的 WCU。例如，大小限制规则语句使用的 WCU 少于根据正则表达式模式集进行检查的语句。

Amazon WAF 管理规则、规则组和 Web ACL 的容量：

- 规则容量-在创建或更新规则时Amazon WAF计算规则容量。有关规则容量要求的一些基本准则，请参阅[Amazon WAF 规则语句 \(p. 81\)](#)上的各种规则语句的列表。您还可以通过创建 Web ACL 或规则组并向其添加单个规则，了解 Amazon WAF 控制台中各种规则类型所需的容量。控制台显示您添加规则时使用的容量单位。
- 规则组容量 —Amazon WAF 要求在创建时为每个规则组分配不可变的容量。对于通过 Amazon WAF 创建的托管规则组和规则组，事实就是如此。修改规则组时，所做更改必须使规则组的 WCU 保持在其容量范围内。这可确保使用该规则组的 Web ACL 保持在其最大容量内。
- Web ACL 容量 — Web ACL 的最大容量为 1,500，这对于大多数用例来说已经足够了。如果您需要更多容量，请联系[Amazon Web Services Support 中心](#)。

您可以用来保护的资源Amazon WAF

您可以使用Amazon WAF Web ACL 来保护全球或区域资源类型。为此，您可以将 Web ACL 与要保护的资源相关联。Web ACL 及其使用的任何Amazon WAF资源都必须位于关联资源所在的区域。对于亚马逊 CloudFront 发行版，此设置为美国东部（弗吉尼亚北部）。

亚马逊 CloudFront 分发

您可以使用Amazon WAF控制台或 API 将Amazon WAF Web ACL 与 CloudFront 分配相关联。在创建或更新 CloudFront 分配本身时，也可以将 Web ACL 与分配相关联。要在中配置关联Amazon CloudFormation，必须使用 CloudFront 分发配置。有关亚马逊的信息 CloudFront，请参阅《亚马逊 CloudFront 开发者指南》中的[“使用Amazon WAF控制对您的内容的访问权限”](#)。

Amazon WAF可在全球范围内进行 CloudFront 分发，但您必须使用美国东部区域（弗吉尼亚北部）来创建 Web ACL 和 Web ACL 中使用的任何资源，例如规则组、IP 集和正则表达式模式集。有些接口提供“Global (CloudFront)”的区域选择。选择此选项与选择美国东部地区（弗吉尼亚北部）或“us-east-1”相同。

区域资源

您可以在所有可用的区域保护区域资源。Amazon WAF您可以在 Amazon Web Services 一般参考中查看[Amazon WAF终端节点和配额](#)列表。

您可以使用Amazon WAF来保护以下区域资源类型：

- Amazon API Gateway I
- Application Load Balancer
- Amazon AppSyncGraphQL API
- Amazon Cognito 用户池
- Amazon App Runner 服务

您只能将 Web ACL 关联到其中的Application Load BalancerAmazon Web Services 区域。例如，您无法将 Web ACL 关联到已开启的Application Load BalancerAmazon Outposts。

Web ACL 及其使用的任何其他Amazon WAF资源必须位于与受保护资源相同的区域中。在监控和管理受保护区域资源的 Web 请求时，Amazon WAF将所有数据与受保护资源保持在同一个区域中。

对多个资源关联的限制

您可以将单个 Web ACL 与一个或多个Amazon资源相关联，但有以下限制：

- 您只能将每个 Amazon 资源与一个 Web ACL 关联。Web ACL 和Amazon资源之间的关系是 one-to-many。
- 您可以将 Web ACL 与一个或多个 CloudFront 分配相关联。您无法将与 CloudFront 分配关联的 Web ACL 与任何其他Amazon资源类型相关联。

Amazon WAF 入门

本教程介绍如何使用 Amazon WAF 执行以下任务：

- 设置 Amazon WAF。
- 使用 Amazon WAF 控制台中的向导创建 Web 访问控制列表 (Web ACL)。
- 选择希望 Amazon WAF 检查其 Web 请求的 Amazon 资源。本教程涵盖了亚马逊的步骤 CloudFront、Amazon API Gateway REST API、Application Load Balancer、GraphQL API、Amazon AppSync GraphQL API、Amazon Cognito 用户池或 Amazon App Runner 服务的流程基本相同。
- 添加要用于筛选 Web 请求的规则和规则组。例如，您可以指定请求来源的 IP 地址，并在请求中指定仅供攻击者使用的值。对于每个规则，您可以指定如何处理匹配的 Web 请求。您可以做诸如格挡或计数之类的事情，也可以像验证码一样进行机器人挑战。您可以为在 Web ACL 中定义的每条规则以及在规则组内定义的每条规则定义一个操作。
- 指定 Web ACL 的默认操作，即 Block 或 Allow。这是在 Web ACL 中的规则未明确允许或阻止请求时对请求采取的操作。Amazon WAF

Note

对于在本教程中创建的资源，Amazon 向您收取的费用通常少于每日 0.25 美元。当您完成本教程时，建议您删除资源以避免产生不必要的费用。

主题

- [步骤 1：设置 Amazon WAF \(p. 8\)](#)
- [步骤 2：创建 Web ACL \(p. 8\)](#)
- [步骤 3：添加字符串匹配规则 \(p. 9\)](#)
- [步骤 4：添加 Amazon 托管规则组 \(p. 10\)](#)
- [第 5 步：完成您的 Web ACL 配置 \(p. 10\)](#)
- [步骤 6：清除资源 \(p. 11\)](#)

步骤 1：设置 Amazon WAF

如果您尚未按照中的常规设置步骤进行操作[设置 \(p. 3\)](#)，请立即执行此操作。

步骤 2：创建 Web ACL

Amazon WAF 控制台会根据指定的条件 (如请求来源的 IP 地址或请求中的值)，会指导您完成设置 Amazon WAF 为阻止或允许 Web 请求的 Web 请求的 Web 请求的 IP 地址或请求中的值。在此步骤中，您将创建一个 Web ACL。有关 Amazon WAF Web ACL 的更多信息，请参阅[Web ACL \(Web ACL \) \(p. 11\)](#)。

创建 Web ACL

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在 Amazon WAF 主页上，选择创建 Web ACL。
3. 对于 Name (名称)，输入要用于标识此 Web ACL 的名称。

Note

Web ACL 在创建之后无法更改名称。

4. (可选) 对于 Description - optional (描述 - 可选)，如果需要，请输入 Web ACL 的较长描述。

5. 对于 CloudWatch metric name (CloudWatch 指标名称)，更改默认名称（如果适用）。按照控制台上的指导进行有效字符操作。该名称不能包含为 Amazon WAF 保留的特殊字符、空格或指标名称，包括“All”和“Default_Action”。

Note

创建 Web ACL 之后，无法更改 CloudWatch 指标名称。

6. 对于资源类型，选择 CloudFront 分配。该区域会自动填充到 Global (CloudFront) 以进行 CloudFront 分配。
7. （可选）对于“关联 Amazon 资源-可选”，选择“添加 Amazon 资源”。在对话框中，选择要关联的资源，然后再选择 Add。Amazon WAF 将您返回到“描述 Web ACL 和相关 Amazon 资源”页面。
8. 选择下一步。

步骤 3：添加字符串匹配规则

在此步骤中，您将使用字符串匹配语句创建规则，并指示如何处理匹配请求。字符串匹配规则语句标识您 Amazon WAF 要在请求中搜索的字符串。字符串通常由可打印 ASCII 字符组成，但您可以指定从十六进制 0x00 到 0xFF（十进制 0 到 255）的任何字符。除了指定要搜索的字符串外，还可以指定要搜索的 Web 请求组件，例如标头、查询字符串或请求正文。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制 [请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见 [网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参阅 [文本转换 \(p. 107\)](#)。

有关 Amazon WAF 规则的更多信息，请参阅 [规则 \(p. 80\)](#)。

创建字符串匹配规则语句

1. 在 Add rules and rule groups (添加规则和规则组) 页面上，选择 Add rules (添加规则)、Add my own rules and rule groups (添加我自己的规则和规则组)、Rule builder (规则生成器)，然后选择 Rule visual editor (规则可视化编辑器)。

Note

控制台提供 Rule visual editor (规则可视化编辑器) 和 Rule JSON editor (规则 JSON 编辑器)。JSON 编辑器使您可以轻松地在 Web ACL 之间复制配置，并且对于更复杂的规则集（如那些具有多个嵌套级别的规则集）是必需的。
此过程使用 Rule visual editor (规则可视化编辑器)。

2. 对于 Name (名称)，输入要用于标识此规则的名称。
3. 对于 Type (类型)，选择 Regular rule (常规规则)。
4. 对于 If a request (如果请求)，选择 matches the statement (与语句匹配)。

其他选项适用于逻辑规则语句类型。您可以使用它们来合并或否定其他规则语句的结果。

5. 在声明中，对于 Inspect，打开下拉列表并选择 Amazon WAF 要检查的 Web 请求组件。对于此示例，选择 Header。

选择 Header (标头) 时, 还可以指定希望 Amazon WAF 检查的标头。输入 **User-Agent**。此值不区分大小写。

6. 对于 Match type (匹配类型), 选择指定的字符串必须出现在 User-Agent 标头中的位置。

在此示例中, 选择 Exactly matches string (完全匹配字符串)。这表示 Amazon WAF 检查每个 Web 请求中的用户代理标头是否存在与您指定的字符串相同的字符串。

7. 对于 String to match (要匹配的字符串), 请指定希望 Amazon WAF 搜索的字符串。String to match (要匹配的字符串) 的最大长度是 200 个字符。如果您要指定 base64 编码值, 您可以指定最多 200 个字符 (编码前)。

在此示例中, 输入MyAgent。 Amazon WAF将检查 Web 请求中的User-Agent标题中的值MyAgent。

8. 将 Text transformation (文本转换) 保留设置为 None (无)。
9. 在“操作”中, 选择您希望规则在与 Web 请求匹配时执行的操作。在此示例中, 选择 Count 并保持其他选项不变。计数操作为符合规则的 Web 请求创建指标, 但不影响请求是被允许还是被阻止。有关操作选择的更多信息, 请参阅[Amazon WAF 规则操作 \(p. 81\)](#)和[Web ACL 规则和规则组评估 \(p. 12\)](#)。
10. 选择 Add rule。

步骤 4：添加Amazon托管规则组

AmazonManaged Rules 提供了一组托管规则组供您使用, 其中大多数对Amazon WAF客户是免费的。有关规则组的更多信息, 请参阅[规则组 \(p. 23\)](#)。我们将向此 Web ACL 添加一个Amazon托管规则组。

添加Amazon托管规则组

1. 在 Add rules and rule groups (添加规则和规则组) 页面上, 选择 Add rules (添加规则), 然后选择 Add managed rule groups (添加托管规则组)。
2. 在添加托管规则组页面上, 展开Amazon托管规则组的列表。(您还将看到为Amazon Web Services Marketplace卖家提供的清单。您可以订阅他们的产品, 然后使用与 Managed Rules 规则组相同的方式使用它们。) Amazon
3. 对您要添加的规则组, 执行以下操作:
 - a. 在“操作”列中, 打开“添加到 Web ACL”开关。
 - b. 选择“编辑”, 然后在规则组的“规则”列表中打开“覆盖所有规则操作”下拉列表并选择Count。这会将规则组中所有规则的操作设置为仅计数。这允许您在使用任何一个 Web 请求之前, 查看规则组中的所有规则是如何处理您的 Web 请求的。
 - c. 选择“保存规则”。
4. 在添加托管规则组页面中, 选择添加规则。这将使您返回到添加规则和规则组页面。

第 5 步：完成您的 Web ACL 配置

完成向 Web ACL 配置中添加规则和规则组后, 通过管理 Web ACL 中规则的优先级并配置诸如指标、标记和日志记录之类的设置来结束。

完成 Web ACL 配置

1. 在 Add rules and rule groups (添加规则和规则组) 页面上, 选择 Next (下一步)。
2. 在设置规则优先级页面上, 您可以看到 Web ACL 中规则和规则组的处理顺序。Amazon WAF从列表顶部开始处理它们。您可以通过向上或向下移动规则来更改处理顺序。要执行此操作, 请在列表中选择一 个, 然后选择 Move up (上移) 或 Move down (下移)。有关规则优先级的更多信息, 请参阅 [Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)。

3. 选择下一步。
4. 在配置指标页面上，对于亚马逊 CloudWatch 指标，您可以查看规则和规则组的计划指标，也可以看到网络请求抽样选项。有关亚马逊 CloudWatch 指标的信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。有关查看示例请求的信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)。
5. 选择下一步。
6. 在 Review and create web ACL (审核和创建 Web ACL) 页面上，查看您的设置，然后选择 Create web ACL (创建 Web ACL)。

该向导将返回到 Web ACL 页面，其中列出了您的新 Web ACL。

步骤 6：清除资源

现在您已成功完成了教程。为了防止您的账户产生额外的 Amazon WAF 费用，需要清除所创建的 Amazon WAF 对象。或者，您可以更改配置以匹配您真正想要管理的 Web 请求 Amazon WAF。

Note

对于在本教程中创建的资源，Amazon 向您收取的费用通常少于每日 0.25 美元。完成后，建议您删除资源以防止产生不必要的费用。

删除 Amazon WAF 进行收费的对象

1. 在 Web ACL 页面中，从列表中选择您的 Web ACL，然后选择 Edit (编辑)。
2. 在关联 Amazon 资源选项卡上，对于每个关联资源，选择资源名称旁边的单选按钮，然后选择取消关联。这将使 Web ACL 与您的 Amazon 资源取消关联。
3. 在以下每个屏幕中，选择 Next (下一步)，直到您返回到 Web ACL 页面。

在 Web ACL 页面中，从列表中选择您的 Web ACL，然后选择 Delete (删除)。

规则和规则语句不存在于规则组和 Web ACL 定义之外。如果您删除某个 Web ACL，则会删除您在该 Web ACL 中定义的所有单独规则。从 Web ACL 中删除规则组时，您只需删除对它的引用即可。

Web ACL (Web ACL)

Web 访问控制列表 (Web ACL) 使您可以对受保护资源响应的所有 HTTP (S) Web 请求进行精细控制。您可以保护亚马逊 CloudFront、Amazon API Gateway、Application Load Balancing、Amazon AppSync、Amazon Cognito 和 Amazon App Runner 资源。

您可以使用如下条件来允许或阻止请求：

- 请求的 IP 地址源
- 请求的源国家/地区
- 部分请求中的字符串匹配或正则表达式匹配
- 请求特定部分的大小
- 检测恶意 SQL 代码或脚本

您还可以针对这些条件的任何组合进行测试。您可以阻止或统计不仅满足指定条件，还在任何 5 分钟周期内超过指定请求数的 Web 请求。您可以使用逻辑运算符组合条件。您还可以根据请求运行 CAPTCHA 谜题和静默客户端会话挑战。

您在Amazon WAF规则声明中提供匹配标准和匹配时要采取的操作。您可以直接在 Web ACL 中定义规则语句，也可以在 Web ACL 中使用的可重用规则组中定义规则语句。有关选项的完整列表，请参阅[Amazon WAF 规则语句 \(p. 81\)](#)和[Amazon WAF 规则操作 \(p. 81\)](#)。

要指定您的 Web 请求检查和处理标准，请执行以下任务：

1. 对于与您指定的任何规则均不匹配的 Web 请求，选择 Web ACL 默认操作Allow或Block。有关更多信息，请参阅[决定 Web ACL 的默认操作 \(p. 16\)](#)：
2. 添加要在 Web ACL 中使用的任何规则组。托管规则组通常包含阻止 Web 请求的规则。有关规则组的信息，请参阅[规则组 \(p. 23\)](#)。
3. 在一个或多个规则中指定其他匹配标准和处理指令。要添加多个规则，请以 oAND rOR 规则语句开头，然后将要合并的规则嵌套在这些语句下。如果要否定某个规则选项，请将该规则嵌套在 NOT 语句中。您可以选择性地使用基于速率的规则（而不是常规规则）来限制来自满足条件的任何单个 IP 地址的请求数。有关规则的信息，请参阅[规则 \(p. 80\)](#)。

如果将多个规则添加到一个 Web ACL，Amazon WAF 按规则在 Web ACL 中的列出顺序来评估规则。有关更多信息，请参阅[Web ACL 规则和规则组评估 \(p. 12\)](#)：

创建 Web ACL 时，您可以指定要使用它的资源类型。有关信息，请参阅[创建 Web ACL \(p. 17\)](#)。定义 Web ACL 后，您可以将其与资源相关联，以开始为资源提供保护。有关更多信息，请参阅[将 Web ACL 与 Amazon资源关联或取消关联 \(p. 22\)](#)：

Amazon资源如何处理来自的响应延迟Amazon WAF

在某些情况下，Amazon WAF 可能会遇到内部错误，该错误会延迟对关联 Amazon 资源有关允许还是阻止请求的响应。在这些情况下，CloudFront 通常允许请求或提供内容，而区域服务通常会拒绝请求并且不提供内容。

主题

- [Web ACL 规则和规则组评估 \(p. 12\)](#)
- [决定 Web ACL 的默认操作 \(p. 16\)](#)
- [Web ACL 的验证码、质询和令牌域配置 \(p. 16\)](#)
- [使用 Web ACL \(p. 17\)](#)

Web ACL 规则和规则组评估

Web ACL 对 Web 请求的处理方式取决于以下几点：

- Web ACL 和内部规则组中规则的数字优先级设置
- 规则和 Web ACL 上的操作设置
- 您在所添加的规则组中的规则上设置的任何替代项

有关规则操作设置的列表，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

您可以在规则操作设置和默认 Web ACL 操作设置中自定义请求和响应处理。有关信息，请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#)。

主题

- [Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)
- [Web ACL 中如何处理规则和规则组操作 \(p. 13\)](#)

- [规则组中的操作替代 \(p. 14\)](#)

Web ACL 中规则和规则组的处理顺序

在 Web ACL 中和任何规则组内，您可以使用数字优先级设置来确定规则的评估顺序。必须为 Web ACL 中的每条规则指定该 Web ACL 中的唯一优先级设置，并且必须为规则组中的每条规则指定该规则组内的唯一优先级设置。

Note

当您通过控制台管理规则组和 Web ACL 时，会根据列表中规则的顺序为您 Amazon WAF 分配唯一的数字优先级设置。Amazon WAF 为列表顶部的规则分配最低的数字优先级，为底部的规则分配最高的数字优先级。

当根据 Web 请求 Amazon WAF 评估任何 Web ACL 或规则组时，它会从最低数字优先级设置开始评估规则，直到找到终止评估的匹配项或用尽所有规则为止。

例如，假设您的 Web ACL 中有以下规则和规则组，优先级如下所示：

- 规则 1 — 优先级 0
- RuleGroupA — 优先级 100
 - 规则 A1 — 优先级 10,000
 - 规则 A2 — 优先级 20,000
- 规则 2 — 优先级 200
- RuleGroupB — 优先级 300
 - 规则 B1 — 优先级 0
 - 规则 B2 — 优先级 1

Amazon WAF 将按以下顺序评估此 Web ACL 的规则：

- Rule1
- RuleGroupA 规则 A1
- RuleGroupA 规则 A2
- Rule2
- RuleGroupB 规则 B1
- RuleGroupB 规则 B2

Web ACL 中如何处理规则和规则组操作

配置规则和规则组时，您可以选择处理匹配的 Web 请求的方式：Amazon WAF

- Allow 并 Block 正在终止操作，Block 操作会停止对匹配的 Web 请求的 Web ACL 的所有其他处理。Allow 如果 Web ACL 中的规则找到请求的匹配项并且该规则操作为 Allow 或 Block，则该匹配将决定 Web ACL 的 Web 请求的最终处置方式。Amazon WAF 不处理 Web ACL 中匹配规则之后的任何其他规则。对于直接添加到 Web ACL 的规则和添加到规则组中的规则，此原理同样适用。通过该 Block 操作，受保护的资源不会接收或处理 Web 请求。
- Count 是非终止操作 — 当带有 Count 操作的规则与请求匹配时，对请求进行 Amazon WAF 计数，然后继续处理 Web ACL 规则集中的规则。
- CAPTCHA 并且 Challenge 可以是非终止操作或终止操作 — 当包含这些操作之一的规则与请求匹配时，Amazon WAF 会检查其令牌状态。如果请求具有有效令牌，则将匹配项 Amazon WAF 视为 Count 匹配

项，然后继续处理 Web ACL 规则集中的规则。如果请求没有有效的令牌，则 Amazon WAF 终止评估并向客户端发送验证码谜题或静默后台客户端会话挑战来解决。

如果规则评估未导致任何终止操作，则将 Web ACL 默认操作 Amazon WAF 应用于请求。

Amazon WAF 适用于 Web 请求的操作受到 Web ACL 中规则的数字优先级设置的影响。例如，假设您的 Web ACL 有一条规则的 Allow 操作和数值优先级为 50，另一条规则的 Count 操作和数值优先级为 100。Amazon WAF 按优先级顺序评估 Web ACL 中的规则，从最低设置开始，因此它将在计数规则之前评估允许规则。如果您的 Web 请求同时匹配这两个规则，则它将首先匹配允许规则。由于 Allow 是终止操作，因此 Amazon WAF 将停止本次比赛的评估，并且不会根据计数规则评估请求。如果您想要计数规则中的计数指标，即使是与允许规则匹配的请求也是如此，则需要为计数规则指定比允许规则更低的数字优先级设置，这样它才能首先运行。有关优先级设置的更多信息，请参阅 [Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)。

在 Web ACL 中，您可以覆盖规则组内规则的操作设置，也可以覆盖规则组返回的操作。有关信息，请参阅 [规则组中的操作替代 \(p. 14\)](#)。

规则组中的操作替代

将规则组添加到 Web ACL 时，可以覆盖它对匹配的 Web 请求所执行的操作。在 Web ACL 配置中覆盖规则组的操作不会改变规则组本身。它仅更改在 Web ACL 上下文中规则组的 Amazon WAF 使用方式。

规则操作替代规则

您可以将规则组内规则的操作改写为任何有效的规则操作。当您执行此操作时，匹配请求的处理方式与配置规则的操作是替代设置完全相同。

Note

规则操作可以是终止的，也可以是非终止的。终止操作会停止对请求的 Web ACL 评估，要么让请求继续访问您的受保护应用程序，要么将其阻止。

以下是规则操作选项：

- **Allow**—Amazon WAF 允许将请求转发到受保护的 Amazon 资源进行处理和响应。这是终止操作。在您定义的规则中，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。
- **Block**—Amazon WAF 阻止请求。这是终止操作。默认情况下，您的受保护 Amazon 资源以 HTTP 403 (Forbidden) 状态码进行响应。在您定义的规则中，您可以自定义响应。当 Amazon WAF 阻止请求时，Block 操作设置决定受保护资源发送回客户端的响应。
- **Count**—对请求进行 Amazon WAF 计数，但不确定是允许还是阻止请求。这是一项非终止操作。Amazon WAF 继续处理 Web ACL 中的其余规则。在您定义的规则中，您可以在请求中插入自定义标头，也可以添加其他规则可以匹配的标签。
- **CAPTCHA 和 Challenge**—Amazon WAF 使用验证码谜题和静默挑战来验证请求不是来自机器人，并让 Amazon WAF 使用代币来跟踪最近的成功客户回应。

Note

当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中用作规则操作替代时，会向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

这些规则操作可以是终止的，也可以是非终止的，具体取决于请求中令牌的状态：

- **有效的、未过期的令牌不可终止** — 如果令牌根据配置的验证码或质询豁免时间有效且未过期，则 Amazon WAF 处理与 Count 操作类似的请求。Amazon WAF 继续基于 Web ACL 中的其余规则检查 Web 请求。与 Count 配置类似，在您定义的规则中，您可以选择使用自定义标头配置这些操作以插入到请求中，还可以添加其他规则可以匹配的标签。
- **终止对无效或过期令牌的请求** — 如果令牌无效或指定的时间戳已过期，则 Amazon WAF 终止对 Web 请求的检查并阻止请求，与 Block 操作类似。Amazon WAF 然后用错误回应客户端。因为 CAPTCHA，

如果请求内容表明客户端浏览器可以处理，则在 JavaScript 插页式广告中 Amazon WAF 发送验证码拼图，该拼图旨在区分人类客户端和机器人。对于动 Challenge 作，Amazon WAF 发送带有静默挑战的 JavaScript 插页式广告，旨在区分普通浏览器和由机器人运行的会话。

有关更多信息，请参阅[CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)。

有关如何使用该选项的信息，请参阅[覆盖规则组中的规则操作 \(p. 20\)](#)。

将规则操作改写为 Count

规则操作覆盖的最常见用例是重写部分或全部规则操作，以便 Count 在将规则组投入生产之前测试和监控规则组的行为。

您也可以使用它来解决产生误报的规则组的问题。当规则组屏蔽了你没想到它会屏蔽的流量时，就会出现误报。如果您在规则组中发现了一条规则，该规则会阻止您希望允许通过的请求，则可以保留该规则的计数操作优先于该规则，使其无法对您的请求采取行动。

有关在测试中使用规则操作替代的更多信息，请参阅[测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

JSON 列表：**RuleActionOverrides** 替换 **ExcludedRules**

如果您在 2022 年 10 月 27 日之前 Count 在 Web ACL 配置中将规则组规则操作设置为，则将网页 ACL JSON 中的覆盖 Amazon WAF 保存为 ExcludedRules。现在，用于替换规则的 JSON 设置 Count 位于 RuleActionOverrides 设置中。

当您使用 Amazon WAF 控制台编辑现有规则组设置时，控制台会自动将 JSON 中的任何 ExcludedRulesRuleActionOverrides 设置转换为设置，并将覆盖操作设置为 Count。

• 当前设置示例：

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAdminProtectionRuleSet",
  "RuleActionOverrides": [
    {
      "Name": "AdminProtection_URI_PATH",
      "ActionToUse": {
        "Count": {}
      }
    }
  ]
}
```

• 旧设置示例：

```
OLD SETTING
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAdminProtectionRuleSet",
  "ExcludedRules": [
    {
      "Name": "AdminProtection_URI_PATH"
    }
  ]
}
OLD SETTING
```

我们建议您将 JSON 列表中的所有 ExcludedRules 设置更新为将操作设置为的 RuleActionOverrides 设置 Count。API 接受任一设置，但如果你只使用新 RuleActionOverrides 设置，你的 JSON 列表以及控制台工作和 API 工作之间的一致性。

将规则组操作改为Count

您可以覆盖规则组返回的操作，将其设置为Count。

Note

这不是测试规则组规则的好选择，因为它不会改变Amazon WAF评估规则组本身的方式。它仅影响如何Amazon WAF处理从规则组评估返回到 Web ACL 的结果。如果要测试规则组中的规则，请使用上一节中描述的选项[规则操作替代规则 \(p. 14\)](#)。

当您规则组操作改写为Count，将正常Amazon WAF处理规则组评估。

如果规则组中没有匹配的规则，或者如果所有匹配的规则都有Count操作，则此替代不会影响规则组或 Web ACL 的处理。

规则组中与 Web 请求匹配且具有终止规则操作的第一个规则会Amazon WAF导致停止评估该规则组并将终止操作结果返回到 Web ACL 评估级别。此时，在 Web ACL 评估中，此替代生效。Amazon WAF覆盖终止操作，因此规则组评估的结果仅为Count操作。Amazon WAF然后继续处理 Web ACL 中的其余规则。

有关如何使用该选项的信息，请参阅[将规则组的评估结果改写为Count \(p. 21\)](#)。

决定 Web ACL 的默认操作

创建和配置 Web ACL 时，必须设置 Web ACL 的默认操作。Amazon WAF将此操作应用于通过所有 Web ACL 规则评估而无需对其应用终止操作的任何 Web 请求。终止操作会停止对请求的 Web ACL 评估，要么让请求继续访问您的受保护应用程序，要么将其阻止。有关规则操作的信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

Web ACL 默认操作必须确定 Web 请求的最终处置方式，因此它是终止操作：

- Allow— 如果您想允许大多数用户访问您的网站，但又想阻止其请求来自指定 IP 地址或其请求似乎包含恶意 SQL 代码或指定值的攻击者的访问，请选择Allow默认操作。然后，向 Web ACL 添加规则时，请添加标识并阻止要阻止的特定请求的规则。通过此操作，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。
- Block— 如果您想阻止大多数用户访问您的网站，但又想允许其请求来自指定 IP 地址或其请求包含指定值 Block的用户访问，请选择默认操作。然后，向 Web ACL 添加规则时，请添加标识并允许要允许的特定请求的规则。默认情况下，对于Block操作，Amazon资源使用 HTTP403 (Forbidden) 状态码进行响应，但您可以自定义响应。

有关自定义请求和响应的信息，请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#)。

您自己的规则和规则组的配置部分取决于您是允许还是阻止大多数 Web 请求。例如，如果您想允许大多数请求，则应将 Web ACL 的默认操作设置为，然后添加标识要阻止的 Web 请求的规则，例如：Allow

- 源自进行数量不合理的请求的 IP 地址的请求
- 源自您不在其中开展业务或是频繁攻击源的国家/地区的请求
- 在 User-agent 标头中包含伪造值的请求
- 表现为包含恶意 SQL 代码的请求

托管规则组规则通常使用该Block操作，但并非所有规则都使用该操作。例如，一些用于机器人控制的规则使用CAPTCHA和Challenge操作设置。有关托管规则组的信息，请参阅[托管规则组 \(p. 24\)](#)。

Web ACL 的验证码、质询和令牌域配置

您可以在 Web ACL 中为使用CAPTCHA或规则操作的Challenge规则以及管理静默客户端挑战以实现Amazon WAF托管保护的应用程序集成 SDK 配置选项。

这些功能通过向最终用户挑战 CAPTCHA 谜题以及向客户会话提供静默挑战来减少机器人活动。当客户端成功响应时，Amazon WAF 提供一个令牌供他们在网络请求中使用，上面标有上次成功的拼图和挑战响应的时间戳。有关更多信息，请参阅[Amazon WAF 智能威胁缓解 \(p. 130\)](#)：

在 Web ACL 配置中，您可以配置如何 Amazon WAF 管理这些令牌：

- CAPTCHA 和挑战免疫时间 — 这些时间指定了验证码或挑战时间戳的有效时间。Web ACL 设置由所有未配置自己的免疫时间设置的规则以及应用程序集成 SDK 继承。有关更多信息，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)：
- 令牌域-默认情况下，仅 Amazon WAF 接受与 Web ACL 关联的资源域的令牌。如果您配置令牌域列表，则 Amazon WAF 接受列表中所有域和关联资源域的令牌。有关更多信息，请参阅[配置 Web ACL 令牌域列表 \(p. 138\)](#)：

使用 Web ACL

本节提供通过 Amazon 控制台创建、管理和使用 Web ACL 的过程。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他 Amazon WAF 资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

主题

- [创建 Web ACL \(p. 17\)](#)
- [编辑 Web ACL \(p. 19\)](#)
- [管理 Web ACL 中的规则组行为 \(p. 20\)](#)
- [将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)
- [删除 Web ACL \(p. 23\)](#)

创建 Web ACL

创建 Web ACL

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 请在导航窗格中选择 Web ACL，然后选择 Create Web ACL (创建 Web ACL)。
3. 对于 Name (名称)，输入要用于标识此 Web ACL 的名称。

Note

Web ACL 在创建之后无法更改名称。

4. (可选) 对于 Description - optional (描述 - 可选)，如果需要，请输入 Web ACL 的较长描述。

5. 对于 CloudWatch metric name (CloudWatch 指标名称), 更改默认名称 (如果适用)。按照控制台上的指导进行有效字符操作。该名称不能包含为 Amazon WAF 保留的特殊字符、空格或指标名称, 包括“all”和“Default_Action”。

Note

创建 Web ACL 之后, 无法更改 CloudWatch 指标名称。

6. 对于 Resource type (资源类型), 请选择要与此 Web ACL 关联的 Amazon 资源类别。有关更多信息, 请参阅[将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)。
7. 对于区域, 如果您选择了区域资源类型, 请选择 Amazon WAF 要存储 Web ACL 的区域。

只需为区域资源类型选择该选项。对于 CloudFront 发行版, 对于全球 () 应用程序, 区域将硬编码为美国东部 (弗吉尼亚北部 CloudFront) 区域中。us-east-1

8. (可选) 对于“关联 Amazon 资源-可选”, 选择“添加 Amazon 资源”。在对话框中, 选择要关联的资源, 然后再选择 Add。Amazon WAF 将您返回到“描述 Web ACL 和相关 Amazon 资源”页面。
9. 选择下一步。
10. (可选) 如果要添加托管规则组, 请在 Add rules and rule groups (添加规则和规则组) 页面上, 选择 Add rules (添加规则), 然后选择 Add managed rule groups (添加托管规则组)。对要添加的每个托管规则组执行以下操作:
 - a. 在 Add managed rule groups (添加托管规则组) 页面上, 展开 Amazon 托管规则组或所选 Amazon Web Services Marketplace 卖家的列表。
 - b. 对于要添加的规则组, 在操作列中, 打开添加到 Web ACL 开关。

要自定义 Web ACL 使用规则组的方式, 请选择编辑。以下是常见的自定义设置:

- 改写部分或所有规则的规则操作。如果您没有为规则定义替代操作, 则评估将使用在规则组内定义的规则操作。有关此选项的更多信息, 请参阅[规则组中的操作替代 \(p. 14\)](#)。
- 通过添加范围缩小语句, 缩小规则组检查的 Web 请求的范围。有关此选项的更多信息, 请参阅[范围缩小声明 \(p. 110\)](#)。
- 某些托管规则组需要您提供其他配置。请参阅您的托管规则组提供商提供的文档。有关“Amazon 托管规则”规则组的特定信息, 请参阅[Amazon 的托管规则 Amazon WAF \(p. 32\)](#)。

完成设置后, 选择“保存规则”。

选择 Add rules (添加规则) 以完成托管规则的添加, 然后返回 Add rules and rule groups (添加规则和规则组) 页面。

11. (可选) 如果要添加您自己的托管规则组, 请在 Add rules and rule groups (添加规则和规则组) 页面上, 选择 Add rules (添加规则), 然后选择 Add my own rules and rule groups (添加我自己的规则和规则组)。对要添加的每个规则组执行以下操作:
 - a. 在 Add my own rules and rule groups (添加我自己的规则和规则组) 页面上, 选择 Rule group (规则组)。
 - b. 在“名称”中, 输入要用于此 Web ACL 中的规则组规则的名称。
 - c. 从列表中选择您的规则组, 然后选择添加规则。
12. (可选) 如果要添加您自己的规则, 请在 Add rules and rule groups (添加规则和规则组) 页面上, 依次选择 Add rules (添加规则)、Add my own rules and rule groups (添加我自己的规则和规则组)、Rule builder (规则生成器), 然后选择 Rule visual editor (规则可视化编辑器)。

Note

控制台 Rule visual editor (规则可视化编辑器) 支持一个嵌套级别。例如, 您可以使用单个逻辑 AND 或 OR 语句并在其中嵌套一层其他语句, 但不能在逻辑语句中嵌套逻辑语句。要管理更复杂的规则语句, 请使用 Rule JSON editor (规则 JSON 编辑器)。有关规则的所有选项的信息, 请参阅[规则 \(p. 80\)](#)。

此过程涵盖 Rule visual editor (规则可视化编辑器)。

- a. 对于 Name (名称), 输入要用于标识此规则的名称。
- b. 根据您的需求输入您的规则定义。可以在逻辑语句AND和规则语句中组合OR规则。该向导将根据上下文指导您学习每个规则的选项。有关规则选项的信息, 请参阅 [规则 \(p. 80\)](#)。
- c. 对于 Action (操作), 选择您希望规则在与 Web 请求匹配时执行的操作。有关您的选择的信息, 请参阅 [Amazon WAF 规则操作 \(p. 81\)](#) 和 [Web ACL 规则和规则组评估 \(p. 12\)](#)。

如果您使用的是CAPTCHA或Challenge操作, 请根据需要调整规则的免疫时间配置。如果您未指定设置, 规则会从 Web ACL 中继承设置。有关更多信息, 请参阅[时间戳到期: 代币豁免时间 \(p. 137\)](#) :

Note

当您在其中一个规则中使用CAPTCHA或Challenge规则操作或在规则组中用作规则操作替代时, 会向您收取额外费用。有关更多信息, 请参阅 [Amazon WAF 定价](#)。

如果您想自定义请求或响应, 请选择相应的选项并填写自定义的详细信息。有关更多信息, 请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#) :

如果您想让您的规则为匹配的网络请求添加标签, 请选择相应的选项并填写您的标签详细信息。有关更多信息, 请参阅[网络请求上的标签 \(p. 123\)](#) :

- d. 选择 Add rule。
13. 选择 Web ACL 的默认操作, 即Block或Allow。这是在 Web ACL 中的规则未明确允许或阻止请求时对请求采取的操作。Amazon WAF有关更多信息, 请参阅[决定 Web ACL 的默认操作 \(p. 16\)](#) :

如果要自定义默认操作, 请选择相应的选项并填写自定义的详细信息。有关更多信息, 请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#) :
14. 您可以定义令牌域列表以启用受保护应用程序之间的令牌共享。令牌由CAPTCHA和Challenge操作以及您在使用防Amazon WAF欺诈控制账户接管 (ATP) 和Amazon WAF机器人控制的Amazon托管规则组时实现的应用程序集成 SDK 使用。

不允许使用公共后缀。例如, 您不能使用usa.gov或co.uk作为令牌域。

默认情况下, 仅Amazon WAF接受受保护资源的域的令牌。如果您在此列表中添加令牌域, 则Amazon WAF接受列表中所有域和关联资源域的令牌。有关更多信息, 请参阅[配置 Web ACL 令牌域列表 \(p. 138\)](#) :

15. 选择下一步。
16. 在“设置规则优先级”页面中, 选择规则和规则组并将其移Amazon WAF至要处理的顺序。Amazon WAF从列表顶部开始处理规则。保存 Web 时, ACL 会按照您列出的顺序为规则Amazon WAF分配数字优先级设置。有关更多信息, 请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#) :
17. 选择下一步。
18. 在配置指标页面中, 查看选项并应用所需的任何更新。您可以通过为多个来源提供相同的CloudWatch指标名称来合并这些指标。
19. 选择下一步。
20. 在 Review and create web ACL (审核和创建 Web ACL) 页面中, 检查您的定义。如果要更改任何区域, 请为该区域选择 Edit (编辑)。这将使您返回到 Web ACL 向导中的页面。进行任何更改, 然后在后续页面中选择 Next (下一步), 直到您返回 Review and create web ACL (审核和创建 Web ACL) 页面。
21. 选择 Create web ACL (创建 Web ACL)。您的新 Web ACL 将在 Web ACL 页面中列出。

编辑 Web ACL

要在 Web ACL 中添加或删除规则或更改配置设置, 请使用本页上的步骤访问 Web ACL。在更新 Web ACL Amazon WAF 时, 可以持续覆盖与 Web ACL 关联的资源。

生产流量风险

在为生产流量部署 Web ACL 的更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整更新后的规则，然后再启用这些规则。有关操作指南，请参阅 [测试和调整您的Amazon WAF保护措施 \(p. 200\)](#)。

编辑 Web ACL

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。

Note

由 Amazon Firewall Manager 管理的 Web ACL 具有以 FMManagedWebACL V2- 开头的名称。Firewall Manager 管理员在Firewall ManagerAmazon WAF 策略中对其进行管理。这些 Web ACL 可能包含指定为在 Web ACL 中最先运行和最后运行的规则组集，这两个规则组集分别位于由您添加和管理的任何规则或规则组的两端。第一个和最后一个规则组的名称分别以PREFMManaged-和POSTFMManaged-开头。有关这些策略的更多信息，请参阅 [Amazon WAF 策略 \(p. 444\)](#)。

4. 浏览 Web ACL 定义，并进行更改。这与您在创建 Web ACL 时使用的过程类似[创建 Web ACL \(p. 17\)](#)，但有以下例外。
 - 您在创建时设置的某些字段不可修改。例如，您无法更改 Web ACL 的名称，对于由Firewall Manager 管理的 Web ACL，您无法更改任何第一和最后一个规则组规范。
 - 您只能在编辑现有 Web ACL 时更改网页 ACL 的验证码和挑战免疫时间。您可以在 Web ACL 的“规则”选项卡下找到这些设置。有关这些设置的信息，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他Amazon WAF资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

管理 Web ACL 中的规则组行为

本节介绍修改在 Web ACL 中如何使用规则组的选项。此信息适用于所有规则组类型。将规则组添加到 Web ACL 后，可以将该规则组中各个规则的操作改写为Count任何其他有效的规则操作设置。您也可以将规则组的结果操作改写为Count，这对规则组内部评估规则的方式没有影响。

有关这些选项的信息，请参阅 [规则组中的操作替代 \(p. 14\)](#)。

覆盖规则组中的规则操作

对于 Web ACL 中的每个规则组，您可以针对部分或全部规则覆盖所含规则的操作。

最常见的用例是重写规则操作Count来测试新的或更新的规则。如果您启用了指标，则您会收到每条规则的计数指标，并将其改写为计数。有关测试的更多信息，请参阅[测试和调整您的Amazon WAF保护措施 \(p. 200\)](#)。

覆盖规则组中的规则操作

在将规则组添加到 Web ACL 或更高版本时，可以进行这些更改。这些说明适用于已添加到 Web ACL 的规则组。有关此选项的其他信息，请访问[规则操作替代规则 \(p. 14\)](#)。

1. 编辑Web ACL。
2. 在 Web ACL 页面规则选项卡中，选择规则组，然后选择编辑。
3. 在规则组的规则部分中，根据需要管理操作设置。
 - 所有规则-要为规则组中的所有规则设置替代操作，请打开“覆盖所有规则操作”下拉列表并选择覆盖操作。要移除所有规则的覆盖，请选择“移除所有覆盖”。
 - 单一规则-要为单个规则设置覆盖操作，请打开该规则的下拉列表并选择覆盖操作。要删除规则的覆盖，请打开该规则的下拉列表并选择移除覆盖。
4. 完成更改后，选择 Save Rule。规则操作和替代操作设置在规则组页面中列出。

以下示例 JSON 列表显示了 Web ACL 中的规则组声明，该声明将规则操作替换Count为CategoryVerifiedSearchEngine和规则CategoryVerifiedSocialMedia。在 JSON 中，您可以通过为每个单独的规则提供一个RuleActionOverrides条目来覆盖所有规则操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryVerifiedSearchEngine"
        },
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryVerifiedSocialMedia"
        }
      ],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

将规则组的评估结果改写为Count

您可以改写规则组评估产生的操作，而无需更改规则组中规则的配置或评估方式。此选项不常用。如果规则组中的任何规则导致匹配，则此替代会将规则组的结果操作设置为Count。

添加或编辑规则组时，可以在 Web ACL 中覆盖该规则组生成的操作。在控制台中，打开规则组的“覆盖规则组操作-可选”窗格并启用覆盖。在规则组语句OverrideAction中设置的 JSON 中，如以下示例列表中所示：

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet"
    }
  },
  "OverrideAction": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

将 Web ACL 与 Amazon 资源关联或取消关联

您可以使用 Amazon WAF 在 Web ACLs 和您的资源之间创建以下关联：

- 将区域 Web ACL 与下面列出的任何区域资源相关联。对于此选项，Web ACL 必须与您的资源位于相同区域中。
 - Amazon API Gateway
 - Application Load Balancer
 - Amazon AppSync GraphQL API
 - Amazon Cognito 用户池
 - Amazon App Runner 服务
- 将全球网络 ACL 与亚马逊 CloudFront 发行版相关联。全局 Web ACL 将具有美国东部（弗吉尼亚北部）区域的硬编码区域。

在创建或更新 CloudFront 分配本身时，也可以将 Web ACL 与分配相关联。有关信息，请参阅《亚马逊 CloudFront 开发者指南》中的[“使用 Amazon WAF 控制对您的内容的访问权限”](#)。

对多重关联的限制

您可以根据以下限制将单个 Web ACL 与一个或多个 Amazon 资源关联：

- 您只能将每个 Amazon 资源与一个 Web ACL 关联。Web ACL 和 Amazon 资源之间的关系是 one-to-many。
- 您可以将 Web ACL 与一个或多个 CloudFront 分配相关联。您无法将与 CloudFront 分配关联的 Web ACL 与任何其他 Amazon 资源类型相关联。

其他限制

以下附加限制适用于 Web ACL 关联：

- 您只能将 Web ACL 关联到其中的 Application Load Balancer Amazon Web Services 区域。例如，您无法将 Web ACL 关联到已开启的 Application Load Balancer Amazon Outposts。

- 您无法将 Amazon Cognito 用户池与使用 Amazon WAF 欺诈控制账户接管预防 (ATP) 托管规则组的 Web ACL 关联AWSManagedRulesATPRuleSet。有关防止账户接管的信息，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) \(p. 155\)](#)。

生产流量风险

在为生产流量部署 Web ACL 之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后在计数模式下使用生产流量测试和调整规则，然后再启用这些规则。有关操作指南，请参阅[测试和调整您的Amazon WAF保护措施 \(p. 200\)](#)。

将 Web ACL 与Amazon资源相关联

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与资源关联的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在关联Amazon资源选项卡上，选择添加Amazon资源。
5. 出现提示时，选择资源类型，选择要关联的资源旁边的单选按钮，然后选择 Add (添加)。

取消 Web ACL 与Amazon资源的关联

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与资源取消关联的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在关联Amazon资源选项卡上，选择要取消此 Web ACL 与之关联的资源，然后选择取消关联。控制台会打开一个确认对话框。确认您选择解除 Web ACL 与Amazon资源的关联。

删除Web ACL

要删除 Web ACL，首先取消 Web ACL 与所有 Amazon 资源的关联。请执行以下过程。

删除 Web ACL

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Web ACL。
3. 选择要删除的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在关联Amazon资源选项卡上，对于每个关联资源，选择资源名称旁边的单选按钮，然后选择取消关联。这将使 Web ACL 与您的 Amazon 资源取消关联。
5. 在导航窗格中，选择 Web ACL。
6. 选择要删除的 Web ACL 旁边的单选按钮，然后选择 Remove (删除)。

规则组

规则组是一组可重复使用的规则，您可以将其添加到 Web ACL 中。有关 Web ACL 的更多信息，请参阅[Web ACL \(Web ACL \) \(p. 11\)](#)。

规则组分为以下主要类别：

- 托管规则组，由Amazon管理规则和Amazon Web Services Marketplace卖家为您创建和维护。
- 您自己的规则组，将由您自己创建和维护列表。
- 由 Shield Advanced 等其他服务拥有和管理的规则组。Amazon Firewall Manager

规则组和 Web ACL 之间的区别

规则组和 Web ACL 都包含规则，这两个地方的定义方式相同。规则组与 Web ACL 的区别如下：

- 规则组不能包含规则组参考语句。
- 通过向每个 Web ACL 添加规则组参考语句，可以在多个 Web ACL 中重复使用单个规则组。您不能重复使用 Web ACL。
- 规则组没有默认操作。在 Web ACL 中，您可以为包含的每个规则或规则组设置默认操作。规则组或 Web ACL 中的每个规则都定义了一个操作。
- 您不直接将规则组与Amazon资源相关联。要使用规则组保护资源，请在 Web ACL 中使用规则组。
- Web ACL 的系统定义的最大容量为 1,500 个 Web ACL 容量单位 (WCU)。每个规则组都有一个 WCU 设置，必须在创建时进行设置。您可以使用此设置来计算使用规则组会增加到 Web ACL 的额外容量要求。有关WCU的更多信息，请参阅[Amazon WAFWeb ACL 容量单位 \(WCU \) \(p. 6\)](#)。

有关规则的信息，请参阅 [规则 \(p. 80\)](#)。

本部分提供创建和管理自己的规则组的指导，介绍了可供您使用的托管规则组，并提供有关使用托管规则组的指导。

主题

- [托管规则组 \(p. 24\)](#)
- [管理您自己的规则组 \(p. 78\)](#)
- [其他服务提供的规则组 \(p. 79\)](#)

托管规则组

托管规则组是预定义 ready-to-use 规则的集合，Amazon由Amazon Web Services Marketplace卖家为您编写和维护。基本Amazon WAF定价适用于您对所有托管规则组的使用。有关Amazon WAF定价信息，请参阅[Amazon WAF定价](#)。

- 除基本费用外，Amazon WAF机器人控制和Amazon WAF欺诈控制账户接管预防 (ATP) 的Amazon托管规则组可收取额外Amazon WAF费用。有关定价的详细信息，请参阅 [Amazon WAF 定价](#)。
- 所有其他Amazon托管规则组均可供Amazon WAF客户使用，无需额外付费。
- Amazon Web Services Marketplace 托管规则组 可通过 Amazon Web Services Marketplace 进行订阅。这些规则组均由Amazon Web Services Marketplace卖家拥有和管理。有关使用托管Amazon Web Services Marketplace管规则组的定价信息，请联系Amazon Web Services Marketplace卖家。

一些托管规则组旨在帮助保护特定类型的 Web 应用程序WordPress，例如 Joomla 或 PHP。其他一些则针对已知威胁或常见的网络应用程序漏洞提供广泛的保护，包括 [OWASP前十名](#)中列出的某些漏洞。如果您需要符合监管合规性（如 PCI 或 HIPAA），您可以使用托管规则组来满足 Web 应用程序防火墙要求。

自动更新

随时了解不断变化的威胁情形会非常耗时且成本高昂。在实施和使用托管规则组时，托管规则组可以为您节省时间Amazon WAF。当出现新的漏洞Amazon和威胁时，许多Amazon Web Services Marketplace卖家会自动更新托管规则组并提供新版本的规则组。

在某些情况下，Amazon 由于它参与了许多私人披露社区，因此会在公开披露之前收到有关新漏洞的通知。在这种情况下，甚至 Amazon 可以在新威胁广为人知之前就更新 Amazon 托管规则组并为您部署它们。

限制访问托管规则组中的规则

每个托管规则组都全面描述了其旨在防范的攻击和漏洞类型。为了保护规则组提供者的知识产权，您无法查看规则组中各个规则的所有详细信息。此限制还有助于避免恶意用户设计专门避开已发布规则的威胁。

主题

- [使用托管规则组进行版本管理 \(p. 25\)](#)
- [使用托管规则组 \(p. 26\)](#)
- [Amazon 的托管规则 Amazon WAF \(p. 32\)](#)
- [Amazon Web Services Marketplace 托管规则组 \(p. 76\)](#)

使用托管规则组进行版本管理

许多托管规则组提供商在新版本的规则组中更新了规则组的选项和功能。通常，托管规则组的特定版本是静态的。有时，提供商可能需要更新托管规则组的部分或全部现有版本，例如，以应对新出现的安全威胁。

将托管规则组添加到 Web ACL 时，如果规则组支持版本控制，则可以选择让提供商管理您使用的版本，也可以自己管理版本设置。

找不到你想要的版本？

如果您在规则组的版本列表中看不到某个版本，则该版本可能已计划到期或已经过期。在预定版本到期后，Amazon WAF 不再允许您为规则组选择该版本。

Amazon 托管规则组的版本控制和 SNS 通知

Amazon 托管规则组均提供版本控制和 SNS 更新通知，IP 信誉、机器人控制和防止账户接管的规则组除外。

提供通知的 Amazon 托管规则组都使用相同的 SNS 主题 Amazon 资源名称 (ARN)。

主题

- [托管规则组的版本生命周期 \(p. 25\)](#)
- [处理托管规则组版本的最佳实践 \(p. 26\)](#)

托管规则组的版本生命周期

提供商处理托管规则组静态版本的以下生命周期阶段：

- 发布和更新-托管规则组提供商通过发送到 Amazon Simple Notification Service (Amazon SNS) 主题的通知，宣布其托管规则组的即将推出和新的静态版本。提供商还可能使用该主题来传达有关其规则组的其他重要信息，例如所需的紧急更新。

您可以订阅规则组的主题并配置接收通知的方式。有关更多信息，请参阅 [获取有关新版本和更新的通知 \(p. 29\)](#)。

- 过期安排-托管规则组提供商将规则组的旧版本安排为过期。计划过期的版本无法添加到 Web ACL 规则中。在某个版本预定到期后，使用亚马逊的倒计时指标 Amazon WAF 跟踪到期时间 CloudWatch。

您可以对中的指标设置警报 CloudWatch，以跟踪您正在使用的版本的到期时间。这使您有时间测试新版本，并在倒计时完成之前离开即将过期的版本。有关更多信息，请参阅 [追踪版本到期 \(p. 30\)](#)：

- 版本过期 — 当版本过期时，规则组提供者决定如何管理仍在使用过期版本的 Web ACL 的过期时间：
 - 对于 Amazon 托管规则组，Amazon WAF 将使用过期版本的任何 Web ACL 移至规则组的默认版本。

- 对于 Amazon Web Services Marketplace 规则组，提供商决定如何处理过期问题。向您的托管规则组提供商询问信息。

处理托管规则组版本的最佳实践

使用托管规则组时，请遵循此版本控制最佳实践指南。

在 Web ACL 中使用托管规则组时，可以选择使用该规则组的特定静态版本，也可以选择使用默认版本：

- 默认版本 — Amazon WAF 始终将默认版本设置为提供者当前推荐的静态版本。当提供商更新其推荐的静态版本时，Amazon WAF 会自动更新 Web ACL 中规则组的默认版本设置。

使用托管规则组的默认版本时，最佳做法是执行以下操作：

- 订阅通知 — 订阅有关规则组更改的通知，并密切关注这些更改。大多数提供商会发送有关新静态版本和默认版本变更的高级通知。它们允许您在将默认版本 Amazon 切换到新的静态版本之前检查该版本的效果。有关更多信息，请参阅 [获取有关新版本和更新的通知 \(p. 29\)](#)。
- 在 @@ 将默认版本设置为静态版本设置之前，查看静态版本设置的效果并根据需要进行调整 — 在将默认设置为新的静态版本之前，请查看静态版本对监视和管理您的 Web 请求的影响。新的静态版本可能有新的规则需要审查。如果您需要修改规则组的使用方式，请注意误报或其他意外行为。例如，您可以将规则设置为计数，以阻止它们在弄清楚如何处理新行为的同时阻止流量。有关更多信息，请参阅 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。
- 静态版本-如果您选择使用静态版本，则在准备采用新版本的规则组时，必须手动更新版本设置。

当您使用托管规则组的静态版本时，最佳做法是执行以下操作：

- 使您的版本保持最新状态-使您的托管规则组尽可能接近最新版本。发布新版本时，对其进行测试，根据需要调整设置，并及时实施。有关测试的信息，请参阅 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。
- 订阅通知-订阅有关规则组更改的通知，这样您就可以知道您的提供商何时发布新的静态版本。大多数提供商会提前通知版本变更。此外，您的提供商可能需要更新您正在使用的静态版本来填补安全漏洞或其他紧急原因。如果你订阅了提供商的通知，你就会知道发生了什么。有关更多信息，请参阅 [获取有关新版本和更新的通知 \(p. 29\)](#)。
- 避免版本过期-不要让静态版本在使用时过期。提供商对过期版本的处理可能有所不同，可能包括强制升级到可用版本或其他可能产生意外后果的更改。跟踪到 Amazon WAF 指标并设置警报，让您有足够的天数成功升级到支持的版本。有关更多信息，请参阅 [追踪版本到期 \(p. 30\)](#)。

使用托管规则组

本节为访问和管理您的托管规则组提供指导。

将托管规则组添加到 Web ACL 时，您可以选择与自己的规则组相同的配置选项以及其他设置。

在 Web ACL 中添加和编辑规则的过程中，您可以通过控制台访问托管规则组信息。通过 API 和命令行界面 (CLI)，您可以直接请求托管规则组信息。

在 Web ACL 中使用托管规则组时，可以编辑以下设置：

- 版本-仅当规则组已版本化时才可用。有关更多信息，请参阅 [使用托管规则组进行版本管理 \(p. 25\)](#)。
- 覆盖规则操作-您可以将规则组中规则的操作改写为任何操作。将它们设置为 Count 对于在使用规则组管理 Web 请求之前对其进行测试很有用。有关更多信息，请参阅 [规则操作替代规则 \(p. 14\)](#)。
- Scope-down 语句-您可以添加范围缩小语句，以筛选出不想在规则组中评估的 Web 请求。有关更多信息，请参阅 [范围缩小声明 \(p. 110\)](#)。
- 覆盖规则组操作 — 您可以覆盖由规则组评估所产生操作，并将其设置为 onCount y。此选项不常用。它不会改变规则组中规则的 Amazon WAF 评估方式。有关更多信息，请参阅 [将规则组操作改为 Count \(p. 16\)](#)。

编辑 Web ACL 中的托管规则组设置

- 控制台
 - (选项) 将托管规则组添加到 Web ACL 时, 可以选择“编辑”来查看和编辑设置。
 - (选项) 将托管规则组添加到 Web ACL 后, 从 Web ACL 页面选择刚才创建的 Web ACL。这会使您转至 Web ACL 编辑页面。
 - 选择 Rules。
 - 选择规则组, 然后选择“编辑”以查看和编辑设置。
- API 和 CLI — 在控制台之外, 您可以在创建和更新 Web ACL 时管理托管规则组设置。

检索托管规则组列表

可供您在 Web ACL 中使用的托管规则组如下：

- 所有 Amazon 托管规则组。
- 您已订阅的 Amazon Web Services Marketplace 规则组。

Note

有关订阅 Amazon Web Services Marketplace 规则组的信息, 请参阅 [Amazon Web Services Marketplace 托管规则组 \(p. 76\)](#)。

当您检索托管规则组列表时, 返回的列表取决于您使用的接口：

- 控制台 — 通过控制台, 您可以查看所有托管 Amazon Web Services Marketplace 规则组, 包括您尚未订阅的规则组。对于您尚未订阅的内容, 该界面提供了一些链接, 您可以点击这些链接进行订阅。
- API 和 CLI — 在控制台之外, 您的请求仅返回可供您使用的规则组。

检索托管规则组列表

- 控制台 — 在创建 Web ACL 的过程中, 在添加规则和规则组页面上, 选择添加托管规则组。在顶层, 列出了提供商名称。展开每个提供者列表以查看托管规则组列表。对于版本化规则组, 此级别显示的信息适用于默认版本。当您添加托管规则组到 Web ACL 时, 控制台会根据命名方案 <Vendor Name>-<Managed Rule Group Name> 列出规则组。
- API —
 - `ListAvailableManagedRuleGroups`
- 命令行界面 —
 - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

检索托管规则组中的规则

您可以检索托管规则组中的规则列表。API 和 CLI 调用返回规则规范, 您可以在 JSON 模型中引用或通过这些规范 Amazon CloudFormation。

检索托管规则组中的规则列表

- 控制台
 - (选项) 将托管规则组添加到 Web ACL 时, 可以选择“编辑”来查看规则。
 - (选项) 将托管规则组添加到 Web ACL 后, 从 Web ACL 页面选择刚才创建的 Web ACL。这会使您转至 Web ACL 编辑页面。
 - 选择 Rules。

- 选择要查看其规则列表的规则组，然后选择 Edit (编辑)。Amazon WAF 随即显示该规则组中的规则列表。
- API —DescribeManagedRuleGroup
- 命令行界面 —aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>

检索托管规则组的可用版本

托管规则组的可用版本是尚未计划过期的版本。该列表指出了哪个版本是该规则组的当前默认版本。

检索托管规则组的可用版本列表

- 控制台
 - (选项) 将托管规则组添加到 Web ACL 时，选择编辑以查看规则组的信息。展开“版本”下拉列表以查看可用版本列表。
 - (选项) 将托管规则组添加到 Web ACL 后，在 Web ACL 上选择“编辑”，然后选择并编辑该规则组规则。展开“版本”下拉列表以查看可用版本列表。
- API —
 - ListAvailableManagedRuleGroupVersions
- 命令行界面 —
 - aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>

通过控制台将托管规则组添加到 Web ACL

本指南适用于所有Amazon托管规则组和您订阅的Amazon Web Services Marketplace规则组。

生产流量风险

在为生产流量部署 Web ACL 的更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整更新后的规则，然后再启用这些规则。有关操作指南，请参阅 [测试和调整您的Amazon WAF保护措施 \(p. 200\)](#)。

通过控制台将托管规则组添加到 Web ACL

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中选择 Web ACL。
3. 在 Web ACL 页面中，从 Web ACL 列表中选择要向其添加规则组的 ACL。这会将您带到单个 Web ACL 的页面。
4. 在 Web ACL 的页面中，选择“规则”选项卡。
5. 在“规则”窗格中，选择添加规则，然后选择添加托管规则组。
6. 在添加托管规则组页面中，扩展规则组供应商的选择范围，以查看可用规则组列表。
7. 对于每个要添加的规则组，请选择 Web ACL。如果要更改规则组的 Web ACL 配置，请选择编辑，进行更改，然后选择保存规则。有关选项的信息，请参阅上的版本控制指南[使用托管规则组进行版本管理 \(p. 25\)](#)和在 Web ACL 中使用托管规则组的指南，网址为[托管规则组语句 \(p. 92\)](#)。
8. 在添加托管规则组页面的底部，选择添加规则。
9. 在设置规则优先级页面中，根据需要调整规则的运行顺序，然后选择保存。有关更多信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)：

在您的 Web ACL 页面中，您添加的托管规则组列在“规则”选项卡下。

在将您的 Amazon WAF 保护措施用于生产流量之前，请先测试和调整对保护措施所做的任何更改。有关信息，请参阅 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他 Amazon WAF 资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

收到有关托管规则组新版本和更新的通知

托管规则组提供商使用 SNS 通知来宣布规则组变更，例如即将发布的新版本和紧急安全更新。

如何订阅 SNS 通知

要订阅规则组的通知，您可在美国东部（弗吉尼亚北部）区域 us-east-1 创建针对规则组的 Amazon SNS 主题 ARN。

有关如何订阅的信息，请参阅 [Amazon Simple Notifince 开发人员指南](#)。

Note

仅在 us-east-st-1 区域创建对 SNS 主题的订阅。

在哪里可以找到托管规则组的 Amazon SNS 主题 ARN

Amazon 托管规则组使用单个 SNS 主题 ARN，因此您可以从其中一个规则组检索主题 ARN 并订阅该主题 ARN 以获取所有提供 SNS 通知的 Amazon 托管规则组的通知。

- 控制台
 - （选项）将托管规则组添加到 Web ACL 时，选择编辑以查看规则组的信息，其中包括规则组的 Amazon SNS 主题 ARN。
 - （选项）将托管规则组添加到 Web ACL 后，在 Web ACL 上选择编辑，然后选择并编辑规则组规则以查看该规则组的 Amazon SNS 主题 ARN。
- API — DescribeManagedRuleGroup
- 命令行界面 — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Amazon 托管规则组的版本控制和 SNS 通知

Amazon 托管规则组均提供版本控制和 SNS 更新通知，IP 信誉、机器人控制和防止账户接管的规则组除外。

提供通知的 Amazon 托管规则组都使用相同的 SNS 主题 Amazon 资源名称 (ARN)。

对于影响保护的部署，例如对默认版本的更改，Amazon 提供 SNS 通知，通知您已计划的部署并告知您部署何时开始。对于不影响保护的部署，例如候选版本和静态版本部署，Amazon 可能会在部署开始后甚至在部署完成后通知您。完成新静态版本的部署后，在变更日志 [Amazon 托管规则变更日志 \(p. 68\)](#) 和文档历史记录页面中 Amazon 更新本指南 [文档历史记录 \(p. 525\)](#)。有关为每种部署类型提供的通知的更多信息，请参阅 [版本化 Amazon 托管规则组的部署 \(p. 61\)](#)。

要接收有关Amazon托管规则组的所有更新，Amazon请订阅本指南任何 HTML 页面上的 RSS 提要，并订阅 Amazon托管规则组的 SNS 主题。

Amazon SNS 通知中的字段始终包括主题、消息和 MessageAttributes。其他字段取决于消息的类型以及通知所针对的托管规则组。下面是一个的通知列表示例AWSManagedRulesCommonRuleSet。

```
{
  "Type": "Notification",
  "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
  "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
  "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
  "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated the regex specification in this version to improve protection coverage, adding protections against insecure deserialization. For details about this change, see http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
  "Timestamp": "2021-08-24T11:12:19.810Z",
  "SignatureVersion": "1",
  "Signature": "EXAMPLEHXgJm...",
  "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-f3ecfb7224c7233fe7bb5f59f96de52f.pem",
  "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-west-2:123456789012:MyTopic&Token=2336412f37...",
  "MessageAttributes": {
    "major_version": {
      "Type": "String",
      "Value": "v1"
    },
    "managed_rule_group": {
      "Type": "String",
      "Value": "AWSManagedRulesCommonRuleSet"
    }
  }
}
```

有关 Amazon SNS 通知格式以及如何筛选您收到的通知的一般信息，请参阅 [《亚马逊简单通知服务开发者指南》中的解析消息格式和 Amazon SNS 订阅筛选政策](#)。

跟踪规则组的版本到期时间

如果您使用规则组的特定版本，请确保不要在过期日期之后继续使用该版本。

Tip

如果您通过 Amazon SNS 跟踪托管规则组即将发生的更改，您将收到有关新版本和推荐版本的通知。如果您定期测试并迁移到新版本，则可以提前防范旧版本的任何过期活动。您还将受益于规则组的最新保护。有关通知的信息，请参阅[获取有关新版本和更新的通知 \(p. 29\)](#)。

如果您使用的版本已过期，则会Amazon WAF阻止对您正在使用规则组的 Web ACL 进行修改。在您将规则组更新到可用版本或将其从 Web ACL 中删除之前，该封禁将一直保持不变。

托管规则组的过期处理取决于规则组提供商。对于Amazon Managed Rules 规则组，版本自动更改为规则组的默认版本。对于Amazon Web Services Marketplace规则组，请咨询提供商如何处理过期问题。

要监控托管规则组的到期日程安排，请从Amazon WAF以下地址跟踪亚马逊 CloudWatch 过期指标：

- Metric name (指标名称) : DaysToExpiry
- 公制维度 : RegionManagedRuleGroup、Vendor、和Version

在 Amazon 中找到您的托管规则组的指标 CloudWatch 并对其设置警报，以便及时通知您切换到规则组的更新版本。有关使用亚马逊 CloudWatch 指标和配置警报的信息，请参阅[亚马逊 CloudWatch 用户指南](#)。

当提供者创建新版本的规则组时，它会设置该版本的预测生命周期。虽然版本未计划过期，但指标值设置为预测生命周期设置，在中 CloudWatch，您将看到该指标的固定值。提供商计划指标过期后，指标值每天都会减少，直到到期当天达到零。

如果您的 Web ACL 中有用于评估流量的托管规则组，您将获得相应的指标。该指标不适用于未使用的规则组。

JSON 和 YAML 中的托管规则组配置示例

API 和 CLI 调用返回可在 JSON 模型中或通过 Amazon CloudFormation 引用的托管规则组中所有规则的列表。

JSON

您可以使用 JSON 在规则语句中引用和修改托管规则组。以下列表显示了 JSON 格式的 Amazon 托管规则组。AWSManagedRulesCommonRuleSet 该 RuleActionOverrides 规范列出了一条规则，该规则的操作已被重写 Count。

```
{
  "Name": "AWS-AWSManagedRulesCommonRuleSet",
  "Priority": 0,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesCommonRuleSet",
      "RuleActionOverrides": [

        {

          "ActionToUse": {

            "Count": {}

          },

          "Name": "NoUserAgent_HEADER"

        }

      ],
      "ExcludedRules": []
    }
  },
  "OverrideAction": {
    "None": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
  }
}
```

YAML

您可以使用 Amazon CloudFormation YAML 模板在规则语句中引用和修改托管规则组。以下列表显示了 Amazon CloudFormation 模板中的“Amazon 托管规则”规则组。AWSManagedRulesCommonRuleSet 该 RuleActionOverrides 规范列出了一条规则，该规则的操作已被重写 Count。

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
```



```
VendorName: AWS
Name: AWSManagedRulesCommonRuleSet
RuleActionOverrides:
- ActionToUse:
  Count: {}
  Name: NoUserAgent_HEADER
ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

Amazon的托管规则Amazon WAF

AmazonManaged Rules forAmazon WAF 是一项托管服务，可针对常见的应用程序漏洞或其他有害流量提供保护。您可以选择从每个 Web ACL 的Amazon管理规则中选择一个或多个规则组，但不得超过最大 Web ACL 容量单位 (WCU) 限制。

减少误报并测试规则组更改

在生产环境中使用任何托管规则组之前，请根据中的指导在非生产环境中对其进行测试[测试和调整您的 Amazon WAF保护措施 \(p. 200\)](#)。将规则组添加到 Web ACL、测试新版本的规则组以及每当规则组未按您的需要处理您的 Web 流量时，请遵循测试和调整指南。

责任共担

Amazon托管规则旨在保护您免受常见的 Web 威胁的攻击。根据文档进行使用时，Amazon托管规则组将为您的应用程序添加另一层安全性。但是，Amazon托管规则组并非用于取代您的安全责任，这些责任由您所选择的Amazon资源决定。请参阅[责任共担模式](#)，以确保妥善保护 Amazon 中的资源。

Amazon托管规则规则组列表

我们发布的有关 ManagAmazon ed Rules 规则组规则的信息旨在为您提供足够的信息来使用规则，同时不提供不良行为者可能用来规避规则的信息。如果您需要比本文档中更多的信息，请联系[Amazon Web Services Support中心](#)。

本节介绍Amazon托管规则组的最新版本。当您托管规则组添加到 Web ACL 时，您可以在控制台上查看这些规则组。通过 API，您可以通过调用检索此列表以及您订阅的Amazon Web Services Marketplace托管规则组ListAvailableManagedRuleGroups。

Note

有关检索“Amazon托管规则”规则组版本的信息，请参阅[检索托管规则组的可用版本 \(p. 28\)](#)。

所有 MAmazon anaged Rules 规则组都支持标签，本节中的规则列表包括标签规范。您可以通过调用 API 检索托管规则组的标签DescribeManagedRuleGroup。标签在响应的AvailableLabels属性中列出。有关标签的信息，请参见[网络请求上的标签 \(p. 123\)](#)。

在将您的Amazon WAF保护措施用于生产流量之前，请先测试和调整对保护措施所做的任何更改。有关信息，请参阅 [测试和调整您的Amazon WAF保护措施 \(p. 200\)](#)。

Amazon托管规则规则组

- [基准规则组 \(p. 33\)](#)
 - [核心规则集 \(CRS\) 托管规则组 \(p. 33\)](#)
 - [管理员保护管理规则组 \(p. 38\)](#)
 - [已知的错误输入管理规则组 \(p. 38\)](#)
- [使用案例特定规则组 \(p. 41\)](#)
 - [SQL 数据库管理规则组 \(p. 41\)](#)

- [Linux 操作系统托管规则组 \(p. 42\)](#)
- [POSIX 操作系统管理的规则组 \(p. 43\)](#)
- [Windows 操作系统托管规则组 \(p. 44\)](#)
- [PHP 应用程序管理规则组 \(p. 46\)](#)
- [WordPress 应用程序管理规则组 \(p. 47\)](#)
- [IP 声誉规则组 \(p. 48\)](#)
 - [亚马逊 IP 信誉列表管理规则组 \(p. 48\)](#)
 - [匿名 IP 列表管理规则组 \(p. 48\)](#)
- [Amazon WAF 机器人控制规则组 \(p. 49\)](#)
 - [机器人控制规则列表 \(p. 50\)](#)
- [Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)
 - [账户收购防范规则列表 \(p. 57\)](#)

基准规则组

基准托管规则组可针对多种常见威胁提供一般保护。请选择以下一个或多个规则组以便为您的资源建立基准保护。

核心规则集 (CRS) 托管规则组

VendorName:AWS, 名称:AWSManagedRulesCommonRuleSet, WCU: 700

核心规则集 (CRS) 规则组包含通常适用于 Web 应用程序的规则。这可以保护人们免受各种漏洞的利用，包括OWASP出版物（例如 [OWASP Top 10](#)）中描述的一些高风险和常见漏洞。请考虑将此规则组用于任何 Amazon WAF 使用案例。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令 [DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
NoUserAgent_HEADER	检查缺少 HTTPUser-Agent 标头的请求。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:NoUserAgent_Header
UserAgent_BadBots_HEADER	检查是否存在表明请求是坏机器人的常见User-Agent标头值。示例模式包括 nessus 和 nmap。有关机器人管理的信息，另请参阅 Amazon WAF 机器人控制规则组 (p. 49) 。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:BadBots_Header
SizeRestrictions_QUERYSTRING	检查是否有超过 2,048 字节的 URI 查询字符串。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:SizeRestrictions_QueryString

Rule name (规则名称)	描述和标注分类
SizeRestrictions_Cookie_HEADER	检查是否有超过 10,240 字节的 cookie 标头。 Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header
SizeRestrictions_BODY	检查超过 8 KB (8,192 字节) 的请求正文。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:SizeRestrictions_Body
SizeRestrictions_URI_PATH	检查超过 1024 字节的 URI 路径。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:SizeRestrictions_URI_Path
EC2MetadataSSRF_BODY	检查是否有人试图从请求正文中泄露 Amazon EC2 元数据。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:EC2MetadataSSRF_Body
EC2MetadataSSRF_COOKIE	检查是否有人试图从请求 Cookie 中泄露 Amazon EC2 元数据。 Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:EC2MetadataSSRF_Cookie

Rule name (规则名称)	描述和标注分类
EC2MetaDataSSRF_URI_PATH	检查是否有人试图从请求 URI 路径中泄露 Amazon EC2 元数据。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_URI_Path
EC2MetaDataSSRF_QUERY_ARGUMENTS	检查是否有人尝试从请求查询参数中提取 Amazon EC2 元数据。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments
GenericLFI_QUERY_ARGUMENTS	检查查询参数中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 ../../ 的技术尝试遍历路径。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:GenericLFI_QueryArguments
GenericLFI_URI_PATH	检查 URI 路径中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 ../../ 的技术尝试遍历路径。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:GenericLFI_URI_Path
GenericLFI_BODY	检查请求正文中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 ../../ 的技术尝试遍历路径。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:GenericLFI_Body
RestrictedExtensions_URI_PATH	检查其 URI 路径是否包含无法安全读取或运行的系统文件扩展名的请求。示例模式包括类似于 .log 和 .ini 的扩展名。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:RestrictedExtensions_URI_Path

Rule name (规则名称)	描述和标注分类
RestrictedExtensions_QUERYARGUMENTS	检查其查询参数是否包含无法安全读取或运行的系统文件扩展名的请求。示例模式包括类似于 .log 和 .ini 的扩展名。 规则操作 : Block 标签 : awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	检查所有查询参数的值, 是否有人试图通过嵌入包含 IPv4 地址的 URL 来利用 Web 应用程序中的 RFI (远程文件包含)。示例包括 http://、https://ftp://、和 file:// 等模式 ftps://, 在尝试利用漏洞时使用 IPv4 主机标头。 规则操作 : Block 标签 : awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments
GenericRFI_BODY	检查请求正文是否有人企图通过嵌入包含 IPv4 地址的 URL 来利用 Web 应用程序中的 RFI (远程文件包含)。示例包括 http://、https://ftp://、和 file:// 等模式 ftps://, 在尝试利用漏洞时使用 IPv4 主机标头。 Warning 此规则仅检查请求正文的前 8 KB, 并使用该 Continue 选项处理超大内容。有关更多信息, 请参阅 请求组件的超大处理 (p. 107) : 规则操作 : Block 标签 : awswaf:managed:aws:core-rule-set:GenericRFI_Body
GenericRFI_URI_PATH	检查 URI 路径是否有人企图通过嵌入包含 IPv4 地址的 URL 来利用 Web 应用程序中的 RFI (远程文件包含)。示例包括 http://、https://ftp://、和 file:// 等模式 ftps://, 在尝试利用漏洞时使用 IPv4 主机标头。 规则操作 : Block 标签 : awswaf:managed:aws:core-rule-set:GenericRFI_URIPath

Rule name (规则名称)	描述和标注分类
CrossSiteScripting_COOKIE	使用内置功能检查 cookie 标头的值以了解常见的跨站脚本 (XSS) 模式Amazon WAF跨站点脚本攻击规则语句 (p. 101)。示例模式包括类似于 <code><script>alert("hello")</script></code> 的脚本。 Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： Note Amazon WAF日志中的规则匹配详细信息未填充此规则组的版本 2.0。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_Cookie
CrossSiteScripting_QUERYARGUMENTS	使用内置函数检查常见跨站脚本 (XSS) 模式的查询参数值Amazon WAF跨站点脚本攻击规则语句 (p. 101)。示例模式包括类似于 <code><script>alert("hello")</script></code> 的脚本。 Note Amazon WAF日志中的规则匹配详细信息未填充此规则组的版本 2.0。 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments
CrossSiteScripting_BODY	使用内置函数检查请求正文中常见的跨站脚本 (XSS) 模式Amazon WAF跨站点脚本攻击规则语句 (p. 101)。示例模式包括类似于 <code><script>alert("hello")</script></code> 的脚本。 Note Amazon WAF日志中的规则匹配详细信息未填充此规则组的版本 2.0。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:core-rule-set:CrossSiteScripting_Body

Rule name (规则名称)	描述和标注分类
CrossSiteScripting_URIPath	使用内置函数检查常见跨站脚本 (XSS) 模式的 URI 路径值Amazon WAF跨站脚本攻击规则语句 (p. 101)。示例模式包括类似于 <code><script>alert("hello")</script></code> 的脚本。 Note Amazon WAF 日志中的规则匹配详细信息未填充此规则组的版本 2.0。 规则操作 : Block 标签 : awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath

管理员保护管理规则组

VendorName:AWS, 名称:AWSManagedRulesAdminProtectionRuleSet, WCU: 100

管理保护规则组包含允许您阻止对公开的管理页面进行外部访问的规则。如果您运行第三方软件，或者希望降低恶意人员获取您的应用程序的管理访问权限的风险，该规则组可能非常有用。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令[DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
AdminProtection_URIPath	检查通常为管理 Web 服务器或应用程序而保留的 URI 路径。示例模式包括 <code>sqlmanager</code>。 规则操作 : Block 标签 : awswaf:managed:aws:admin-protection:AdminProtection_URIPath

已知的错误输入管理规则组

VendorName:AWS, 名称:AWSManagedRulesKnownBadInputsRuleSet, WCU: 200

已知错误输入规则组包含用于阻止请求模式的规则，这些模式确认无效且与漏洞攻击或发现相关联。这可以帮助降低恶意行为者发现有漏洞的应用程序的风险。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令[DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
JavaDeserializationRCE_HEADER	检查 HTTP 请求标头的键和值，寻找表明 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。

Rule name (规则名称)	描述和标注分类
	示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。 Warning 此规则仅检查请求标头的前 8 KB 或前 200 个标头，以先达到限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header
JavaDeserializationRCE_BODY	检查请求正文中是否存在表示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。 示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body
JavaDeserializationRCE_URI_PATH	检查请求 URI 中是否存在表示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。 示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath
JavaDeserializationRCE_QUERYSTRING	检查请求查询字符串中是否存在表示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞 (CVE-2022-22963、CVE-2022-22965)。 示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami")。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString

Rule name (规则名称)	描述和标注分类
Host_localhost_HEADER	检查请求中的主机标头是否有指示本地主机的模式。示例模式包括 localhost。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Host_Localhost_Header
PROPFIND_METHOD	检查请求中用于 PROPFIND 的 HTTP 方法，这是一种类似于 HEAD 的方法，但具有泄漏 XML 对象的额外意图。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Propfind_Method
ExploitablePaths_URI_PATH	检查 URI 路径中是否有恶意方试图访问可利用的 Web 应用程序路径。示例模式包括类似于 web-inf 的路径。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:ExploitablePaths_URI_Path
Log4JRCE_HEADER	检查请求标头的密钥和值是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，并防止尝试远程执行代码 (RCE)。示例模式包括 <code>\${jndi:ldap://example.com/}</code>。 Warning 此规则仅检查请求标头的前 8 KB 或前 200 个标头，以先达到限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_Header
Log4JRCE_QUERYSTRING	检查查询字符串中是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105)，并防止尝试远程执行代码 (RCE)。示例模式包括 <code>\${jndi:ldap://example.com/}</code>。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_QueryString

Rule name (规则名称)	描述和标注分类
Log4JRCE_BODY	检查主体是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) , 并防止尝试远程执行代码 (RCE)。示例模式包括 <code>\${jndi:ldap://example.com/}</code>。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_Body
Log4JRCE_URI_PATH	检查 URI 路径中是否存在 Log4j 漏洞 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) , 并防止尝试远程执行代码 (RCE)。示例模式包括 <code>\${jndi:ldap://example.com/}</code>。 规则操作：Block 标签：aws:waf:managed:aws:known-bad-inputs:Log4JRCE_URIPath

使用案例特定规则组

使用案例特定规则组为许多不同的 Amazon WAF 使用案例提供增量保护。选择适用于您的应用程序的规则组。

SQL 数据库管理规则组

VendorName:AWS, 名称:AWSManagedRulesSQLiRuleSet, WCU: 200

SQL 数据库规则组包含阻止与 SQL 数据库攻击 (如 SQL 注入攻击) 相关的请求模式的规则。该规则组有助于防止远程注入未经授权的查询。如果应用程序与 SQL 数据库相连，请评估此规则组以便使用。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令[DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
SQLi_QUERYARGUMENTS	使用内置Amazon WAFSQL 注入攻击规则语句 (p. 99)的 (敏感度级别设置为Low) 检查所有查询参数的值，寻找与恶意 SQL 代码匹配的模式。 规则操作：Block 标签：aws:waf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	检查所有查询参数的值，以查找与恶意 SQL 代码匹配的模式。该规则检查的模式不在规则的涵盖范围内SQLi_QUERYARGUMENTS。

Rule name (规则名称)	描述和标注分类
	规则操作 : Block aws:waf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
SQLi_BODY	使用内置Amazon WAFSQL 注入攻击规则语句 (p. 99)的 (敏感度级别设置为Low) 检查请求正文中是否存在与恶意 SQL 代码匹配的模式。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作 : Block 标签 : aws:waf:managed:aws:sql-database:SQLi_Body
SQLiExtendedPatterns_BODY	检查请求正文中是否存在与恶意 SQL 代码匹配的模式。该规则检查的模式不在规则的涵盖范围内SQLi_BODY。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作 : Block aws:waf:managed:aws:sql-database:SQLiExtendedPatterns_Body
SQLi_COOKIE	使用内置Amazon WAFSQL 注入攻击规则语句 (p. 99)的 (敏感度级别设置为) 检查请求 Cookie 标头中是否存在与恶意 SQL 代码匹配的模式。Low Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作 : Block 标签 : aws:waf:managed:aws:sql-database:SQLi_Cookie

Linux 操作系统托管规则组

VendorName:AWS, 名称:AWSManagedRulesLinuxRuleSet, WCU: 200

Linux 操作系统规则组包含阻止请求模式的规则，这些请求模式与利用 Linux 特定漏洞（包括 Linux 特定的本地文件包含 (LFI) 攻击）相关。这可以帮助防止泄露文件或运行攻击者本不应有权访问的代码的攻击。如果应用程序的任何部分在 Linux 上运行，则应评估此规则组。您应将此规则组与 [POSIX 操作系统 \(p. 43\)](#) 规则组结合使用。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令 [DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
LFI_URIPATH	检查请求路径，以查找是否有恶意方试图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 规则操作：Block 标签：aws:waf:managed:aws:linux-os:LFI_URIPath
LFI_QUERYSTRING	检查 querystring 的值是否有人企图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 规则操作：Block 标签：aws:waf:managed:aws:linux-os:LFI_QueryString
LFI_HEADER	检查请求标头是否有人企图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 Warning 此规则仅检查请求标头的前 8 KB 或前 200 个标头，以先达到限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:linux-os:LFI_Header

POSIX 操作系统管理的规则组

VendorName:AWS, 名称:AWSManagedRulesUnixRuleSet, WCU: 100

POSIX 操作系统规则组包含的规则可阻止与利用 POSIX 和类似 POSIX 的操作系统特定漏洞（包括 Linux 特定的本地文件包含 (LFI) 攻击）相关的请求模式。这可以帮助防止泄露文件或运行攻击者本不应有权访问的代码的攻击。如果应用程序的任何部分在 POSIX 或类似 POSIX 的操作系统（包括 Linux、AIX、HP-UX、macOS、Solaris、FreeBSD 和 OpenBSD）上运行，则应评估此规则组。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令 [DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
UNIXShellCommandsVariables_QUERYARGUMENTS	检查所有查询参数的值，以查找是否有恶意方试图利用在 Unix 系统上运行的 Web 应用程序中的命令注入、LFI 和路径遍历漏洞。示例包括类似于 echo \$HOME 和 echo \$PATH 的模式。 规则操作：Block 标签：aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_QUERYARGUMENTS
UNIXShellCommandsVariables_BODY	检查请求正文，以查找是否有恶意方试图利用在 Unix 系统上运行的 Web 应用程序中的命令注入、LFI 和路径遍历漏洞。示例包括类似于 echo \$HOME 和 echo \$PATH 的模式。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:posix-os:UNIXShellCommandsVariables_BODY

Windows 操作系统托管规则组

VendorName:AWS, 名称:AWSManagedRulesWindowsRuleSet, WCU: 200

Windows 操作系统规则组包含阻止与利用 Windows 特定漏洞（例如远程执行 PowerShell 命令）相关的请求模式的规则。这有助于防止利用允许攻击者运行未经授权的命令或运行恶意代码的漏洞。如果应用程序的任何部分在 Windows 操作系统上运行，则应评估此规则组。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令 [DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
WindowsShellCommands_COOKIE	检查 Web 应用程序中请求的 cookie 标头中是否有 WindowsShell 命令注入尝试。匹配模式代表WindowsShell 命令。示例模式包括 nslookup和;cmd。 Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。

Rule name (规则名称)	描述和标注分类
	有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:windows-os:WindowsShellCommands_Cookie
WindowsShellCommands_QUERYARGUMENTS	检查 Web 应用程序中所有查询参数的值，以进行WindowsShell 命令注入尝试。匹配模式代表WindowsShell 命令。示例模式包括 nslookup和;cmd。 规则操作：Block 标签：aws:waf:managed:aws:windows-os:WindowsShellCommands_QueryArguments
WindowsShellCommands_BODY	检查请求正文中是否有 Web 应用程序中的WindowsShell 命令注入尝试。匹配模式代表 WindowsShell 命令。示例模式包括 nslookup和;cmd。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:windows-os:WindowsShellCommands_Body
PowerShellCommands_COOKIE	检查 Web 应用程序中请求的 cookie 标头中是否有 PowerShell 命令注入尝试。匹配模式代表 PowerShell 命令。例如，Invoke-Expression。 Warning 此规则仅检查请求 cookie 的前 8 KB 或前 200 个 Cookie，以先达到的限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:windows-os:PowerShellCommands_Cookie

Rule name (规则名称)	描述和标注分类
PowerShellCommands_QUERYARGUMENTS	检查 Web 应用程序中所有查询参数的值，以进行 PowerShell 命令注入尝试。匹配模式代表 PowerShell 命令。例如，Invoke-Expression。 规则操作：Block 标签：aws:waf:managed:aws:windows-os:PowerShellCommands_QueryArguments
PowerShellCommands_BODY	检查请求正文中是否有 Web 应用程序中的 PowerShell 命令注入尝试。匹配模式代表 PowerShell 命令。例如，Invoke-Expression。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:windows-os:PowerShellCommands_Body

PHP 应用程序管理规则组

VendorName:AWS, 名称:AWSManagedRulesPHPRuleSet, WCU: 100

PHP 应用程序规则组包含阻止请求模式的规则，这些请求模式与利用特定于 PHP 编程语言使用的漏洞相关，包括注入不安全的 PHP 函数。这有助于防止利用允许攻击者远程运行未经授权的代码或命令的漏洞。如果 PHP 安装在与应用程序相连的任何服务器上，则评估此规则组。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令[DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
PHPHighRiskMethodsVariables_HEADER	检查所有标头中是否有 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 \$_GET 超全局变量的函数。 Warning 此规则仅检查请求标头的前 8 KB 或前 200 个标头，以先达到限制为准，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header

Rule name (规则名称)	描述和标注分类
PHPHighRiskMethodsVariables_QUERYSTRING	检查请求 URL? 中第一个之后的所有内容，查找 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 \$_GET 超全局变量的函数。 规则操作：Block 标签：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString
PHPHighRiskMethodsVariables_BODY	检查请求主体的值以查找 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 \$_GET 超全局变量的函数。 Warning 此规则仅检查请求正文的前 8 KB，并使用该Continue选项处理超大内容。有关更多信息，请参阅请求组件的超大处理 (p. 107)： 规则操作：Block 标签：aws:waf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

WordPress 应用程序管理规则组

VendorName:AWS, 名称:AWSManagedRulesWordPressRuleSet, WCU: 100

WordPress 应用程序规则组包含阻止与利用特定于WordPress 站点的漏洞相关的请求模式的规则。如果您正在运行，则应评估此规则组WordPress。此规则组应与 [SQL 数据库 \(p. 41\)](#) 和 [PHP 应用程序 \(p. 46\)](#) 规则组一起使用。

Note

下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令[DescribeManagedRuleGroup](#)。

Rule name (规则名称)	描述和标注分类
WordPressExploitableCommands_QUERYSTRING	检查请求查询字符串中是否存在可在有漏洞的安装或插件中利用的高风险WordPress 命令。示例模式包括类似于 do-reset-wordpress 的命令。 规则操作：Block 标签：aws:waf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING
WordPressExploitablePaths_URI_PATH	检查诸如如此的 WordPress 文件的请求 URI 路径xmlrpc.php，这些文件已知存在可轻松利用的漏洞。 规则操作：Block 标签：aws:waf:managed:aws:wordpress-app:WordPressExploitablePaths_URI_PATH

IP 声誉规则组

IP 信誉规则组根据其源 IP 地址阻止请求。

Note

这些规则使用 Web 请求源中的源 IP 地址。如果您的流量通过一个或多个代理或负载均衡器，则 Web 请求源将包含最后一个代理的地址，而不是客户端的源地址。

如果您希望减少自动程序流量、尝试攻击的风险，或者如果您要对内容强制地理限制，请选择其中一个或多个规则组。有关机器人管理的信息，另请参阅[Amazon WAF 机器人控制规则组 \(p. 49\)](#)。

此类别中的规则组不提供版本控制或 SNS 更新通知。

亚马逊 IP 信誉列表管理规则组

VendorName:AWS, 名称:AWSManagedRulesAmazonIpReputationList, WCU: 25

Amazon IP 声誉列表规则组包含基于 Amazon 内部威胁情报的规则。如果您想阻止通常与自动程序或其他威胁相关联的 IP 地址，此规则组非常有用。阻止这些 IP 地址有助于规避自动程序，并降低恶意人员发现易受攻击的应用程序的风险。

Rule name (规则名称)	描述和标注分类
AWSManagedIPReputationList	检查是否有被识别为机器人的 IP 地址。 规则操作：Block 标签：aws:waf:managed:aws:amazon-ip-list:AWSManagedIPReputationList
AWSManagedReconnaissanceList	检查来自正在对 Amazon 资源进行侦测的 IP 地址的连接。 规则操作：Block 标签：aws:waf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList
AWSManagedIPDDoSList	检查被确定为积极参与 DDoS 活动的 IP 地址。 规则操作：Count 标签：aws:waf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList

匿名 IP 列表管理规则组

VendorName:AWS, 名称:AWSManagedRulesAnonymousIpList, WCU: 50

匿名 IP 列表规则组包含用于阻止来自允许模糊处理查看者身份的服务的请求的规则。其中包括来自 VPN、代理、Tor 节点和托管提供商的请求。如果要筛选出可能试图从应用程序中隐藏其身份的查看者，则此规则组非常有用。屏蔽这些服务的 IP 地址可以帮助缓解机器人和规避地理限制的情况。

Rule name (规则名称)	描述和标注分类
AnonymousIpList	检查已知用于匿名处理客户端信息的源的 IP 地址列表，例如 TOR 节点、临时代理和其他遮蔽服务。 规则操作：Block

Rule name (规则名称)	描述和标注分类
	标签 : awswaf:managed:aws:anonymous-ip-list:AnonymousIPList
HostingProviderIPList	检查来自托管和云提供商的 IP 地址列表, 这些提供商不太可能产生最终用户流量。IP 列表不包括 Amazon IP 地址。 规则操作 : Block 标签 : awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList

Amazon WAF 机器人控制规则组

VendorName:AWS, 名称:AWSManagedRulesBotControlRuleSet, WCU: 50

Bot Control 托管规则组提供用于阻止和管理来自机器人的请求的规则。机器人可能会消耗多余的资源、歪曲业务指标、造成停机并进行恶意活动。

保护级别

Bot Control 托管规则组提供两种保护级别供您选择：

- 常见 — 检测各种自我识别的机器人，例如网页抓取框架、搜索引擎和自动浏览器。此级别的机器人控制保护使用传统的机器人检测技术（例如静态请求数据分析）识别常见的机器人。这些规则会标记来自这些机器人的流量，并屏蔽他们无法验证的流量。
- 定向 — 包括通用级保护，并增加了对无法自我识别的高级机器人的检测。定向保护使用浏览器查询、指纹识别和行为启发式等高级检测技术来识别恶意机器人流量。这些保护措施结合了速率限制、验证码和后台浏览器挑战，针对这些机器人。提供定向保护的规则的名称以开头TGT_。

Note

您还可以使用Amazon WAF基于速率的规则语句来限制速率。要进行比较，请参见[基于速率的规则和有针对性的机器人控制规则中的速率限制选项 \(p. 134\)](#)。

使用此规则组

此规则组是中的智能威胁缓解保护的一部分Amazon WAF。有关信息，请参阅[Amazon WAF智能威胁缓解 \(p. 130\)](#)。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

为了降低成本并确保根据需要管理网络流量，请按照中的指南使用此规则组[智能威胁缓解最佳实践 \(p. 135\)](#)。

机器人控制规则组不提供版本控制或 SNS 更新通知。

代币标注

该规则组使用Amazon WAF令牌管理根据其令牌的状态检查和标Amazon WAF记 Web 请求。Amazon WAF使用令牌进行客户端会话跟踪和验证。

Amazon WAF在检查 Web 请求的令牌和质询时间戳时应用以下标签之一。Amazon WAF不添加关于 CAPTCHA 时间戳状态的标签。

- awswaf:managed:token:accepted— 请求令牌存在且具有未过期的质询时间戳。

- `aws:waf:managed:token:rejected`— 请求令牌存在但已损坏或质询时间戳已过期。
- `aws:waf:managed:token:absent`— 请求没有令牌。

有关更多信息，请参阅[Amazon WAF网络请求令牌 \(p. 136\)](#)：

机器人控制标签

Bot Control 托管规则组生成带有命名空间前缀`aws:waf:managed:aws:bot-control:`缀和自定义命名空间的标签。规则组可能会向请求添加多个标签。

每个标签都反映了机器人控制规则的调查结果：

- `aws:waf:managed:aws:bot-control:bot:category:<category>`— 机器人的类别Amazon WAF，例如由`bot:category:search_engine`和定义`bot:category:content_fetcher`。
- `aws:waf:managed:aws:bot-control:bot:name:<name>`— 机器人名称（如果有），例如，自定义命名空间`bot:name:slurpbot`、`bot:name:googlebot`、和`bot:name:pocket_parser`。
- `aws:waf:managed:aws:bot-control:bot:verified`— 用于表示经过验证的机器人。这用于常见的理想机器人，与类别标签（如`bot:category:search_engine`或名称标签）结合使用时可能很有用`bot:name:googlebot`。

Note

Bot Control 使用从 Web 请求源向该 IP 地址发送的 IP 地址。您无法将其配置为使用Amazon WAF转发的 IP 配置来检查不同的 IP 地址源。如果您已验证通过代理或负载均衡器路由的机器人，则可以添加在 Bot Control 规则组之前运行的规则来帮助解决此问题。将您的新规则配置为使用转发的 IP 地址，并明确允许来自经过验证的机器人的请求。有关使用转发的 IP 地址的信息，请参阅[转发的 IP 地址 \(p. 110\)](#)。

- `aws:waf:managed:aws:bot-control:signal:<signal-details>`— 用于请求的属性，这些属性表示机器人不常用或未经过验证。
- `aws:waf:managed:aws:bot-control:targeted:<additional-details>`— 由机器人控制定向保护使用。

您可以通过调用通过 API 检索标签`DescribeManagedRuleGroup`。标签在响应的`AvailableLabels`属性中列出。

Bot Control 托管规则组将标签应用于一组通常允许的可验证机器人。规则组不会屏蔽这些经过验证的机器人，也不会贴上任何`signal:`标签。如果需要，您可以通过编写使用 Bot Control 托管规则组应用的标签的自定义规则来屏蔽它们或其中的一部分。有关此问题的更多信息以及示例，请参阅[Amazon WAF机器人控制 \(p. 142\)](#)。

机器人控制规则列表

下表列出了机器人控制规则。

Rule name (规则名称)	描述
CategoryAdvertising	检查用于广告目的的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:advertising 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。

Rule name (规则名称)	描述
CategoryArchiver	检查用于存档目的的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:archiver 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryContentFetcher	检查是否存在代表用户获取内容的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:content_fetcher 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryEmailClient	检查电子邮件客户端。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:email_client 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryHttpLibrary	检查机器人使用的 HTTP 库。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:http_library 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。

Rule name (规则名称)	描述
CategoryLinkChecker	检查是否有检查失效链接的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:link_checker 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryMiscellaneous	检查杂项机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:miscellaneous 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryMonitoring	检查用于监控目的的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:monitoring 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategoryScrapingFramework	检查网页抓取框架。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:scraping_framework 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。

Rule name (规则名称)	描述
CategorySearchEngine	检查搜索引擎机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:search_engine 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategorySecurity	检查是否存在与安全相关的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:security 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategorySeo	检查用于搜索引擎优化的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:seo 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
CategorySocialMedia	检查社交媒体平台用来提供内容摘要的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：aws:waf:managed:aws:bot-control:bot:category:social_media 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。
SignalAutomatedBrowser	检查是否有自动网络浏览器的迹象。 规则操作：Block
SignalKnownBotDataCenter	检查机器人通常使用的数据中心。 规则操作：Block

Rule name (规则名称)	描述
SignalNonBrowserUserAgent	检查似乎不是来自 Web 浏览器的用户代理字符串。 规则操作：Block
TGT_VolumetricIpTokenAbsent	检查客户在过去 5 分钟内是否有 5 个或更多不包含有效质询代币的请求。有关令牌的信息，请参阅Amazon WAF 网络请求令牌 (p. 136)。 Note 由于延迟，此规则适用的阈值可能会略有不同。 此规则处理缺失令牌的方法与代币标签的处理方式不同:awsaf:managed:token:absent. 令牌标签会标记没有令牌的单个请求。此规则会为每个客户端会话保留缺失令牌的请求计数，并与超过限制的客户端进行匹配。如果来自同一客户端的请求最近缺少令牌，则此规则可能会在具有令牌的请求上匹配。 规则操作，仅适用于未经验证的机器人的客户端：Challenge 标签：awsaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_ab 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签awsaf:managed:aws:bot-control:bot:verified。 此规则不同于代币标签:awsaf:managed:token:absent，后者仅标记没有令牌的单个请求。该规则会对每个客户端会话中丢失令牌的请求进行计数，并对超过限制的未经验证的机器人采取行动。

Rule name (规则名称)	描述
TGT_VolumetricSession	检查来自客户端会话的请求数量是否异常多。该评估基于与使用历史交通模式Amazon WAF维持的标准体积基线的比较。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作，仅适用于未经验证的机器人的客户端：CAPTCHA 标签：awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high 规则组将以下标签应用于高于最低阈值的中等容量和低容量请求。对于这些级别，无论客户端是否经过验证，规则均不执行任何操作：awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium control:targeted:aggregate:volumetric:session:low 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签awswaf:managed:aws:bot-control:bot:verified。
TGT_SignalAutomatedBrowser	检查浏览器自动化框架。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作，仅适用于未经验证的机器人的客户端：CAPTCHA 标签：awswaf:managed:aws:bot-control:targeted:signal:automated_browser 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签awswaf:managed:aws:bot-control:bot:verified。

Rule name (规则名称)	描述
TGT_SignalBrowserInconsistency	检查浏览器询问数据是否不一致。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作，仅适用于未经验证的机器人的客户端： CAPTCHA 标签：aws:waf:managed:aws:bot-control:targeted:signal:browser_inconsistency 对于经过验证的机器人，规则组不采取任何操作，但会添加规则标签和标签aws:waf:managed:aws:bot-control:bot:verified。

Amazon WAF 欺诈控制账户收购预防 (ATP) 规则组

VendorName:AWS, 名称:AWSManagedRulesATPRuleSet, WCU: 50

FAmazon WAF Fraud Control 账户接管预防 (ATP) 管理规则组标记和管理可能属于恶意账户接管企图一部分的请求。规则组通过检查客户端发送到您的应用程序的登录端点的登录尝试来实现此目的。

- 请求检查 — ATP 使您可以查看和控制使用被盗凭证的异常登录尝试和登录尝试，以防止可能导致欺诈活动的账户接管。ATP 根据其被盗的凭证数据库检查电子邮件和密码组合，随着在暗网上发现新的泄露凭证，该数据库会定期更新。ATP 通过 IP 地址和客户端会话聚合数据，以检测和阻止发送过多可疑请求的客户端。
- 响应检查 — 对于 CloudFront 分配，除了检查传入的登录请求外，ATP 规则组还会检查您的应用程序对登录尝试的响应，以跟踪成功率和失败率。利用这些信息，ATP 可以暂时阻止登录失败次数过多的客户端会话或 IP 地址。Amazon WAF 异步执行响应检查，因此这不会增加网络流量的延迟。

使用此规则组

此规则组需要特定的配置。要配置和实现此规则组，请参阅中的指南[Amazon WAF 欺诈控制账户收购预防 \(ATP\) \(p. 155\)](#)。

此规则组是中的智能威胁缓解保护的一部分Amazon WAF。有关信息，请参阅 [Amazon WAF 智能威胁缓解 \(p. 130\)](#)。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

为了降低成本并确保根据需要管理网络流量，请按照中的指南使用此规则组[智能威胁缓解最佳实践 \(p. 135\)](#)。

此规则组不适用于 Amazon Cognito 用户池。您无法将使用此规则组的 Web ACL 与用户池相关联，也无法将此规则组添加到已与用户池关联的 Web ACL。

此规则组不提供版本控制或 SNS 更新通知。

代币标注

该规则组使用Amazon WAF令牌管理根据其令牌的状态检查和标Amazon WAF记 Web 请求。Amazon WAF使用令牌进行客户端会话跟踪和验证。

Amazon WAF在检查 Web 请求的令牌和质询时间戳时应用以下标签之一。Amazon WAF不添加关于CAPTCHA 时间戳状态的标签。

- `aws:waf:managed:token:accepted`— 请求令牌存在且具有未过期的质询时间戳。
- `aws:waf:managed:token:rejected`— 请求令牌存在但已损坏或质询时间戳已过期。
- `aws:waf:managed:token:absent`— 请求没有令牌。

有关更多信息，请参阅[Amazon WAF网络请求令牌 \(p. 136\)](#)：

ATP 标签

ATP 托管规则组生成带有命名空间前缀`aws:waf:managed:aws:atp:`和自定义命名空间的标签。

账户收购防范规则列表

下表列出了中的 ATP 规则AWSManagedRulesATPRuleSet以及规则组添加到 Web 请求的标签。

Rule name (规则名称)	描述和标注分类
UnsupportedCognitoIDP	检查流向 Amazon Cognito 用户池的网络流量。ATP 不可用于 Amazon Cognito 用户池，此规则有助于确保其他 ATP 规则组规则不用于评估用户池流量。 规则操作：Block 标签：<code>aws:waf:managed:aws:atp:unsupported:cognito_idp</code>
VolumetricIpHigh	检查从单个 IP 地址发送的大量请求。高容量是指在 10 分钟窗口内超过 20 个请求。 Note 由于延迟，此规则适用的阈值可能会略有不同。对于高容量，在应用规则操作之前，一些请求可能会超过限制。 规则操作：Block 标签：<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip</code> 规则组将以下标签应用于中等容量（每 10 分钟窗口为 16-20 个请求）和低容量（每 10 分钟窗口为 11-15 个请求）的请求，但不对它们采取任何操作：<code>aws:waf:managed:aws:atp:aggregate:volumetric:ip</code>
VolumetricSession	检查从单个客户会话发送的大量请求。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF网络请求令牌 (p. 136)：

Rule name (规则名称)	描述和标注分类
	Note 由于延迟，此规则适用的阈值可能会略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:volumetric:s
AttributeCompromisedCredentials	检查来自同一客户端会话的多个使用被盗证书的请求。 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:attribute:com
AttributeUsernameTraversal	检查来自同一客户端会话的多个使用用户名遍历的请求。 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:attribute:use
AttributePasswordTraversal	检查来自同一客户端会话的多个使用密码遍历的请求。 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:attribute:pas
AttributeLongSession	检查来自同一客户端会话的多个使用长时间会话的请求。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:attribute:lon

Rule name (规则名称)	描述和标注分类
TokenRejected	检查令牌管理拒绝的带有令Amazon WAF牌的请求。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作：Block 标签：无。要检查令牌是否被拒绝，请使用标签匹配规则在标签上进行匹配 配：aws:waf:managed:token:rejected
SignalMissingCredential	检查带有缺少用户名或密码的凭证的请求。 规则操作：Block 标签：aws:waf:managed:aws:atp:signal:missing_credential
没有规则。对于每个匹配的请求，规则组都会添加标签并且不对该请求采取任何操作。	在被盗的凭证数据库中搜索请求中提交的证书。 规则操作：不执行任何操作 标签：aws:waf:managed:aws:atp:signal:credential_compromised
没有规则。对于每个匹配的请求，规则组都会添加标签并且不对该请求采取任何操作。	检查来自同一客户端会话的多个使用可疑 TLS 指纹的请求。 Note 仅适用于受保护的亚马逊 CloudFront 发行版。 规则操作：不执行任何操作 标签：aws:waf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint

Rule name (规则名称)	描述和标注分类
VolumetricIpFailedLoginResponseHigh	检查最近登录尝试失败率过高的 IP 地址。如果您已将规则组配置为检查响应正文或 JSON 组件，则 Amazon WAF 可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指标。 该规则根据受保护资源对来自同一 IP 地址的最近登录尝试的成功和失败响应，将规则操作和标签应用于来自 IP 地址的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败次数。 Note Amazon WAF 仅在保护亚马逊 CloudFront 发行版的网络 ACL 中评估此规则。 Note 由于延迟，此规则适用的阈值可能会略有不同。客户端发送的失败登录尝试次数可能超过规则在后续尝试中开始匹配之前允许的次數。 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:volumetric:ip

Rule name (规则名称)	描述和标注分类
VolumetricSessionFailedLoginResponseHigh	检查最近是否导致登录尝试失败率过高的客户端会话。如果您已将规则组配置为检查响应正文或 JSON 组件，则Amazon WAF可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指标。 此规则根据受保护资源对来自同一客户端会话的最近登录尝试的成功和失败响应，将规则操作和标签应用于来自客户端会话的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败次数。 Note Amazon WAF仅在保护亚马逊 CloudFront 发行版的网络 ACL 中评估此规则。 Note 由于延迟，此规则适用的阈值可能会略有不同。客户端发送的失败登录尝试次数可能超过规则在后续尝试中开始匹配之前允许的次數。 此检查仅在 Web 请求包含令牌时适用。令牌由应用程序集成 SDK 和规则操作CAPTCHA和添加到请求中Challenge。有关更多信息，请参阅Amazon WAF 网络请求令牌 (p. 136)： 规则操作：Block 标 签：aws:waf:managed:aws:atp:aggregate:volumetric:s

版本化Amazon托管规则组的部署

Amazon在三个标准部署中部署对其版本化Amazon管理规则组的更改：候选版本、静态版本和默认版本。此外，有时Amazon可能需要发布异常部署或回滚默认版本部署。

Note

本节仅适用于版本控制的Amazon托管规则组。未进行版本控制的规则组是 IP 信誉、机器人控制和 ATP 规则组。

注册接收部署通知

对于版本控制规则组的每次部署，都Amazon提供至少一个 SNS 通知。在某些情况下，我们还会更新本指南中的托管规则组描述、Amazon托管规则组的变更日志和文档历史记录页面。要注册接收通知，请参阅[收到有关托管规则组新版本和更新的通知 \(p. 29\)](#)。

主题

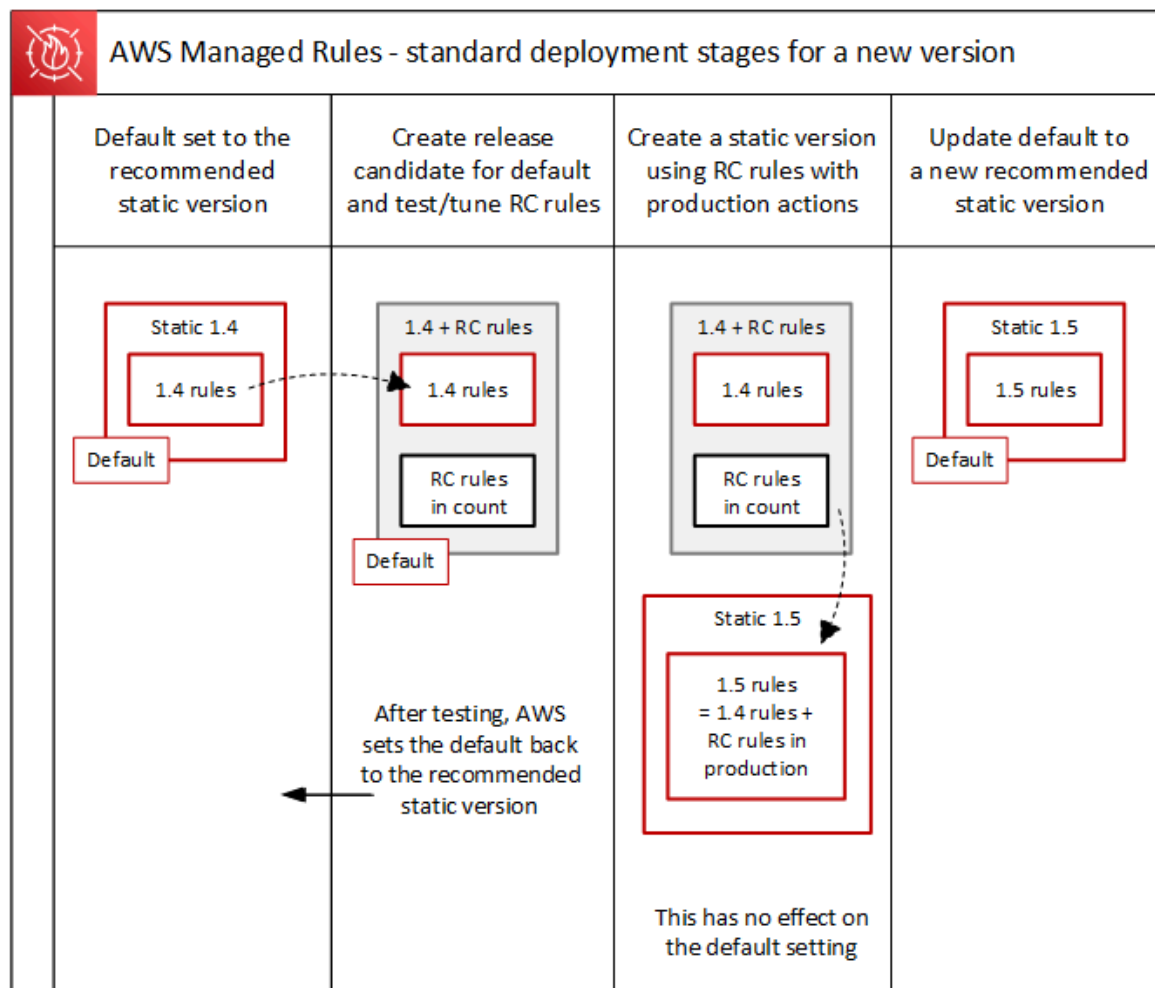
- [Amazon托管规则标准部署概述 \(p. 62\)](#)
- [Amazon托管规则的典型版本状态 \(p. 62\)](#)
- [发布Amazon托管规则的候选部署 \(p. 63\)](#)
- [Amazon托管规则的静态版本部署 \(p. 65\)](#)
- [Amazon托管规则的默认版本部署 \(p. 66\)](#)

- [Amazon托管规则的例外部署 \(p. 67\)](#)
- [Amazon托管规则的默认部署回退 \(p. 67\)](#)

Amazon托管规则标准部署概述

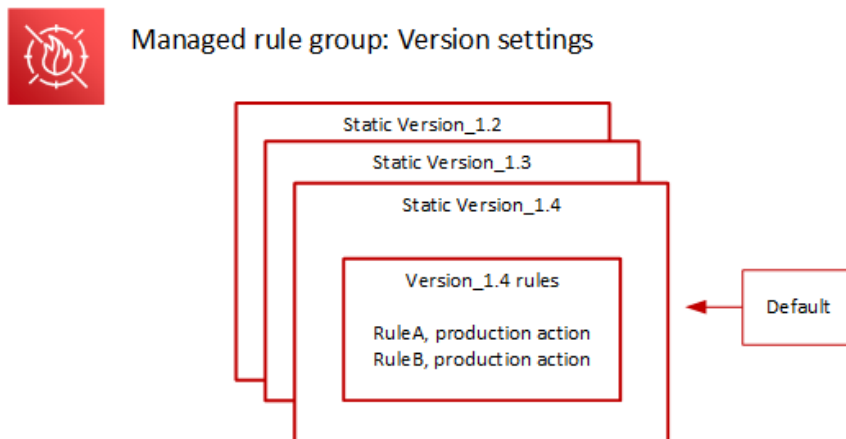
Amazon使用三个标准部署阶段推出新的Amazon托管规则功能：候选版本、静态版本和默认版本。

下图描述了这些标准部署。以下各节详述其中每个内容。



Amazon托管规则的典型版本状态

通常，受版本控制的托管规则组有许多未过期的静态版本，默认版本指向Amazon推荐的静态版本。下图显示了一组典型的静态版本和默认版本设置的示例。



静态版本中大多数规则的生产操作是Block，但可能会设置为不同的内容。有关规则操作设置的详细信息，请参阅每个规则组的规则列表，网址为[Amazon托管规则规则组列表 \(p. 32\)](#)。

发布Amazon托管规则的候选部署

当托管规则组Amazon有一组候选规则更改时，它会在临时的候选版本部署中对其进行测试。Amazon根据生产流量在计数模式下评估候选规则，并执行最终调整活动，包括减少误报。Amazon测试以这种方式为所有使用默认版本的规则组的客户发布候选规则。候选版本部署不适用于使用规则组静态版本的客户。

如果您使用默认版本，则候选版本部署不会改变规则组管理您的网络流量的方式。在测试候选规则时，您可能会注意到以下内容：

- 默认版本名称从更改Default (using Version_X.Y)为Default (using Version_X.Y_PLUS_RC_COUNT)。
- 亚马逊RC_COUNT中 CloudWatch 带有名称的其他计数指标。这些是由候选版本规则生成的。

Amazon对候选版本进行大约一周的测试，然后将其删除并将默认版本重置为当前推荐的静态版本。

Amazon为候选版本部署执行以下步骤：

1. 创建候选发行版 — 根据当前推荐的静态版本（即默认版本指向的版本）Amazon添加候选发行版。

候选版本的名称是附加的静态版本名称_PLUS_RC_COUNT。例如，如果当前推荐的静态版本是Version_2.1，则将命名候选发行版Version_2.1_PLUS_RC_COUNT。

候选版本包含以下规则：

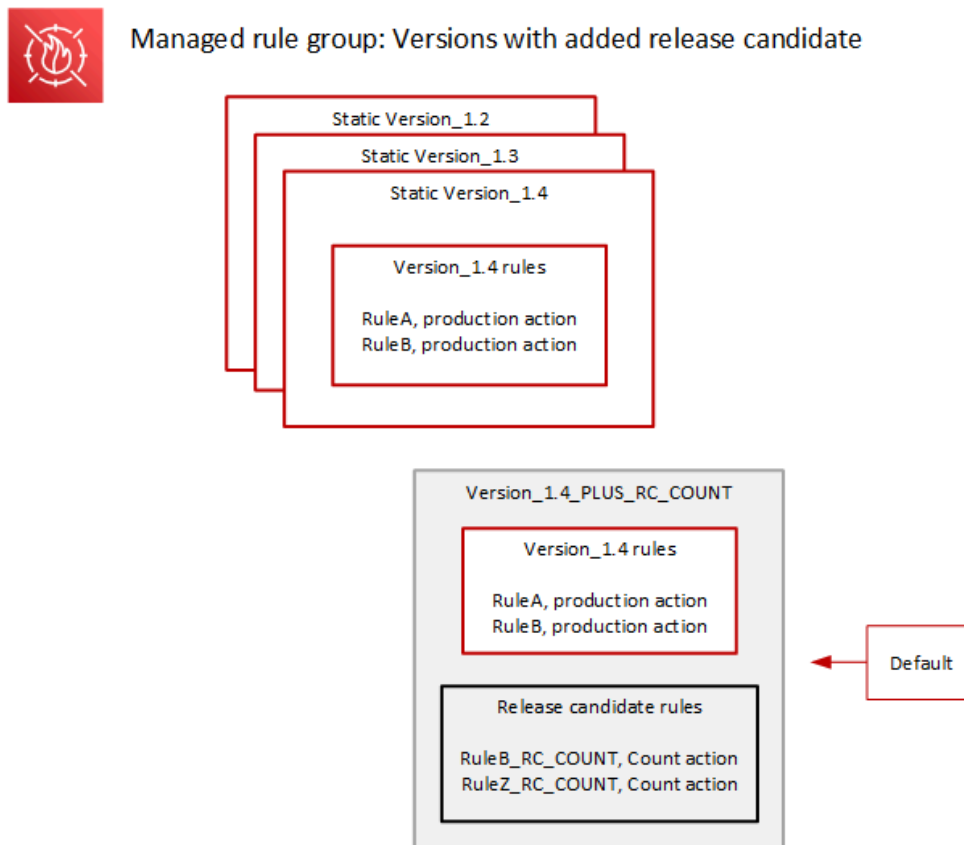
- 规则完全复制自当前推荐的静态版本，未更改规则配置。
- 候选新规则，规则操作设置为Count且名称以结尾_RC_COUNT。

大多数候选规则都对规则组中已存在的规则提出了改进建议。每条规则的名称都是附加的现有规则的名称_RC_COUNT。

2. 将默认版本设置为候选版本并进行测试 — Amazon 将默认版本设置为指向新的候选版本，以针对您的生产流量进行测试。测试通常需要大约一周的时间。

您将看到默认版本的名称从仅表示静态版本的名称（例如）更改为Default (using Version_1.4)表示静态版本加上候选发布规则的名称，例如Default (using Version_1.4_PLUS_RC_COUNT)。此命名方案使您可以确定使用哪个静态版本来管理您的网络流量。

下图显示了此时示例规则组版本的状态。



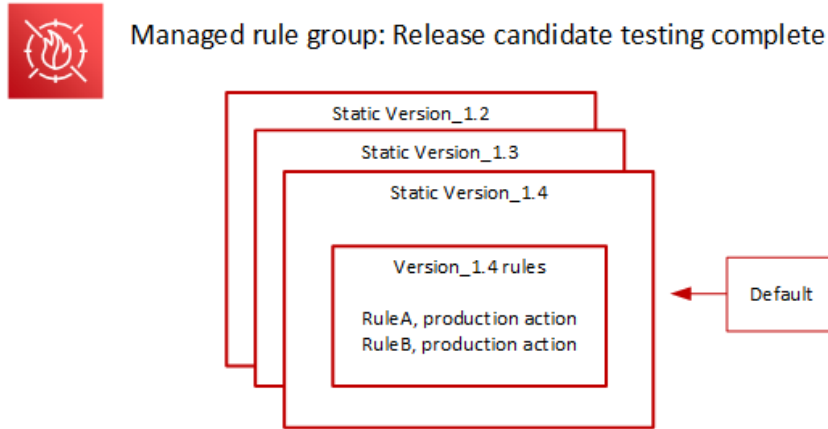
候选版本规则始终配置有Count操作，因此它们不会改变规则组管理 Web 流量的方式。

候选版本规则生成亚马逊 CloudWatch 计数指标，Amazon用于验证行为和识别误报。Amazon根据需要进行调整，以调整候选版本数量规则的行为。

候选发行版本不是静态版本，您无法从静态规则组版本列表中进行选择。您只能在默认版本规范中看到候选发行版本的名称。

3. 将默认版本恢复为推荐的静态版本-测试候选版本规则后，Amazon将默认版本设置回当前推荐的静态版本。默认版本名称设置删除结_PLUS_RC_COUNT尾，规则组停止为候选版本规则生成 CloudWatch 计数指标。这是一项静默更改，与部署默认版本回滚不同。

下图显示了候选版本测试完成后示例规则组版本的状态。



时间和通知

Amazon根据需要部署候选发行版本，以测试对规则组的改进。

- SNS — 在部署开始时Amazon发送 SNS 通知。通知指出了测试候选版本的预计时间。测试完成后，静Amazon默地将默认值恢复为静态版本设置，无需再次通知。
- 更改日志 —Amazon 不更新此类部署的变更日志或本指南的其他部分。

Amazon托管规则的静态版本部署

当Amazon确定候选版本为规则组提供了有价值的更改时，会根据候选版本为规则组Amazon部署新的静态版本。此部署不会更改规则组的默认版本。

新的静态版本包含候选版本的以下规则：

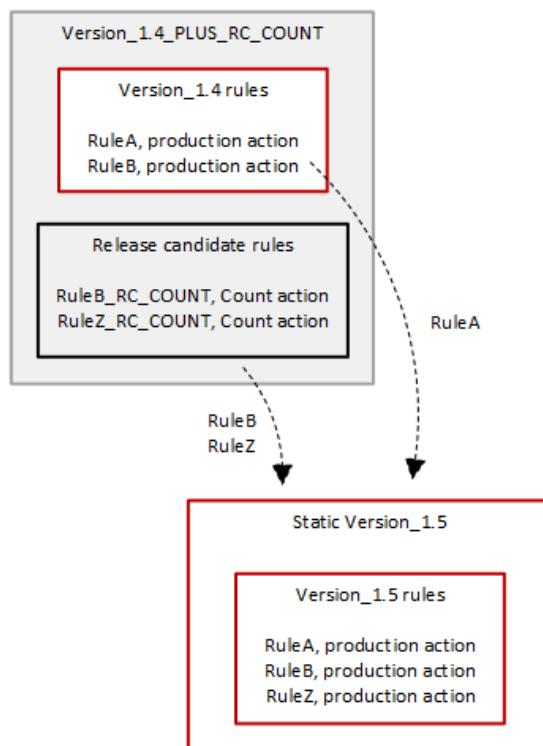
- 来自先前静态版本的规则，在候选版本规则中没有替代候选规则。
- 发布候选规则，但有以下更改：
 - Amazon通过删除候选版本后缀来更改规则名称_RC_COUNT。
 - Amazon将规则操作从更改Count为其生产规则操作。

对于替代先前现有规则的候选版本规则，这将取代新静态版本中先前规则的功能。

下图描述了从候选版本创建新的静态版本的过程。



Managed rule group: Create a new static version with tested release candidate rules



部署后，新的静态版本可供您测试，如果您愿意，也可以在保护中使用。您可以在规则组的规则列表中查看新的和更新的规则操作和描述，网址为[Amazon托管规则规则组列表 \(p. 32\)](#)。

静态版本在部署后是不可变的，并且只有在Amazon过期时才会更改。有关版本生命周期的信息，请参阅[使用托管规则组进行版本管理 \(p. 25\)](#)。

时间和通知

Amazon根据需要部署新的静态版本，以便部署对规则组功能的改进。静态版本的部署不会影响默认版本设置。

- SNS — 在部署开始时Amazon发送 SNS 通知。
- 更改日志 — 在所有可用的部署完成后Amazon WAF，根据需要Amazon更新本指南中的规则组定义，然后在 Managed Rules 规则组更改日志和文档历史记录页面中宣布发布。Amazon

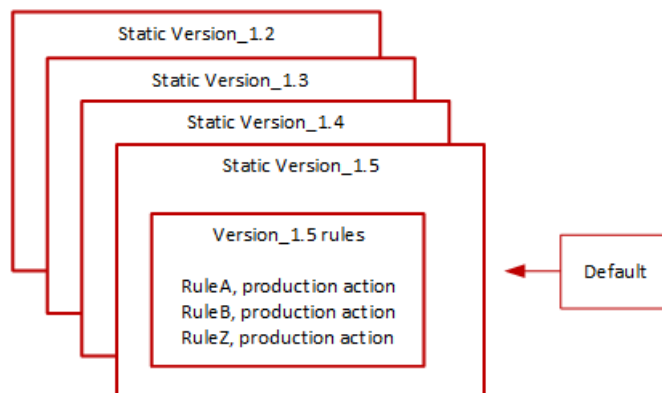
Amazon托管规则的默认版本部署

当Amazon确定新的静态版本与当前默认版本相比，新的静态版本为规则组提供了更好的保护时，会将默认版本Amazon更新为新的静态版本。Amazon可能会在将一个静态版本升级为规则组的默认版本之前发布多个静态版本。

下图显示了将默认版本设置Amazon移至新的静态版本后，示例规则组版本的状态。



Managed rule group: Update the default to a new recommended static version



在将此更改部署到默认版本之前，会Amazon提供通知，以便您可以测试和准备即将到来的更改。如果您使用默认版本，则可以不执行任何操作并在更新期间继续使用该版本。相反，如果您想在默认版本部署的计划开始之前延迟切换到新版本，则可以明确配置您的规则组以使用默认设置为的静态版本。

时间和通知

Amazon当它为规则组推荐的静态版本与当前使用的静态版本不同的静态版本时，会更新默认版本。

- SNS — 在目标部署日前至少一周Amazon发送 SNS 通知，然后在部署当天，即部署开始时发送另一个 SNS 通知。每条通知都包括规则组名称、默认版本更新到的静态版本、部署日期以及执行更新的每个 Amazon 区域的预定部署时间。
- 更改日志 — Amazon 不更新此类部署的变更日志或本指南的其他部分。

Amazon托管规则的例外部署

Amazon可能会绕过标准部署阶段，以便快速部署解决关键安全风险的更新。例外部署可能涉及任何标准部署类型，并且可能会在各个Amazon区域快速推出。

Amazon为异常部署提供尽可能多的提前通知。

时间和通知

Amazon仅在需要时执行异常部署。

- SNS — 尽可能在目标部署日之前Amazon发送 SNS 通知，然后在部署开始时再发送一次 SNS 通知。每条通知都包括规则组名称、正在进行的更改和部署日期。
- 更改日志 — 如果部署是针对静态版本，则在所有可用的部署完成后，Amazon WAF根据需要Amazon更新本指南中的规则组定义，然后在 Managed Rules 规则组更改日志和文档历史记录页面中宣布发布。Amazon

Amazon托管规则的默认部署回退

在某些情况下，Amazon可能会将默认版本还原到其先前的设置。所有Amazon区域的回滚时间通常少于十分钟。

Amazon执行回滚只是为了缓解静态版本中的重大问题，例如误报率高得令人无法接受。

回滚默认版本设置后，会Amazon加快存在问题的静态版本的到期时间，也加快发布新的静态版本以解决这个问题。

时间和通知

Amazon 仅在需要时执行默认版本回滚。

- SNS — 在回滚时 Amazon 发送单个 SNS 通知。通知包括规则组名称、默认版本设置为的版本以及部署日期。这种部署类型非常快，因此通知不提供区域的时间信息。
- 更改日志 — Amazon 不更新此类部署的变更日志或本指南的其他部分。

Amazon 托管规则免责声明

Amazon 托管规则旨在保护您免受常见的 Web 威胁的攻击。根据文档进行使用时，Amazon 托管规则组将为您的应用程序添加另一层安全性。但是，Amazon 托管规则组并非用于取代您的安全责任，这些责任由您所选择的 Amazon 资源决定。请参阅[责任共担模式](#)，以确保妥善保护 Amazon 中的资源。

Amazon 托管规则变更日志

本节列出了自 2019 年 11 月发布 Amazon 托管规则 Amazon WAF 以来对其所做的更改。

Note

此变更日志报告了 Managed Rules 中对规则 Amazon 和规则组的更改 Amazon WAF。
对于[IP 声誉规则组 \(p. 48\)](#)，此变更日志会报告规则和规则组的更改，但由于这些列表的动态性质，它不报告规则所使用的 IP 地址列表的更改。

规则组和规则	说明	日期
PHP 应用程序管理规则组 (p. 46) • 更新了 PHPHighRiskMethodsVariables_BODY • 已移除 PHPHighRiskMethodsVariables_QUERYARGUMENTS • 添加了 PHPHighRiskMethodsVariables_QUERYSTRING • 添加了 PHPHighRiskMethodsVariables_HEADER	发布了该规则组的静态版本 2.0。 添加了签名以改善所有规则的检测。 将规则 PHPHighRiskMethodsVariables_QUERYARGUMENTS 替换为 PHPHighRiskMethodsVariables_QUERYSTRING，它检查整个查询字符串，而不仅仅是查询参数。 添加了规则 PHPHighRiskMethodsVariables_HEADER，以扩大覆盖范围以包括所有标题。 更新了以下标签，使其与标准 Amazon 托管规则标签保持一致： • 旧名称：PHPHighRiskMethodsVariables_BODY 新名称：PHPHighRiskMethodsVariables_Body • 旧名称：PHPHighRiskMethodsVariables_QUERYARGUMENTS 新名称：PHPHighRiskMethodsVariables_QueryString	2023-02-27
Amazon WAF 欺诈控制账户收购预防 (ATP) 规则组 (p. 56)	添加了用于受保护的亚马逊 CloudFront 发行版的登录响应检查规则。这些规则可以阻止来自	2023 年 2 月 15 日

规则组和规则	说明	日期
• VolumetricIpFailedLoginResponse • VolumetricSessionFailedLoginResponse	IP 地址和客户端会话的新登录尝试，而这些地址和会话是最近多次登录尝试失败的根源。	
核心规则集 (CRS) 托管规则组 (p. 33) • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	发布了该规则组的静态版本 1.5。 更新了跨站点脚本 (XSS) 过滤器以改善检测。	2023 年 01 月 25 日
Linux 操作系统托管规则组 (p. 42) • LFI_COOKIE-已删除 • LFI_HEADER-已添加 • LFI_URIPATH • LFI_QUERYSTRING • LFI_BODY	发布了该规则组的静态版本 2.1。 删除了规则LFI_COOKIE及其标签aws:waf:managed:aws:linux-os:LFI_Cookie，并将其替换为新规则LFI_HEADER及其标签aws:waf:managed:aws:linux-os:LFI_Header。此更改将检查范围扩展到多个标题。 为所有规则添加了文本转换和签名以改善检测。	2022-12-15
核心规则集 (CRS) 托管规则组 (p. 33) • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	发布了该规则组的静态版本 1.4。 添加了文本转换NoUserAgent_HEADER以删除所有空字节。更新了跨站点脚本规则中的过滤器以改善检测。	2022-12-05
已知的错误输入管理规则组 (p. 38) • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER	发布了该规则组的静态版本 1.17。 更新了 Java 反序列化规则，增加了对与 Apache CVE-2022-42889 匹配的请求的检测，Apache 是 1.10.0 之前的 Apache Commons Text 版本中的远程代码执行 (RCE) 漏洞。有关更多信息，请参阅 NIST：国家漏洞数据库：CVE-2022-42889 详细信息和 CVE-2022-42889：1.10.0 之前的 Apache Commons Text 在应用于不可信输入时允许 RCE，这是因为插值默认值不安全。 改进了中的检测Host_localhost_HEADER。	2022 年 10 月 20 日

规则组和规则	说明	日期
已知的错误输入管理规则组 (p. 38) - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI_PATH - Log4JRCE_BODY	发布了该规则组的静态版本 1.16。 删除了版本 1.15 中 Amazon 发现的误报。	2022 年 10 月 5 日
POSIX 操作系统管理的规则组 (p. 43) PHP 应用程序管理规则组 (p. 46) WordPress 应用程序管理规则组 (p. 47)	更正了记录在案的标签名称。	2022 年 09 月 19 日
IP 声誉规则组 (p. 48) AWSManagedIPDDoSList	此更改不会改变规则组处理您的网络流量的方式。 根据亚马逊威胁情报，添加了一项包含 Count 检查积极参与 DDoS 活动的 IP 地址的新规则。	2022 年 8 月 30 日
已知的错误输入管理规则组 (p. 38) - Log4JRCE - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI_PATH - Log4JRCE_BODY - JavaDeserializationRCE_HEADER - JavaDeserializationRCE_BODY - JavaDeserializationRCE_URI_PATH - JavaDeserializationRCE_QUERYSTRING - Host_localhost_HEADER - PROPFIND_METHOD	发布了该规则组的静态版本 1.15。 将其移除 Log4JRCE 并替换为 Log4JRCE_HEADER、Log4JRCE_QUERYSTRING、Log4JRCE_URI_PATH 和 Log4JRCE_BODY，以便对误报进行更精细的监控和管理。 添加了签名以改进对所有 PROP_FIND_METHOD 和 Log4JRCE* 规则的检测。 更新了所有 JavaDeserializationRCE* 和 Log4JRCE* 规则的标签以更正所有 JavaDeserializationRCE* 规则中的 Host_localhost_HEADER 大小写。 更正了描述 JavaDeserializationRCE_HEADER。	2022 年 8 月 22 日
Amazon WAF 欺诈控制账户收购预防 (ATP) 规则组 (p. 56) UnsupportedCognitoIDP	添加了一条规则，以防止对 Amazon Cognito 用户池网络流量使用账户防盗托管规则组。	2022 年 8 月 11 日

规则组和规则	说明	日期
核心规则集 (CRS) 托管规则组 (p. 33)	Amazon 已为版本 Version_1.2 和 Version_2.0 规则组预定过期。这些版本将于 2022 年 9 月 9 日到期。有关版本过期的信息，请参阅 使用托管规则组进行版本管理 (p. 25) 。	2022 年 6 月 9 日
核心规则集 (CRS) 托管规则组 (p. 33) - GenericLFI_URIPATH - GenericRFI_URIPATH	已发布此规则组的版本 1.3。此版本更新了规则 GenericLFI_URIPATH 和中的匹配签名 GenericRFI_URIPATH，以改善检测。	2022 年 5 月 24 日
Amazon WAF 机器人控制规则组 (p. 49) CategoryEmailClient	将规则 CategoryEmailClient 添加到规则组。	2022 年 4 月 6 日
已知的错误输入管理规则组 (p. 38) - JavaDeserializationRCE_HEADER - JavaDeserializationRCE_BODY - JavaDeserializationRCE_URI - JavaDeserializationRCE_QUERYSTRING	已发布此规则组的 1.14 版本。这四 JavaDeserializationRCE 条规则已移至 BLOCK 模式。	2022 年 3 月 31 日
已知的错误输入管理规则组 (p. 38) - JavaDeserializationRCE_HEADER_RC_COUNT - JavaDeserializationRCE_BODY_RC_COUNT - JavaDeserializationRCE_URI_RC_COUNT - JavaDeserializationRCE_QUERYSTRING_RC_COUNT	已发布此规则组的 1.13 版本。更新了 Spring Core 和 Cloud Function RCE 漏洞的文本转换。这些规则处于计数模式，用于收集指标和评估匹配的模式。该标签可用于阻止自定义规则中的请求。后续版本将在块模式下使用这些规则进行部署。	2022 年 3 月 31 日
已知的错误输入管理规则组 (p. 38) - JavaDeserializationRCE_HEADER_RC_COUNT - JavaDeserializationRCE_BODY_RC_COUNT - JavaDeserializationRCE_URI_RC_COUNT - JavaDeserializationRCE_QUERYSTRING_RC_COUNT - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI - Log4JRCE_BODY - Log4JRCE	已发布此规则组的 1.12 版本。添加了 Spring 核心和云函数 RCE 漏洞的签名。这些规则处于计数模式，用于收集指标和评估匹配的模式。该标签可用于阻止自定义规则中的请求。后续版本将在块模式下使用这些规则进行部署。 删除了规则 Log4JRCE_HEADER、Log4JRCE_QUERYSTRING、Log4JRCE_URI、和，Log4JRCE_BODY 并将其替换为规则 Log4JRCE。	2022 年 3 月 30 日
IP 声誉规则组 (p. 48) AWSManagedReconnaissanceList	更新了 AWSManagedReconnaissanceList 规则，将操作从计数更改为阻止。	2022 年 2 月 15 日

规则组和规则	说明	日期
Amazon WAF 欺诈控制账户收购预防 (ATP) 规则组 (p. 56) 新规则组中的所有规则	添加了规则组AWSManagedRulesATPRuleSet。	2022 年 2 月 11 日
已知的错误输入管理规则组 (p. 38) - Log4JRCE - Log4JRCE_HEADER - Log4JRCE_QUERYSTRING - Log4JRCE_URI - Log4JRCE_BODY	已发布此规则组的版本 1.9。删除了规则Log4JRCE，将其替换为规则Log4JRCE_HEADERLog4JRCE_QUERYSTRINGLog4JRCE_URI、Log4JRCE_BODY和，以便灵活地使用此功能。添加了签名以改善检测和阻止。	2022 年 01 月 28 日
核心规则集 (CRS) - CrossSiteScripting_URI_PATH - CrossSiteScripting_BODY - CrossSiteScripting_QUERY_ARGUMENTS - CrossSiteScripting_COOKIE	已发布此规则组的 2.0 版。对于这些规则，调整了检测签名以减少误报。将URL_DECODE文本转换替换为双URL_DECODE_UNI文本转换。添加了HTML_ENTITY_DECODE文本转换。	2022 年 01-10
核心规则集 (CRS) - RestrictedExtensions_URI_PATH - RestrictedExtensions_QUERY_ARGUMENTS	作为该规则组版本 2.0 版本的一部分，添加URL_DECODE_UNI文本转换。从规则集中删除了URL_DECODE文本转换RestrictedExtensions_URI_PATH。	2022 年 01-10
SQL 数据库 - SQLi_BODY - SQLi_QUERY_ARGUMENTS - SQLi_COOKIE - SQLi_URI_PATH - SQLiExtendedPatterns_BODY - SQLiExtendedPatterns_QUERY_ARGUMENTS	已发布此规则组的 2.0 版。将URL_DECODE文本转换替换为双URL_DECODE_UNI文本转换，并添加了COMPRESS_WHITE_SPACE文本转换。 向中添加了更多检测签名SQLiExtendedPatterns_QUERY_ARGUMENTS。 添加了 JSON 检查SQLi_BODY。 添加了规则SQLiExtendedPatterns_BODY。 删除了规则SQLi_URI_PATH。	2022 年 01-10
已知错误输入 Log4JRCE	发布了该规则的 1.8 版Log4JRCE，以改进标题检查和匹配标准。	2021-12-17
已知错误输入 Log4JRCE	发布了该规则的版本 1.4，Log4JRCE以调整匹配标准并检查其他标题。发布了版本 1.5 以调整匹配标准。	2021-12-11

规则组和规则	说明	日期
已知错误输入 - Log4JRCE - BadAuthToken_COOKIE_AUTHORIZATION	添加了规则Log4JRCE版本 1.2 以回应最近在 Log4j 中披露的安全问题。有关信息，请参阅 AWS 公告 2021-44228 。该规则检查常见的 URI 路径、查询字符串、请求正文的前 8KB 和常见标头。该规则使用双重URL_DECODE_UNI文本转换。发布了 1.3 版Log4JRCE，以调整匹配标准并检查其他标头。 删除了规则BadAuthToken_COOKIE_AUTHORIZATION。	2021-12-10

下表列出了 2021 年 12 月之前的变化。

规则组和规则	说明	日期	
Amazon IP 声誉列表	AWSManagedReconnaissanceList	在监控计数模式下添加了AWSManagedReconnaissanceList规则。此规则包含正在对Amazon资源进行侦测的IP 地址。	2021-11-23
Windows 操作系统	WindowsShellCommands PowerShellCommands	为 WindowsShell 命令添加了三条新规则：WindowsShellCommands_COOKIEWindowsShellCommands_BODY。 添加了新 PowerShell 规则:PowerShellCommands_COOKIE。 通过删除字符串_Set1 和 _Set2 重构了PowerShellComands规则命名。 向添加了更全面的检测签名PowerShellRules。 为所有 Windows 操作系统规则添加了URL_DECODE_UNI文本转换。	2021-11-23
Linux 操作系统	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	将双重URL_DECODE文本转换替换为双重文本转换URL_DECODE_UNI。 NORMALIZE_PATH_WIN作为第二个文本转换添加。	2021-11-23

规则组和规则	说明	日期	
		用LFI_BODY规则替换了LFI_COOKIE规则。 为所有LFI规则添加了更全面的检测签名。	
核心规则集 (CRS)	SizeRestrictions_BODY	降低了阻止正文有效负载大于 8 KB 的 Web 请求的大小限制。以前，限制为 10 KB。	2021-10-27
核心规则集 (CRS)	EC2MetaDataSSRF_BODY EC2MetaDataSSRF_COOKIE EC2MetaDataSSRF_URI EC2MetaDataSSRF_URI_PATH EC2MetaDataSSRF_QUERY_ARGUMENTS	添加了更多检测签名。 添加了双重 unicode URL 解码以改善屏蔽效果。	2021-10-27
核心规则集 (CRS)	GenericLFI_QUERY_ARGUMENTS GenericLFI_URI_PATH RestrictedExtensions_URI_PATH RestrictedExtensions_QUERY_ARGUMENTS	添加了双重 unicode URL 解码以改善屏蔽效果。	2021-10-27
核心规则集 (CRS)	GenericRFI_QUERY_ARGUMENTS GenericRFI_BODY GenericRFI_URI_PATH	根据客户反馈更新了规则签名以减少误报。添加了双重 unicode URL 解码以改善屏蔽效果。	2021-10-27
全部	所有规则	为所有尚未支持Amazon WAF标签的规则添加了对标签的支持。	2021-10-25
Amazon IP 声誉列表	AWSManagedIPReputationList	重构了 IP 信誉列表，删除了规则名称的后缀，并添加了对Amazon WAF标签的支持。	2021 年 5 月 4 日
匿名 IP 列表	AnonymousIPList HostingProviderList	增加了对Amazon WAF标签的支持。	2021 年 5 月 4 日
机器人控制	全部	添加了机器人控制规则集。	2021 年 4 月 1 日
核心规则集 (CRS)	GenericRFI_QUERY_ARGUMENTS	添加了双重 URL 解码。	2021 年 3 月 3 日
核心规则集 (CRS)	RestrictedExtensions_BODY	改进了规则的配置并添加了额外的 URL 解码。	2021 年 3 月 3 日
管理保护	AdminProtection_URI_PATH	添加了双重 URL 解码。	2021 年 3 月 3 日
已知错误输入	ExploitablePaths_URI_PATH	改进了规则的配置并添加了额外的 URL 解码。	2021 年 3 月 3 日

规则组和规则	说明	日期	
Linux 操作系统	LFI_QUERYARGUMENTS	改进了规则的配置并添加了额外的 URL 解码。	2021 年 3 月 3 日
Windows 操作系统	全部	改进了规则的配置。	2020-09-23
PHP 应用程序	PHPHighRiskMethodsVariablesQueryStringArguments PHPHighRiskMethodsVariablesBody	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-09-16
POSIX 操作系统	UNIXShellCommandsVariablesQueryStringArguments UNIXShellCommandsVariablesBody	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-09-16
核心规则集	GenericLFI_QUERYARGUMENTS GenericLFI_URI_PATH GenericLFI_BODY	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-08-07
Linux 操作系统	LFI_URI_PATH LFI_QUERYARGUMENTS LFI_BODY	将文本转换从 HTML 实体解码更改为 URL 解码，以改善检测和阻止。	2020-05-19
匿名 IP 列表	全部	加入了新的规则组， IP 声誉规则组 (p. 48) 以阻止来自允许模糊处理查看者身份的服务的请求，以帮助缓解机器人和规避地理限制的情况。	2020-03-06
WordPress 应用程序	WordPressExploitableCommandStrings	用于检查查询字符串中是否存在可利用的命令的新规则。	2020-03-03
核心规则集 (CRS)	SizeRestrictions_QueryArguments SizeRestrictions_Cookie_Header SizeRestrictions_Body SizeRestrictions_URIPath	调整了大小值约束以提高准确性。	2020-03-03
SQL 数据库	SQLi_URI_PATH	这些规则现在会检查消息 URI。	2020-01-23
SQL 数据库	SQLi_BODY SQLi_QUERYARGUMENTS SQLi_COOKIE	更新了文本转换。	2019-12-20

规则组和规则	说明	日期	
核心规则集 (CRS)	CrossSiteScripting_UPDATE CrossSiteScripting_BODY CrossSiteScripting_QUERYARGUMENTS CrossSiteScripting_COOKIE	更新 HTML 文本转换。	2019-12-20

Amazon Web Services Marketplace 托管规则组

Amazon Web Services Marketplace 托管规则组可通过 Amazon Web Services Marketplace 控制台订阅，网址为 [Amazon Web Services Marketplace](#)。订阅 Amazon Web Services Marketplace 托管规则组后，您可以在 Amazon WAF 中使用它。要在 Amazon Firewall Manager Amazon WAF 策略中使用 Amazon Web Services Marketplace 规则组，组织中的每个账户都必须订阅该规则组。

在将您的 Amazon WAF 保护措施用于生产流量之前，请先测试和调整对保护措施所做的任何更改。有关信息，请参阅 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

Amazon Web Services Marketplace 规则组定价

Amazon Web Services Marketplace 规则组不需要签订长期合同即可使用，也没有最低费用限制。当您订阅规则组时，将按月收取费用（按小时比例）和根据数量收取持续请求费用。有关更多信息，请参阅 [Amazon WAF 定价](#) 和每个 Amazon Web Services Marketplace 规则组的描述，网址为 [Amazon Web Services Marketplace](#)。

对 Amazon Web Services Marketplace 规则组有疑问？

如对 Amazon Web Services Marketplace 卖家管理的规则组有疑问或要求更改功能，请联系提供商的客户支持团队。要查找联系信息，请参阅提供商的列表，网址为 [Amazon Web Services Marketplace](#)。

Amazon Web Services Marketplace 规则组提供者决定如何管理规则组，例如如何更新规则组以及规则组是否已版本化。提供者还确定规则组的详细信息，包括规则、规则操作以及规则为匹配的 Web 请求添加的任何标签。

订阅 Amazon Web Services Marketplace 托管规则组

您可以在 Amazon WAF 控制台上订阅和取消订阅 Amazon Web Services Marketplace 规则组。

Important

要在 Amazon Firewall Manager 策略中使用 Amazon Web Services Marketplace 规则组，组织中的每个账户必须首先订阅该规则组。

订阅 Amazon Web Services Marketplace 托管规则组

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，请选择 Amazon Web Services Marketplace。
3. 在可用 Marketplace 产品部分中，选择规则组的名称以查看详细信息和定价信息。
4. 如果您要订阅规则组，请选择继续。

Note

如果您不想订阅此规则组，只需在您的浏览器中关闭此页面。

5. 选择设置您的账户。

6. 将规则组添加到 Web ACL 中，就像您添加单个规则一样。有关更多信息，请参阅 [创建 Web ACL \(p. 17\)](#) 或 [编辑 Web ACL \(p. 19\)](#)。

Note

向 Web ACL 添加规则组时，可以覆盖规则组中规则的操作和规则组结果的操作。有关更多信息，请参阅[规则组中的操作替代 \(p. 14\)](#)：

订阅 Amazon Web Services Marketplace 规则组后，您可以在 Web ACL 中使用该规则组，就像使用其他托管规则组一样。有关信息，请参阅 [创建 Web ACL \(p. 17\)](#)。

取消订阅托管 Amazon Web Services Marketplace 规则组

您可以在 Amazon WAF 控制台上取消订阅 Amazon Web Services Marketplace 规则组。

Important

要停止对 Amazon Web Services Marketplace 托管规则组收取订阅费用，除了取消订阅外，还必须将其从任何 Firewall Manager Amazon WAF 策略 Amazon WAF 及其中的所有 Web ACL 中删除。如果您取消订阅 Amazon Web Services Marketplace 托管规则组，但未将其从 Web ACL 中删除，则将继续向您收取订阅费用。

取消订阅 Amazon Web Services Marketplace 托管规则组

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 从所有 Web ACL 中删除规则组。有关更多信息，请参阅[编辑 Web ACL \(p. 19\)](#)：
3. 在导航窗格中，请选择 Amazon Web Services Marketplace。
4. 选择 Manage your subscriptions。
5. 选择您想取消订阅的规则组旁边的取消订阅。
6. 选择是，取消订阅。

Amazon Web Services Marketplace 规则组问题排查

如果您发现 Amazon Web Services Marketplace 规则组阻塞了合法流量，则可以通过执行以下步骤来解决问题。

Amazon Web Services Marketplace 规则组故障排除

1. 改写操作以计入阻塞合法流量的规则。您可以使用 Amazon WAF 抽样请求或 Amazon WAF 日志来确定哪些规则在阻止特定请求。您可以通过查看日志中的 ruleGroupId 字段或采样请求中的 RuleWithinRuleGroup 来标识规则。您可以在模式中识别规则 <Seller Name>#<RuleGroup Name>#<Rule Name>。
2. 如果将特定规则设置为仅对请求进行计数并不能解决问题，则可以覆盖所有规则操作，或者将 Amazon Web Services Marketplace 规则组本身的操作从“不覆盖”更改为“覆盖”以进行计数。这会允许 Web 请求通过，而不管规则组中的各个规则操作是什么。
3. 覆盖单个规则操作或整个 Amazon Web Services Marketplace 规则组操作后，请联系规则组提供商的客户支持团队进一步解决问题。有关联系信息，请参阅 Amazon Web Services Marketplace 产品列表页面上的规则组列表。

联系 Amazon 支持人员

有关 Amazon WAF 或由其管理的规则组出现问题 Amazon，请联系 Amazon Web Services Support。如果由 Amazon Web Services Marketplace 卖家管理的规则组出现问题，请联系提供商的客户支持团队。要查找联系信息，请参阅提供商的列表 Amazon Web Services Marketplace。

管理您自己的规则组

您可以创建您自己的规则组，以重复使用托管规则组产品中不包含或您希望自行处理的规则集合。

您创建的规则组保存规则的方式与 Web ACL 保存规则的方式类似，向规则组添加规则的方式与向 Web ACL 添加规则的方式相同。当您创建自己的规则组时，必须为其设置不可变的最大容量。

您可以与其他 Amazon 账户共享您拥有的规则组，供该账户使用。此选项可通过 Amazon WAF API 获得。有关更多信息，请参阅 [PutPermissionPolicy](#) Amazon WAF API 参考中的。

主题

- [创建规则组 \(p. 78\)](#)
- [在 Web ACL 中使用您的规则组 \(p. 78\)](#)
- [删除规则组 \(p. 79\)](#)

创建规则组

创建规则组

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Rule groups (规则组)，然后选择 Create rule group (创建规则组)。
3. 为规则输入名称和描述。您将使用名称和描述来标识该集合以便管理和使用它。

Note

规则组在创建之后无法更改名称。

4. 对于 Region (区域)，选择要存储规则组的区域。要在保护 Amazon CloudFront 发行版的 Web ACL 中使用规则组，必须使用全局设置。您也可以对区域应用程序使用全局设置。
5. 选择下一步。
6. 使用 Rule builder (规则生成器) 向导将规则添加到规则组，这与 Web ACL 管理中的操作相同。唯一区别在于您无法将规则组添加到另一个规则组。
7. 对于 Capacity (容量)，请为规则组使用 Web ACL 容量单位 (WCU) 设置最大值。这是一个不可变的设置。有关 WCU 的信息，请参阅 [Amazon WAF Web ACL 容量单位 \(WCU\) \(p. 6\)](#)。

向规则组添加规则时，Add rules and set capacity (添加规则和设置容量) 窗格会显示所需的最小容量，该容量基于已添加的规则。您可以根据此容量和规则组的未来计划来帮助估算规则组将需要的容量。

8. 查看规则组的设置，然后选择创建。

在 Web ACL 中使用您的规则组

要在 Web ACL 中使用规则组，请在规则组参考语句中将其添加到 Web ACL 中。

生产流量风险

在为生产流量部署 Web ACL 的更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整更新后的规则，然后再启用这些规则。有关操作指南，请参阅 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

在控制台上，当您在 Web ACL 中添加或更新规则时，在添加规则和规则组页面上，选择添加规则，然后选择添加我自己的规则和规则组。然后选择 Rule group (规则组)，并从列表中选择规则组。

在 Web ACL 中，您可以通过将单个规则操作设置为计数或任何其他操作以及将生成的规则组操作改写为计数，来更改规则组及其规则的行为。这可以帮助您执行一些操作，例如测试规则组、识别规则组中的规则中

的误报，以及自定义托管规则组如何处理您的请求。有关这些选项的详细信息，请参阅 [规则组中的操作替代 \(p. 14\)](#)。

如果您的规则组包含基于速率的语句，则您使用该规则组的每个 Web ACL 对基于速率的规则都有自己的单独速率跟踪和管理，与您使用该规则组的任何其他 Web ACL 无关。有关更多信息，请参阅 [基于速率的规则语句 \(p. 95\)](#)：

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他 Amazon WAF 资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

删除规则组

按照本部分中的指导删除规则组。

删除引用的集合和规则组

当您删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时，将 Amazon WAF 检查该实体当前是否正在 Web ACL 中使用。如果发现它正在使用，则 Amazon WAF 警告您。Amazon WAF 几乎每次都能确定 Web ACL 是否引用实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在 Web ACL 中进行检查。如果实体是引用的集合，请检查是否有规则组正在使用它。

删除规则组

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Rule groups (规则组)。
3. 选择要删除的规则组，然后选择 Delete (删除)。

其他服务提供的规则组

如果您或组织中的管理员使用 Amazon Firewall Manager 或 Amazon Shield Advanced 使用管理资源保护，则可能会看到规则组参考语句已添加到账户的 Web ACL 中。Amazon WAF

这些规则组的名称以以下字符串开头：

- **ShieldMitigationRuleGroup**— 这些规则组由管理 Amazon Shield Advanced。当您为相关资源启用应用层 DDoS 自动缓解时，Shield Advanced 会将其添加到用于 Shield Advanced 应用层（第 7 层）保护的 Web ACL 中。有关这些规则组更多信息，请参阅 [Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

Warning

请勿从 Web ACL 中手动删除此规则组参考语句。这样做可能会对与 Web ACL 关联的所有资源产生意想不到的后果。而是使用 Shield Advanced 禁用与 Web ACL 关联的资源的自动缓解功能。当不需要自动缓解规则组时，Shield Advanced 会将其删除。

- **PREFManaged**和**POSTFManaged** — 这些规则组由管理Amazon Firewall Manager。Firewall Manager 在Firewall Manager 创建和管理的 Web ACL 中提供它们。Web ACL 的名称以开头FManagedWebACLV2。有关这些 Web ACL 和规则组的信息，请参阅[Amazon WAF 策略 \(p. 444\)](#)。

规则

Amazon WAF规则定义了如何检查 HTTP (S) Web 请求以及在请求符合检查标准时对请求采取的操作。只能在规则组或 Web ACL 的上下文中定义规则。

您可以定义检查条件的规则，如下所示：

- 可能是恶意的脚本。攻击者会嵌入可以利用 Web 应用程序漏洞的脚本。这称为跨站脚本攻击 (XSS)。
- 请求源自的 IP 地址或地址范围。
- 请求源自的国家/地区或地理位置。
- 请求的指定部分的长度，例如查询字符串。
- 可能是恶意的 SQL 代码。攻击者会尝试通过在 Web 请求中嵌入恶意 SQL 代码从数据库提取数据。这称为 SQL 注入。
- 请求中出现的字符串，例如，在 User-Agent 标头中出现的值或是在查询字符串中出现的文本字符串。您还可以使用正则表达式 (regex) 指定这些字符串。
- Web ACL 中先前的规则已添加到请求中的标签。

每条规则都需要一条顶级语句，该语句可能包含任何深度的嵌套语句，具体取决于规则和语句类型。某些规则类型采用一组标准。例如，您可以在 IP 地址规则中指定最多 10,000 个 IP 地址或 IP 地址范围。

除了带有 Web 请求检查标准的语句（如前面的列表中的语句）外，还Amazon WAF支持ANDOR、和的逻辑语句NOT，您可以使用这些语句在规则中组合语句。

例如，根据您发现的来自某个攻击者的最近请求，您可以创建一个规则，该规则含有包含以下嵌套AND语句的逻辑语句：

- 请求来自 192.0.2.44。
- 请求在 User-Agent 标头中包含值 BadBot。
- 请求表现为在查询字符串中包含类似 SQL 的代码。

在这种情况下，Web 请求需要匹配所有语句才能匹配顶级语句AND。

规则不独立存在。Amazon WAF它们不是Amazon资源，也没有Amazon 资源名称 (ARN)。您可以在定义规则的规则组或 Web ACL 中按名称访问规则。您可以使用规则组的 JSON 格式或包含规则的 Web ACL 来管理规则并将其复制到其他 Web ACL。或者，您可以通过Amazon WAF控制台规则生成器对其进行管理，该规则生成器可用于 Web ACL 和规则组。

主题

- [Amazon WAF 规则名称 \(p. 80\)](#)
- [Amazon WAF 规则操作 \(p. 81\)](#)
- [Amazon WAF 规则语句 \(p. 81\)](#)

Amazon WAF 规则名称

必须为 Web ACL 或规则组中的每条规则分配一个唯一的名称。

该名称只能包含字符 A-Z、a-z、0-9、-（连字符）和 _（下划线）。在规则组或 Web ACL 中创建规则后，您无法更改其名称。

Amazon WAF 规则操作

规则操作会Amazon WAF在 Web 请求与规则中定义的条件匹配时，如何处理 Web 请求。您可以选择向每个规则操作添加自定义行为。

Note

规则操作可以是终止的，也可以是非终止的。终止操作会停止对请求的 Web ACL 评估，要么让请求继续访问您的受保护应用程序，要么将其阻止。

以下是规则操作选项：

- **Allow**—Amazon WAF 允许将请求转发到受保护的Amazon资源进行处理和响应。这是终止操作。在您定义的规则中，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。
- **Block**—Amazon WAF 阻止请求。这是终止操作。默认情况下，您的受保护Amazon资源以 HTTP403 (Forbidden) 状态码进行响应。在您定义的规则中，您可以自定义响应。当Amazon WAF阻止请求时，Block操作设置决定受保护资源发送回客户机的响应。
- **Count**—对请求进行Amazon WAF计数，但不确定是允许还是阻止请求。这是一项非终止操作。Amazon WAF继续处理 Web ACL 中的其余规则。在您定义的规则中，您可以在请求中插入自定义标头，也可以添加其他规则可以匹配的标签。
- **CAPTCHA和Challenge**—Amazon WAF 使用验证码谜题和静默挑战来验证请求不是来自机器人，并Amazon WAF使用代币来跟踪最近的成功客户回应。

Note

当您在其中一个规则中使用CAPTCHA或Challenge规则操作或在规则组中用作规则操作替代时，会向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

这些规则操作可以是终止的，也可以是非终止的，具体取决于请求中令牌的状态：

- **有效的、未过期的令牌不可终止** — 如果令牌根据配置的验证码或质询豁免时间有效且未过期，则Amazon WAF处理与Count操作类似的请求。Amazon WAF继续基于 Web ACL 中的其余规则检查 Web 请求。与Count配置类似，在您定义的规则中，您可以选择使用自定义标头配置这些操作以插入到请求中，还可以添加其他规则可以匹配的标签。
- **终止对无效或过期令牌的请求** — 如果令牌无效或指定的时间戳已过期，则Amazon WAF终止对 Web 请求的检查并阻止请求，与Block操作类似。Amazon WAF然后用错误回应客户端。因为CAPTCHA，如果请求内容表明客户端浏览器可以处理，则在 JavaScript 插页式广告中Amazon WAF发送验证码拼图，该拼图旨在区分人类客户端和机器人。对于动Challenge作，Amazon WAF发送带有静默挑战的JavaScript 插页式广告，旨在区分普通浏览器和由机器人运行的会话。

有关更多信息，请参阅[CAPTCHA以及中的Challenge操作Amazon WAF \(p. 175\)](#)。

有关自定义请求和响应的信息，请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#)。

有关向匹配请求添加标签的信息，请参阅[网络请求上的标签 \(p. 123\)](#)。

有关 Web ACL 和规则设置如何交互的信息，请参阅[Web ACL 规则和规则组评估 \(p. 12\)](#)。

Amazon WAF 规则语句

规则语句是指明Amazon WAF如何检查 Web 请求的规则的一部分。当在 Web 请求中Amazon WAF找到检查标准时，我们说该 Web 请求与声明相符。每个规则语句都根据语句类型指定要查找的内容和方式。

中的每个规则Amazon WAF都有一个顶级规则语句，该语句可以包含其他语句。规则语句可能非常简单。例如，您可以有一份声明，提供一组来源国家/地区供您检查您的网络请求。规则语句也可能非常复杂。例如，您可以使用一条将许多其他语句与逻辑AND、OR和语句组合在一起的NOT语句。

Web ACL 也可以包含仅引用规则组的规则语句。在控制台上，您不会看到以规则语句形式表示的 Web ACL，但每个 Web ACL 都具有 JSON 格式的表示形式。在 JSON 中，您可以看到这些特殊类型的规则语句。对于任何复杂的规则，使用 JSON 编辑器管理 Web ACL 是最简单的方法。您可以检索 JSON 格式的 Web ACL 的完整配置，根据需要进行修改，然后 Amazon WAF 通过控制台、API 或 CLI 将其提供给。您自己管理的规则组也是如此。

嵌套规则语句

Amazon WAF 支持嵌套许多规则语句，但不支持所有规则语句的嵌套。例如，您不能将规则组语句嵌套在另一个语句中。在某些场景中，您需要使用嵌套，例如缩小范围语句和逻辑语句。下面的规则声明和规则详细信息描述了每个类别和规则的嵌套能力和要求。

控制台中文本的可视化编辑器仅支持规则语句的一个嵌套级别。例如，可以在逻辑 AND 或 OR 规则中嵌套多种类型的语句，但不能嵌套其他语句 AND 或 OR 规则，因为这需要第二级嵌套。要实现多级嵌套，您需要在 JSON 中提供规则定义，要么通过控制台中的 JSON 规则编辑器，要么通过 API。

主题

- [规则语句列表 \(p. 82\)](#)
- [网络请求组件 \(p. 102\)](#)
- [引用集合或规则组的语句 \(p. 109\)](#)
- [范围缩小声明 \(p. 110\)](#)
- [转发的 IP 地址 \(p. 110\)](#)

规则语句列表

本节介绍可以添加到规则中的语句，并提供一些计算每个 Web ACL 容量单位 (WCU) 使用情况的指导原则。有关 WCU 的信息，请参阅 [Amazon WAF Web ACL 容量单位 \(WCU\) \(p. 6\)](#)。

此页按类别对规则语句进行分组，对每个语句提供高级描述，并提供指向包含语句类型更多信息的部分的链接。

比赛声明

匹配语句将 Web 请求或其来源与您提供的标准进行比较。对于许多此类语句，会 Amazon WAF 比较匹配内容请求的特定部分。

匹配语句是可嵌套的。您可以将它们嵌套在逻辑规则语句中，并在范围缩小语句中使用它们。

比赛声明	描述	WCU
地理匹配 (p. 87)	检查请求的原产国并贴上原产国和地区的标签。	1
IP 集匹配 (p. 91)	根据一组 IP 地址和地址范围检查请求。	大多数情况下为 1。如果您将语句配置为使用带有转发 IP 地址的标头并在的标头中指定位置 Any，则 WCU 为 5。
标签匹配规则声明 (p. 92)	检查对同一 Web ACL 中其他规则添加的标签的请求。	1
正则表达式匹配规则声明 (p. 97)	将正则表达式模式与指定的请求组件进行比较。	3，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您

比赛声明	描述	WCU
		使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。
正则表达式模式集 (p. 98)	将正则表达式模式与指定的请求组件进行比较。	每个模式集 25 美元，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。
大小约束 (p. 99)	根据指定的请求组件检查大小限制。	1，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。
SQLi 攻击 (p. 99)	检查指定请求组件中是否存在恶意 SQL 代码。	20，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。
字符串匹配 (p. 100)	将字符串与指定的请求组件进行比较。	基本成本取决于字符串匹配的类型，介于 1 到 10 之间。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。
XSS 脚本攻击 (p. 101)	检查指定请求组件中是否存在跨站脚本攻击。	40，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

逻辑规则语句

使用逻辑规则语句组合其他语句或否定其结果。每个逻辑规则语句都至少需要一个嵌套语句。

要对规则语句结果进行逻辑组合或否定，请将语句嵌套在逻辑规则语句下。

Note

控制台上的可视化编辑器支持单级规则语句嵌套，适用于许多需求。要嵌套更多级别，请在控制台上编辑规则的 JSON 表示形式或使用 API。

逻辑规则语句是可嵌套的。您可以将它们嵌套在其他逻辑规则语句中，并在范围缩小语句中使用它们。有关范围缩小语句的信息，请参见[范围缩小声明 \(p. 110\)](#)。

逻辑语句	描述	WCU
AND 逻辑 (p. 84)	将嵌套语句与AND逻辑相结合。	基于嵌套语句
NOT 逻辑 (p. 93)	否定嵌套语句的结果。	基于嵌套语句
OR 逻辑 (p. 93)	将嵌套语句与OR逻辑相结合。	基于嵌套语句

复杂语句

Amazon WAF支持基于费率的语句和规则组语句。您不能将这些语句类型嵌套在其他规则语句中。对于其中一些语句，您可以通过添加向下作用域语句来缩小他们检查的请求的范围。

Statement	描述	WCU
托管规则组 (p. 92)	运行在指定托管规则组中定义的规则。 您可以通过添加 scope-down 语句来缩小规则组评估的请求范围。 您不能将托管规则组语句嵌套在任何其他语句类型中。	由规则组定义，以及范围缩小语句的任何其它 WCU。
规则组 (p. 98)	运行您管理的规则组中定义的规则。 您不能将规则组语句嵌套在任何其他语句类型中。	在创建规则组时，您可以为其定义 WCU 限制。
基于速率 (p. 95)	跟踪来自单个 IP 地址的请求速率，并在地址发送过多请求时暂时屏蔽这些地址。 您可以通过添加范围缩小语句，缩小基于速率的语句评估的请求的范围。 您不能在任何规则声明下嵌套基于速率的声明。您可以在自己管理的规则组内定义基于速率的语句。	2，再加上任何用于范围缩小声明的其他 WCU。

AND规则语句

AND规则语句将嵌套语句与逻辑AND运算组合在一起，因此所有嵌套语句都必须匹配才能使AND语句匹配。这需要至少一个嵌套语句。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU-取决于嵌套语句。

在何处查找此规则声明

- 控制台上的@@ 规则生成器-对于 If 请求，选择匹配所有语句 (AND)，然后填写嵌套语句。
- API — [AndStatement](#)

示例

以下清单显示了如何使用NOT逻辑规则语句来消除 SQL 注入攻击语句的匹配项中的误报。AND在此示例中，假设我们可以编写一个单字节 match 语句来匹配导致误报的请求。

AND 语句匹配与字节匹配语句不匹配且与 SQL 注入攻击语句不匹配的请求。

```
{
  "Name": "SQLiExcludeFalsePositives",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "NotStatement": {
            "Statement": {
              "ByteMatchStatement": {
                "SearchString": "string identifying a false positive",
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "CONTAINS"
              }
            }
          }
        },
        {
          "SqliMatchStatement": {
            "FieldToMatch": {
              "Body": {
                "OversizeHandling": "MATCH"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  }
}
```

```
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "SQLiExcludeFalsePositives"
    }
  }
}
```

使用控制台规则可视化编辑器，可以在或语句下嵌套非逻辑NOT语句OR或AND语句。前面的示例显示了NOT语句的嵌套。

使用控制台规则可视化编辑器，您可以将大多数可嵌套语句嵌套在逻辑规则语句下，例如上一个示例中显示的语句。你不能使用可视化编辑器来嵌套OR或AND语句。要配置这种类型的嵌套，您需要在JSON中提供规则语句。例如，以下JSON规则列表包含嵌套在OR语句内的AND语句。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "aws:waf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "aws:waf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        }
      ]
    },
    {
      "OrStatement": {
        "Statements": [
          {
            "GeoMatchStatement": {
              "CountryCodes": [
                "JM",
                "JP"
              ]
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "JCountryString",
              "FieldToMatch": {
                "Body": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "CONTAINS"
            }
          }
        ]
      }
    }
  ]
}
```



```
    }  
  }  
]  
}  
,  
"Action": {  
  "Block": {}  
},  
"VisibilityConfig": {  
  "SampledRequestsEnabled": true,  
  "CloudWatchMetricsEnabled": true,  
  "MetricName": "match_rule"  
}  
}
```

地理匹配规则语句

使用地理或地理匹配声明根据来源国家和地区管理网络请求。

Note

对于 CloudFront 发行版，如果您使用 CloudFront 地理限制功能，则该功能不会将被阻止的请求转发给 Amazon WAF。该功能会将允许的请求转发到 Amazon WAF。如果您想根据地理位置和其他 Amazon WAF 标准阻止请求，请使用 Amazon WAF 地理匹配声明，不要使用 CloudFront 地理限制功能。

您可以使用地理匹配语句进行国家和地区匹配，如下所示：

- 国家/地区-使用地理匹配规则本身根据请求来源国管理请求。
- 区域-使用地理匹配规则和标签匹配规则，根据请求的原产国和地区管理请求。有关使用标签匹配规则的信息，请参阅[标签匹配规则声明 \(p. 92\)](#)和[网络请求上的标签 \(p. 123\)](#)。

使用 geo match 语句，按如下方式 Amazon WAF 管理每个 Web 请求：

1. 确定请求的国家和地区代码 — 根据请求的 IP 地址 Amazon WAF 确定请求的国家和地区。默认情况下，Amazon WAF 使用 Web 请求来源的 IP 地址。您可以指示使用备 Amazon WAF 用请求标头中的 IP 地址，例如 X-Forwarded-For 在规则语句设置中启用转发 IP 配置。

Amazon WAF 使用国际标准化组织 (ISO) 3166 标准中的 alpha-2 国家和地区代码。您可以在以下位置找到代码：

- 在 ISO 网站上，您可以在 [ISO 在线浏览平台 \(OBP\)](#) 上搜索国家/地区代码。
- 在维基百科上，国家代码列在 [ISO 3166-2](#) 中。

URL 中列出了国家/地区的区域代码 https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code>。例如，美国的区域为 [ISO 3166-2: US](#)，乌克兰的区域为 [ISO 3166-2: UA](#)。

2. 确定要添加到请求中的国家/地区标签和区域标签-标签表明地理匹配声明使用的是原始 IP 还是转发的 IP 配置。

- 原产地 IP

国家标签是 `aws:waf:clientip:geo:country:<ISO country code>`。以美国为例：`aws:waf:clientip:geo:country:US`。

区域标签是 `aws:waf:clientip:geo:region:<ISO country code>-<ISO region code>`。以美国俄勒冈州为例：`aws:waf:clientip:geo:region:US-OR`。

- 转发的 IP

国家标签是 `aws:waf:forwardedip:geo:country:<ISO country code>`。以美国为例：`aws:waf:forwardedip:geo:country:US`。

区域标签是`aws:waf:forwardedip:geo:region:<ISO country code>-<ISO region code>`。以美国俄勒冈州为例：`aws:waf:forwardedip:geo:region:US-OR`。

如果国家或地区代码不适用于请求的指定 IP 地址，则在标签XX中Amazon WAF使用该值来代替该值。例如，以下标签适用于国家/地区代码不可用的客户端 IP：`aws:waf:clientip:geo:country:XX`以下标签适用于国家/地区为美国但区域代码不可用的转发 IP：`aws:waf:forwardedip:geo:region:US-XX`。

3. 根据规则标准评估请求的国家/地区代码

无论是否找到匹配项，地理匹配语句都会对其检查的所有请求进行标记。

Note

Amazon WAF在规则的 Web 请求评估结束时添加任何标签。因此，您对地理匹配语句中的标签使用的任何标签匹配都必须在与地理匹配语句规则不同的规则中定义。

如果您只想检查区域值，则可以使用 Count 操作和单个国家/地区代码匹配编写地理匹配规则，然后为区域标签编写标签匹配规则。即使采用这种方法，您也需要提供国家/地区代码以供评估地理匹配规则。您可以通过指定极不可能成为您网站流量来源的国家/地区，来减少日志记录和统计指标。

可@@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 1 WCU。

设置-此语句使用以下设置：

- 国家/地区代码-用于比较地理匹配的国家/地区代码数组。例如，它们必须是 ISO 3166 国际标准的 alpha-2 国家/地区 ISO 代码中的双字符国家/地区代码["US", "CN"]。
- (可选) 转发 IP 配置-默认情况下，Amazon WAF使用 Web 请求来源中的 IP 地址来确定来源国家。或者，您可以将规则配置为在 HTTP 标头中X-Forwarded-For改用转发 IP。Amazon WAF使用标头中的第一个 IP 地址。使用此配置，您还可以指定后备行为，以应用于指定标头中格式错误的 IP 地址的 Web 请求。备用行为将请求的匹配结果设置为匹配或不匹配。有关更多信息，请参阅[转发的 IP 地址 \(p. 110\)](#)：

在何处查找此规则声明

- 控制台上的@@@ 规则生成器-对于请求选项，选择“源自所在国家”。
- API — [GeoMatchStatement](#)

示例

您可以使用地理匹配声明来管理来自特定国家或地区的请求。例如，如果您想阻止来自某些国家/地区的请求，但仍允许来自这些国家/地区的一组特定 IP 地址的请求，则可以创建一个规则，将操作设置为，Block并使用以下嵌套语句，以伪代码显示：

- AND statement
 - 地理匹配声明，列出您要屏蔽的国家
 - NOT statement
 - IP set 语句，用于指定您要允许通过的 IP 地址

或者，如果您想屏蔽某些国家/地区的某些区域，但仍允许来自这些国家/地区的其他地区的请求，则可以先定义地理匹配规则，将操作设置为Count。然后，定义与添加的地理匹配标签的标签匹配规则，并根据需要处理请求。

以下伪代码描述了这种方法的示例：

1. Geo match 语句列出了您想要封锁的区域但操作设置为 Count 的国家/地区。无论匹配状态如何，这都会标记每个网络请求，还会为您提供感兴趣的国家/地区的计数指标。
2. AND带有屏蔽操作的声明
 - 标签匹配声明，用于指定要屏蔽的国家/地区的标签
 - NOT statement
 - 标签匹配声明，用于指定您希望允许通过的国家/地区的标签

以下 JSON 列表显示了前面伪代码中描述的两条规则的实现。这些规定禁止来自美国的所有流量，但来自俄勒冈州和华盛顿州的流量除外。地理匹配声明在其检查的所有请求中添加了国家和地区标签。标签匹配规则在地理匹配规则之后运行，因此它可以与地理匹配规则刚刚添加的国家和地区标签进行匹配。地理匹配语句使用转发的 IP 地址，因此标签匹配还指定了转发的 IP 标签。

```
{
  "Name": "geoMatchForLabels",
  "Priority": 10,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "X-Forwarded-For",
        "FallbackBehavior": "MATCH"
      }
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "blockUSButNotOROrWA",
  "Priority": 11,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awsaf:forwardedip:geo:country:US"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "OrStatement": {
                "Statements": [
                  {
                    "LabelMatchStatement": {
                      "Scope": "LABEL",
                      "Key": "awsaf:forwardedip:geo:region:US-OR"
                    }
                  }
                ],
              },
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awsaf:forwardedip:geo:region:US-WA"
              }
            }
          ]
        }
      ]
    }
  }
}
```

```
    }
  }
}
},
"Action": {
  "Block": {}
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "blockUSButNotORorWA"
}
}
```

再举一个例子，您可以将地理匹配与基于费率的规则相结合，为特定国家或地区的用户设置资源优先级。您可以为每个用于区分用户的地理匹配或标签匹配语句创建不同的基于费率的声明。为首选国家或地区的用户设置更高的速率限制，为其他用户设置较低的速率限制。

以下 JSON 列表显示了地理匹配规则，其次是限制来自美国的流量速率的基于速率的规则。这些规定允许来自俄勒冈州的流量比来自该国其他任何地方的流量更高的速度进入。

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "aws:waf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
}
```

```
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rateLimit0regon"
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "aws:waf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "aws:waf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

IP 集匹配规则语句

IP 集匹配语句根据一组 IP 地址和地址范围检查 Web 请求的 IP 地址。使用此选项可根据请求源自的 IP 地址允许或阻止 Web 请求。默认情况下，Amazon WAF 使用来自 Web 请求来源的 IP 地址，但您可以将规则配置为 X-Forwarded-For 改用 HTTP 标头。

Amazon WAF 支持除... 之外的所有 IPv4 和 IPv6 CIDR 范围/0。有关 CIDR 表示法的更多信息，请参阅维基百科条目 [无类别域间路由](#)。一个 IP 集可以容纳多达 10,000 个 IP 地址或 IP 地址范围以供检查。

Note

每个 IP 集匹配规则都引用一个 IP 集，您可以独立于规则创建和维护该集。您可以在多个规则中使用一个 IP 集，并且在更新引用的集合时，Amazon WAF 自动更新引用它的所有规则。

有关创建和管理 IP 集的信息，请参阅 [创建和管理 IP 集 \(p. 114\)](#)。

在规则组或 Web ACL 中添加或更新规则时，选择 IP 集选项，然后选择要使用的 IP 集的名称。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 大多数 1 个 WCU。如果您将语句配置为使用转发的 IP 地址并将位置指定为 ANY，则 WCU 的使用量为 5。

此语句使用以下设置：

- IP 集规范 — 从列表中选择要使用的 IP 集或创建新的 IP 集。
- (可选) 转发 IP 配置 — 用于代替请求源的备用转发 IP 标头名称。您可以指定是否与标题中的第一个、最后一个或任何地址进行匹配。您还可以指定回退行为以应用于指定标头中格式不正确 IP 地址的 Web 请求。备用行为将请求的匹配结果设置为匹配或不匹配。有关更多信息，请参阅[转发的 IP 地址 \(p. 110\)](#)：

在何处查找此规则声明

- 控制台上的 @@ 规则生成器-对于“请求”选项，选择“源自中的 IP 地址”。
- 在控制台上的 @@ 添加我自己的规则和规则组页面 — 选择 IP 设置选项。
- API — [IPSetReferenceStatement](#)

标签匹配规则声明

标签匹配语句根据字符串规范检查 Web 请求中的标签。可用于检查规则的标签是指在同一 Web ACL 评估中其他规则已添加到 Web 请求的标签。标签不会在 Web ACL 评估之外持续存在。

Note

标签匹配语句只能看到之前在 Web ACL 中评估过的规则中的标签。有关如何 Amazon WAF 评估 Web ACL 中的规则和规则组的信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)。

有关标签的更多信息，请参阅[网络请求上的标签 \(p. 123\)](#)。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 1 个 WCU

此语句使用以下设置：

- 匹配范围 — 将其设置为 Label 以匹配标签名称以及 (可选) 前面的命名空间和前缀。将其设置为 Namespace 以匹配部分或全部命名空间规范以及 (可选) 前面的前缀。
- 密钥 — 要与之匹配的字符串。如果您指定命名空间匹配范围，则应仅指定命名空间和前缀 (可选)，并以冒号结尾。如果您指定标签匹配范围，则该范围必须包括标签名称，并且可以选择包括前面的命名空间和前缀。

有关这些设置的信息，请参阅[与标签匹配 \(p. 127\)](#)和[标注分类 \(p. 127\)](#)。

在何处查找此规则声明

- 控制台上的 @@ 规则生成器-对于“请求”选项，选择“有标签”。
- API — [LabelMatchStatement](#)

托管规则组语句

托管规则组规则语句将 Web ACL 规则列表中的引用添加到托管规则组。您在控制台的规则语句下看不到此选项，但是当您使用 Web ACL 的 JSON 格式时，您添加的任何托管规则组都会以这种类型显示在 Web ACL 规则下。

托管规则组要么是Amazon托管规则组（其中大多数对Amazon WAF客户免费），要么是Amazon Web Services Marketplace托管规则组。将付费的Amazon托管规则组添加到 Web ACL 时，您会自动订阅这些规则组。您可以通过订阅Amazon Web Services Marketplace托管规则组Amazon Web Services Marketplace。有关更多信息，请参阅[托管规则组 \(p. 24\)](#)：

将规则组添加到 Web ACL 时，可以将该组中规则的操作改写为其他规则操作。Count有关更多信息，请参阅[规则组中的操作替代 \(p. 14\)](#)：

您可以缩小由规则组Amazon WAF评估的请求范围。为此，您需要在规则组语句内添加范围缩小语句。有关范围缩小语句的信息，请参见[范围缩小声明 \(p. 110\)](#)。这可以帮助您管理规则组如何影响您的流量，并可以帮助您在使用规则组时控制与流量相关的成本。有关在Amazon WAF Bot Control 托管规则组中使用范围缩小语句的信息和示例，请参阅[Amazon WAF机器人控制 \(p. 142\)](#)。

不可嵌套 — 您不能将此语句类型嵌套到其他语句中，也不能将其包含在规则组中。您可以将其直接包含在 Web ACL 中。

（可选）Scope-down 语句 — 此规则类型采用可选的缩小范围语句，以缩小规则组评估的请求的范围。有关更多信息，请参阅[范围缩小声明 \(p. 110\)](#)：

WCU — 在创建时为规则组设置。

在何处查找此规则声明

- 控制台 — 在创建 Web ACL 的过程中，在添加规则和规则组页面上，选择添加托管规则组，然后找到并选择要使用的规则组。
- API — [ManagedRuleGroupStatement](#)

NOT规则语句

NOT规则语句在逻辑上否定单个嵌套语句的结果，因此嵌套语句必须不匹配才能使NOT语句匹配，反之亦然。这需要一个嵌套语句。

例如，如果您要屏蔽并非来自特定国家/地区的请求，请创建一个将操作设置为屏蔽的NOT语句，然后嵌套一个指定国家/地区的地理匹配语句。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU-取决于嵌套语句。

在何处查找此规则声明

- 控制台上的@@ 规则生成器-对于如果请求不匹配，请选择与语句不匹配（不匹配），然后填写嵌套语句。
- API — [NotStatement](#)

OR规则语句

OR规则语句将嵌套语句与OR逻辑结合在一起，因此其中一个嵌套语句必须匹配才能使OR语句匹配。这需要至少一个嵌套语句。

例如，如果您想阻止来自特定国家/地区或包含特定查询字符串的请求，则可以创建一个OR语句并在其中嵌套该国家/地区的地理匹配语句和查询字符串的字符串匹配语句。

相反，如果您想阻止不是来自特定国家/地区或包含特定查询字符串的请求，则应修改先前的OR语句，将地理匹配语句嵌套在语NOT句内低一级。此级别的嵌套要求您使用 JSON 格式，因为控制台仅支持一个级别的嵌套。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU-取决于嵌套语句。

在何处查找此规则声明

- 控制台上的@@ 规则生成器-对于 If 请求，请选择与至少一个语句匹配 (OR)，然后填写嵌套语句。
- API — [OrStatement](#)

示例

以下清单显示了如何使用合并另外两个语句。OR如果任一嵌套OR语句匹配，则该语句为匹配。

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

使用控制台规则可视化编辑器，您可以将大多数可嵌套语句嵌套在逻辑规则语句下，但不能使用可视化编辑器嵌套OR或AND语句。要配置这种类型的嵌套，您需要在 JSON 中提供规则语句。例如，以下 JSON 规则列表包含嵌套在OR语句内的AND语句。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {

```

```
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "aws:waf:managed:aws:bot-control:bot:name:pingdom"
        }
      },
    ],
    {
      "OrStatement": {
        "Statements": [
          {
            "GeoMatchStatement": {
              "CountryCodes": [
                "JM",
                "JP"
              ]
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "JCountryString",
              "FieldToMatch": {
                "Body": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "CONTAINS"
            }
          }
        ]
      }
    ]
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

基于速率的规则语句

基于速率的规则跟踪每个源 IP 地址的请求速率，并在速率超过您所设置的限制的 IP 上触发规则操作。您可以使用这种规则来临时阻止来自发送过多请求的 IP 地址的请求。默认情况下，此规则使用 Web 请求来源的 IP 地址，但您可以配置不同的 IP 地址源。

您可以将范围缩小语句添加到规则中，以便仅跟踪和限制与范围缩小语句匹配的请求并对其进行速率限制。

当触发某个 IP 地址的规则操作时，将该操作Amazon WAF应用于来自与规则的 scope-down 语句相匹配的 IP 地址的请求，直到这些请求的速率降至限制以下。操作更改可能需要一两分钟的时间才能生效。

Note

您还可以使用Amazon WAF机器人控制规则组的目标级别进行速率限制。要进行比较，请参见[基于速率的规则和有针对性的机器人控制规则中的速率限制选项 \(p. 134\)](#)。

您可以设置的最小速率为 100。Amazon WAF 每 30 秒检查一次请求速率，每次对前 5 分钟请求进行计数。因此，IP 地址有可能在 Amazon WAF 检测和阻止请求之前，在 30 秒内以过高的速率发送请求。

Amazon WAF 分别跟踪和管理您使用的基于速率的规则每个实例的 Web 请求。例如，如果您在两个 Web ACL 中提供相同的基于速率的规则设置，则两条规则语句中的每一条都表示基于速率规则的单独实例，并通过 Amazon WAF 进行自己的跟踪和管理。如果在规则组内定义基于速率的规则，然后在多个位置使用该规则组，则每次使用都会创建一个单独的基于速率规则的实例，并通过 Amazon WAF 进行自己的跟踪和管理。

每个基于速率的规则实例最多可以对 10,000 个 IP 地址进行速率限制。如果规则实例识别的 IP 地址超过 10,000 个达到速率限制，则它只会限制最大的 10,000 个发件人。

您可以检索基于速率的规则当前限制速率的 IP 地址列表。任何 IP 地址的速率限制请求都是与基于速率的限制规则中的 scope-down 语句相匹配的请求。有关信息，请参阅 [列出受基于速率的规则进行速率限制的 IP 地址 \(p. 199\)](#)。

缩小基于速率的规则的范围

您可以缩小在基于速率的规则中 Amazon WAF 跟踪和管理的请求范围。为此，您需要在基于速率的语句中嵌套范围缩小语句。

- 如果不使用范围缩小语句，则基于速率的规则会按 IP 地址聚合请求，并对来自超出限制的 IP 地址的所有请求执行操作。
- 使用 scope-down 语句时，该规则仅计算与 scope down 语句匹配的请求，并按 IP 地址汇总这些请求。如果 IP 地址的请求数超过限制，则基于速率的规则仅对来自该 IP 地址且与范围缩减语句匹配的请求执行操作。该规则不检查来自 IP 地址的任何其他请求或对其采取任何操作。

有关范围缩小语句的信息，请参见 [范围缩小声明 \(p. 110\)](#)。

不可嵌套 — 您不能将此语句类型嵌套在其他语句中。您可以将其直接包含在 Web ACL 和规则组中。

(可选) 范围缩小语句-此规则类型采用可选的范围缩小语句，以缩小基于速率的语句所跟踪的请求范围。有关更多信息，请参阅 [范围缩小声明 \(p. 110\)](#)：

WCU — 2 加上嵌套语句的任何其他 WCU。

此语句使用以下可选设置：

- (可选) 转发 IP 配置 — 默认情况下，在 Web 请求来源的 IP 地址上 Amazon WAF 聚合，但您可以改为将规则配置为在 HTTP 标头中使用转发的 IP 地址，例如 X-Forwarded-For。Amazon WAF 使用标头中的第一个 IP 地址。使用此配置，您还可以指定后备行为，以应用于指定标头中格式错误的 IP 地址的 Web 请求。备用行为将请求的匹配结果设置为匹配或不匹配。有关更多信息，请参阅 [转发的 IP 地址 \(p. 110\)](#)：

在何处查找此规则声明

- 控制台上的 Web ACL 中的 @@ 规则生成器 — 在“规则”下的“类型”中，选择基于速率的规则。
- API — [RateBasedStatement](#)

示例

如果您想在不影响网站其他部分的流量的情况下限制网站登录页面的请求数量，则可以创建基于速率的规则，其中包含范围缩小语句来匹配对登录页面的请求。例如，scope-down 语句可能是字符串匹配语句，用于检查 URI 路径并匹配以开头的字符串/login。

再举一个例子，为了应对美国攻击者最近发出的大量请求，您可以创建一个基于速率的规则，该规则含有以下范围缩小语句：

- 包含以下第二层嵌套语句的 AND 规则语句：

- 一个 geo match 语句，用于指定源自美国的请求。
- 一条字符串匹配语句，用于在 User-Agent 标头中搜索字符串 BadBot。

正则表达式匹配规则声明

regex match 语句指示 Amazon WAF 将请求组件与单个正则表达式 (regex) 进行匹配。如果请求组件与您指定的正则表达式匹配，则 Web 请求与语句匹配。

[正则表达式模式集匹配规则语句 \(p. 98\)](#) 对于想要使用数学逻辑组合匹配标准的情况，此语句类型是一个很好的替代方案。例如，如果您希望请求组件与某些正则表达式模式匹配而不与其他正则表达式模式匹配，则可以使用 [AND 规则语句 \(p. 84\)](#) 和组合正则表达式匹配语句 [NOT 规则语句 \(p. 93\)](#)。

Amazon WAF 支持 PCRE 库使用的模式语法 libpcre。该库记录在 [PCRE-Perl 兼容正则表达式](#) 中。

正则表达式模式使用限制

Amazon WAF 不支持 PCRE 库的所有结构。例如，它支持一些零宽度断言，但不是全部。我们没有支持的构造的完整列表。但是，如果您提供的正则表达式模式无效或使用不支持的结构，则 Amazon WAF API 会报告失败。

Amazon WAF 不支持以下 PCRE 模式：

- 反向引用和捕获子表达式
- 子例程引用和递归模式
- 条件模式
- 回溯控制动词
- \C 单字节指令
- \R 换行符匹配指令
- 匹配重置指令的 \K 开头
- 标注和嵌入式代码
- 原子分组和占有式限定符

可 @@ 嵌套 — 您可以嵌套此语句类型。

WCU — 3 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制 [请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见 [网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参阅 [文本转换 \(p. 107\)](#)。

在何处查找此规则声明

- 控制台上的 @@ 规则生成器-对于“匹配类型”，选择“匹配正则表达式”。
- API — [RegexMatchStatement](#)

正则表达式模式集匹配规则语句

正则表达式模式集匹配检查您在正则表达式模式集内指定的正则表达式模式指定的网络请求部分。

Note

每个正则表达式模式集匹配规则引用一个正则表达式模式集，该集的创建和维护独立于规则。您可以在多个规则中使用单个正则表达式模式集，并且在更新引用的集合时，Amazon WAF 自动更新引用它的所有规则。

有关创建和管理正则表达式模式集的信息，请参见[创建和管理正则表达式模式集 \(p. 116\)](#)。

正则表达式模式集合 match 语句指示 Amazon WAF 在您选择的请求组件内搜索集合中的任何模式。如果请求组件与集合中的任何模式匹配，则 Web 请求将与模式集规则语句匹配。

如果你想使用逻辑组合你的正则表达式模式匹配，例如匹配某些正则表达式而不匹配其他正则表达式，可以考虑使用[正则表达式匹配规则声明 \(p. 97\)](#)。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 25 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制[请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见[网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参阅[文本转换 \(p. 107\)](#)。

此语句需要以下设置：

- 正则表达式模式集规范 — 从列表中选择要使用的正则表达式模式集或创建一个新的正则表达式模式集。

在何处查找此规则声明

- 控制台上的@@ 规则生成器-对于匹配类型，选择字符串匹配条件 > 从正则表达式集合中选择匹配模式。
- API — [RegexPatternSetReferenceStatement](#)

规则组语句

规则组规则语句将对您的 Web ACL 规则列表的引用添加到您管理的规则组中。您在控制台的规则语句下看不到这个选项，但是当您使用 Web ACL 的 JSON 格式时，你自己添加的任何规则组都会以这种类型显示在 Web ACL 规则下。有关如何使用您自己的规则组的信息，请参阅[管理您自己的规则组 \(p. 78\)](#)。

将规则组添加到 Web ACL 时，可以将该组中规则的操作改写为其他规则操作。Count 有关更多信息，请参阅[规则组中的操作替代 \(p. 14\)](#)：

不可嵌套 — 您不能将此语句类型嵌套到其他语句中，也不能将其包含在规则组中。您可以将其直接包含在 Web ACL 中。您可以通过在规则组语句中添加一个可嵌套语句作为范围缩小语句来缩小规则组评估的请求的范围。

WCU — 在创建时为规则组设置。

在何处查找此规则声明

- 控制台 — 在创建 Web ACL 的过程中，在添加规则和规则组页面上，选择添加我自己的规则和规则组、规则组，然后添加要使用的规则组。
- API — [RuleGroupReferenceStatement](#)

大小约束规则语句

大小约束语句使用比较运算符（如大于（>）或小于（<））将某个字节数与请求组件大小相比较。例如，您可以使用大小限制语句，查找长度超过 100 字节的查询字符串。

Note

如果选择 URI 作为 Part of the request to filter on 的值，则 URI 中的 / 算作一个字符。例如，URI / logo.jpg 的长度是 9 个字符。

可@@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 1 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制[请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见[网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参见[文本转换 \(p. 107\)](#)。

此外，此语句需要以下设置：

- 大小匹配条件 — 这表示用于将您提供的大小与您选择的请求组件进行比较的数字比较运算符。从列表中选择运算符。
- 大小-比较中使用的大小设置（以字节为单位）。

在何处查找此规则声明

- 控制台上的@@@ 规则生成器-对于匹配类型，在大小匹配条件下，选择要使用的条件。
- API — [SizeConstraintStatement](#)

SQL 注入攻击规则语句

SQL 注入规则语句检查恶意 SQL 代码。攻击者将恶意 SQL 代码插入到 Web 请求中，以便执行修改数据库或从中提取数据等操作。

可@@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 基本成本取决于规则语句的灵敏度级别设置：Low 成本 20 和 High 成本 30。

如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制[请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见[网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参阅[文本转换 \(p. 107\)](#)。

此外，此语句需要以下设置：

- 敏感度级别-此设置调整 SQL 注入匹配条件的敏感度。选项为 LOW 和 HIGH。默认设置为 LOW。

该 HIGH 设置可检测更多 SQL 注入攻击，是推荐设置。由于灵敏度更高，此设置会产生更多误报，尤其是在您的 Web 请求通常包含非常规字符串时。在 Web ACL 测试和调整期间，您可能需要做更多的工作来减少误报。有关信息，请参阅[测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

较低的设置提供不那么严格的 SQL 注入检测，这也会减少误报。LOW 对于具有针对 SQL 注入攻击的其他保护或对误报具有低容忍度的资源，可能是一个更好的选择。

在何处查找此规则声明

- 控制台上的 @@ 规则生成器-对于匹配类型，选择攻击匹配条件 > 包含 SQL 注入攻击。
- API — [SqliMatchStatement](#)

字符串匹配规则语句

字符串匹配语句指示 Amazon WAF 要在请求中搜索的字符串、在请求中的搜索位置以及如何搜索。例如，您可以在请求中查找任何查询字符串开头的特定字符串，也可以查找请求 User-agent 标头的精确匹配项。通常，该字符串由可打印的 ASCII 字符组成，但您可以使用从十六进制 0x00 到 0xFF (十进制 0 到 255) 的任何字符。

可@@ 嵌套 — 您可以嵌套此语句类型。

WCU — 基本成本取决于您使用的比赛类型。

- 与字符串完全匹配 — 2
- 以字符串开头 — 2
- 以@@ 字符串结尾 — 2
- 包含字符串 — 10
- 包含文字 — 10

如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制[请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见[网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前 Amazon WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序 Amazon WAF 处理它们。有关信息，请参阅[文本转换 \(p. 107\)](#)。

此外，此语句需要以下设置：

- 要匹配的字符串-这是您 Amazon WAF 要与指定请求组件进行比较的字符串。通常，该字符串由可打印的 ASCII 字符组成，但您可以使用从十六进制 0x00 到 0xFF（十进制 0 到 255）的任何字符。
- 字符串匹配条件-这表示您 Amazon WAF 要执行的搜索类型。
 - 与字符串完全匹配-字符串和请求组件的值相同。
 - 以字符串开头-字符串出现在请求组件的开头。
 - 以字符串结尾-字符串出现在请求组件的末尾。
 - 包含字符串-该字符串出现在请求组件的任何地方。
 - 包含 word — 您指定的字符串必须出现在请求组件中。对于此选项，您指定的字符串必须仅包含字母数字字符或下划线（A-Z、0-9 或 _）。

请求必须满足以下条件之一：

- 该字符串与请求组件的值完全匹配，例如标头的值。
- 字符串位于请求组件的开头，后跟字母数字字符或下划线（_）以外的字符，例如 BadBot；。
- 字符串位于请求组件的末尾，前面是字母数字字符或下划线（_）以外的字符，例如；BadBot。
- 字符串位于请求组件的中间，并且前面和后面是字母数字字符或下划线（_）之外的字符，例如， - BadBot；。

在何处查找此规则声明

- 控制台上的 @@ 规则生成器-对于匹配类型，选择字符串匹配条件，然后填写要匹配的字符串。
- API — [ByteMatchStatement](#)

跨站点脚本攻击规则语句

XSS（跨站点脚本）攻击语句检查 Web 请求组件中是否存在恶意脚本。在 XSS 攻击中，攻击者将良性网站中的漏洞作为载体，以将恶意客户端站点脚本，注入到其它合法 Web 浏览器中。

可 @@ 嵌套 — 您可以嵌套此语句类型。

WCU — 40 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则基本成本 WCU 的两倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件-Web 请求中要检查的部分，例如，查询字符串或正文。

Warning

如果您检查请求组件 Body、JSON 正文、标头或 Cookie，请阅读有关 Amazon WAF 可以检查多少内容的限制[请求组件的超大处理 \(p. 107\)](#)。

有关 Web 请求组件的信息，请参见[网络请求组件 \(p. 102\)](#)。

- 可选的文本转换-在检查请求组件之前Amazon WAF要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定多个转换，将按列出顺序Amazon WAF处理它们。有关信息，请参阅 [文本转换 \(p. 107\)](#)。

在何处查找此规则声明

- 控制台上的@@ 规则生成器-对于匹配类型，选择攻击匹配条件 > 包含 XSS 注入攻击。
- API — [XssMatchStatement](#)

网络请求组件

本节介绍您可以为检查 Web 请求组件的规则语句指定的设置。有关用法的信息，请参阅各个规则语句。

对于请求组件设置，您需要指定组件类型本身，以及依赖于该类型的其他选项。例如，如果您选择包含要检查的文本的组件类型，则可以在评估检查标准之前指定Amazon WAF要应用的文本转换。

除非另有说明，否则如果 Web 请求没有规则语句中指定的请求组件，则请求结果与规则不匹配。

目录

- [请求组件选项 \(p. 102\)](#)
 - [HTTP method \(p. 103\)](#)
 - [单个标头 \(p. 103\)](#)
 - [所有标题 \(p. 103\)](#)
 - [Cookie \(p. 103\)](#)
 - [URI path \(p. 104\)](#)
 - [查询字符串 \(p. 104\)](#)
 - [Single query parameter \(单个查询参数\) \(p. 104\)](#)
 - [All query parameters \(所有查询参数\) \(p. 104\)](#)
 - [Body \(p. 104\)](#)
 - [json 正文 \(p. 105\)](#)
- [如何检查 HTTP/2 伪标头 \(p. 106\)](#)
- [请求组件的超大处理 \(p. 107\)](#)
- [文本转换 \(p. 107\)](#)

请求组件选项

本节介绍可以指定用于检查的 Web 请求的组件。您可以为在 Web 请求中查找模式的匹配规则语句指定请求组件。这些类型的语句包括字符串匹配、正则表达式匹配、大小限制和 SQL 注入攻击语句。有关如何使用这些请求组件设置的信息，请参阅各个规则语句。有关规则语句的更多信息，请参阅[规则语句列表 \(p. 82\)](#)

除非另有说明，否则如果 Web 请求不包含规则语句中指定的请求组件，则请求结果与规则不匹配。

Note

您可以为每个需要它的规则语句指定一个请求组件。要检查请求的多个组件，请为每个组件创建一条规则语句。

Amazon WAF控制台和 API 文档为以下位置的请求组件设置提供指导：

- 控制台上的@@ 规则生成器-在常规规则类型的语句设置中，在请求组件下的“检查”对话框中选择要检查的组件。

- API 语句内容 —FieldToMatch

本节的其余部分将介绍要检查的 Web 请求部分的选项。

主题

- [HTTP method \(p. 103\)](#)
- [单个标头 \(p. 103\)](#)
- [所有标题 \(p. 103\)](#)
- [Cookie \(p. 103\)](#)
- [URI path \(p. 104\)](#)
- [查询字符串 \(p. 104\)](#)
- [Single query parameter \(单个查询参数\) \(p. 104\)](#)
- [All query parameters \(所有查询参数\) \(p. 104\)](#)
- [Body \(p. 104\)](#)
- [json 正文 \(p. 105\)](#)

HTTP method

检查请求的 HTTP 方法。HTTP 方法指示 Web 请求要求您的受保护资源执行的操作的类型，例如POST或GET。

单个标头

检查请求中的单个命名标头。对于此选项，您可以在标题字段名称中指定标题键，例如User-Agent或Referer。密钥的字符串匹配不区分大小写。

所有标题

检查所有请求标头，包括 Cookie。您可以应用筛选器检查所有标头的子集。对于此选项，您需要提供以下规格：

- 匹配模式-用于获取标题子集以供检查的过滤器。Amazon WAF在标题键中查找这些模式。
匹配模式设置可以是以下之一：
 - 全部 — 匹配所有按键。评估所有标题的规则检查标准。
 - 排除的标头 — 仅检查其键与此处指定的任何字符串都不匹配的标头。密钥的字符串匹配不区分大小写。
 - 包含标头 — 仅检查键与此处指定的字符串之一匹配的标头。密钥的字符串匹配不区分大小写。
- 匹配范围 —Amazon WAF 应使用规则检查标准检查的标头部分。您可以为键和值指定键、值或全部。
- 超大处理 —Amazon WAF 应如何处理标头数据大于Amazon WAF可检查范围的请求。您最多可以检查请求标头的前 8 KB (8,192 字节)，最多检查前 200 个标头。在达到第一个限制之前Amazon WAF，内容可供检查。您可以选择继续检查，也可以选择跳过检查并将请求标记为与规则匹配或不匹配。有关处理超大内容的更多信息，请参阅[请求组件的超大处理 \(p. 107\)](#)。

Cookie

检查所有请求 Cookie。您可以应用筛选器检查所有 Cookie 的子集。对于此选项，您需要提供以下规格：

- 匹配模式 — 用于获取 Cookie 子集以供检查的过滤器。Amazon WAF在 cookie 键中查找这些图案。
匹配模式设置可以是以下之一：
 - 全部 — 匹配所有按键。评估所有 Cookie 的规则检查标准。

- 排除的 Cookie — 仅检查其键与此处指定的任何字符串都不匹配的 Cookie。密钥的字符串匹配区分大小写且必须精确。
- 包含的 Cookie — 仅检查键与此处指定的字符串之一匹配的 Cookie。密钥的字符串匹配区分大小写且必须精确。
- 匹配范围 — Amazon WAF 应使用规则检查标准检查的 Cookie 部分。您可以为键和值指定键、值或全部。
- 超大处理 — Amazon WAF 应如何处理 Cookie 数据超出 Amazon WAF 可检查范围的请求。您最多可以检查请求 cookie 的前 8 KB (8,192 字节)，最多可以检查前 200 个 cookie。在达到第一个限制之前 Amazon WAF，内容可供检查。您可以选择继续检查，也可以选择跳过检查并将请求标记为与规则匹配或不匹配。有关处理超大内容的更多信息，请参阅[请求组件的超大处理 \(p. 107\)](#)。

URI path

检查 URL 中标识资源的部分 (例如) /images/daily-ad.jpg。有关信息，请参阅[统一资源标识符 \(URI\)：一般语法](#)。

如果您不使用带有此选项的文本转换，则 Amazon WAF 不会对 URI 进行标准化，而是会完全按照请求中从客户端收到的 URI 进行检查。有关文本转换的信息，请参见[文本转换 \(p. 107\)](#)。

查询字符串

检查 URL 中在 ? 字符之后出现的部分 (如果有)。

Note

对于跨站点脚本匹配语句，我们建议您选择所有查询参数而不是查询字符串。选择“所有查询参数”会在基本成本的基础上增加 10 个 WCU。

Single query parameter (单个查询参数)

检查您定义为查询字符串一部分的单个查询参数。Amazon WAF 检查您指定的参数的值。

对于此选项，您还需要指定查询参数。例如，如果 URL 为 `www.xyz.com?UserName=abc&SalesRegion=seattle`，则可以 `SalesRegion` 为查询参数指定 `UserName` 或。参数名称的最大长度为 30 个字符。名称不区分大小写，因此，如果您指定 `UserName`，则会 Amazon WAF 匹配包括 `username` 和在内的所有 `UserName` 变体 `UsERName`。

如果查询字符串包含您指定的查询参数的多个实例，则使用 OR 逻辑 Amazon WAF 检查所有值是否匹配。例如，在 URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle` 中，Amazon WAF 根据 `boston` 和 `seattle` 评估您指定的名称。如果匹配其中任意一个，则检查匹配。

All query parameters (所有查询参数)

检查请求中的所有查询参数。这与单个查询参数组件的选择类似，但 Amazon WAF 会检查查询字符串中所有参数的值。例如，如果 URL 为 `www.xyz.com?UserName=abc&SalesRegion=seattle`，并且如果 `UserName` 或 `SalesRegion` 的值与检查条件匹配，Amazon WAF 则会触发匹配。

选择此选项会在基本成本的基础上增加 10 个 WCU。

Body

检查请求正文，以纯文本形式评估。您还可以使用 JSON 内容类型将正文评估为 JSON。

请求正文是请求的一部分，它紧跟请求标头后面。它包含网络请求所需的任何其他数据，例如，来自表单的数据。

- 在控制台中，通过选择内容类型选项纯文本，在请求选项正文下选择此选项。

- 在 API 中，在规则的FieldToMatch规范中，您指定Body以纯文本形式检查请求正文。

必须为此组件类型指定超大处理。您可以检查请求正文的前 8 KB (8,192 字节)。OversizeAmazon WAF 处理定义了如何处理正文数据大于Amazon WAF可检查范围的请求。您可以选择继续检查，也可以选择跳过检查并将请求标记为与规则匹配或不匹配。有关处理超大内容的更多信息，请参阅[请求组件的超大处理 \(p. 107\)](#)。

您也可以将正文评估为已解析的 JSON。有关此问题的信息，请参阅以下部分。

json 正文

检查请求正文，以 JSON 形式评估。您也可以以纯文本形式评估正文。

请求正文是请求的一部分，它紧跟请求标头后面。它包含网络请求所需的任何其他数据，例如，来自表单的数据。

- 在控制台中，通过选择内容类型选项 JSON，在请求选项正文下选择此选项。
- 在 API 中，在规则的FieldToMatch规范中，您可以指定JsonBody。

必须为此组件类型指定超大处理。您可以检查请求正文的前 8 KB (8,192 字节)。OversizeAmazon WAF 处理定义了如何处理正文数据大于Amazon WAF可检查范围的请求。您可以选择继续检查，也可以选择跳过检查并将请求标记为与规则匹配或不匹配。有关处理超大内容的更多信息，请参阅[请求组件的超大处理 \(p. 107\)](#)。

当以已解析的 JSON 形式Amazon WAF检查 Web 请求正文时，它会解析并从 JSON 中提取元素，并使用规则的匹配语句标准检查您指定的部分。

选择此选项会使匹配语句的基本成本 WCU 翻倍。例如，如果不使用 JSON 解析的匹配语句基本成本为 5 个 WCU，则使用 JSON 解析会将成本翻倍至 10 个 WCU。

使用此选项，对 Web 请求正文Amazon WAF运行两种匹配模式。第一个匹配模式的输出用作第二个匹配模式的输入：

1. Amazon WAF解析和提取 JSON 内容并识别要检查的元素。为此，请Amazon WAF使用您在规则的 JSON 正文规范中提供的标准。
2. Amazon WAF将任何文本转换应用于提取的元素，然后将生成的 JSON 元素集与规则语句的匹配标准进行匹配。如果有任何元素匹配，则 Web 请求与规则匹配。

您可以指定以下标准用于第一个模式匹配步骤，Amazon WAF以确定要检查的 JSON 元素：

- 正文解析后备行为 — 如果无法完全解析 JSON 正文，Amazon WAF应该怎么做。这些选项如下所示：
 - 无 (默认行为) - 仅在内容遇到解析错误时才对其进行Amazon WAF评估。
 - 以@@ 字符串形式计算-以纯文本形式检查正文。Amazon WAF将您为 JSON 检查定义的文本转换和检查标准应用于正文文本字符串。
 - Match-将 Web 请求视为与规则语句匹配。Amazon WAF将规则操作应用于请求。
 - 不匹配 — 将 Web 请求视为与规则语句不匹配。

Amazon WAF 会尽最大努力解析整个 JSON 正文，但可能会因为无效字符、重复键、截断以及其根节点不是对象或数组的任何内容等原因而被迫停止。

Amazon WAF将以下示例中的 JSON 解析为两个有效的键:值对：

- 缺少逗号：{"key1":"value1""key2":"value2"}
- 缺少冒号：{"key1":"value1","key2""value2"}
- 额外的冒号：{"key1"::"value1","key2""value2"}
- JSON 匹配范围 — JSON 中Amazon WAF应检查的元素类型。您可以为键和值指定键、值或全部。

- 要检查的内容-已解析和提取的 JSON 中 Amazon WAF 要检查的元素。

您必须指定以下几项之一：

- 完整的 JSON 内容-评估已解析的 JSON 中的所有元素。
- 仅包含元素-仅评估 JSON 中与您提供的 JSON 指针标准相匹配的元素。有关 JSON 指针语法的信息，请参阅互联网工程任务组 (IETF) 文档[JavaScript 对象表示法 \(JSON\) 指针](#)。

不要使用此选项将 JSON 中的所有路径包含为。改用完整 JSON 内容。

例如，在控制台中，您可以提供以下各项：

```
/dogs/0/name  
/dogs/1/name
```

在 API 或 CLI 中，您可以提供以下内容：

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

JSON 车身检查场景示例

如果包含的元素设置为 /a/b，则对于以下 JSON 正文：

```
{  
  "a": {  
    "c": "d",  
    "b": {  
      "e": {  
        "f": "g"  
      }  
    }  
  }  
}
```

以下列表描述了每种匹配范围设置的计算结果。Amazon WAF 密钥 b（包含元素路径的一部分）未经过评估。

- 对于将匹配范围设置为全部：e、f 和 g。
- 对于将匹配范围设置为 keys：e 和 f。
- 对于设置为值的匹配范围：g。

如何检查 HTTP/2 伪标头

支持 HTTP/2 流量的受保护 Amazon 资源不会将 HTTP/2 伪标头转发到 Amazon WAF 进行检查，但它们在 Amazon WAF 检查的 Web 请求组件中提供伪标头的内容。您可以使用 Amazon WAF 此属性仅检查下表中列出的 Visual 标头。

HTTP/2 伪标头内容映射到 Web 请求组件

HTTP/2 伪标头	要检查的 Web 请求组件	文档
:method	HTTP method	HTTP method (p. 103)
:authority	Host 标头	单个标头 (p. 103) 所有标题 (p. 103)

HTTP/2 伪标头	要检查的 Web 请求组件	文档
:pathURI 路径	URI path	URI path (p. 104)
:path query	查询字符串	查询字符串 (p. 104) Single query parameter (单个查询参数) (p. 104) All query parameters (所有查询参数) (p. 104)

请求组件的超大处理

Amazon WAF 不支持检查正文、标头或 Cookie 请求组件的超大内容。底层主机服务对转发给 Amazon WAF 检查的内容有数量和大小限制。例如，主机服务发送的标头不超过 200 个，因此对于包含 205 个标头的 Web 请求，Amazon WAF 无法检查最后 5 个标头。Amazon WAF 当 Amazon WAF 允许 Web 请求继续访问您的受保护资源时，将发送整个 Web 请求，包括能够检查的超出数量和大小限制的任何 Amazon WAF 内容。

限制如下：

- **Body 和 JSON Body** — 您可以检查请求正文的前 8 KB (8,192 字节)。
- **Headers** — 您最多可以检查请求标头的前 8 KB (8,192 字节)，最多检查前 200 个标头。在达到第一个限制之前 Amazon WAF，内容可供检查。
- **Cookies** — 您最多可以检查请求 cookie 的前 8 KB (8,192 字节)，最多可以检查前 200 个 cookie。在达到第一个限制之前 Amazon WAF，内容可供检查。

对于这些组件，在定义规则语句时，需要提供超大处理指令。超大处理指示 Amazon WAF 当规则检查的请求组件超出限制时如何处理 Web 请求。

超大处理选项如下：

- **Continue** — 根据规则检查标准，正常检查请求组件。Amazon WAF 将检查大小限制内的请求组件内容。
- **Match** — 将 Web 请求视为与规则语句匹配。Amazon WAF 将规则操作应用于请求，而不对照规则的检查标准进行评估。
- **No match** — 将 Web 请求视为与规则语句不匹配，而无需根据规则检查标准进行评估。Amazon WAF 继续使用 Web ACL 中的其余规则检查 Web 请求，就像检查任何不匹配的规则一样。

在 Amazon WAF 控制台中，您需要选择以下处理选项之一。在控制台外部，默认值为 Continue。

如果您在将操作设置为的规则中使用该 Match 选项 Block，则该规则将阻止组件类型过大的请求。对于其他配置，请求的最终处置取决于各种因素，例如 Web ACL 中其他规则的配置以及 Web ACL 的默认操作设置。

大小和数量限制适用于您使用的所有规则。这包括您在托管规则组以及其他账户与您共享的规则组中使用但未管理的任何规则。有关在这些情况下管理超大组件的信息，请参见 [检查请求正文、标题和 Cookie \(p. 113\)](#)。

文本转换

在查找模式或设置约束的语句中，您可以提供 Amazon WAF 要在检查请求之前应用的转换。转换会重新设置 Web 请求的格式，消除了一些不寻常的格式，可防范攻击者使用它们以试图绕过 Amazon WAF。

当您将其与 JSON 正文请求组件选择一起使用时，会在解析并从 JSON 中提取要检查的元素后 Amazon WAF 应用转换。有关更多信息，请参阅前一部分：[json 正文 \(p. 105\)](#)。

如果提供多个转换，还应当设置 Amazon WAF 应用这些转换的顺序。

WCU — 每个文本转换都是 10 个 WCU。

Amazon WAF 控制台和 API 文档还在以下位置提供有关这些设置的指南：

- 控制台上的@@ 规则生成器-文本转换。当您使用请求组件时，可使用此选项。
- API 语句内容 —TextTransformations

文本转换的选项

Base64 解码

Amazon WAF对 Base64 编码字符串进行解码。

Base64 解码文本

Amazon WAF解码 Base64 编码的字符串，但使用忽略无效字符的宽容实现。

Command line

此选项可减少攻击者可能注入操作系统命令行命令并使用不寻常的格式伪装部分或全部命令的情况。

使用此选项可执行以下转换：

- 删除以下字符：\ " ' ^
- 删除以下字符之前的空格：/ (
- 将以下字符替换为空格：, ;
- 将多个空格替换为一个空格
- 将大写字母 A-Z 转换为小写字母 a-z

压缩空格空间

Amazon WAF 用一个空格替换多个空格，并将以下字符替换为空格字符（十进制 32）：

- \f，换页符，十进制 12
- \t，制表符，十进制 9
- \n，换行符，十进制 10
- \r，回车符，十进制 13
- \v，垂直制表符，十进制 11
- 不间断空格，十进制 160

CSS 解码

Amazon WAF解码使用 CSS 2.x 转义规则编码的字符syndata.html#characters。此函数在解码过程中最多使用两个字节，因此它可以帮助发现使用 CSS 编码而通常不会被编码的 ASCII 字符。它也可用于反规避，规避是反斜杠和非十六进制字符的组合。例如，javascript 使用 ja\vascript。

逃版标注分类

Amazon WAF解码以下 ANSI C 转义序列:\a, \b, \f, \n, \r, \t, \v, \\\, \?, \', \", \xHH (hexadecimal), \0000 (octal). 无效的编码保留在输出中。

十六进制解码

Amazon WAF将十六进制字符串解码为二进制。

HTML 实体解码代码

Amazon WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 " 替换为 "
- 将 替换为不间断空格（十进制 160）

- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符
- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

JS 解码

Amazon WAF解码 JavaScript 转义序列。如果\uHHHH代码在 ASCII 码的全角 ASCII 码范围内FF01-FF5E，则较高的字节用于检测和调整较低的字节。如果不是，则仅使用较低的字节，将较高的字节归零，从而可能导致信息丢失。

小写

Amazon WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

MD5

Amazon WAF根据输入中的数据计算 MD5 哈希。计算的哈希是原始二进制形式。

无

Amazon WAF检查接收到的 Web 请求，不进行任何文本转换。

标准化路径

Amazon WAF从输入字符串中删除不在输入开头的多个斜杠、目录自引用和目录反向引用。

标准化路径获胜

Amazon WAF处理方式是这样的NORMALIZE_PATH，但首先将反斜杠字符转换为正斜杠。

移除空值

Amazon WAF从输入中删除所有NULL字节。

替换注释

Amazon WAF将每次出现的 C 样式注释 (/*... */) 替换为一个空格。它不会压缩多次连续出现的次数。它将未终止的注释替换为空格 (ASCII 0x20)。它不会更改独立终止的注释 (*/)。

替换空值

Amazon WAF将输入中的NULL字节替换为空格字符 (ASCII 0x20)。

SQL 十六进制解码

Amazon WAF解码 SQL 十六进制数据。例如，(0x414243) 被解码为 (ABC)。

URL decode

Amazon WAF解码 URL 编码的值。

网址解码单元

类似URL_DECODE，但支持微软特定的%u编码。如果代码在 FF01-FF5E 的全角 ASCII 码范围内，则较高的字节用于检测和调整较低的字节。否则，仅使用较低的字节，将较高的字节归零。

UTF8 转 Unicode

Amazon WAF将所有 UTF-8 字符序列转换为 Unicode。这有助于输入规范化，并最大限度地减少非英语语言的误报。

引用集合或规则组的语句

某些规则使用由您、Amazon 或 Amazon Web Services Marketplace 卖家在 Web ACL 之外管理的可重用实体。更新可重用实体时，Amazon WAF 会将更新传播到您的规则。例如，如果您在 Web ACL 中使用

Amazon托管规则组，则在Amazon更新规则组时，会将更改Amazon传播到您的 Web ACL，以更新其行为。如果您在规则中使用 IP set 语句，则在更新该集合时，会将更改Amazon WAF传播到引用该语句的所有规则，因此使用这些规则的任何 Web ACL 都会 up-to-date 与您的更改一起保留。

以下是可在规则语句中使用的可重用实体。

- IP 集 — 您可以创建和管理自己的 IP 集。您可以在控制台上从导航窗格访问这些内容。有关管理 IP 集的信息，请参阅 [IP 集和正则表达式模式集 \(p. 114\)](#)。
- 正则表达式匹配集 — 您可以创建和管理自己的正则表达式匹配集。您可以在控制台上从导航窗格访问这些内容。有关管理正则表达式模式集的信息，请参阅 [IP 集和正则表达式模式集 \(p. 114\)](#)。
- Amazon托管规则组 — Amazon 管理这些规则组。当您托管规则组添加到 Web ACL 时，您可以在控制台上使用这些规则组。有关这些规则组的更多信息，请参阅 [Amazon托管规则组列表 \(p. 32\)](#)。
- Amazon Web Services Marketplace管理规则组 — Amazon Web Services Marketplace 卖家管理这些规则组，您可以订阅它们以使用它们。要管理您的订阅，请在控制台的导航窗格中选择 Amazon Web Services Marketplace。将托管规则组添加到 Web ACL 时，会列出 Amazon Web Services Marketplace 托管规则组。对于尚未订阅的规则组，该页面还会显示指向 Amazon Web Services Marketplace 的链接。有关 Amazon Web Services Marketplace 卖家托管规则组的更多信息，请参阅 [Amazon Web Services Marketplace 托管规则组 \(p. 76\)](#)。
- 您自己的规则组-您可以管理自己的规则组，通常是在您需要一些托管规则组无法实现的行为时。您可以在控制台上从导航窗格访问这些内容。有关更多信息，请参阅[管理您自己的规则组 \(p. 78\)](#)：

删除引用的集合或规则组

当删除引用的实体时，Amazon WAF 会检查当前是否正在 Web ACL 中使用该实体。如果 Amazon WAF 发现该实体正在使用中，它会向您发送警告。Amazon WAF 几乎总能确定实体是否正由 Web ACL 引用。但是在极少数情况下，它可能无法执行此操作。如果您需要确保要删除的实体未在使用中，请在删除它之前先在 Web ACL 中进行检查。

范围缩小声明

scope-down 语句是一种可嵌套的规则语句，您可以将其添加到托管规则组语句或基于速率的语句中，以缩小包含规则评估的请求集。包含规则仅评估与范围缩小语句匹配的请求。

- 托管规则组语句-如果您向托管规则组语句添加范围缩小语句，则任何与缩小范围语句不匹配的请求都将导致与规则组不匹配。仅对与范围缩小语句匹配的请求，才会针对规则组进行评估。对于根据评估的请求数量进行定价的托管规则组，范围缩小声明可以帮助控制成本。有关托管规则组语句的更多信息，请参阅[托管规则组语句 \(p. 92\)](#)。
- 基于速率的规则声明 — 基于速率的规则不带范围缩小语句控制其评估的所有请求的速率。如果您只想控制特定类别请求的速率，则可以在基于速率的规则中添加范围缩小语句。例如，要仅跟踪和控制来自特定地理区域的请求速率，可以在地理匹配规则中指定该地理区域，并将其作为范围缩小语句添加到基于速率的规则中。有关基于速率的规则声明的更多信息，请参阅[基于速率的规则语句 \(p. 95\)](#)。

您可以在范围缩小语句中使用任何可嵌套规则。范围缩小语句的 WCU 是根据您在其中使用的规则语句所需的 WCU 计算的。有关可用语句的列表，请参阅[规则语句列表 \(p. 82\)](#)。

转发的 IP 地址

本节适用于使用 Web 请求的 IP 地址的规则语句。默认情况下，Amazon WAF使用 Web 请求源的 IP 地址。但是，如果 Web 请求通过一个或多个代理或负载均衡器，Web 请求源将包含最后一个代理的地址，而不是客户端的源地址。在这种情况下，原始客户端地址通常在另一个 HTTP 标头中转发。这个标头通常是X-Forwarded-For (XFF)，但可以是不同的标头。

使用 IP 地址的规则语句

使用 IP 地址的规则语句如下：

- [IP 集匹配 \(p. 91\)](#)-检查 IP 地址是否与 IP 集中定义的地址相匹配。
- [地理匹配 \(p. 87\)](#)-使用 IP 地址确定原产国和地区，并将原产国与国家列表进行匹配。
- [基于速率 \(p. 95\)](#)-按其 IP 地址聚合请求，确保没有单个 IP 地址以过高的速率发送请求。

您可以指示Amazon WAF对任何这些规则语句使用转发的 IP 地址，无论是来自X-Forwarded-For标头还是来自其他 HTTP 标头，而不是使用 Web 请求的来源。有关如何提供规范的详细信息，请参阅各个规则语句类型的指南。

Amazon WAF机器人控制中使用的 IP 地址

Bot Control 托管规则组使用来自 IP 地址验证机器人Amazon WAF。如果您使用 Bot Control 并且已验证通过代理或负载均衡器路由的机器人，则需要使用自定义规则明确允许它们。例如，您可以配置自定义 IP 集匹配规则，该规则使用转发的 IP 地址来检测和允许经过验证的机器人。您可以使用该规则通过多种方式自定义机器人管理。有关信息以及示例，请参阅 [Amazon WAF机器人控制 \(p. 142\)](#)。

使用转发 IP 地址的一般注意事项

在使用转发的 IP 地址之前，请注意以下一般注意事项：

- 在此过程中，代理可以修改标头，代理可能会以不同的方式处理标头。
- 攻击者可能会更改标题的内容以尝试绕过Amazon WAF检查。
- 标头内的 IP 地址可能格式错误或无效。
- 您指定的标头可能根本不在请求中。

使用转发 IP 地址的注意事项Amazon WAF

以下列表描述了在中使用转发的 IP 地址的要求和注意事项Amazon WAF：

- 对于任何单个规则，您可以为转发的 IP 地址指定一个标头。标头规范不区分大小写。
- 对于基于速率的规则语句，任何嵌套的作用域语句都不会继承转发的 IP 配置。为使用转发 IP 地址的每条语句指定配置。
- 对于地理匹配和基于费率的规则，Amazon WAF使用标题中的第一个地址。例如，如果标头包含“10.1.1.1、127.0.0.0、10.10.10.10”，则Amazon WAF使用“10.1.1.1”。
- 对于 IP 集匹配，您可以指明是与标头中的第一个、最后一个或任何地址进行匹配。如果您指定任何地址，则Amazon WAF检查标题中的所有地址是否匹配，最多 10 个地址。如果标头中含有超过 10 个地址，Amazon WAF将会检查最后 10 个。
- 包含多个地址的标头必须在地址之间使用逗号分隔符。如果请求使用逗号以外的分隔符，则Amazon WAF认为标头中的 IP 地址格式不正确。
- 如果标头内的 IP 地址格式错误或无效，Amazon WAF则根据您在转发 IP 配置中指定的回退行为将 Web 请求指定为匹配规则或不匹配。
- 如果您指定的标头不在请求中，则根本Amazon WAF不会将规则应用于请求。这意味着Amazon WAF它不应用规则操作，也不应用后备行为。
- 使用转发 IP 标头作为 IP 地址的规则语句不会使用 Web 请求源报告的 IP 地址。

使用转发 IP 地址的最佳实践Amazon WAF

使用转发的 IP 地址时，使用以下最佳实践：

- 在启用转发 IP 配置之前，请仔细考虑请求标头的所有可能状态。您可能需要使用多个规则来获得你想要的行为。
- 要检查多个转发的 IP 标头或检查 Web 请求来源和转发的 IP 标头，请对每个 IP 地址源使用一条规则。

- 要阻止标头无效的 Web 请求，请将规则操作设置为阻止，并将转发的 IP 配置的备用行为设置为匹配。

转发 IP 地址的 JSON 示例

仅当X-Forwarded-For标头包含来源国为 IP 时，以下 geo match 语句才会匹配US：

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

以下基于速率的规则根据X-Forwarded-For标头中的第一个 IP 汇总请求。该规则仅计算与嵌套的 geo match 语句匹配的请求，并且仅阻止与 geo match 语句匹配的请求。嵌套的 geo match 语句还使用X-Forwarded-For标头来确定 IP 地址是否表示原产国US。如果是，或者标题存在但格式不正确，geo match 语句将返回匹配结果。

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      }
    }
  },
  "ForwardedIPConfig": {
    "HeaderName": "x-forwarded-for",
    "FallbackBehavior": "MATCH"
  }
}
```

```
        "HeaderName": "x-forwarded-for",  
        "FallbackBehavior": "MATCH"  
    }  
}  
}
```

检查请求正文、标题和 Cookie

Amazon WAF不支持检查正文、标头或 Cookie 请求组件的超大内容。底层主机服务对转发给Amazon WAF检查的内容有数量和大小限制。例如，主机服务发送的标头不超过 200 个，因此对于包含 205 个标头的 Web 请求，Amazon WAF无法检查最后 5 个标头。Amazon WAF当Amazon WAF允许 Web 请求继续访问您的受保护资源时，将发送整个 Web 请求，包括能够检查的超出数量和大小限制的任何Amazon WAF内容。

限制如下：

- **Body和JSON Body** — 您可以检查请求正文的前 8 KB (8,192 字节)。
- **Headers** — 您最多可以检查请求标头的前 8 KB (8,192 字节)，最多检查前 200 个标头。在达到第一个限制之前Amazon WAF，内容可供检查。
- **Cookies** — 您最多可以检查请求 cookie 的前 8 KB (8,192 字节)，最多可以检查前 200 个 cookie。在达到第一个限制之前Amazon WAF，内容可供检查。

当您添加或更新检查任何受限请求组件的规则时，您需要在组件规范中指定超大内容处理。有关信息，请参阅 [请求组件的超大处理 \(p. 107\)](#)。

当您使用托管规则组或其他账户与您共享的规则组时，该规则组可能具有检查有限请求组件的规则，但该规则无法按照您需要的方式处理超大内容。有关Amazon托管规则的信息，请参阅[Amazon托管规则规则组列表 \(p. 32\)](#)。有关其他规则组的信息，请咨询您的规则组提供商。

处理 Web ACL 中超大组件的方式可能取决于多种因素，例如请求组件内容的预期大小、Web ACL 的默认请求处理以及 Web ACL 中的其他规则如何匹配和处理请求。

以下是管理超大的 Web 请求组件的一般准则：

- 如果您需要允许某些包含超大组件内容的请求，请尽可能添加规则以明确仅允许这些请求。确定这些规则的优先级，使它们在 Web ACL 中检查相同组件类型的任何其他规则之前运行。使用这种方法，您将无法使用Amazon WAF来检查允许传递给受保护资源的超大组件的全部内容。
- 对于所有其他请求，您可以通过阻止超过限制的请求来防止任何额外的字节通过：
 - 您的规则和规则组-在检查大小有限的组件的规则中，配置超大处理，以便阻止超过限制的请求。例如，如果您的规则阻止了具有特定标头内容的请求，则可以将超大处理设置为与标头内容过大的任何请求相匹配。再举一个例子，如果你的 Web ACL 在默认情况下阻止请求并且你的规则允许特定的标头内容，那么你可以配置规则的超大处理，使其不匹配任何标头内容过大的请求。有关处理选项的信息，请参阅[请求组件的超大处理 \(p. 107\)](#)。
 - 您未管理的规则组-为防止未管理的规则组允许超大请求组件，您可以添加单独的规则，检查请求组件类型并阻止超出限制的请求。确定Web ACL 中规则的优先级，使其在规则组之前运行。例如，您可以在 Web ACL 中运行任何正文检查规则之前，阻止正文内容过大的请求。以下过程介绍如何添加此类型的规则。

添加阻止超大内容的规则

1. 创建或编辑 Web ACL 时，在规则设置中，选择添加规则、添加我自己的规则和规则组、规则生成器，然后选择规则可视化编辑器。有关创建或编辑 Web ACL 的指导，请参阅[使用 Web ACL \(p. 17\)](#)。
2. 输入规则的名称，并将“类型”设置保留为“常规”。

3. 将以下匹配设置更改为默认设置：
 - a. 在声明中，对于 Inspect，打开下拉列表并选择所需的 Web 请求组件，即正文、标题或 Cookie。
 - b. 对于匹配类型，选择大于的尺寸。
 - c. 对于大小，键入一个至少为的数字8192。
 - d. 对于超大尺寸处理，请选择“匹配”。
4. 对于“操作”，选择“阻止”。
5. 选择 Add rule。
6. 添加规则后，在“设置规则优先级”页面上，将其移至 Web ACL 中检查相同组件类型的任何规则或规则组之上。这为其设置了较低的数值优先级，这会Amazon WAF导致首先对其进行评估。有关更多信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)：

IP 集和正则表达式模式集

Amazon WAF 将一些更复杂的信息存储在集中，通过在规则中引用它们来加以使用。其中每个集都有一个名称，并在创建时分配了一个 Amazon 资源名称 (ARN)。您可以在规则语句内部管理这些集，也可以通过控制台导航窗格自行访问和管理它们。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他Amazon WAF资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

主题

- [创建和管理 IP 集 \(p. 114\)](#)
- [创建和管理正则表达式模式集 \(p. 116\)](#)

创建和管理 IP 集

IP 集提供要在规则语句中一起使用的 IP 地址和 IP 地址范围的集合。IP 集是Amazon资源。

要在 Web ACL 或规则组中使用 IP 集，您首先创建一个IPSet包含地址规格的Amazon资源。然后，在将 IP 集规则语句添加到 Web ACL 或规则组时引用该集。

主题

- [创建 IP 集 \(p. 115\)](#)
- [在规则组或 Web ACL 中使用 IP 集 \(p. 115\)](#)
- [编辑 IP 集 \(p. 115\)](#)
- [删除 IP 集 \(p. 116\)](#)

创建 IP 集

按照本部分中的过程创建新的 IP 集。

Note

除了本部分中的过程之外，您还可以选择在将 IP 匹配规则添加到 Web ACL 或规则组时添加新的 IP 集。选择该选项需要您提供与此过程所需相同的设置。

创建 IP 集

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 IP sets (IP 集)，然后选择 Create IP set (创建 IP 集)。
3. 输入 IP 集的名称和说明。当您想要使用集时，您可以使用这些信息来标识集。

Note

IP 集在创建之后无法更改名称。

4. 对于区域，选择全球 (CloudFront) 或选择要存储 IP 集的区域。只能在保护区域资源的 Web ACL 中使用区域 IP 集。要在 Web ACL 中使用保护亚马逊 CloudFront 发行版的 IP 集，必须使用 Global (CloudFront)。
5. 对于 IP version (IP 版本)，请选择要使用的版本。
6. 在 IP 地址文本框中，以 CIDR 表示法每行输入一个 IP 地址或 IP 地址范围。Amazon WAF支持除... 之外的所有 IPv4 和 IPv6 CIDR 范围/0。有关 CIDR 表示法的更多信息，请参阅维基百科条目 [Classless Inter-Domain Routing](#)。

下面是一些示例：

- 要指定 IPv4 地址 192.0.2.44，请键入 192.0.2.44/32。
 - 要指定 IPv6 地址 2620:0:2 d 0:200:0:0:0，请键入 2620:0:2 d 0:200:0:0:0/128。
 - 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请键入 192.0.2.0/24。
 - 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。
7. 查看 IP 集的设置，然后选择 Create IP set (创建 IP 集)。

在规则组或 Web ACL 中使用 IP 集

要使用 IP 集，请添加一个规则语句，将其引用到您需要的规则组或 Web ACL。有关信息，请参阅 [IP 集匹配规则语句 \(p. 91\)](#)。

编辑 IP 集

要从 IP 集中添加或删除 IP 地址或 IP 地址范围，或者更改其描述，请执行以下过程。

编辑 IP 集

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 IP sets (IP 集)。
3. 选择要编辑的 IP 集并选择 Edit (编辑)。
4. 根据需要修改 IP 版本和地址。在 IP 地址文本框中，每行必须有一个 IP 地址或 IP 地址范围，采用 CIDR 表示法。Amazon WAF支持除... 之外的所有 IPv4 和 IPv6 CIDR 范围/0。有关 CIDR 表示法的更

多信息，请参阅维基百科条目 [Classless Inter-Domain Routing](#)。对于地址，使用 CIDR 表示法每行输入一个 IP 地址或 IP 地址范围。

下面是一些示例：

- 要指定 IPv4 地址 192.0.2.44，请键入 192.0.2.44/32。
- 要指定 IPv6 地址 2620:0:2 d 0:200:0:0:0，请键入 2620:0:2 d 0:200:0:0:0 /128。
- 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请键入 192.0.2.0/24。
- 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。

5. 选择保存更改。

删除 IP 集

按照本部分中的指导删除引用集。

删除引用的集合和规则组

当您删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时，将 Amazon WAF 检查该实体当前是否正在在 Web ACL 中使用。如果发现它正在使用，则 Amazon WAF 警告您。Amazon WAF 几乎每次都能确定 Web ACL 是否引用实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在 Web ACL 中进行检查。如果实体是引用的集合，请检查是否有规则组正在使用它。

删除 IP 集

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 IP sets (IP 集)。
3. 选择要删除的 IP 集，然后选择 Delete (删除)。

创建和管理正则表达式模式集

正则表达式模式集提供了要在规则语句中一起使用的正则表达式的集合。正则表达式模式集是 Amazon 资源。

要使用在 Web ACL 或规则组中设置的正则表达式模式，首先 `RegexPatternSet` 使用正则表达式模式规范创建 Amazon 资源。然后，在将正则表达式模式集规则语句添加到 Web ACL 或规则组时引用该集。正则表达式模式集必须至少包含一个正则表达式模式。

如果您的正则表达式模式集包含多个正则表达式模式，则在规则中使用该模式时，模式匹配将与 OR 逻辑相结合。也就是说，如果请求组件与集合中的任何模式匹配，Web 请求将匹配模式集规则语句。

Amazon WAF 支持 PCRE 库使用的模式语法 `libpcre`。该库记录在 [PCRE-Perl 兼容正则表达式](#) 中。

正则表达式模式使用限制

Amazon WAF 不支持 PCRE 库的所有结构。例如，它支持一些零宽度断言，但不是全部。我们没有支持的构造的完整列表。但是，如果您提供的正则表达式模式无效或使用不支持的结构，则 Amazon WAF API 会报告失败。

Amazon WAF 不支持以下 PCRE 模式：

- 反向引用和捕获子表达式

- 子例程引用和递归模式
- 条件模式
- 回溯控制动词
- \C 单字节指令
- \R 换行符匹配指令
- 匹配重置指令的 \K 开头
- 标注和嵌入式代码
- 原子分组和占有式限定符

主题

- [创建正则表达式模式集 \(p. 117\)](#)
- [在规则组或 Web ACL 中使用正则表达式模式集 \(p. 118\)](#)
- [删除正则表达式模式集 \(p. 118\)](#)

创建正则表达式模式集

按照本部分中的过程创建新的正则表达式模式集。

创建正则表达式模式集

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Regex pattern sets (正则表达式模式集)，然后选择 Create regex pattern set (创建正则表达式模式集)。
3. 输入正则表达式模式集的名称和描述。当您想要使用集时，您可以使用这些信息来标识集。

Note

正则表达式模式集在创建之后无法更改名称。

4. 对于区域，选择 Global (CloudFront) 或选择要存储正则表达式模式集的区域。只能在保护区域资源的 Web ACL 中使用区域正则表达式模式集。要使用保护亚马逊 CloudFront 发行版的 Web ACL 中设置的正则表达式模式，必须使用 Global (CloudFront)。
5. 在 Regular expressions (正则表达式) 文本框中，每行输入一个正则表达式模式。

例如，正则表达式 `I[a@]mAB[a@]dRequest` 与以下字符串匹

配：`IamABadRequest`、`IamAB@dRequest`、`I@mABadRequest` 和 `I@mAB@dRequest`。

Amazon WAF支持 PCRE 库使用的模式语法`libpcre`。该库记录在 [PCRE-Perl 兼容正则表达式](#)中。

Amazon WAF不支持库的所有结构。例如，它支持一些零宽度断言，但不是全部。我们没有支持的构造的完整列表。但是，如果您提供的正则表达式模式无效或使用不支持的结构，则Amazon WAF API 会报告失败。

Amazon WAF不支持以下 PCRE 模式：

- 反向引用和捕获子表达式
- 子例程引用和递归模式
- 条件模式
- 回溯控制动词
- \C 单字节指令
- \R 换行符匹配指令

- 匹配重置指令的 \K 开头
 - 标注和嵌入式代码
 - 原子分组和占有式限定符
6. 查看正则表达式模式集的设置，然后选择 Create regex pattern set (创建正则表达式模式集)。

在规则组或 Web ACL 中使用正则表达式模式集

要在规则组或 Web ACL 中使用正则表达式模式集，在控制台中，当在规则组或 Web ACL 中添加或更新规则时，请在 Rule builder (规则生成器) 界面中针对 Request option (请求选项) 选择您想要与模式集进行比较的请求组件。选择 Match type (匹配类型) > String match condition (字符串匹配条件) > Matches pattern from regular expression (匹配正则表达式中的模式)，然后选择要使用的正则表达式模式集的名称。

删除正则表达式模式集

按照本部分中的指导删除引用集。

删除引用的集合和规则组

当您删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时，将 Amazon WAF 检查该实体当前是否正在 Web ACL 中使用。如果发现它正在使用，则 Amazon WAF 警告您。Amazon WAF 几乎每次都能确定 Web ACL 是否引用实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在 Web ACL 中进行检查。如果实体是引用的集合，请检查是否有规则组正在使用它。

删除正则表达式模式集

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Regex pattern sets (正则表达式模式集)。
3. 选择要删除的正则表达式模式集，然后选择 Delete (删除)。

中的自定义 Web 请求和响应 Amazon WAF

您可以将自定义 Web 请求和响应处理行为添加到 Amazon WAF 规则操作和默认 Web ACL 操作。只要您的自定义设置所附加的操作适用，它们就会生效。

您可以通过以下方式自定义 Web 请求和响应：

- 使用 Allow、CountCAPTCHA、和 Challenge 操作，您可以在 Web 请求中插入自定义标头。将 Web 请求 Amazon WAF 转发到受保护资源时，请求包含整个原始请求以及您插入的自定义标头。对于 CAPTCHA 和 Challenge 操作，Amazon WAF 仅当请求通过 CAPTCHA 或质询令牌检查时才应用自定义。
- 通过 Block 操作，您可以定义完整的自定义响应，包括响应代码、标头和正文。受保护的资源使用提供的自定义响应来响应请求 Amazon WAF。您的自定义响应替换了默认 Block 操作响应 403 (Forbidden)。

您可以自定义的操作设置

在定义以下操作设置时，可以指定自定义请求或响应：

- 规则操作。有关信息，请参阅 [Amazon WAF 规则操作 \(p. 81\)](#)。
- 网页 ACL 的默认操作。有关信息，请参阅 [决定 Web ACL 的默认操作 \(p. 16\)](#)。

您无法自定义的操作设置

您无法在替换操作中为在 Web ACL 中使用的规则组指定自定义请求处理。请参阅[Web ACL 规则和规则组评估 \(p. 12\)](#)。另请参阅[托管规则组语句 \(p. 92\)](#)和[规则组语句 \(p. 98\)](#)。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他 Amazon WAF 资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

对您使用自定义请求和响应的限制

Amazon WAF 定义了您使用自定义请求和响应的最大设置。例如，每个 Web ACL 或规则组的最大请求标头数，以及单个自定义响应定义的最大自定义标头数。有关信息，请参阅[Amazon WAF 配额 \(p. 230\)](#)。

主题

- [为非阻塞操作插入自定义请求标头 \(p. 119\)](#)
- [对Block操作的自定义响应 \(p. 120\)](#)
- [自定义响应支持的状态码 \(p. 122\)](#)

为非阻塞操作插入自定义请求标头

当规则操作未阻止请求时，您可以指示 Amazon WAF 将自定义标头插入到原始 HTTP 请求中。使用此选项，您只能添加到请求中。您不能修改或替换原始请求的任何部分。自定义标头插入的用例包括向下游应用程序发出信号，要求其根据插入的标头以不同的方式处理请求，以及标记请求以供分析。

此选项适用于规则操作 AllowCountCAPTCHA、Challenge 和以及设置为的 Web ACL 默认操作 Allow。有关规则操作的更多信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。有关默认 Web ACL 操作的更多信息，请参阅[决定 Web ACL 的默认操作 \(p. 16\)](#)。

自定义请求标头名称

Amazon WAF 为它插入的所有请求标头添加前缀 x-amzn-waf-，以避免与请求中已有的标头混淆。例如，如果您指定标题名称 sample，则 Amazon WAF 插入标题 x-amzn-waf-sample。

同名标题

如果请求中已经有 Amazon WAF 正在插入的同名标头，则 Amazon WAF 覆盖该标头。因此，如果您在多个具有相同名称的规则中定义标头，则检查请求并找到匹配项的最后一条规则将添加其标头，而之前的任何规则都不会。

带有非终止规则操作的自定义标头

与 Allow 操作不同，该 Count 操作不会停止 Amazon WAF 使用 Web ACL 中的其余规则处理 Web 请求。同样 CAPTCHA，当 Challenge 确定请求令牌有效时，这些操作不会停止 Amazon WAF 处理 Web 请求。因此，如果您使用包含其中一项操作的规则插入自定义标头，则后续规则也可能插入自定义标头。有关规则操作行为的更多信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

例如，假设您具有以下规则，按所示顺序确定优先级：

1. RuleA 包含Count操作和名为的自定义标头RuleAHeader。
2. RuleB 包含一个Allow操作和一个名为的自定义标头RuleBHeader。

如果请求同时匹配 RuleA 和 RuleB，则Amazon WAF插入标头x-amzn-waf-RuleAHeader和x-amzn-waf-RuleBHeader，然后将请求转发到受保护的资源。

Amazon WAF在 Web 请求完成检查后，将自定义标头插入到 Web 请求中。因此，如果您在将操作设置为的规则下使用自定义请求处理Count，则后续规则不会检查您添加的自定义标头。

自定义请求处理示例

您可以为规则的操作或 Web ACL 的默认操作定义自定义请求处理。以下清单显示了添加到 Web ACL 默认操作中的用于自定义处理的 JSON。

```
{
  "Name": "SampleWebACL",
  "Scope": "REGIONAL",
  "DefaultAction": {
    "Allow": {
      "CustomRequestHandling": {
        "InsertHeaders": [
          {
            "Name": "fruit",
            "Value": "watermelon"
          },
          {
            "Name": "pie",
            "Value": "apple"
          }
        ]
      }
    }
  },
  "Description": "Sample web ACL with custom request handling configured for default action.",
  "Rules": [],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "SampleWebACL"
  }
}
```

对Block操作的自定义响应

对于设置Amazon WAF为的规则操作或 Web ACL 默认操作，您可以指示将自定义 HTTP 响应发送回客户端Block。有关规则操作的更多信息，请参阅 [Amazon WAF 规则操作 \(p. 81\)](#)。有关默认 Web ACL 操作的更多信息，请参阅 [决定 Web ACL 的默认操作 \(p. 16\)](#)。

为操作定义自定义响应处理时，需要定义状态码、标头和响应正文。Block有关您可以使用的状态码列表Amazon WAF，请参阅以下部分 [自定义响应支持的状态码 \(p. 122\)](#)。

使用案例

自定义响应的使用场景包括：

- 将非默认状态码发送回客户端。

- 将静态错误页面发送回客户端。
- 将客户端重定向到不同的 URL。为此，您需要指定一个 3xx 重定向状态代码，例如 301（Moved Permanently）或 302（Found），然后指定一个以新 URL 命名的新 Location 头。

与您在受保护资源中定义的响应的交互

您为 Amazon WAFBlock 操作指定的自定义响应优先于您在受保护资源中定义的任何响应规范。

用于保护的 Amazon 资源的主机服务 Amazon WAF 可能允许对 Web 请求进行自定义响应处理。示例包括：

- 使用亚马逊 CloudFront，您可以根据状态代码自定义错误页面。有关信息，请参阅《亚马逊 CloudFront 开发者指南》中的“[生成自定义错误响应](#)”。
- 使用 Amazon API Gateway，您可以为网关定义响应和状态代码。有关信息，请参阅《亚马逊 API Gateway 开发者指南》中的 API 网关 [中的网关响应](#)。

您无法在受保护 Amazon 资源中将 Amazon WAF 自定义响应设置与自定义响应设置合并。任何单个 Web 请求的响应规范要么完全来自受保护的资源，要么完全来自 Amazon WAF。

对于 Amazon WAF 阻塞的 Web 请求，以下内容显示了优先顺序。

1. Amazon WAF 自定义响应-如果 Amazon WAFBlock 操作启用了自定义响应，则受保护的资源会将配置的自定义响应发送回客户端。无论中定义的自定义响应仅指定 HTTP 代码、仅 Amazon WAF 指定自定义页面，还是两者都适用。您可能在受保护资源本身中定义的任何响应设置都无效。
2. 在 @@@ 受保护资源中定义的自定义响应-否则，如果受保护资源指定了自定义响应设置，则受保护资源使用这些设置来响应客户端。
3. Amazon WAF 默认 Block 响应 — 否则，受保护的资源将使用 Amazon WAF 默认 Block 响应响应客户端 403（Forbidden）。

对于 Amazon WAF 允许的 Web 请求，您对受保护资源的配置决定了它发送回客户端的响应。您无法在 Amazon WAF 为允许的请求配置响应设置。您可以 Amazon WAF 为允许的请求配置的唯一自定义设置是在原始请求中插入自定义标头，然后再将请求转发到受保护的资源。此选项在上一节中进行了描述 [为非阻塞操作插入自定义请求标头 \(p. 119\)](#)。

自定义响应正文

您可以在要使用自定义响应的 Web ACL 或规则组的上下文中定义自定义响应的正文。定义自定义响应正文后，可以在创建自定义响应正文的 Web ACL 或规则组中的任何其他位置通过引用使用它。在单个 Block 操作设置中，您可以引用要使用的自定义正文，并定义自定义响应的状态代码和标题。

当您在控制台中创建自定义响应时，可以从已定义的响应正文中进行选择，也可以创建新的响应正文。在控制台之外，您可以在 Web ACL 或规则组级别定义自定义响应正文，然后从 Web ACL 或规则组中的操作设置中引用它们。如下部分的示例 JSON 所示。

自定义响应示例

以下示例列出了具有自定义响应设置的规则组的 JSON。为整个规则组定义自定义响应正文，然后在规则操作中按键引用。

```
{
  "ARN": "test_rulegroup_arn",
  "Capacity": 1,

  "CustomResponseBodies": {
    "CustomResponseBodyKey1": {
      "Content": "This is a plain text response body.",
      "ContentType": "TEXT_PLAIN"
    }
  }
}
```



```
},
"Description": "This is a test rule group.",
"Id": "test_rulegroup_id",
"Name": "TestRuleGroup",
"Rules": [
{
  "Action": {
    "Block": {
      "CustomResponse": {
        "CustomResponseBodyKey": "CustomResponseBodyKey1",
        "ResponseCode": 404,
        "ResponseHeaders": [
          {
            "Name": "BlockActionHeader1Name",
            "Value": "BlockActionHeader1Value"
          }
        ]
      }
    }
  },
  "Name": "GeoMatchRule",
  "Priority": 1,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestRuleGroupReferenceMetric",
    "SampledRequestsEnabled": true
  }
},
{
  "Name": "TestRuleGroupMetric",
  "Priority": 1,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestRuleGroupMetric",
    "SampledRequestsEnabled": true
  }
}
]
```

自定义响应支持的状态码

有关 HTTP 状态码的详细信息，请参阅互联网工程任务组 (IETF) 的[状态码](#)和维基百科上的[HTTP 状态码列表](#)。

以下是Amazon WAF支持自定义响应的 HTTP 状态码。

- 2xx Successful
 - 200 – OK
 - 201 – Created
 - 202 – Accepted
 - 204 – No Content
 - 206 – Partial Content
- 3xx Redirection
 - 300 – Multiple Choices

- 301 – Moved Permanently
- 302 – Found
- 303 – See Other
- 304 – Not Modified
- 307 – Temporary Redirect
- 308 – Permanent Redirect
- 4xx Client Error
 - 400 – Bad Request
 - 401 – Unauthorized
 - 403 – Forbidden
 - 404 – Not Found
 - 405 – Method Not Allowed
 - 408 – Request Timeout
 - 409 – Conflict
 - 411 – Length Required
 - 412 – Precondition Failed
 - 413 – Request Entity Too Large
 - 414 – Request-URI Too Long
 - 415 – Unsupported Media Type
 - 416 – Requested Range Not Satisfiable
 - 421 – Misdirected Request
 - 429 – Too Many Requests
- 5xx Server Error
 - 500 – Internal Server Error
 - 501 – Not Implemented
 - 502 – Bad Gateway
 - 503 – Service Unavailable
 - 504 – Gateway Timeout
 - 505 – HTTP Version Not Supported

网络请求上的标签

标签是通过匹配规则添加到 Web 请求的元数据。您可以使用标签将规则匹配结果传达给稍后在同一 Web ACL 中评估的规则。

- 任何不是规则组参考声明的规则都可以为匹配的 Web 请求添加标签。当 Web 请求与规则匹配时，Amazon WAF 将该规则的标签添加到请求中。对于地理匹配规则，Amazon WAF 将规则的标签添加到规则检查、匹配或不匹配的任何请求中。
- Amazon WAF 在规则对请求的检查结束时为请求添加标签。因此，当单个规则包含多个语句时，例如在逻辑 AND 或 OR 语句中，只有在评估了所有包含的语句之后，包含的语句分配的任何标签才在 Web 请求中可用。
- 添加后，只要根据 Web ACL 对请求进行评估 Amazon WAF，标签就会在请求上保持可用。
- 您可以使用标签匹配语句与规则的请求检查标准中的标签进行匹配。有关声明的详细信息，请参阅[标签匹配规则声明 \(p. 92\)](#)。

Amazon WAF 标签的常见使用场景包括：

- 在对请求采取操作之前，根据多个规则语句评估 Web 请求-在 Web ACL 中找到与 Web ACL 中的规则匹配后，如果规则操作是，则 Amazon WAF 继续根据 Web ACL 评估该请求 Count。在决定允许或阻止请求之前，您可以使用标签评估和收集来自多个规则的信息。为此，请将现有规则的操作更改为，Count 并将其配置为向匹配的请求添加标签。然后，添加一个或多个新规则，在您的其他规则之后运行，并将它们配置为评估标签并根据标签匹配组合管理请求。
- 按地理区域管理 Web 请求 — 您可以单独使用地理匹配规则来管理来源国的 Web 请求。要将位置微调到区域级别，您可以使用地理匹配规则，然后使用计数操作和标签匹配规则。有关地理匹配规则的信息，请参阅[地理匹配规则语句 \(p. 87\)](#)。
- 在多个规则之间重用逻辑-如果您需要在多个规则中重复使用相同的逻辑，则可以使用标签来单一来源逻辑，然后测试结果。当您有多个使用嵌套规则语句的常见子集的复杂规则时，在复杂规则中复制通用规则集可能既耗时又容易出错。使用标签，您可以使用公共规则子集创建新规则，该子集对匹配的请求进行计数并为其添加标签。您可以将新规则添加到 Web ACL，使其在原始复杂规则之前运行。然后，在原始规则中，将共享规则子集替换为检查标签的单个规则。

例如，假设你有多条规则，只想应用于你的登录路径。与其让每条规则指定相同的逻辑来匹配潜在的登录路径，不如实现包含该逻辑的单个新规则。让新规则为匹配的请求添加标签，以表明该请求位于登录路径上。在您的 Web ACL 中，将此新规则的数字优先级设置为比原始规则更低的数值优先级，以便它首先运行。然后，在原始规则中，将共享逻辑替换为检查标签是否存在。有关优先级设置的信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)。

- 为规则组中的规则创建例外-此选项对于您无法查看或更改的托管规则组特别有用。许多托管规则组规则都会为匹配的 Web 请求添加标签，以指明匹配的规则，并可能提供有关匹配的更多信息。当您使用向请求添加标签的规则组时，您可以改写规则组规则以计算匹配次数，然后在根据规则组标签处理 Web 请求的规则组之后运行规则。所有 Amazon 托管规则组将标签添加到匹配的 Web 请求。有关详细信息，请参阅中的规则描述[Amazon 托管规则组列表 \(p. 32\)](#)。

Amazon 托管规则组向其评估的 Web 请求添加标签。这些标签大多是由规则组中的规则添加的。有些标签是由托管规则使用的 Amazon 进程添加的。例如，防止账户盗用和机器人控制管理规则组使用 Amazon WAF 令牌管理为请求添加标签，以指示其代币的状态。有关托管规则组及其添加的标签的信息，请参阅[Amazon 托管规则组列表 \(p. 32\)](#)。

标注分类

当规则与 Web 请求匹配时，如果规则已定义标签，则 Amazon WAF 会将标签添加到请求中。在同一 Web ACL 中匹配规则之后评估的规则可以访问该规则添加的标签，并且可以与这些标签进行匹配。

- 单个 Web ACL 中包含的任何规则都可以访问已在同一 Web ACL 中运行的任何规则添加的标签。这包括直接在 Web ACL 中定义的规则以及在 Web ACL 中使用的规则组内部定义的规则。Web ACL 评估结束后，标签不会保留在 Web 请求中。
- 为了使其他规则与您的规则添加的标签相匹配，您的规则操作不得终止 Web ACL 对 Web 请求的评估。规则操作必须设置为 CountCAPTCHA、或 Challenge。当 Web ACL 评估未终止时，Web ACL 中的后续规则可以根据请求运行其标签匹配标准。有关规则操作的更多信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。
- 标签会在任何单个请求中发出前 100 个标签的亚马逊 CloudWatch 指标。有关信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。
- Amazon WAF 在日志中记录请求的前 100 个标签的标签。您可以使用标签和规则操作来筛选 Amazon WAF 记录的日志。有关信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)。
- 您的 Web ACL 评估可以将 100 多个标签应用于 Web 请求并与 100 多个标签进行匹配，但 Amazon WAF 只能在日志和指标中记录前 100 个。

标签语法和命名要求

标签是由前缀、可选命名空间和名称组成的字符串。标签的组成部分用冒号分隔。标签具有以下要求和特征：

- 标签区分大小写。
- 每个标签命名空间或标签名称最多可包含 128 个字符。
- 您最多可以在标签中指定五个命名空间。
- 标签的组成部分由冒号 (:) 分隔。
- 您不能在为标签指定的命名空间或名称中使用以下保留字符串：`aws:wafaws`、`waf`、`rulegroup`、`webacl`、`regexpatternset` 和 `managed`。

标签语法

完全限定的标签具有前缀、可选命名空间和标签名称。前缀用于标识添加标签的规则或 Web ACL 上下文。命名空间可用于为标签添加更多上下文。标签名称为标签提供了最低的详细级别。它通常表示向请求添加标签的特定规则。

标签前缀因其来源而异。

- 您的标签-以下显示了您在 Web ACL 和规则组规则中创建的标签的完整标签语法。实体类型为 `rulegroup` 和 `webacl`。

```
aws:waf:<entity owner account id>:<entity type>:<entity name>:<custom namespace>:...:<label name>
```

- 标签命名空间前缀：`aws:waf:<entity owner account id>:<entity type>:<entity name>`;
- 添加自定义命名空间：`<custom namespace>:...:`

在规则组或 Web ACL 中为规则定义标签时，您可以控制自定义命名空间字符串和标签名称。其余部分由您生成 Amazon WAF。Amazon WAF 自动为所有标签加上账户 `aws:waf` 和 Web ACL 或规则组实体设置的前缀。

- 托管规则组标签-以下显示了由托管规则组中的规则创建的标签的完整标签语法。

```
aws:waf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

- 标签命名空间前缀：`aws:waf:managed:<vendor>:<rule group name>`;
- 添加自定义命名空间：`<custom namespace>:...:`

所有 Amazon 托管规则组都添加标签。有关托管规则组的信息，请参阅[托管规则组 \(p. 24\)](#)。

- 来自其他 Amazon 进程的标签-这些进程由 Amazon Managed Rules 规则组使用，因此您可以看到它们已添加到使用托管规则组评估的 Web 请求中。以下显示了由托管规则组调用的进程创建的标签的完整标签语法。

```
aws:waf:managed:<process>:<custom namespace>:...:<label name>
```

- 标签命名空间前缀：`aws:waf:managed:<process>`;
- 添加自定义命名空间：`<custom namespace>:...:`

列出了调用该 Amazon 进程的托管规则组的此类标签。有关托管规则组的信息，请参阅[托管规则组 \(p. 24\)](#)。

您的规则的标签示例

以下示例标签由名为 `testRules` 的规则组中的规则定义，该规则组属于该账户 `111122223333`。

```
aws:waf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
aws:waf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
aws:waf:111122223333:rulegroup:testRules:LabelNameZ
```

下面的列表显示 JSON 中的标签规范示例。这些标签名称包括结束标签名称之前的自定义命名空间字符串。

```
Rule: {
  Name: "label_rule",
  Statement: {...}
  RuleLabels: [
    Name: "header:encoding:utf8",
    Name: "header:user_agent:firefox"
  ],
  Action: { Count: {} }
}
```

Note

您可以通过规则 JSON 编辑器在控制台中访问此类列表。

如果您在与前面的标签示例相同的规则组和账户中运行上述规则，则生成的完全限定标签将如下所示：

```
aws:waf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
aws:waf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

托管规则组的标签示例

以下显示了 Amazon 托管规则规则组及其调用的进程的示例标签。

```
aws:waf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
aws:waf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
aws:waf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
aws:waf:managed:token:accepted
```

为匹配的 Web 请求添加标签

为规则定义标签时，Amazon WAF 会将标签添加到与规则匹配的请求中。通过指定要附加到标签命名空间前缀的自定义命名空间字符串和名称，可以在规则中定义标签。Amazon WAF 从定义规则的上下文中派生前缀。有关此问题的信息，请参阅下面的标签语法信息 [标签语法和命名要求 \(p. 124\)](#)。

除以下内容外，您可以向任何规则添加标签，Amazon WAF 并将您的标签添加到与规则匹配语句的任何 Web 请求中：

- 对于基于速率的规则，标签仅添加到特定 IP 地址的 Web 请求中，而 Amazon WAF 由于速率限制，该 IP 地址会被阻止。有关基于速率的规则的信息，请参阅 [基于速率的规则语句 \(p. 95\)](#)。

- 您不能在引用规则组的语句中使用标签。如果您尝试通过 API 向规则组规则语句添加标签，则该操作会引发验证异常。有关这些语句类型的信息，请参见[托管规则组语句 \(p. 92\)](#)和[规则组语句 \(p. 98\)](#)。

WCU — 在 Web ACL 或规则组规则中每定义 5 个标签 1 个 WCU。

此语句的查找位置

- 控制台上的@@ 规则生成器-在规则的“操作”设置下，在“标签”下。
- API 数据类型 —RuleRuleLabels

与标签匹配

您可以使用标签匹配语句来评估 Web 请求标签。您可以与 Label 进行匹配，前者需要标签名称，也可以与 Name space 匹配，后者需要命名空间规范。对于标签或命名空间，您可以选择在规范中包含前面的命名空间和前缀。有关此语句类型的一般信息，请参见[标签匹配规则声明 \(p. 92\)](#)。

标签的前缀用于定义标签规则的规则组或 Web ACL 的上下文。在规则的标签匹配语句中，如果您的标签或命名空间匹配字符串未指定前缀，则 Amazon WAF 使用标签匹配规则的前缀。

- 直接在 Web ACL 中定义的规则的标签带有指定 Web ACL 上下文的前缀。
- 规则组内部规则的标签带有指定规则组上下文的前缀。这可能是您自己的规则组，也可以是为您管理的规则组。

有关这方面的信息，请参阅下面的标签语法[标签语法和命名要求 \(p. 124\)](#)。

Note

一些托管规则组会添加标签。您可以通过调用通过 API 检索这些信息 DescribeManagedRuleGroup。标签在响应的 AvailableLabels 属性中列出。

如果您想匹配与规则上下文不同的规则，则必须在匹配字符串中提供前缀。例如，如果您想与托管规则组中规则添加的标签进行匹配，则可以在您的 Web ACL 中添加一个带有标签匹配语句的规则，其匹配字符串指定了规则组的前缀，然后是其他匹配条件。

在标签匹配语句的匹配字符串中，指定标签或命名空间：

- 标签 — 比赛的标签规范由标签的结尾部分组成。可以在标签名称前面加上任意数量的连续命名空间。您可以通过以前缀开头的规范来提供完全合格的标签。

示例规范：

- testNS1:testNS2:LabelNameA
- awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA
- 命名空间 — 匹配的命名空间规范由标签规范的任何连续子集组成，名称除外。您可以包含前缀，也可以包含一个或多个命名空间字符串。

示例规范：

- testNS1:testNS2:
- awswaf:managed:aws:managed-rule-set:testNS1:

标注分类

本节提供标签匹配规则语句的匹配规范示例。

Note

这些 JSON 列表是在控制台中创建的，方法是向带有标签匹配规范的 Web ACL 添加规则，然后编辑规则并切换到规则 JSON 编辑器。您还可以通过 API 或命令行界面获取规则组或 Web ACL 的 JSON。

主题

- [与本地唱片公司匹配 \(p. 128\)](#)
- [与其他上下文的标签进行匹配 \(p. 128\)](#)
- [与托管规则组标签进行匹配 \(p. 129\)](#)
- [与本地命名空间匹配 \(p. 129\)](#)
- [匹配托管规则组命名空间 \(p. 130\)](#)

与本地唱片公司匹配

以下 JSON 列表显示了已在本地添加到 Web 请求中的标签的标签匹配语句，其上下文与此规则相同。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

如果您在账户 111122223333 中使用此匹配语句，则在您为 Web ACL 定义的规则中 testWebACL，它将与以下标签相匹配。

```
awsfaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awsfaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

它与以下标签不匹配，因为标签字符串不完全匹配。

```
awsfaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

它与以下标签不匹配，因为上下文不一样，所以前缀不匹配。即使您将规则组 productionRules 添加到定义规则的 Web ACL 中 testWebACL，也是如此。

```
awsfaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

与其他上下文的标签进行匹配

以下 JSON 列表显示了与用户创建的规则组内规则中的标签匹配的标签匹配规则。对于在 Web ACL 中运行但不属于命名规则组的所有规则，规范中都需要使用前缀。此示例标签规范仅与确切的标签相匹配。


```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "aws:waf:111122223333:rulegroup:testRules:header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

与托管规则组标签进行匹配

这是与来自匹配规则以外的其他上下文的标签进行匹配的特殊情况。以下 JSON 列表显示了托管规则组标签的标签匹配语句。这仅匹配标签匹配语句的键设置中指定的精确标签。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "LABEL",
      Key: "aws:waf:managed:aws:managed-rule-set:header:encoding:utf8"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

与本地命名空间匹配

以下 JSON 列表显示了本地命名空间的标签匹配语句。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
      Key: "header:encoding:"
    }
  },
  Labels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

与本地 Label 匹配类似，如果您在账户 111122223333 中使用此语句，则在您为 Web ACL 定义的规则中 testWebACL，它将与以下标签匹配。

```
aws:waf:111122223333:webacl:testWebACL:header:encoding:utf8
```

它与以下标签不匹配，因为账户不一样，所以前缀不匹配。

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

前缀也与托管规则组应用的任何标签都不匹配，如下所示。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

匹配托管规则组命名空间

以下 JSON 列表显示了托管规则组命名空间的标签匹配语句。对于您拥有的规则组，您还需要提供前缀以匹配规则上下文之外的命名空间。

```
Rule: {
  Name: "match_rule",
  Statement: {
    LabelMatchStatement: {
      Scope: "NAMESPACE",
      Key: "awswaf:managed:aws:managed-rule-set:header:"
    }
  },
  RuleLabels: [
    ...generate_more_labels...
  ],
  Action: { Block: {} }
}
```

此规范与以下示例标签相匹配。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

它与以下标签不匹配。

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

Amazon WAF 智能威胁缓解

本节介绍由提供的托管智能威胁缓解功能 Amazon WAF。这些是高级的专业保护措施，您可以实施这些保护措施来防范恶意机器人和帐户接管企图等威胁。

Note

除了基本使用费用外，此处描述的功能还会产生额外费用 Amazon WAF。有关更多信息，请参阅 [Amazon WAF 定价](#)。

本节提供的指南适用于一般了解如何创建和管理 Amazon WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前几部分所涵盖的。

主题

- [智能威胁缓解选项 \(p. 131\)](#)
- [智能威胁缓解最佳实践 \(p. 135\)](#)

- [Amazon WAF网络请求令牌 \(p. 136\)](#)
- [Amazon WAF机器人控制 \(p. 142\)](#)
- [Amazon WAF欺诈控制账户收购预防 \(ATP\) \(p. 155\)](#)
- [Amazon WAF客户机应用程序集成 \(p. 164\)](#)
- [CAPTCHA以及中的Challenge操作Amazon WAF \(p. 175\)](#)

智能威胁缓解选项

本节详细比较了实施智能威胁缓解的选项。

Amazon WAF为智能威胁缓解提供以下类型的保护。

- Amazon WAF防欺诈控制账户接管 (ATP) — 检测和管理应用程序登录页面上的恶意接管尝试。核心功能由 ATP 托管规则组提供。有关更多信息，请参阅 [Amazon WAF欺诈控制账户收购预防 \(ATP\) \(p. 155\)](#) 和 [Amazon WAF欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。
- Amazon WAF机器人控制 — 识别、标记和管理友好和恶意机器人。此功能为具有跨应用程序唯一签名的常见机器人提供管理，也为具有特定应用程序签名的目标机器人提供管理。核心功能由 Bot Control 托管规则组提供。有关更多信息，请参阅 [Amazon WAF机器人控制 \(p. 142\)](#) 和 [Amazon WAF机器人控制规则组 \(p. 49\)](#)。
- 客户端应用程序集成 SDK — 验证客户端会话并获取Amazon WAF令牌以供客户端在其 Web 请求中使用。如果您使用 ATP 或 Bot Control，请尽可能在客户端应用程序中实现应用程序集成 SDK，以充分利用所有规则组功能。仅当需要快速保护关键资源且没有足够的时间进行 SDK 集成时，我们才建议使用这些未集成 SDK 的规则组作为临时措施。有关实现开发工具包的信息，请参阅[Amazon WAF客户机应用程序集成 \(p. 164\)](#)。
- Challenge和CAPTCHA规则操作 — 验证客户端会话和最终用户并获取Amazon WAF令牌供客户端在其 Web 请求中使用。您可以在指定规则操作的任何地方、在规则中实现这些操作，也可以在您使用的规则组中将其作为替代项实现。这些操作使用Amazon WAF JavaScript 插页式广告来询问客户机或最终用户，并且需要支持的客户端应用程序 JavaScript。有关更多信息，请参阅[CAPTCHA以及中的Challenge操作 Amazon WAF \(p. 175\)](#)：

ATP 和 Bot Control 管理规则组使用令牌进行高级检测。有关令牌在规则组中启用的功能的信息，请参阅[为什么要将应用程序集成 SDK 与 ATP 一起使用 \(p. 156\)](#)和[为什么要使用带有 Bot Control 的应用程序集成 SDK \(p. 143\)](#)。

实施智能威胁缓解的选项从基本使用规则操作来发起挑战和强制获取代币，到Bot Control和ATPAmazon Managed Rules规则组提供的高级功能，不一而足。

下表详细比较了基本功能和高级功能的选项。

主题

- [挑战和代币收购 \(p. 131\)](#)
- [机器人控制和 ATP 管理规则组 \(p. 133\)](#)
- [基于速率的规则和有针对性的机器人控制规则中的速率限制选项 \(p. 134\)](#)

挑战和代币收购

您可以使用Amazon WAF应用程序集成 SDK 或规则操作提供挑战并获取代币，以Challenge及CAPTCHA。从广义上讲，规则操作更容易实施，但它们会增加成本，对您的客户体验造成更多干扰，并且要求更高 JavaScript。SDK 需要在您的客户端应用程序中进行编程，但它们可以提供更好的客户体验，可以免费使用，并且可以与 Android 或 iOS 应用程序一起使用，也可以在 Android JavaScript 或 iOS 应用程序中使用。您只能将应用程序集成 SDK 与使用以下部分所述的付费智能威胁缓解托管规则组之一的 Web ACL 一起使用。

挑战和代币获取选项的比较

	Challenge 规则操作	CAPTCHA 规则操作	JavaScript SDK 挑战赛	移动 SDK 挑战赛
什么是	规则操作，通过向浏览器客户端提供无声的插页式挑战来强制获取 Amazon WAF 代币	规则操作，通过向客户终端用户提供插页式视频或音频挑战来强制获取 Amazon WAF 代币	应用程序集成层，用于执行的客户端浏览器和其他设备 JavaScript。进行无声挑战并获得代币	应用程序集成层，适用于 Android 和 iOS 应用程序。原生呈现无声挑战并获得代币
... 的好选择	对机器人会话进行静默验证，并强制支持的客户获取代币 JavaScript	针对支持机器人会话的最终用户和静默验证，并强制执行代币获取 JavaScript	对机器人会话进行静默验证，并强制支持的客户获取代币 JavaScript。 软件开发工具包提供了最低的延迟，并且可以最佳地控制挑战脚本在应用程序中的运行位置。	针对机器人会话进行静默验证，并强制在 Android 和 iOS 上对原生移动应用程序进行代币获取。 软件开发工具包提供了最低的延迟，并且可以最佳地控制挑战脚本在应用程序中的运行位置。
实施注意事项	作为规则操作设置实现	作为规则操作设置实现	需要 Web ACL 中的 ATP 或 Bot Control 付费规则组之一。 需要在客户端应用程序中编码。	需要 Web ACL 中的 ATP 或 Bot Control 付费规则组之一。 需要在客户端应用程序中编码。
运行版标注分类	没有有效令牌的请求的侵入式流程。客户端被重定向到插页式 Amazon WAF 挑战赛。添加网络往返行程，需要对 Web 请求进行第二次评估。	没有有效令牌的请求的侵入式流程。客户端被重定向到 Amazon WAF 验证码插页式广告。添加网络往返行程，需要对 Web 请求进行第二次评估。	可以在幕后运行。让你更好地控制挑战体验。	可以在幕后运行。让你更好地控制挑战体验。
需要 JavaScript	是	是	是	否
支持的客户端	执行 JavaScript 的浏览器和设备	执行 JavaScript 的浏览器和设备	执行 JavaScript 的浏览器和设备	Android iOS 设备
支持单页应用程序 (SPA)	否	否	是	不适用
额外费用	是，对于您明确指定的操作设置，可以在您定义的规则中指定，也可以在您使用的规则组中作为规则操作替代项。在所有其他情况下都不是。	是，对于您明确指定的操作设置，可以在您定义的规则中指定，也可以在您使用的规则组中作为规则操作替代项。在所有其他情况下都不是。	否，但需要付费规则组 ATP 或 Bot Control 之一。	否，但需要付费规则组 ATP 或 Bot Control 之一。

有关与这些选项相关的成本的详细信息，请参阅[Amazon WAF 价](#)中的智能威胁缓解信息。

只需添加带有 `oChallenge r` 操作的规则，即可更轻松地进行挑战并提供基本的代币强制CAPTCHA执行。如果您无权访问应用程序代码，或者不想使用 Bot Control 或 ATP 托管规则组，则可能需要使用规则操作。

但是，与使用以下Challenge操作相比，如果您能实现软件开发工具包，则可以节省成本，还可以减少客户端 Web 请求的 Web ACL 评估延迟：

- 您可以编写 SDK 实现，以便在应用程序的任何时候运行挑战。在客户采取任何行动向您的受保护资源发送 Web 请求之前，您可以在后台获取令牌。这样，代币就可以在客户的第一个请求时发送。
- 相反，如果您通过使用Challenge操作实现规则来获取令牌，则在客户端首次发送请求和令牌过期时，规则和操作需要额外评估和处理 Web 请求。该Challenge操作阻止了没有有效未过期代币的请求，并将挑战插页式广告发送回客户端。客户端成功响应质询后，插页式会使用有效令牌重新发送原始 Web 请求，然后由 Web ACL 对其进行第二次评估。

机器人控制和 ATP 管理规则组

提供智能威胁缓解的 Managed Rules 规则组包括管理基本机器人、检测和缓解高级恶意机器人，以及检测和缓解账户接管企图。Amazon这些规则组与上一节中描述的应用程序集成 SDK 相结合，可提供最先进的保护并与您的客户端应用程序进行安全耦合。

管理规则组选项的比较

	机器人控制常用级别	机器人控制目标等级	ATP
什么是	管理可自我识别的常见机器人，签名在应用程序中是唯一的。 请参阅Amazon WAF 机器人控制规则组 (p. 49)。	使用特定于应用程序的签名管理无法自我识别的有针对性的机器人。 请参阅Amazon WAF 机器人控制规则组 (p. 49)。	管理可能是应用程序登录页面上恶意接管尝试的一部分的请求。 不管理机器人。 请参阅Amazon WAF 欺诈控制账户收购预防 (ATP) 规则组 (p. 56)。
... 的好选择	对常见的自动机器人流量进行基本的机器人保护和标记。	针对高级机器人的定向防护，包括在客户端会话级别进行速率限制以及检测和缓解浏览器自动化工具（例如 Selenium 和 Puppeteer）。	检查登录流量是否存在帐户盗用攻击，例如尝试遍历密码的登录以及来自同一 IP 地址的多次登录尝试。与令牌一起使用时，还提供聚合保护，例如在 IP 和客户端会话级别对大量流量进行速率限制。
添加指示评估结果的标签	是	是	是
添加代币标签	是	是	是
阻止没有有效令牌的请求	不包括在内。 请参阅阻止没有有效令牌的请求 (p. 139)。	阻止发送 5 个不带令牌的请求的客户端会话。	不包括在内。 请参阅阻止没有有效令牌的请求 (p. 139)。
需要代Amazon WAF 币aws-waf-token	否	是	许多规则都是必需的。

	机器人控制常用级别	机器人控制目标等级	ATP
			请参阅 为什么要将应用程序集成 SDK 与 ATP 一起使用 (p. 156) 。
获取代Amazon WAF 币aws-waf-token	否	有些规则使用Challenge或CAPTCHA规则操作，这些操作会获取代币。	否

有关与这些选项相关的成本的详细信息，请参阅[Amazon WAF价](#)中的智能威胁缓解信息。

基于速率的规则和有针对性的机器人控制规则中的速率限制选项

Amazon WAFBot Control 规则组的目标级别和Amazon WAF基于速率的规则语句都提供 Web 请求速率限制。下表比较了两个选项。

基于速率的检测和缓解选项的比较

	Amazon WAF基于速率的规则	Amazon WAF机器人控制目标规则	
如何应用速率限制	阻止来自以过高的速率发送请求的 IP 地址的流量。	通过使用请求令牌强制执行类似于人类的访问模式并应用动态速率限制。	
基于历史流量基线？	否	是	
累积历史交通基线所需的时间	不适用	动态阈值需要五分钟。代币不存在则不适用。	
缓解滞后	通常为 30-50 秒。可能长达几分钟。	通常不到 10 秒。可能长达几分钟。	
缓解目标	IP 地址	IP 地址和客户端会话	
触发缓解措施所需的流量水平	中等-可以低至每 5 分钟 100 个请求	低-旨在检测客户端模式，例如慢速抓取器	
可自定义的阈值	是	否	
默认缓解措施	控制台默认为 Block。API 中没有默认设置；该设置是必需的。 您可以将其设置为任何有效的规则操作，除外 Allow。	规则组规则操作设置 Challenge适用于令牌缺失和CAPTCHA来自单个客户端会话的大量流量。 您可以将其中任一规则设置为任何有效的规则操作。	
抵御高度分布式攻击的弹性	中等-限于 10,000 个 IP 地址	中等-IP 地址和代币之间的总数限制为 50,000	
Amazon WAF 定价	包含在的基本费用中 Amazon WAF。	包含在 Bot Control 智能威胁缓解的目标级别中。	

	Amazon WAF基于速率的规则	Amazon WAF机器人控制目标规则	
欲了解更多信息	基于速率的规则语句 (p. 95)	Amazon WAF机器人控制规则组 (p. 49)	

智能威胁缓解最佳实践

遵循本节中的最佳实践，以最有效、最具成本效益的方式实施智能威胁缓解功能。

- 实施 JavaScript 和移动应用程序集成 SDK — 实施应用程序集成，以尽可能有效的方式启用全套 ATP 或 Bot Control 功能。托管规则组使用软件开发工具包提供的令牌在会话级别将合法的客户端流量与不需要的流量分开。应用程序集成 SDK 确保这些令牌始终可用。有关详细信息，请参阅[为什么要使用带有 Bot Control 的应用程序集成 SDK \(p. 143\)](#)和[为什么要将应用程序集成 SDK 与 ATP 一起使用 \(p. 156\)](#)。

要实现软件开发工具包，请参阅[Amazon WAF客户机应用程序集成 \(p. 164\)](#)。

- 限制向 ATP 和 Bot Control 规则组发送的请求 — 使用智能威胁缓解Amazon管理规则组需要支付额外费用。机器人控制规则组会检查 Web ACL 评估中到达它的每个请求。ATP 规则组仅检查登录请求，但如果您计划出于地理来源等原因拒绝登录请求，请在 ATP 规则组之前运行这些规则。

考虑使用以下方法来减少对这些规则组的使用：

- 在托管规则组语句中使用范围缩小语句将请求排除在检查范围之外。您可以使用任何可嵌套的语句来做到这一点。有关信息，请参阅[范围缩小声明 \(p. 110\)](#)。
- 通过在规则组之前添加规则，将请求排除在检查范围之外。对于不能在范围缩小语句中使用的规则以及更复杂的情况，例如先加标签再进行标签匹配，可能需要添加在规则组之前运行的规则。有关信息，请参阅[范围缩小声明 \(p. 110\)](#)和[Amazon WAF 规则语句 \(p. 81\)](#)。
- 按照较便宜的规则运行规则组。如果您有其他出于任何原因阻止请求的标准Amazon WAF规则，请在这些付费规则组之前运行这些规则。有关规则和规则管理的更多信息，请参阅[Amazon WAF 规则语句 \(p. 81\)](#)。
- 如果您同时使用 ATP 和机器人控制规则组，请先运行机器人控制规则组。这是更便宜的规则组。

有关详细定价信息，请参阅[Amazon WAF 定价](#)。

- 对于分布式拒绝服务 (DDoS) 防护，请使用 Shield Advanced 自动应用层 DDoS 缓解——智能威胁缓解规则组不提供 DDoS 保护。ATP 可防止有人企图接管您的登录页面的账户。Bot Control 专注于使用令牌和对客户端会话进行动态速率限制来强制执行类似人类的访问模式。

当您使用启用了自动应用层 DDoS 缓解功能的 Shield AdvancedAmazon WAF 时，Shield Advanced 会通过代表您创建、评估和部署自定义缓解措施来自动响应检测到的 DDoS 攻击。有关 Shield Advanced 的更多信息[Amazon Shield Advanced 概览 \(p. 331\)](#)，请参阅和[Amazon Shield Advanced应用层 \(第 7 层\) 保护 \(p. 353\)](#)。

- 调整和配置令牌处理-调整 Web ACL 的令牌处理以获得最佳用户体验。
 - 要降低运营成本并改善最终用户体验，请将代币管理免疫时间调整到安全要求允许的最长时间。这样可以降低验证码谜题和无声挑战的使用降至最低。有关信息，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)。
 - 要在受保护的应用程序之间启用令牌共享，请为 Web ACL 配置令牌域列表。有关信息，请参阅[代币域和域名列表 \(p. 138\)](#)。
- 拒绝具有任意主机规格的请求-将您的受保护资源配置为要求 Web 请求中的Host标头与目标资源相匹配。您可以接受一个值或一组特定的值，例如myExampleHost.com和www.myExampleHost.com，但不接受主机的任意值。
- 对于作为 CloudFront 发行来源的Application Load Balancer，请配置 CloudFront 并Amazon WAF进行适当的令牌处理 — 如果您将 Web ACL 关联到Application Load Balancer，并将应用程序负载均衡器部署为 CloudFront 分配的来源，请参阅[作为 CloudFront来源的应用程序负载均衡器需要配置 \(p. 142\)](#)。

- 部署前进行测试和调整 — 在对 Web ACL 进行任何更改之前，请按照本指南中的测试和调整程序进行操作，以确保获得预期的行为。这对于这些付费功能特别重要。有关一般指导，请参见[测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。有关付费管理规则组的特定信息，请参阅[测试和部署 Amazon WAF 机器人控制 \(p. 145\)](#)和[测试和部署 ATP \(p. 159\)](#)。

Amazon WAF 网络请求令牌

Amazon WAF 代币是 Amazon WAF 智能威胁缓解所提供的增强保护不可或缺的一部分。令牌，有时称为指纹，是有关单个客户端会话的信息的集合，客户端存储并随每个 Web 请求提供这些信息。Amazon WAF 使用令牌识别恶意客户端会话并将其与合法会话分开，即使两者都来自单个 IP 地址。代币的使用给合法用户带来的成本可以忽略不计，但对于僵尸网络来说，代币的使用却是大规模昂贵的。

Amazon WAF 使用令牌来支持其浏览器和最终用户挑战功能，该功能由应用程序集成 SDK 和规则操作 Challenge 和提供 CAPTCHA。此外，代币还支持 Amazon WAF 机器人控制和防止账户盗用管理规则组的功能。

Amazon WAF 为成功应对无声挑战和验证码难题的客户创建、更新和加密代币。当拥有令牌的客户端发送 Web 请求时，它会包含加密的令牌，然后 Amazon WAF 解密令牌并验证其内容。

主题

- [如何使用代币 \(p. 136\)](#)
- [代币标注分类 \(p. 137\)](#)
- [时间戳到期：代币豁免时间 \(p. 137\)](#)
- [代币域和域名列表 \(p. 138\)](#)
- [由机器人控制和 ATP 管理规则组标记代币 \(p. 139\)](#)
- [阻止没有有效令牌的请求 \(p. 139\)](#)
- [作为 CloudFront 来源的应用程序负载均衡器需要配置 \(p. 142\)](#)

如何使用代币

Amazon WAF 使用令牌来记录和验证以下类型的客户端会话验证：

- CAPTCHA — 验证码拼图有助于区分机器人和人类用户。验证码只能通过 CAPTCHA 规则操作运行。成功完成拼图后，CAPTCHA 脚本会更新代币的 CAPTCHA 时间戳。有关更多信息，请参阅[CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)：
- 挑战 — 挑战以静默方式进行，以帮助区分常规客户端会话和机器人会话，并增加机器人的运行成本。挑战成功完成后，挑战脚本会根据 Amazon WAF 需要自动从中获取新代币，然后更新代币的挑战时间戳。

Amazon WAF 在以下情况下运行挑战：

- 应用程序集成 SDK — 应用程序集成 SDK 在您的客户端应用程序会话中运行，有助于确保只有在客户端成功响应挑战后才允许尝试登录。有关更多信息，请参阅[Amazon WAF 客户机应用程序集成 \(p. 164\)](#)：
- Challenge 规则操作-有关更多信息，请参阅[CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)。
- CAPTCHA — 当 CAPTCHA 插页式运行时，如果客户端还没有令牌，则脚本会自动先运行质询，验证客户端会话并初始化令牌。

ATP 和 Bot Control Amazon 管理规则组中的许多规则都需要令牌。这些规则使用令牌来区分会话级别的客户端。这些规则组调用 Amazon WAF 令牌管理，该令牌管理应用令牌标签，然后由规则组检查。

- Amazon WAF 防欺诈控制账户盗用 (ATP) — 防止高容量和长期客户会话的 ATP 规则要求网络请求必须包含带有未过期质询时间戳的有效代币。有关更多信息，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)：

- Amazon WAF 机器人控制 — 此规则组中的目标规则限制了客户端在没有有效令牌的情况下可以发送的 Web 请求数量，它们使用令牌会话跟踪进行会话级别的监控和管理。根据需要，规则应用 Challenge 和 CAPTCHA 规则操作来强制执行代币获取和有效的客户行为。有关更多信息，请参阅[Amazon WAF 机器人控制规则组 \(p. 49\)](#)：

代币标注分类

每个代币都具有以下特征：

- 令牌存储在名为的 cookie 中 `aws-waf-token`。
- 令牌已加密。
- 令牌使用粘性粒度标识符对客户端会话进行指纹识别，该标识符包含以下信息：
 - 客户端最近一次成功响应无声挑战的时间戳。
 - 最终用户最近一次成功响应验证码的时间戳。只有当您在保护中使用验证码时，这才会出现。
 - 有关客户和客户行为的其他信息，这些信息可以帮助将您的合法客户与有害流量区分开。这些信息包括可用于检测自动化活动的各种客户端标识符和客户端信号。收集的信息不是唯一的，无法映射到个人身上。

出于安全原因，Amazon 未提供 Amazon WAF 令牌内容的完整描述或有关令牌加密过程的详细信息。

时间戳到期：代币豁免时间

Amazon WAF 使用挑战和 CAPTCHA 免疫时间来控制向单个客户端会话呈现挑战或 CAPTCHA 的频率。最终用户成功响应验证码后，CAPTCHA 免疫时间决定了最终用户在多长时间内免受另一个 CAPTCHA 的侵害。同样，挑战免疫时间决定了客户端会话在成功响应挑战后在多长时间内不受再次挑战。

Amazon WAF 通过更新令牌内的相应时间戳，记录对挑战或验证码的成功响应。当 Amazon WAF 检查代币是否存在挑战或验证码时，它会从当前时间中减去时间戳。如果结果大于配置的免疫时间，则时间戳已过期。

您可以在 Web ACL 以及任何使用 CAPTCHA 或 Challenge 规则操作的规则中配置质询和 CAPTCHA 免疫时间。

- 两个免疫时间的默认 Web ACL 设置均为 300 秒。
- 您可以为使用 CAPTCHA 或 Challenge 操作的任何规则指定豁免时间。如果您未指定规则的豁免时间，它会继承 Web ACL 中的设置。
- 对于使用 CAPTCHA 或 Challenge 操作的规则组内的规则，如果您未指定该规则的豁免时间，它将继承您使用该规则组的每个 Web ACL 的设置。
- 应用程序集成 SDK 使用 Web ACL 的挑战免疫时间。

挑战免疫时间的最小值为 300 秒。验证码免疫时间的最小值为 60 秒。两个免疫时间的最大值均为 259,200 秒，即三天。

您可以使用 Web ACL 和规则级别的免疫时间设置来调整 CAPTCHA 操作或 SDK 挑战管理行为。Challenge 例如，您可以配置控制对免疫时间较低的高敏感数据的访问的规则，然后在 Web ACL 中为要继承的其他规则和软件开发工具包设置更高的免疫时间。

特别是对于 CAPTCHA 而言，解开难题可能会降低客户的网站体验，因此调整 CAPTCHA 免疫时间可以帮助您减轻对客户体验的影响，同时还能提供你想要的保护。

有关调整免疫时间以使用 Challenge 和 CAPTCHA 规则操作的更多信息，请参阅[使用 CAPTCHA 和 Challenge 操作的最佳实践 \(p. 179\)](#)。

设置代币豁免时间

您可以在 Web ACL 和使用和规则操作的规则中设置豁免时间。Challenge CAPTCHA

有关管理 Web ACL 及其规则的一般信息，请参见[使用 Web ACL \(p. 17\)](#)。

在哪里设置 Web ACL 的免疫时间

- 控制台 — 编辑 Web ACL 时，在“规则”选项卡中编辑和更改 Web ACL CAPTCHA 配置和 Web ACL Challenge 配置窗格中的设置。在控制台中，只有在创建 Web ACL 之后，您才能配置 Web ACL 验证码和质疑免疫时间。
- 控制台外部 — Web ACL 数据类型具有 CAPTCHA 和质询配置参数，您可以配置这些参数并将其提供给 Web ACL 上的创建和更新操作。

在哪里设置规则的豁免时间

- 控制台 — 创建或编辑规则并指定 CAPTCHA 或 Challenge 操作时，可以修改规则的免疫时间设置。
- 控制台外部 — 规则数据类型包含 CAPTCHA 和质询配置参数，您可以在定义规则时对其进行配置。

代币域和域名列表

为客户端 Amazon WAF 创建令牌时，它会为其配置令牌域。在 Amazon WAF 检查 Web 请求中的令牌时，如果该令牌的域与任何被认为对 Web ACL 有效的域不匹配，则会拒绝该令牌为无效。

默认情况下，Amazon WAF 仅接受域设置与与 Web ACL 关联的资源的主机域完全匹配的令牌。这是 Web 请求中 Host 标头的值。在浏览器中，您可以在 JavaScript `window.location.hostname` 属性和用户在地址栏中看到的地址中找到此域。

您可以指定在设置域名 Amazon WAF 和评估 Web ACL 中的令牌时使用的令牌域。您指定的域不能是公共后缀，例如 `usa.gov`。

配置 Web ACL 令牌域列表

您可以通过提供包含您想要接受的其他域的令牌域列表来配置 Web ACL。Amazon WAF 以在多个受保护的资源之间共享令牌。使用令牌域列表，Amazon WAF 仍接受资源的主机域。此外，它接受令牌域列表中的所有域，包括其前缀子域。

例如，您的令牌域列表 `example.com` 中的域规格与 `example.com` (自 `http://example.com/`)、`api.example.com`、(自 `http://api.example.com/`) 和 `www.example.com` (自 `http://www.example.com/`) 相匹配。它不匹配 `example.api.com`、(来自 `http://example.api.com/`) 或 `apiexample.com` (来自 `http://apiexample.com/`)。

创建或编辑令牌域列表时，可以在 Web ACL 中配置令牌域列表。有关管理 Web ACL 的一般信息，请参见[使用 Web ACL \(p. 17\)](#)。

控制令牌内的域名设置

Amazon WAF 应质询脚本的请求创建令牌，这些脚本由应用程序集成 SDK 和 Challenge 和 CAPTCHA 规则操作运行。

在令牌中 Amazon WAF 设置的域由请求该令牌的质询脚本的类型以及您提供的任何其他令牌域配置决定。Amazon WAF 将令牌中的域设置为在配置中可以找到的最短、最通用的设置。

- JavaScript SDK — 您可以使用令牌域规范配置 JavaScript SDK，该规范可以包括一个或多个域。根据受保护的主机域和 Web ACL 的 Amazon WAF 令牌域列表，您配置的域必须是接受的域。

Amazon WAF 将令牌域设置为与主机域匹配的令牌域，并且是主机域和列表中域中最短的令牌域。例如，如果主机域为 `api.example.com`，令牌域列表为 `example.com`，则在令牌 `example.com` 中 Amazon WAF 使用，因为它与主机域匹配且较短。如果您未在 JavaScript SDK 配置中提供令牌域列表，则将域 Amazon WAF 设置为受保护资源的主机域。

有关更多信息，请参阅[提供用于代币的域名 \(p. 166\)](#)：

- 移动 SDK — 必须使用令牌域配置移动 SDK。Amazon WAF 才能在令牌中使用。根据受保护的主机域和 Web ACL 的 Amazon WAF 令牌域列表，您配置的域必须是接受的域。Amazon WAF 不考虑移动 SDK 的令牌域设置中的主机域。

有关更多信息，请参阅中的 WAFConfigurationDomainName 设置 [移 Amazon WAF 动 SDK 规范 \(p. 169\)](#)。

- Challenge 操作 — 如果您在 Web ACL 中指定令牌域列表，则将令牌域 Amazon WAF 设置为与主机域匹配且最短的令牌域，即主机域和列表中的域中的令牌域。例如，如果主机域为 `api.example.com`，令牌域列表为 `example.com`，则在令牌 `example.com` 中 Amazon WAF 使用，因为它与主机域匹配且较短。如果您未在 Web ACL 中提供令牌域列表，则 Amazon WAF 将该域设置为受保护资源的主机域。

由机器人控制和 ATP 管理规则组标记代币

当您使用 ATP 和 Bot Control Amazon 管理规则组时，规则组使用 Amazon WAF 令牌管理来检查 Web 请求令牌并将令牌标签应用于请求。

Note

Amazon WAF 令牌管理仅在您使用 Bot Control 或 ATP 托管规则组时应用令牌标签。

Amazon WAF 在检查 Web 请求的令牌和质询时间戳时应用以下标签之一。Amazon WAF 不添加关于 CAPTCHA 时间戳状态的标签。

- `aws:waf:managed:token:accepted` — 请求令牌存在且具有未过期的质询时间戳。
- `aws:waf:managed:token:rejected` — 请求令牌存在但已损坏或质询时间戳已过期。
- `aws:waf:managed:token:absent` — 请求没有令牌。

您可以在 Web ACL 中的任一托管规则组之后添加自己的规则，以与令牌标签相匹配。有关规则中标签匹配的信息，请参阅[与标签匹配 \(p. 127\)](#)。

有关托管规则组及其规则添加到 Web 请求的标签的信息，请参阅[Amazon WAF 机器人控制规则组 \(p. 49\)](#)和[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

阻止没有有效令牌的请求

当您使用 Amazon 托管规则组 `AWSManagedRulesATPRuleSet` 和 `AWSManagedRulesBotControlRuleSet` 时，规则组会调用 Amazon WAF 令牌管理来评估 Web 请求中 Amazon 令牌的状态并相应地对其进行标记。

Note

令牌标签仅适用于您使用这两个托管规则组之一进行评估的 Web 请求。

Amazon WAF 在检查 Web 请求的令牌和质询时间戳时应用以下标签之一。Amazon WAF 不添加关于 CAPTCHA 时间戳状态的标签。

- `aws:waf:managed:token:accepted` — 请求令牌存在且具有未过期的质询时间戳。
- `aws:waf:managed:token:rejected` — 请求令牌存在但已损坏或质询时间戳已过期。
- `aws:waf:managed:token:absent` — 请求没有令牌。

区 `AWSManagedRulesATPRuleSet` 块请求带有 `aws:waf:managed:token:rejected` 标签。在客户发送了五个没有被接受的代币的请求后，他们会向他们提出质 `AWSManagedRulesBotControlRuleSet` 疑。有关

规则组的详细信息，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)和[Amazon WAF 机器人控制规则组 \(p. 49\)](#)。

Bot Control 规则组不会阻止带有被拒绝令牌的请求，也没有一个规则组阻止缺少令牌的单个请求。如果请求未被规则组中的其他规则阻止，则可以退出规则组评估并继续由 Web ACL 进行评估。

要阻止所有丢失令牌或令牌被拒绝的请求，请添加一条在托管规则组之后立即运行的规则，以捕获和阻止规则组未为您处理的请求。

以下是使用 ATP 托管规则组的 Web ACL 的 JSON 列表示例。Web ACL 添加了捕获和处理 `aws:waf:managed:token:absent` 标签的规则。该规则将其评估范围缩小到发送到登录端点的 Web 请求，以匹配 ATP 规则组的范围。添加的规则以粗体列出。

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                }
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
```

```
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSManagedRulesATPRuleSet"
  }
},
{
  "Name": "RequireTokenForLogins",
  "Priority": 2,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "Statement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:token:absent"
            }
          }
        },
        {
          "ByteMatchStatement": {
            "SearchString": "/web/login",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "STARTS_WITH"
          }
        },
        {
          "ByteMatchStatement": {
            "SearchString": "POST",
            "FieldToMatch": {
              "Method": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "RequireTokenForLogins"
  }
},
{
  "Name": "exampleWebACL",
  "Priority": 1,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "Statement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:token:absent"
            }
          }
        },
        {
          "ByteMatchStatement": {
            "SearchString": "/web/login",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "STARTS_WITH"
          }
        },
        {
          "ByteMatchStatement": {
            "SearchString": "POST",
            "FieldToMatch": {
              "Method": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
  }
}
```



```
}  
  "Capacity": 51,  
  "ManagedByFirewallManager": false,  
  "LabelNamespace": "aws:waf:111111111111:webacl:exampleWebACL:"  
}
```

作为 CloudFront 来源的应用程序负载均衡器需要配置

如果您将 Web ACL 关联到 Application Load Balancer，并将 Application Load Balancer 部署为 CloudFront 分配的来源，请阅读本节。

使用此架构，您需要提供以下额外配置，以便正确处理令牌信息。

- 配置为将 aws-waf-token cookie 转发 CloudFront 到 Application Load Balancer。默认情况下，在将 Web 请求转发到源之前，将其从 Web 请求中 CloudFront 删除 Cookie。要在网络请求中保留令牌 cookie，请将 CloudFront 缓存行为配置为仅包含令牌 cookie 或所有 Cookie。有关如何执行此操作的信息，请参阅亚马逊 CloudFront 开发者指南中的[基于 Cookie 缓存内容](#)。
- 进行配置，Amazon WAF 使其将 CloudFront 分配的域识别为有效的令牌域。默认情况下，CloudFront 将 Host 标头设置为 Application Load Balancer 源，并将其 Amazon WAF 用作受保护资源的域。但是，客户端浏览器将 CloudFront 发行版视为主机域，为客户端生成的令牌使用该 CloudFront 域作为令牌域。如果不进行任何其他配置，当 Amazon WAF 将受保护的资源域与令牌域进行对比时，会出现不匹配的情况。要解决此问题，请将 CloudFront 分发域名添加到 Web ACL 配置中的令牌域列表中。有关如何执行此操作的信息，请参阅[配置 Web ACL 令牌域列表 \(p. 138\)](#)。

Amazon WAF 机器人控制

Bot Control 托管规则组提供基本的通用保护级别，为自识别机器人添加标签，验证通常需要的机器人，并检测高可信度的机器人签名。这使您能够监视和控制常见类别的机器人流量。Bot Control 还提供有针对性的保护级别，增加了对无法自我识别的高级机器人的检测。定向保护使用浏览器查询、指纹识别和行为启发式等高级检测技术来识别恶意机器人流量，然后应用缓解控制措施，例如速率限制 CAPTCHA 和 Challenge 规则操作。有关其他详细信息，请参阅[Amazon WAF 机器人控制规则组 \(p. 49\)](#)。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

借助 Bot Control，您可以轻松监控、屏蔽或限制机器人，例如抓取工具、扫描器、爬虫、状态监视器和搜索引擎。如果你使用规则组的针对性检查级别，你还可以挑战无法自我识别的机器人，这使得恶意机器人更难对你的网站进行操作，也更昂贵。您可以单独使用 Bot Control 托管规则组来保护您的应用程序，也可以与其他 Amazon 托管规则组和您自己的自定义 Amazon WAF 规则结合使用。

Bot Control 包括一个控制台控制面板，该仪表板根据请求采样显示您当前有多少流量来自机器人。将 Bot Control 托管规则组添加到 Web ACL 后，您可以对机器人流量采取措施，并接收有关进入应用程序的常见机器人流量的详细信息、实时信息。

当 Amazon WAF 根据 Bot Control 托管规则组评估 Web 请求时，规则组会为其检测为与机器人相关的请求添加标签，例如机器人类别和机器人名称。您可以在自己的 Amazon WAF 规则中与这些标签进行匹配以自定义处理。机器人控制托管规则组生成的标签包含在亚马逊 CloudWatch 指标和您的网络 ACL 日志中。

您还可以使用 Amazon Firewall Manager Amazon WAF 策略在属于您的组织的多个账户的应用程序中部署 Bot Control 托管规则组 Amazon Organizations。

机器人控制组件

机器人控制实现的主要组件如下：

- AWSManagedRulesBotControlRuleSet**— Bot Control 托管规则组，其规则可检测和处理各种类别的机器人。有关规则组规则的信息，请参阅[Amazon WAF 机器人控制规则组 \(p. 49\)](#)。您可以使用托管规

则组参考语句将此规则组包含在 Web ACL 中，并指明要使用的检查级别。该规则组为检测为机器人流量的 Web 请求添加标签。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

- 机器人控制仪表板 — Web ACL 的机器人监控仪表板，可通过 Web ACL 机器人控制选项卡访问。使用该仪表板监控您的流量，并了解其中有多少来自各种类型的机器人。如本主题所述，这可以作为自定义机器人管理的起点。您还可以使用它来验证您的更改并监控各种机器人和机器人类别的活动。
- JavaScript 和移动应用程序集成 SDK — 如果您使用 Bot Control 规则组的目标保护级别，则应实现 Amazon WAF JavaScript 和移动 SDK。目标规则使用客户端令牌中软件开发工具包提供的信息来增强对恶意机器人的检测。有关开发工具包的更多信息，请参阅 [Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。
- 日志和指标 — 您可以通过研究 Web ACL 的日志和亚马逊 CloudWatch 指标，监控机器人流量，了解 Bot Control 托管规则组如何评估和处理您的流量。Bot Control 在您的网络请求中添加的标签包含在日志和亚马逊 CloudWatch 指标中。有关配置和使用日志和指标的信息，请参阅 [记录 Web ACL 流量 \(p. 180\)](#) 和 [使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。

根据您的需求和看到的流量，您可能需要自定义您的 Bot Control 实现。以下是一些最常用的选项。

- Scope-down 语句 — 通过在 Bot Control 托管规则组参考语句中添加缩小范围语句，可以从 Bot Control 托管规则组评估的 Web 请求中排除某些流量。范围缩小语句可以是任何可嵌套的规则语句。当请求与 scope-down 语句不匹配时，Amazon WAF 会将其评估为与规则组参考语句不匹配，而不根据规则组对其进行评估。有关缩小范围语句的更多信息，请参阅 [范围缩小声明 \(p. 110\)](#)。

Bot Control 托管规则组的定价随其 Amazon WAF 评估的 Web 请求数量而增加。您可以使用范围缩小语句来限制规则组评估的请求，从而帮助降低这些成本。例如，您可能希望允许所有人（包括机器人）加载您的主页，然后将规则组规则应用于发送到您的应用程序 API 或包含特定类型内容的请求。

- 标签和标签匹配规则-您可以使用 Amazon WAF 标签匹配规则语句自定义 Bot Control 规则组处理其识别的某些机器人流量的方式。机器人控制规则组为您的 Web 请求添加标签。您可以在 Bot Control 标签上匹配的 Bot Control 规则组之后添加标签匹配规则，然后应用所需的处理。有关标注和使用标签匹配语句的更多信息，请参见 [标签匹配规则声明 \(p. 92\)](#) 和 [网络请求上的标签 \(p. 123\)](#)。
- 自定义请求和响应-您可以向允许的请求添加自定义标头，也可以通过将标签匹配与自定义请求和响应功能配对来为阻止的请求发送 Amazon WAF 自定义响应。有关自定义请求和响应的更多信息，请参阅 [中的自定义 Web 请求和响应 Amazon WAF \(p. 118\)](#)。

为什么要使用带有 Bot Control 的应用程序集成 SDK

Bot Control 托管规则组的定向保护需要应用程序集成 SDK 生成的质询令牌。如果没有挑战令牌，您只能使用 Bot Control 普通级保护。有关规则组提供的保护级别的比较，请参阅 [Amazon WAF 机器人控制规则组 \(p. 49\)](#)。

我们强烈建议实施应用程序集成 SDK，以便最有效地使用 Bot Control 规则组。质询脚本必须在 Bot Control 规则组之前运行，规则组才能从脚本获取的令牌中受益。这是在应用程序集成 SDK 中自动发生的。如果您无法使用 SDK，则可以交替配置 Web ACL，使其对将由 Bot Control CAPTCHA 规则组检查的所有请求运行 Challenge 或规则操作。使用 Challenge 或 CAPTCHA 规则操作可能会产生额外费用。有关定价的详细信息，请参阅 [Amazon WAF 定价](#)。

在客户端中实现应用程序集成 SDK 或使用运行挑战脚本的规则操作之一时，可以扩展规则组和整体客户端应用程序安全的功能。

令牌为每个 Web 请求提供客户信息。这些附加信息使 Bot Control 规则组能够将合法的客户端会话与行为不良的客户端会话分开，即使两者都来自单个 IP 地址。规则组使用令牌中的信息来聚合客户端会话请求行为，以微调目标保护级别提供的检测和缓解措施。

有关开发工具包的信息，请参阅 [Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。有关 Amazon WAF 令牌的信息，请参阅 [Amazon WAF 网络请求令牌 \(p. 136\)](#)。有关规则操作的信息，请参阅 [CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)。

将Amazon WAF Bot Control 托管规则组添加到 Web ACL 中

Bot Control AWS Managed Rules Bot Control Rule Set | 托管规则组需要额外配置才能确定要实现的保护级别。

有关规则组描述和规则列表，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

本指南适用于一般知道如何创建和管理 Amazon WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前几部分所涵盖的。

遵循最佳实践

按照中的最佳做法使用 Bot Control 规则组 [智能威胁缓解最佳实践 \(p. 135\)](#)。

在 Web ACL 中使用 **AWSManagedRulesBotControlRuleSet** 规则组

1. 将 Amazon 托管规则组 **AWSManagedRulesBotControlRuleSet** 添加到您的 Web ACL。有关规则组的完整描述，请参阅 [the section called “机器人控制规则组” \(p. 49\)](#)。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

添加规则组时，对其进行编辑以打开规则组的配置页面。

2. 在规则组的配置页面的检查级别窗格中，选择要使用的检查级别。
 - 常见 — 检测各种自我识别的机器人，例如网页抓取框架、搜索引擎和自动浏览器。此级别的机器人控制保护使用传统的机器人检测技术（例如静态请求数据分析）识别常见的机器人。这些规则会标记来自这些机器人的流量，并屏蔽他们无法验证的流量。
 - 定向 — 包括通用级保护，并增加了对无法自我识别的高级机器人的检测。定向保护使用浏览器查询、指纹识别和行为启发式等高级检测技术来识别恶意机器人流量。这些保护措施结合了速率限制、验证码和后台浏览器挑战，针对这些机器人。提供定向保护的规则的名称以开头 TGT_。

有关此选项的更多信息，请参阅 [Amazon WAF 机器人控制规则组 \(p. 49\)](#)。

3. 为规则组添加范围缩小语句，以控制使用该规则组的成本。范围缩小语句缩小了规则组检查的请求集的范围。例如用例，以 [Amazon WAF 机器人控制示例：仅对登录页面使用机器人控制 \(p. 152\)](#) 和开头 [Amazon WAF 机器人控制示例：仅对动态内容使用机器人控制 \(p. 153\)](#)。
4. 提供规则组所需的任何其他配置。
5. 保存您对 Web ACL 所做的更改。

在为生产流量部署 Bot Control 实现之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整规则，然后再启用这些规则。有关指导，请参阅以下各节。

Amazon WAF 机器人控制出现误报

我们精心选择了 Amazon WAF Bot Control 管理规则组中的规则，以最大限度地减少误报。我们针对全球流量测试规则，并监控其对测试 Web ACL 的影响。但是，由于流量模式的变化，仍然有可能出现误报。此外，已知某些用例会导致误报，需要针对您的网络流量进行自定义。

您可能会遇到误报的情况包括：

- 移动应用程序通常具有非浏览器用户代理，SignalNonBrowserUserAgent 规则默认情况下会屏蔽这些代理。如果您预计来自移动应用程序的流量，或者来自非浏览器用户代理的任何其他合法流量，则需要添加一个例外来允许流量。

- 您可能依赖某些特定的机器人流量来进行正常运行时间监控、集成测试或营销工具之类的事情。如果 Bot Control 识别并阻止了您想要允许的机器人流量，则需要通过添加自己的规则来更改处理方式。虽然这不是所有客户的误报情况，但如果是针对您的情况，则需要像处理误报情况一样处理。
- Bot Control 托管规则组使用来自 IP 地址验证机器人 Amazon WAF。如果您使用 Bot Control 并且已验证通过代理或负载均衡器路由的机器人，则可能需要使用自定义规则明确允许它们。有关如何创建此类自定义规则的信息，请参阅[转发的 IP 地址 \(p. 110\)](#)。
- 全局误报率低的 Bot Control 规则可能会严重影响特定的设备或应用程序。例如，在测试和验证中，我们可能没有观察到来自低流量应用程序或不太常见的浏览器或设备的请求。
- 误报率处于历史最低的 Bot Control 规则可能会增加有效流量的误报。这可能是由于新的流量模式或请求属性与有效流量一起出现，导致其与以前不匹配的规则相匹配。这些更改可能是由于以下情况造成的：
 - 流量详细信息随着流量流经网络设备（例如负载均衡器或内容分发网络 (CDN)）而发生变化。
 - 流量数据的新变化，例如新浏览器或现有浏览器的新版本。

有关如何处理可能从 Amazon WAF Bot Control 托管规则组获得的误报的信息，请参阅下一节中的指南[测试和部署 Amazon WAF 机器人控制 \(p. 145\)](#)。

测试和部署 Amazon WAF 机器人控制

本节提供为您的站点配置和测试 Amazon WAF Bot Control 实现的一般指导。您选择遵循的具体步骤将取决于您的需求、资源和收到的网络请求。

此信息是上提供的有关测试和调整的一般信息的补充[测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

Note

Amazon 托管规则旨在保护您免受常见的 Web 威胁的攻击。根据文档进行使用时，Amazon 托管规则组将为您的应用程序添加另一层安全性。但是，Amazon 托管规则组并非用于取代您的安全责任，这些责任由您所选择的 Amazon 资源决定。请参阅[责任共担模式](#)，以确保妥善保护 Amazon 中的资源。

生产流量风险

在为生产流量部署 Bot Control 实现之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整规则，然后再启用这些规则。

本指南适用于一般知道如何创建和管理 Amazon WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前几部分所涵盖的。

配置和测试机器人控制实现

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 添加机器人控制托管规则组

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

将托管 Amazon 规则组 `AWSManagedRulesBotControlRuleSet` 添加到新的或现有的 Web ACL 中，并对其进行配置，使其不会改变当前 Web ACL 的行为。

- 添加托管规则组时，对其进行编辑并执行以下操作：
 - 在“检查级别”窗格中，选择要使用的检查级别。
 - 常见 — 检测各种自我识别的机器人，例如网页抓取框架、搜索引擎和自动浏览器。此级别的机器人控制保护使用传统的机器人检测技术（例如静态请求数据分析）识别常见的机器人。这些规则会标记来自这些机器人的流量，并屏蔽他们无法验证的流量。

- 定向 — 包括通用级保护，并增加了对无法自我识别的高级机器人的检测。定向保护使用浏览器查询、指纹识别和行为启发式等高级检测技术来识别恶意机器人流量。这些保护措施结合了速率限制、验证码和后台浏览器挑战，针对这些机器人。提供定向保护的规则的名称以开头TGT_。

有关此选项的更多信息，请参阅[Amazon WAF机器人控制规则组 \(p. 49\)](#)。

- 在“规则”窗格中，打开“覆盖所有规则操作”下拉列表并选择Count。使用此配置，将根据规则组中的所有规则Amazon WAF评估请求，仅计算结果的匹配结果，同时仍会为请求添加标签。有关更多信息，请参阅[覆盖规则组中的规则操作 \(p. 20\)](#)：

通过这种替换，您可以监控 Bot Control 规则对您的流量的潜在影响，以确定是否要为内部用例或所需机器人之类的事情添加例外情况。

- 放置规则组，使其在 Web ACL 中排在最后一位，优先级设置比你已经使用的任何其他规则或规则组都要高。有关更多信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)：

这样，您当前对流量的处理就不会受到干扰。例如，如果您有检测恶意流量（例如 SQL 注入或跨站点脚本）的规则，则它们将继续检测和记录这些请求。或者，如果您的规则允许已知的非恶意流量，则它们可以继续允许该流量，而不必被 Bot Control 管理规则组阻止。在测试和调整活动期间，你可能会决定调整处理顺序，但这是一个不错的开始方式。

2. 为 Web ACL 启用采样、记录和指标

根据需要，配置 Web ACL 的日志记录，并启用采样和 Amazon CloudWatch 指标。您可以使用指标和日志来监控 Web 流量与 Bot Control 托管规则组的交互。

- 有关配置和使用日志记录的信息，请参见[记录 Web ACL 流量 \(p. 180\)](#)。
- 有关亚马逊 CloudWatch 指标的信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。
- 有关 Web 请求采样的信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)。

3. 将 Web ACL 与资源相关联

如果 Web ACL 尚未与资源关联，请将其关联。有关信息，请参阅[将 Web ACL 与Amazon资源关联或取消关联 \(p. 22\)](#)。

4. 监控流量和机器人控制规则匹配情况

确保流量畅通，并且 Bot Control 托管规则组规则正在为匹配的 Web 请求添加标签。您可以在日志中看到标签，也可以查看亚马逊指标中的机器人和标签 CloudWatch 指标。在日志中，您在规则组中替换为计数的规则显示在 with seaction truleGroupList to count 中，并overriddenAction表示您改写了已配置的规则操作。

Note

Bot Control 托管规则组使用来自 IP 地址验证机器人Amazon WAF。如果您使用 Bot Control 并且已验证通过代理或负载均衡器路由的机器人，则可能需要使用自定义规则明确允许它们。有关如何创建自定义规则的信息，请参阅[转发的 IP 地址 \(p. 110\)](#)。有关如何使用该规则自定义 Bot Control Web 请求处理的信息，请参阅下一步。

仔细查看 Web 请求处理中是否存在可能需要通过自定义处理来缓解的任何误报。有关误报的示例，请参见[Amazon WAF机器人控制出现误报 \(p. 144\)](#)。

5. 自定义机器人控制 Web 请求处理

根据需要，添加您自己的规则，明确允许或阻止请求，以更改 Bot Control 规则处理请求的方式。

如何执行此操作取决于您的用例，但以下是常见的解决方案：

- 明确允许具有您在 Bot Control 托管规则组之前添加的规则。这样，允许的请求永远不会到达规则组进行评估。这有助于控制使用 Bot Control 托管规则组的成本。
- 通过在 Bot Control 托管规则组语句中添加范围缩小语句，将请求排除在 Bot Control 评估之外。其功能与前面的选项相同。它可以帮助控制使用 Bot Control 托管规则组的成本，因为与范围缩小语句不匹配的请求永远不会到达规则组评估。有关范围缩小语句的信息，请参见[范围缩小声明 \(p. 110\)](#)。

有关示例，请参阅以下内容：

- [将 IP 范围排除在机器人管理之外 \(p. 154\)](#)
- [允许来自您控制的机器人的流量 \(p. 154\)](#)
- 在请求处理中使用 Bot Control 标签来允许或阻止请求。在 Bot Control 托管规则组之后添加标签匹配规则，从要阻止的带标签请求中过滤掉要允许的带标签的请求。

测试后，将相关的 Bot Control 规则保持在计数模式，并在自定义规则中保留请求处理决策。有关标签匹配语句的信息，请参见[标签匹配规则声明 \(p. 92\)](#)。

有关此类型自定义的示例，请参阅以下：

- [为被封禁的用户代理创建例外 \(p. 151\)](#)
- [允许特定被屏蔽的机器人 \(p. 149\)](#)
- [屏蔽经过验证的机器人 \(p. 148\)](#)

有关其他示例，请参阅 [Amazon WAF 机器人控制示例 \(p. 147\)](#)。

6. 根据需要启用 Bot Control 托管规则组设置

根据您的情况，您可能已决定将某些 Bot Control 规则保留为计数模式或使用不同的操作替代规则。对于要在规则组内部配置时运行的规则，请启用常规规则配置。为此，请编辑 Web ACL 中的规则组语句，然后在“规则”窗格中进行更改。

Amazon WAF 机器人控制示例

本节显示了满足 Amazon WAF Bot Control 实现的各种常见用例的示例配置。

每个示例均提供用例描述，然后在 JSON 列表中显示自定义配置规则的解决方案。

Note

这些示例中显示的 JSON 列表是在控制台中创建的，方法是配置规则，然后使用规则 JSON 编辑器对其进行编辑。您还可以通过 API 或命令行界面使用 get 命令检索整个规则组或 Web ACL 中规则的 JSON。

主题

- [Amazon WAF 机器人控制示例：简单配置 \(p. 147\)](#)
- [Amazon WAF 机器人控制示例：明确允许经过验证的机器人 \(p. 148\)](#)
- [Amazon WAF 机器人控制示例：屏蔽经过验证的机器人 \(p. 148\)](#)
- [Amazon WAF 机器人控制示例：允许特定被屏蔽的机器人 \(p. 149\)](#)
- [Amazon WAF 机器人控制示例：为被封禁的用户代理创建例外 \(p. 151\)](#)
- [Amazon WAF 机器人控制示例：仅对登录页面使用机器人控制 \(p. 152\)](#)
- [Amazon WAF 机器人控制示例：仅对动态内容使用机器人控制 \(p. 153\)](#)
- [Amazon WAF 机器人控制示例：从机器人管理中排除 IP 范围 \(p. 154\)](#)
- [Amazon WAF 机器人控制示例：允许来自您控制的机器人的流量 \(p. 154\)](#)

Amazon WAF 机器人控制示例：简单配置

以下 JSON 列表显示了带有 Amazon WAF 机器人控制托管规则组的 Web ACL 示例。请注意可见性配置，这会 Amazon WAF 导致存储请求示例和指标以供监控之用。

```
{
  "Name": "Bot-Beta-WebACL",
  "Id": "...",
```

```
"ARN": "...",
"DefaultAction": {
  "Allow": {}
},
"Description": "Bot-Beta-WebACL",
"Rules": [
  {
    ...
  },
  {
    "Name": "AWS-AWSBotControl-Example",
    "Priority": 5,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet"
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
      }
    }
  },
  "VisibilityConfig": {
    ...
  },
  "Capacity": 1496,
  "ManagedByFirewallManager": false
}
```

Amazon WAF 机器人控制示例：明确允许经过验证的机器人

Amazon WAF Bot Control 不会屏蔽已知是常见且可验证的机器人。Amazon 当 Bot Control 识别 Web 请求来自经过验证的机器人时，它会添加一个命名该机器人的标签和一个表明它是经过验证的机器人的标签。Bot Control 不会添加任何其他标签，例如信号标签，以防止已知的正常机器人被屏蔽。

您可能还有其他阻止经过验证的机器人的 Amazon WAF 规则。如果您想确保允许经过验证的机器人，请添加自定义规则，根据 Bot Control 标签允许他们使用。您的新规则必须在 Bot Control 托管规则组之后运行，这样标签才能与之匹配。

以下规则明确允许经过验证的机器人。

```
{
  "Name": "match_rule",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "aws:waf:managed:aws:bot-control:bot:verified"
    }
  },
  "RuleLabels": [],
  "Action": {
    "Allow": {}
  }
}
```

Amazon WAF 机器人控制示例：屏蔽经过验证的机器人

要屏蔽经过验证的机器人，必须添加一条规则来阻止在 Amazon WAF Bot Control 托管规则组之后运行的机器人。为此，请确定要屏蔽的机器人名称，然后使用标签匹配语句来识别和屏蔽它们。如果你只想屏蔽所有经过验证的机器人，你可以省略与 bot:name: 标签的匹配项。

以下规则仅阻止bingbot经过验证的机器人。该规则必须在 Bot Control 托管规则组之后运行。

```
{
  "Name": "match_rule",
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
          }
        },
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:verified"
          }
        }
      ]
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  }
}
```

以下规则阻止所有经过验证的机器人。

```
{
  "Name": "match_rule",
  "Statement": {
    "LabelMatchStatement": {
      "Scope": "LABEL",
      "Key": "awswaf:managed:aws:bot-control:bot:verified"
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  }
}
```

Amazon WAF机器人控制示例：允许特定被屏蔽的机器人

一个机器人可能会被多个机器人控制规则阻止。针对每条阻塞规则运行以下步骤。

如果Amazon WAF Bot Control 规则阻止了您不想屏蔽的机器人，请执行以下操作：

1. 通过检查日志来确定阻止机器人的机器人控制规则。将在日志中名称以开头的字段中指定屏蔽规则terminatingRule。有关 Web ACL 日志的信息，请参见[记录 Web ACL 流量 \(p. 180\)](#)。请注意规则添加到请求的标签。
2. 在您的 Web ACL 中，替换阻塞规则的操作以计算在内。要在控制台中执行此操作，请编辑 Web ACL 中的规则组规则，然后Count为该规则选择规则操作替换。这样可以确保机器人不会被规则阻止，但规则仍会将其标签应用于匹配的请求。
3. 在 Bot Control 托管规则组后面，将标签匹配规则添加到 Web ACL。将规则配置为与被替换规则的标签相匹配，并阻止除您不想屏蔽的机器人之外的所有匹配请求。

您的 Web ACL 现已配置，因此您想要允许的机器人不再被您在日志中确定的阻止规则所阻止。

再次检查流量和日志，确保机器人被允许通过。如果不是，请再次运行上述程序。

例如，假设您要阻止除以下之外的所有监控机器人pingdom。在这种情况下，您可以将CategoryMonitoring规则改写为计数，然后编写一条规则来屏蔽除带有机器人名称标签的机器人之外的所有监控机器人pingdom。

以下规则使用 Bot Control 托管规则组，但会覆盖规则操作才算CategoryMonitoring在内。类别监控规则照常将其标签应用于匹配的请求，但仅对请求进行计数，而不是执行通常的封锁操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

以下规则与前面CategoryMonitoring规则添加到匹配的 Web 请求中的类别监控标签相匹配。在类别监控请求中，该规则会屏蔽除带有机器人名称标签的请求以外的所有请求pingdom。

以下规则必须在 Web ACL 处理顺序中前面的 Bot Control 托管规则组之后运行。

```
{
  "Name": "match_rule",
  "Priority": 10,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "aws:waf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "aws:waf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        }
      ]
    }
  }
}
```

```
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
  }
}
```

Amazon WAF 机器人控制示例：为被封禁的用户代理创建例外

如果错误地阻止了来自某些非浏览器用户代理的流量，则可以通过将违规的 Bot Control 规则设置为 Count，然后将该规则的标签与您的例外标准相结合 SignalNonBrowserUserAgent 来创建异常。

Note

移动应用程序通常具有非浏览器用户代理，SignalNonBrowserUserAgent 规则默认情况下会屏蔽这些代理。

以下规则使用 Bot Control 托管规则组，但会将规则操作改 SignalNonBrowserUserAgent 为 Count。信号规则照常将其标签应用于匹配的请求，但仅对请求进行计数，而不是执行通常的阻塞操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

以下规则与 Bot Control SignalNonBrowserUserAgent 规则添加到其匹配的 Web 请求中的信号标签相匹配。在信号请求中，除了那些拥有我们想要允许的用户代理的请求外，该规则会阻止所有请求。

以下规则必须在 Web ACL 处理顺序中前面的 Bot Control 托管规则组之后运行。

```
{
  "Name": "match_rule",
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
```

```
        "Scope": "LABEL",
        "Key": "aws:waf:managed:aws:bot-control:signal:non_browser_user_agent"
    },
    {
        "NotStatement": {
            "Statement": {
                "ByteMatchStatement": {
                    "FieldToMatch": {
                        "SingleHeader": {
                            "Name": "user-agent"
                        }
                    },
                    "PositionalConstraint": "EXACTLY",
                    "SearchString": "PostmanRuntime/7.29.2",
                    "TextTransformations": [
                        {
                            "Priority": 0,
                            "Type": "NONE"
                        }
                    ]
                }
            }
        }
    }
],
"RuleLabels": [],
"Action": {
    "Block": {}
},
"VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
}
}
```

Amazon WAF 机器人控制示例：仅对登录页面使用机器人控制

以下示例使用范围缩小语句将 Amazon WAF Bot Control 仅应用于进入网站登录页面的流量，该页面由 URI 路径标识 login。您的登录页面的 URI 路径可能与示例不同，具体取决于您的应用程序和环境。

```
{
    "Name": "AWS-AWSBotControl-Example",
    "Priority": 5,
    "Statement": {
        "ManagedRuleGroupStatement": {
            "VendorName": "AWS",
            "Name": "AWSManagedRulesBotControlRuleSet",
            "RuleActionOverrides": [],
            "ExcludedRules": []
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Example"
        },
        "ScopeDownStatement": {
            "ByteMatchStatement": {
                "SearchString": "login",
                "FieldToMatch": {
                    "UriPath": {}
                }
            }
        }
    }
}
```

```
    },
    "TextTransformations": [
      {
        "Priority": 0,
        "Type": "NONE"
      }
    ],
    "PositionalConstraint": "CONTAINS"
  }
}
}
```

Amazon WAF机器人控制示例：仅对动态内容使用机器人控制

此示例使用范围缩小语句将Amazon WAF Bot Control 仅应用于动态内容。

scope-down 语句通过否定正则表达式模式集的匹配结果来排除静态内容：

- 正则表达式模式集配置为匹配静态内容的扩展。例如，正则表达式模式集规范可能是`(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`。有关正则表达式模式集和语句的信息，请参见[正则表达式模式集匹配规则语句 \(p. 98\)](#)。
- 在 scope-down 语句中，我们通过在语句内嵌套正则表达式模式集语句来排除匹配的NOT静态内容。有关该NOT声明的信息，请参见[NOT规则语句 \(p. 93\)](#)。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

Amazon WAF机器人控制示例：从机器人管理中排除 IP 范围

如果您想从Amazon WAF Bot Control 管理中排除 Web 流量的子集，并且可以使用规则语句识别该子集，则可以通过在 Bot Control 托管规则组语句中添加缩小范围语句来排除该子集。

以下规则对所有网络流量执行正常的 Bot Control 机器人管理，但来自特定 IP 地址范围的 Web 请求除外。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/000000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

Amazon WAF机器人控制示例：允许来自您控制的机器人的流量

您可以配置一些站点监控机器人和自定义机器人来发送自定义标头。如果您想允许来自这些类型的机器人的流量，可以将其配置为在标头中添加共享密钥。然后，您可以通过在Amazon WAF Bot Control 托管规则组语句中添加范围缩小语句来排除带有标题的消息。

以下示例规则将带有秘密标头的流量排除在机器人控制检查之外。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
```

```
        "SearchString": "YSBzZWNyZXQ=",
        "FieldToMatch": {
            "SingleHeader": {
                "Name": "x-bypass-secret"
            }
        },
        "TextTransformations": [
            {
                "Priority": 0,
                "Type": "NONE"
            }
        ],
        "PositionalConstraint": "EXACTLY"
    }
}
```

Amazon WAF 欺诈控制账户收购预防 (ATP)

账户接管是一种在线非法活动，在这种活动中，攻击者获得对个人帐户的未经授权的访问权限。攻击者可能通过多种方式执行此操作，例如使用被盗的凭据或通过一系列尝试猜测受害者的密码。当攻击者获得访问权限时，他们可能会从受害者那里窃取金钱、信息或服务。攻击者可能会冒充受害者，以获取受害者拥有的其他帐户的访问权限，或者获取访问其他人或组织的帐户的权限。此外，他们可能会尝试更改用户的密码，以阻止受害者访问自己的帐户。

您可以通过实施 Amazon WAF 欺诈控制账户接管预防 (ATP) 功能来监控和控制账户接管尝试。Amazon WAF 在 Managed RuAmazonIes 规则组 AWSManagedRulesATPRuleSet 和配套应用程序集成 SDK 中提供此功能。

ATP 托管规则组标记和管理可能属于恶意账户接管企图一部分的请求。规则组通过检查客户端发送到您的应用程序的登录端点的登录尝试来实现此目的。

- **请求检查** — ATP 使您可以查看和控制使用被盗凭据的异常登录尝试和登录尝试，以防止可能导致欺诈活动的账户接管。ATP 根据其被盗的凭证数据库检查电子邮件和密码组合，随着在暗网上发现新的泄露凭据，该数据库会定期更新。ATP 通过 IP 地址和客户端会话聚合数据，以检测和阻止发送过多可疑请求的客户端。
- **响应检查** — 对于 CloudFront 分配，除了检查传入的登录请求外，ATP 规则组还会检查您的应用程序对登录尝试的响应，以跟踪成功率和失败率。利用这些信息，ATP 可以暂时阻止登录失败次数过多的客户端会话或 IP 地址。Amazon WAF 异步执行响应检查，因此这不会增加网络流量的延迟。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

Note

ATP 功能不适用于 Amazon Cognito 用户池。

主题

- [ATP 成分 \(p. 156\)](#)
- [为什么要将应用程序集成 SDK 与 ATP 一起使用 \(p. 156\)](#)
- [将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)
- [测试和部署 ATP \(p. 159\)](#)
- [Amazon WAF 欺诈控制账户收购预防 \(ATP\) 示例 \(p. 161\)](#)

ATP 成分

Amazon WAF 欺诈控制账户接管预防 (ATP) 的主要组成部分如下：

- **AWSManagedRulesATPRuleSet**— 此 ManagedAmazon Rules 规则组中的规则检测、标记和处理各种类型的账户接管活动。规则组检查客户端发送到指定登录端点的 HTTPPOST Web 请求。对于受保护的 CloudFront 发行版，规则组还会检查发行版发送回这些请求的响应。有关规则组规则的列表，请参阅[Amazon WAF 欺诈控制账户接管预防 \(ATP\) 规则组 \(p. 56\)](#)。您可以使用托管规则组参考语句将此规则组包含在 Web ACL 中。有关使用此规则组的信息，请参阅[将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

- 有关应用程序登录页面的详细信息-将AWSManagedRulesATPRuleSet规则组添加到 Web ACL 时，必须提供有关登录页面的信息。这使规则组可以缩小其检查的请求范围，并正确验证 Web 请求中的凭证使用情况。ATP 规则组使用电子邮件格式的用户名。有关更多信息，请参阅[将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)：
- 对于受保护的 CloudFront 发行版，有关您的应用程序如何响应登录尝试的详细信息-您提供有关应用程序对登录尝试的响应的详细信息，规则组会跟踪和管理发送过多失败登录尝试的客户端。有关配置该选项的信息，请参阅[将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)。
- JavaScript 和移动应用程序集成 SDK — 在您的 ATP 实施中实施Amazon WAF JavaScript 和移动 SDK，以启用规则组提供的全套功能。许多 ATP 规则使用软件开发工具包提供的信息进行会话级客户端验证和行为聚合，这是将合法的客户端流量与机器人流量分开所必需的。有关开发工具包的更多信息，请参阅[Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。

您可以将 ATP 的实施与以下内容相结合，以帮助您监控、调整 and 自定义保护措施。

- 日志和指标 — 通过为网页 ACL 配置和启用日志和 Amazon CloudWatch 指标，您可以监控您的流量，了解 ATP 托管规则组如何影响流量。AWSManagedRulesATPRuleSet添加到您的网络请求的标签包含在日志和亚马逊 CloudWatch 指标中。有关日志和指标的信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)和[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。

根据您的需求和看到的流量，您可能需要自定义您的AWSManagedRulesATPRuleSet实现。例如，您可能想将某些流量排除在 ATP 评估之外，或者您可能想使用范围缩小声明或标签匹配规则等Amazon WAF 功能，更改其处理某些帐户接管尝试的方式。

- 标签和标签匹配规则-对于中的任何规则AWSManagedRulesATPRuleSet，您可以将阻塞行为切换为计数，然后与规则添加的标签进行匹配。使用此方法自定义处理由 ATP 托管规则组识别的 Web 请求的方式。有关标注和使用标签匹配语句的更多信息，请参见[标签匹配规则声明 \(p. 92\)](#)和[网络请求上的标签 \(p. 123\)](#)。
- 自定义请求和响应-您可以向允许的请求添加自定义标头，也可以为阻止的请求发送自定义响应。为此，您需要将标签匹配与Amazon WAF自定义请求和响应功能配对。有关自定义请求和响应的更多信息，请参阅[中的自定义 Web 请求和响应Amazon WAF \(p. 118\)](#)。

为什么要将应用程序集成 SDK 与 ATP 一起使用

ATP 托管规则组需要应用程序集成 SDK 生成的质询令牌。这些令牌启用了规则组提供的全套保护。

我们强烈建议实施应用程序集成 SDK，以便最有效地使用 ATP 规则组。质询脚本必须在 ATP 规则组之前运行，规则组才能从脚本获取的令牌中受益。这是在应用程序集成 SDK 中自动发生的。如果您无法使用 SDK，则可以交替配置 Web ACL，使其对将由 ATPCAPTCHA 规则组检查的所有请求运行Challenge或规则操作。使用Challenge或CAPTCHA规则操作可能会产生额外费用。有关定价的详细信息，请参阅[Amazon WAF 定价](#)。

不需要令牌的 ATP 规则组的功能

当 Web 请求没有令牌时，ATP 托管规则组能够阻止以下类型的流量：

- 发出大量登录请求的单个 IP 地址。
- 在短时间内发出大量失败的登录请求的单个 IP 地址。
- 尝试遍历密码，使用相同的用户名但更改密码。

需要令牌的 ATP 规则组的功能

挑战令牌中提供的信息扩展了规则组和整体客户端应用程序安全的功能。

该令牌为每个 Web 请求提供客户信息，使 ATP 规则组能够将合法的客户端会话与行为不良的客户端会话分开，即使两者都来自单个 IP 地址。规则组使用令牌中的信息来聚合客户端会话请求行为，以进行微调检测和缓解措施。

当令牌在 Web 请求中可用时，ATP 规则组可以在会话级别检测和屏蔽以下其他类别的客户端：

- 未能通过 SDK 管理的静默挑战的客户端会话。
- 遍历用户名或密码的客户端会话。这也称作凭证填充。
- 反复使用被盗凭据登录的客户端会话。
- 花费很长时间尝试登录的客户端会话。
- 提出大量登录请求的客户端会话。与 Amazon WAF 基于速率的规则相比，ATP 规则组提供的客户端隔离效果更好，后者通过 IP 地址阻止客户端。ATP 规则组还使用较低的阈值。
- 在短时间内发出大量失败的登录请求的客户端会话。此功能适用于受保护的亚马逊 CloudFront 发行版。

有关规则组功能的更多信息，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

有关开发工具包的信息，请参阅[Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。有关 Amazon WAF 令牌的信息，请参阅[Amazon WAF 网络请求令牌 \(p. 136\)](#)。有关规则操作的信息，请参阅[CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)。

将 ATP 托管规则组添加到您的 Web ACL

要配置 ATP 托管规则组以识别 Web 流量中的账户接管活动，您需要提供有关客户机如何向应用程序发送登录请求的信息。对于受保护的亚马逊 CloudFront 发行版，您还需要提供有关您的应用程序如何响应登录请求的信息。此配置是对托管规则组的常规配置的补充。

有关规则组描述和规则列表，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

Note

ATP 被盗凭证数据库仅包含电子邮件格式的用户名。

本指南适用于一般知道如何创建和管理 Amazon WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前几部分所涵盖的。

遵循最佳实践

按照中的最佳做法使用 ATP 规则组[智能威胁缓解最佳实践 \(p. 135\)](#)。

在 Web ACL 中使用 `AWSManagedRulesATPRuleSet` 规则组

1. 将 Amazon 托管规则组添加 `AWSManagedRulesATPRuleSet` 到 Web ACL，并在保存之前编辑规则组设置。

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

Note

有关如何将托管规则组添加到 Web ACL 的基本信息，请参阅[通过控制台将托管规则组添加到 Web ACL \(p. 28\)](#)。

2. 在规则组配置窗格中，提供 ATP 规则组用来检查登录请求的信息。
 - a. 对于登录路径，请提供应用程序登录终端节点的路径。例如，对于 URL `https://example.com/web/login`，您将提供路径 `/web/login`。以您提供的路径开头的登录路径被视为匹配路径。例如，`/web/login` 匹配登录路径 `/web/login`、`/web/login/web/loginPage/web/login/thisPage`、和，但与登录路径 `/home/web/login` 或不匹配 `/website/login`。

规则组仅检查对您指定登录端点的 HTTPPOST 请求。

- b. 对于请求检查，通过提供请求负载类型以及请求正文中提供用户名和密码的字段名称，指定您的应用程序如何接受登录尝试。您对字段名称的指定取决于负载类型。
 - JSON 负载类型-以 JSON 指针语法指定字段名称。有关 JSON 指针语法的信息，请参阅互联网工程任务组 (IETF) 文档[JavaScript对象表示法 \(JSON\) 指针](#)。

例如，对于以下示例 JSON 负载，用户名字段规范为 `/login/username`，密码字段规范为 `/login/password`。

```
{
  "login": {
    "username": "THE_USERNAME",
    "password": "THE_PASSWORD"
  }
}
```

- FORM_CONDEDED 负载类型 — 使用 HTML 表单名称。

例如，对于输入元素名为 `username1` 和的 HTML 表单 `password1`，用户名字段规范为 `username1`，密码字段规范为 `password1`。

- c. 如果您要保护亚马逊 CloudFront 发行版，则在“响应检查”下，指定您的应用程序如何显示其对登录尝试的响应是成功还是失败。

Note

ATP 响应检查仅在保护 CloudFront 发行版的 Web ACL 中可用。

在登录响应中指定您希望 ATP 检查的单个组件。对于 Body 和 JSON 组件类型，Amazon WAF 可以检查组件的前 65,536 字节 (64 KB)。

如界面所示，提供组件类型的检查标准。您必须提供要在组件中检查的成功和失败标准。

例如，假设您的应用程序在响应的状态码中指示了登录尝试的状态，并使用 200 OK 成功和 401 Unauthorized 或 403 Forbidden 表示失败。您可以将响应检查组件类型设置为状态代码，然后在成功文本框中输入，200 然后在失败文本框的第一行和 403 第二行中输 401 入。

ATP 规则组仅计算与您的成功或失败检查标准相匹配的回复。当客户端在计数的响应中失败率过高时，规则组规则会对客户端起作用。为确保规则组规则的行为准确，请务必提供成功和失败的登录尝试的完整信息。

要查看检查登录响应的规则，请在规则列

表 `VolumetricSessionFailedLoginResponseHigh` 中查

找 `VolumetricIpFailedLoginResponseHigh` 和 [Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

3. 为规则组提供所需的任何其他配置。

您可以通过向托管规则组语句中添加 scope-down 语句来进一步限制规则组检查的请求范围。例如，您只能检查带有特定查询参数或 cookie 的请求。规则组将仅检查发往您的指定登录端点的 HTTPPOST 请求，这些请求与您的 scope-down 语句中的条件相匹配。有关范围缩小语句的信息，请参见[范围缩小声明 \(p. 110\)](#)。

4. 保存您对 Web ACL 所做的更改。

在为生产流量部署 ATP 实现之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整规则，然后再启用这些规则。有关指导，请参阅以下部分。

测试和部署 ATP

本节提供在您的站点配置和测试 Amazon WAF 欺诈控制账户接管预防 (ATP) 实施的一般指导。您选择遵循的具体步骤将取决于您的需求、资源和收到的网络请求。

此信息是上提供的有关测试和调整的一般信息的补充[测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

Note

Amazon 托管规则旨在保护您免受常见的 Web 威胁的攻击。根据文档进行使用时，Amazon 托管规则组将为您的应用程序添加另一层安全性。但是，Amazon 托管规则组并非用于取代您的安全责任，这些责任由您所选择的 Amazon 资源决定。请参阅[责任共担模式](#)，以确保妥善保护 Amazon 中的资源。

生产流量风险

在为生产流量部署 ATP 实现之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整规则，然后再启用这些规则。

Amazon WAF 提供可用于验证 ATP 配置的测试凭证。在以下步骤中，您将配置测试 Web ACL 以使用 ATP 托管规则组，配置规则以捕获规则组添加的标签，然后使用这些测试凭证尝试登录。您将通过检查登录尝试的亚马逊 CloudWatch 指标，验证您的网络 ACL 是否已正确管理了该尝试。

本指南适用于一般知道如何创建和管理 Amazon WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前几部分所涵盖的。

配置和测试 Amazon WAF 欺诈控制账户接管预防 (ATP) 的实施

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 在计数模式下添加防 Amazon WAF 欺诈控制账户接管 (ATP) 管理规则组

Note

使用此托管规则组时，需要向您收取额外费用。有关更多信息，请参阅[Amazon WAF 定价](#)。

将 Amazon 托管规则组 AWSManagedRulesATPRuleSet 添加到新的或现有的 Web ACL 中，并对其进行配置，使其不会改变当前 Web ACL 的行为。有关此规则组的规则和标签的详细信息，请参阅[Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

- 添加托管规则组时，对其进行编辑并执行以下操作：
 - 在规则组配置窗格中，提供应用程序登录页面的详细信息。ATP 规则组使用此信息来监控登录活动。有关更多信息，请参阅[将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)：
 - 在“规则”窗格中，打开“覆盖所有规则操作”下拉列表并选择 Count。使用此配置，将根据规则组中的所有规则 Amazon WAF 评估请求，仅计算结果的匹配结果，同时仍会为请求添加标签。有关更多信息，请参阅[覆盖规则组中的规则操作 \(p. 20\)](#)：

通过此改写，您可以监控 ATP 管理规则的潜在影响，以确定是否要添加例外，例如内部用例的例外。

- 放置规则组，使其根据您在 Web ACL 中的现有规则进行评估，优先级设置在数字上高于您已经使用的任何规则或规则组。有关更多信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)：

这样，您当前对流量的处理就不会受到干扰。例如，如果您有检测恶意流量（例如 SQL 注入或跨站点脚本）的规则，他们将继续检测并记录这些流量。或者，如果您的规则允许已知的非恶意流量，则它们可以继续允许该流量，而不必被 ATP 管理规则组阻止。在测试和调整活动期间，您可能会决定调整处理顺序。

2. 为 Web ACL 启用采样、记录和指标

根据需要，配置 Web ACL 的日志记录，并启用采样和 Amazon CloudWatch 指标。您可以使用这些可见性工具来监控 ATP 托管规则组与您的流量的交互。

- 有关配置和使用日志记录的信息，请参见[记录 Web ACL 流量 \(p. 180\)](#)。
- 有关亚马逊 CloudWatch 指标的信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。
- 有关 Web 请求采样的信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)。

3. 将 Web ACL 与资源相关联

如果 Web ACL 尚未与测试资源关联，请将其关联。有关信息，请参阅[将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)。

4. 监控流量和 ATP 规则匹配情况

确保您的正常流量畅通，并且 ATP 托管规则组规则正在为匹配的 Web 请求添加标签。您可以在日志中看到标签，也可以查看亚马逊指标中的 ATP 和标签 CloudWatch 指标。在日志中，您在规则组中替换为计数的规则显示在 `with seaction truleGroupList to count` 中，并 `overriddenAction` 表示您改写了已配置的规则操作。

5. 测试规则组的凭证检查功能

尝试使用测试泄露的凭据进行登录，并检查规则组是否符合预期。

a. 使用以下 Amazon WAF 测试凭证对登录到受保护资源的登录页面：

- 用户：WAF_TEST_CREDENTIAL@wafexample.com
- 密码：WAF_TEST_CREDENTIAL_PASSWORD

这些测试凭证被归类为已泄露的凭据，ATP 托管规则组将在登录请求中添加 `awswaf:managed:aws:atp:signal:credential_compromised` 标签，您可以在日志中看到该标签。

b. 在 Web ACL 日志中，查找测试登录 Web 请求的日志条目 `labels` 字段中的 `awswaf:managed:aws:atp:signal:credential_compromised` 标签。有关日志记录的信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)。

在验证规则组按预期捕获泄露的证书后，您可以根据受保护资源的需要采取措施配置其实现。

6. 对于 CloudFront 发行版，测试规则组的登录失败管理

a. 针对您为 ATP 规则组配置的每个故障响应标准运行测试。两次测试之间至少等待 10 分钟。

要测试单个失败标准，请在响应中使用该条件确定会失败的登录尝试。然后，在不到 10 分钟的时间内，从单个客户端 IP 地址执行至少 10 次失败的登录尝试。

在前 6 次失败后，`volumetric` 失败的登录规则应开始与您的其余尝试进行匹配，对其进行标记和计数。由于延迟，该规则可能会错过前一两个。

b. 在 Web ACL 日志中，查找测试登录 Web 请求的日志条目 `labels` 字段中的 `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` 标签。有关日志记录的信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)。

这些测试通过检查失败的登录次数是否超过规则的阈值来验证您的失败标准是否与您的响应相符 `VolumetricIpFailedLoginResponseHigh`。达到阈值后，如果您继续从同一 IP 地址发送登录请求，则规则将继续匹配，直到失败率降至阈值以下。当超过阈值时，该规则会匹配从 IP 地址成功或失败的登录。

7. 自定义 ATP 网络请求处理

根据需要，添加您自己的规则，明确允许或阻止请求，以更改 ATP 规则处理请求的方式。

例如，您可以使用 ATP 标签来允许或阻止请求，或者自定义请求处理。您可以在 ATP 托管规则组之后添加标签匹配规则，以筛选已贴标签的请求以进行要应用的处理。测试后，将相关的 ATP 规则保持在计数模式，并在自定义规则中保留请求处理决策。有关示例，请参阅 [ATP 示例：对丢失和泄露的凭据进行自定义处理 \(p. 162\)](#)。

8. 删除您的测试规则并启用 ATP 托管规则组设置

根据您的情况，您可能已经决定要将某些 ATP 规则保留在计数模式。对于要按照规则组内部的配置运行的规则，请在 Web ACL 规则组配置中禁用计数模式。完成测试后，您还可以删除测试标签匹配规则。

9. 监视和调谐

为确保按您的需要处理 Web 请求，请在启用要使用的 ATP 功能后密切监控您的流量。根据需要调整行为，在规则组上改写规则数并使用您自己的规则。

完成对 ATP 规则组实现的测试后，我们建议您将 Amazon WAF ATP JavaScript SDK 集成到浏览器登录页面中，以增强检测能力。Amazon WAF 还提供用于集成 iOS 和安卓设备的移动 SDK。有关集成开发工具包的更多信息，请参阅 [Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。

Amazon WAF 欺诈控制账户收购预防 (ATP) 示例

本节显示了满足 Amazon WAF 欺诈控制账户接管预防 (ATP) 实施的常见用例的示例配置。

每个示例均提供用例描述，然后在 JSON 列表中显示自定义配置规则的解决方案。

Note

您可以通过控制台 Web ACL JSON 下载或规则 JSON 编辑器或通过 API 和命令行界面中的 `getWebACL` 操作来检索 JSON 列表，如这些示例中所示的列表。

主题

- [ATP 示例：简单配置 \(p. 161\)](#)
- [ATP 示例：对丢失和泄露的凭据进行自定义处理 \(p. 162\)](#)

ATP 示例：简单配置

以下 JSON 列表显示了带有防 Amazon WAF 欺诈控制账户接管 (ATP) 管理规则组的示例 Web ACL。请注意额外的登录页面配置，它为规则组提供了监控和管理您的登录请求所需的信息。此 JSON 包含 Web ACL 自动生成的设置，例如标签命名空间和 Web ACL 的应用程序集成 URL。

```
{
  "WebACL": {
    "LabelNamespace": "awsaf:111122223333:webacl:ATPModuleACL:",
    "Capacity": 50,
    "Description": "This is a test web ACL for ATP.",
    "Rules": [
      {
        "Priority": 1,
        "OverrideAction": {
```



```
    "None": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AccountTakeOverValidationRule"
  },
  "Name": "DetectCompromisedUserCredentials",
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesATPRuleSet"
      "ManagedRuleGroupConfigs": [
        {
          "UsernameField": {
            "Identifier": "/form/username"
          }
        },
        {
          "PasswordField": {
            "Identifier": "/form/password"
          }
        },
        {
          "PayloadType": "JSON"
        },
        {
          "LoginPath": "/web/login"
        }
      ]
    }
  }
},
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "ATPValidationAcl"
},
"DefaultAction": {
  "Allow": {}
},
"ManagedByFirewallManager": false,
"Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
"ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
"Name": "ATPModuleACL"
},
"ApplicationIntegrationURL": "https://9z87abce34ea.us-east-1.sdk.aws.waf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

ATP 示例：对丢失和泄露的凭据进行自定义处理

默认情况下，规则组执行的证书检查按如下方式AWSManagedRulesATPRuleSet处理 Web 请求：

- 缺少凭据-标记和屏蔽请求。
- 凭证泄露 — 为请求添加标签，但不要将其屏蔽或计算在内。

有关规则组和规则行为的详细信息，请参阅[Amazon WAF欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#)。

您可以通过执行以下操作，为证书缺失或泄露的 Web 请求添加自定义处理：

- 将**MissingCredential**规则改写为Count-此规则操作覆盖会使规则仅计算和标记匹配请求。
- 添加带有自定义处理的标签匹配规则-将此规则配置为与两个 ATP 标签匹配并执行自定义处理。例如，您可以将客户重定向到您的注册页面。

以下规则显示了前面示例中的 ATP 管理规则组，MissingCredential规则操作已改写为计数。这会导致规则将其标签应用于匹配的请求，然后仅对请求进行计数，而不是阻止请求。

```
"Rules": [
  {
    "Priority": 1,
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AccountTakeOverValidationRule"
    },
    "Name": "DetectCompromisedUserCredentials",
    "Statement": {
      "ManagedRuleGroupStatement": {
        "ManagedRuleGroupConfigs": [
          {
            "UsernameField": {
              "Identifier": "/form/username"
            }
          },
          {
            "PasswordField": {
              "Identifier": "/form/password"
            }
          },
          {
            "PayloadType": "JSON"
          },
          {
            "LoginPath": "/web/login"
          }
        ],
        "VendorName": "AWS",
        "Name": "AWSManagedRulesATPRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "MissingCredential"
          }
        ],
        "ExcludedRules": []
      }
    }
  },
  {
    "Name": "redirectToSignup",
    "Priority": 10,
```

使用此配置，当此规则组评估任何缺失或已泄露凭据的 Web 请求时，它将标记该请求，但不会将其阻止。

以下规则的数字优先级高于前面的规则组，因此在规则组评估之后对其进行评估。该规则配置为匹配任一凭据标签，并为匹配的请求发送自定义响应。

```
"Name": "redirectToSignup",
"Priority": 10,
```



```
"Statement": {
  "OrStatement": {
    "Statements": [
      {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "aws:waf:managed:aws:atp:signal:missing_credential"
        }
      },
      {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "aws:waf:managed:aws:atp:signal:credential_compromised"
        }
      }
    ]
  },
  "Action": {
    "Block": {
      "CustomResponse": {
        your custom response settings
      }
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "redirectToSignup"
  }
}
```

Amazon WAF 客户端应用程序集成

使用 Amazon WAF 应用程序集成 SDK 将客户端保护与 Amazon 服务器端 Web ACL 保护结合起来，进一步验证向您的受保护资源发送 Web 请求的客户端应用程序是否为预期应用程序。应用程序 SDK 通过静默质询验证客户端应用程序，并提供 Amazon 代币获取和管理，类似于 Amazon WAFChallenge 规则操作提供的功能。

集成 SDK 管理您的客户端应用程序会话的令牌授权，并帮助确保只有在客户端获得有效令牌后才允许尝试登录您的受保护资源。此外，SDK 还会收集有关客户端的信息，以帮助确定它是由机器人操作还是由人类操作。

应用程序集成 SDK 可与使用规则组 `AWSManagedRulesATPRuleSet` 或规则组目标保护级别的 Web ACL 一起使用 `AWSManagedRulesBotControlRuleSet`。软件开发工具包支持这些高级托管规则组的全部功能。

- Amazon WAF 欺诈控制账户接管预防 (ATP) 管理规则组 `AWSManagedRulesATPRuleSet`。

账户接管是一种在线非法活动，在这种活动中，攻击者获得对个人账户的未经授权的访问权限。ATP 托管规则组提供用于阻止、标记和管理可能是恶意账户接管企图一部分的请求的规则。

软件开发工具包支持微调的客户端验证和行为聚合，ATP 规则使用这些聚合将有效的客户端流量与恶意流量分开。

有关更多信息，请参阅 [Amazon WAF 欺诈控制账户收购预防 \(ATP\) 规则组 \(p. 56\)](#) 和 [Amazon WAF 欺诈控制账户收购预防 \(ATP\) \(p. 155\)](#)。

- Amazon WAF Bot Control 托管规则组 `AWSManagedRulesBotControlRuleSet`。

机器人从自我识别和有用的机器人（例如大多数搜索引擎和爬虫）到针对您的网站运行且不进行自我识别的恶意机器人。Bot Control 托管规则组提供监控、标记和管理网络流量中机器人活动的规则。

当您使用此规则组的目标保护级别时，目标规则使用软件开发工具包提供的客户端会话信息来更好地检测恶意机器人。

有关更多信息，请参阅 [Amazon WAF 机器人控制规则组 \(p. 49\)](#) 和 [Amazon WAF 机器人控制 \(p. 142\)](#)。

要将其中一个托管规则组添加到 Web ACL，请参阅过程 [将 Amazon WAF Bot Control 托管规则组添加到 Web ACL 中 \(p. 144\)](#) 和 [将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)。

Note

托管规则组目前不阻止缺少令牌请求。要阻止缺少令牌请求，在实现应用程序集成 SDK 后，请按照中的指导进行操作 [阻止没有有效令牌请求 \(p. 139\)](#)。

S JavaScript DK 已正式可用，您可以将其用于浏览器和其他可执行的设备 JavaScript。对于安卓和 iOS 移动应用程序，Amazon WAF 还提供适用于安卓版本 23 及更高版本以及 iOS 版本 13 及更高版本的自定义 SDK。

要访问移动 SDK，请通过联系方式 [联系](#) 销售人员 Amazon。

通过控制台访问应用程序集成 SDK

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中选择应用程序集成。
3. 在应用程序集成 SDK 页面中，您可以看到以下内容：
 - 为托管应用程序集成启用的 Web ACL。列出了使用规则组 AWSManagedRulesATPRuleSet 或规则组目标保护级别的每个 Web ACL。AWSManagedRulesBotControlRuleSet 在实现 SDK 时，您可以使用要集成的 Web ACL 的集成 URL。
 - 您有权访问的 SDK。S JavaScript DK 始终可用。要访问移动 SDK，请通过联系方式 [联系](#) 销售人员 Amazon。

要实现 SDK，请遵循有关 SDK 类型的指南。实现 SDK 后，要阻止缺少令牌请求，请按照中的指南进行操作 [阻止没有有效令牌请求 \(p. 139\)](#)。

主题

- [Amazon WAF JavaScript SDK \(p. 165\)](#)
- [Amazon WAF 移动软件开发工具包 \(p. 168\)](#)

Amazon WAF JavaScript SDK

您可以使用 Amazon WAF JavaScript SDK 在浏览器和其他执行的设备中实现 Amazon WAF 应用程序集成 JavaScript。S JavaScript DK 允许您管理令牌授权，并将令牌包含在您发送到受保护资源的请求中。通过使用 SDK，您可以确保客户端的远程过程调用包含有效的令牌。此外，在应用程序页面上进行集成后，您可以在 Web ACL 中实施缓解规则，例如阻止不包含有效令牌请求。

以下清单显示了 Web 应用程序页面中 JavaScript SDK 的典型实现的基本组件。

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
})
```

```
});  
</script>
```

安装 Amazon WAF JavaScript 开发工具包

首先在测试环境中实现 JavaScript SDK，然后在生产环境中实现。

开始使用 JavaScript SDK

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Application integration (应用程序集成)。这会将您带到应用程序集成 SDK 页面。
3. 在“应用程序集成 SDK”页面中，在启用应用程序集成的 Web ACL 窗格中，找到要集成的 Web ACL。复制并保存 Web ACL 集成 URL 以供在实现中使用。您也可以通过 API 调用获取此 URLGetWebACL。
4. 在应用程序页面代码的<head>部分中，插入以下<script>标签，并使用您的 Web ACL 的集成 URL 填充其中。这种包含会使您的客户端应用程序在页面加载时自动在后台检索令牌。

```
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></script>
```

此<script>列表使用defer属性进行配置，但async如果您希望页面具有不同的行为，则可以将设置更改为。

5. 完成集成编码，确保在发送客户端登录请求之前完成令牌检索。如果您已经在使用fetch API 进行调用，则可以替换Amazon WAF集成fetch封装器。如果您不使用fetch API，则可以改用Amazon WAF集成getToken操作。

有关编码指导，请参阅以下部分。

提供用于代币的域名

您可以为 SDKAmazon WAF 创建的令牌提供域配置。为此，请window.awsWafCookieDomainList使用一个或多个令牌域配置全局变量。

示例设置：

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

不允许使用公共后缀。例如，您不能使用usa.gov或co.uk作为令牌域。

根据受保护的主机域和为 Web ACL 配置的令牌域列表，您指定的域必须是可以接受的域。Amazon WAF 有关更多信息，请参阅[配置 Web ACL 令牌域列表 \(p. 138\)](#)：

Amazon WAF创建令牌时，它使用window.awsWafCookieDomainList配置和与 Web ACL 关联的资源的主机域组合中最合适、最短的域。

对于AWSManagedRulesATPRuleSet托管规则组，这通常是一个与您提供给规则组配置的登录路径中的域相匹配的单个域。

如何使用fetch封装器

您可以通过更改AwsWafIntegration命名空间下对fetch API 的常规fetch调用来使用fetch封装器。Amazon WAF封装器支持与标准 JavaScriptfetch API 调用相同的所有选项。这种方法通常是集成应用程序的最简单方法。

在何处查找器

以下示例清单显示了实现AwsWafIntegrationfetch包装器之前的标准代码。

```
const login_response = await fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
```

在包装器实现之后

以下清单显示了与AwsWafIntegrationfetch包装器实现相同的代码。

```
const login_response = await AwsWafIntegration.fetch(login_url, {
  method: 'POST',
  headers: {
    'Content-Type': 'application/json'
  },
  body: login_body
});
```

如何使用 getToken

Amazon WAF要求您的登录请求包含以当前令牌值命名aws-waf-token的 cookie。

该getToken操作是一次异步 SDK 调用，用于检索Amazon WAF令牌并将其存储在当前页面的 cookie 中aws-waf-token，名称和值设置为令牌值。您可以根据需要在页面中使用此令牌 cookie。

当你打电话时getToken，它会执行以下操作：

- 如果未过期的令牌已经可用，则调用会立即将其返回。
- 否则，调用会从代币提供者那里检索新代币，等待代币获取工作流程完成最多 2 秒钟后才会超时。如果操作超时，则会引发错误，您的调用代码必须处理该错误。

该getToken操作有一项附带hasToken操作，该操作指示aws-waf-token cookie 当前是否持有未过期的令牌。

基本getToken实现

以下示例清单显示了实现该getToken操作的标准代码。

```
const login_response = await AwsWafIntegration.getToken()
  .catch(e => {
    // Implement error handling logic for your use case
  })
// The getToken call returns the token, and doesn't typically require special handling
.then(token => {
  return loginToMyPage()
})

async function loginToMyPage() {
  // Your existing login code
}
```

仅在代币可用后才提交表单**getToken**

以下清单显示了如何注册事件侦听器来拦截表单提交，直到有有效的令牌可供使用。

```
<body>
  <h1>Login</h1>
  <p></p>
  <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-form-urlencoded">
    <label for="input_username">USERNAME</label>
    <input type="text" name="input_username" id="input_username"><br>
    <label for="input_password">PASSWORD</label>
    <input type="password" name="input_password" id="input_password"><br>
    <button type="submit">Submit</button>
  </form>

  <script>
    const form = document.querySelector("#login-form");

    // Register an event listener to intercept form submissions
    form.addEventListener("submit", (e) => {
      // Submit the form only after a token is available
      if (!AwsWafIntegration.hasToken()) {
        e.preventDefault();
        AwsWafIntegration.getToken().then(() => {
          e.target.submit();
        }, (reason) => { console.log("Error:"+reason) });
      }
    });
  </script>
</body>
```

Amazon WAF 移动软件开发工具包

您可以使用 Amazon WAF 移动 SDK 实现 Amazon WAF Android 和 iOS 移动应用程序的应用程序集成。使用移动 SDK，您可以管理令牌授权，并将令牌包含在发送到受保护资源的请求中。通过使用 SDK，您可以确保客户端的这些远程过程调用包含有效的令牌。此外，在应用程序页面上进行集成后，您可以在 Web ACL 中实施缓解规则，例如阻止不包含有效令牌的请求。

Note

Amazon WAF 移动软件开发工具包适用于安卓版本 23 及更高版本以及 iOS 版本 13 及更高版本。

要访问移动 SDK，请通过联系方式[联系](#)销售人员 Amazon。

使用 SDK 的基本方法是使用配置对象创建令牌提供者，然后使用令牌提供者从中检索令牌 Amazon WAF。默认情况下，令牌提供者将检索到的令牌包含在您对受保护资源的网络请求中。

以下是 SDK 实现的部分列表，其中显示了主要组件。有关更多详细示例，请参阅[为 Amazon WAF 移动 SDK 编写代码 \(p. 172\)](#)。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
  "Domain name")
let tokenProvider = WAFTokenProvider(configuration)
let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
```

```
String domainName = "Domain name";
WAFConfiguration configuration =
    WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(domainName)
        .wafTokenProvider(new WAFTokenProvider(applicationContext, configuration))
        .build();
WAFToken token = tokenProvider.getToken();
```

安装Amazon WAF移动 SDK

首先在测试环境中实现移动 SDK，然后在生产环境中实现。

安装Amazon WAF移动 SDK

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Application integration (应用程序集成)。这会将您带到应用程序集成 SDK 页面。
3. 在应用程序集成 SDK 页面中，执行以下操作：
 - a. 在启用了应用程序集成的 Web ACL 窗格中，找到要集成的 Web ACL。复制并保存 Web ACL 集成 URL 以供在实现中使用。您也可以通过 API 调用获取此 URL `GetWebACL`。
 - b. 选择移动设备类型和版本，然后选择下载。您可以选择自己喜欢的任何版本，但我们建议使用最新版本。Amazon WAF将设备上的zip文件下载到您的标准下载位置。
4. 在您的应用程序开发环境中，将文件解压缩到您选择的工作位置。在 zip 文件的顶级目录中，找到并打开README。按照README文件中的说明安装用于Amazon WAF移动应用程序代码的移动 SDK。
5. 根据以下各部分中的指导对应用程序进行编程。

移Amazon WAF动 SDK 规范

本部分列出了Amazon WAF移动 SDK 的 SDK 对象、操作和配置设置。有关令牌提供者和操作如何运作于各种配置设置组合的详细信息，请参阅[Amazon WAF移动 SDK 的工作原理 \(p. 171\)](#)。

WAFToken

持有Amazon WAF代币。

getValue()

检索. 的String表示形式WAFToken。

WAFTokenProvider

在您的移动应用程序中管理代币。使用WAFConfiguration对象实现这一点。

getToken()

如果启用了后台刷新，则会返回缓存的令牌。如果禁用了后台刷新，则会进行同步的阻塞调用Amazon WAF以检索新令牌。

onTokenReady(WAFTokenResultCallback)

指示令牌提供者刷新令牌并在活动令牌准备就绪时调用提供的回调。令牌缓存完毕并准备就绪后，代币提供者将在后台线程中调用您的回调。在你的应用程序首次加载以及它回到活动状态时调用这个函数。有关返回活动状态的更多信息，请参阅[the section called “在应用程序不活动后检索令牌” \(p. 172\)](#)。

对于 Android 或 iOS 应用程序，您可以设置WAFTokenResultCallback为在请求的令牌准备就绪时希望令牌提供者调用的操作。你的实现WAFTokenResultCallback必须采用参数WAFToken，SdkError。对于 iOS 应用程序，您可以交替创建内联函数。

WAFConfiguration

保存用于实现的配置WAFTokenProvider。实现此功能时，您需要提供 Web ACL 的集成 URL、令牌中使用的域名以及您希望令牌提供商使用的任何非默认设置。

以下列表指定了您可以在WAFConfiguration对象中管理的配置设置。

applicationIntegrationUrl

应用程序集成 URL。从Amazon WAF控制台或通过getWebACL API 调用获取此信息。

必需：是

类型：特定于应用程序的 URL。对于 iOS，请参阅 [iOS 网址](#)。对于安卓系统，请参阅 [java.net 网址](#)。

backgroundRefreshEnabled

表示您是否希望令牌提供者在后台刷新令牌。如果您设置了此设置，则令牌提供者会根据管理自动令牌刷新活动的配置设置在后台刷新您的令牌。

必需：否

类型：Boolean

默认值：TRUE

domainName

令牌中使用的域，用于代币获取和 cookie 存储。例如，example.com 或 aws.amazon.com。这通常是与 Web ACL 关联的资源的主机域，您将在其中发送 Web 请求。对于AWSManagedRulesATPRuleSet托管规则组，这通常是一个与您提供给规则组配置的登录路径中的域相匹配的单个域。

不允许使用公共后缀。例如，您不能使用usa.gov或co.uk作为令牌域。

根据受保护的主机域和 Web ACL 的令牌域列表，该域必须是可以接受的域。Amazon WAF有关更多信息，请参阅[配置 Web ACL 令牌域列表 \(p. 138\)](#)：

必需：是

类型：String

maxErrorTokenRefreshDelayMsec

尝试失败后重复令牌刷新之前等待的最长时间（以毫秒为单位）。此值在令牌检索失败并重试maxRetryCount次数后使用。

必需：否

类型：Integer

默认值：5000（5 秒）

允许的最小值：1（1 毫秒）

允许的最大值：30000（30 秒）

maxRetryCount

请求令牌时使用指数退避执行的最大重试次数。

必需：否

类型：Integer

默认值：如果启用了后台刷新，5。否则为 3。

允许的最小值：0

允许的最大值：10

setTokenCookie

表示您是否希望 SDK 的 Cookie 管理器在您的请求中添加令牌 cookie。默认情况下，这会向所有请求添加一个令牌 cookie。Cookie 管理器向路径位于中指定路径下的任何请求添加标记 cookieTokenCookiePath。

必需：否

类型：Boolean

默认值：TRUE

tokenCookiePath

在setTokenCookie为时使用TRUE。表示您希望 SDK 的 Cookie 管理器在其中添加标记 cookie 的顶级路径。管理器将令牌 cookie 添加到您发送到此路径和所有子路径的所有请求中。

例如，如果您将其设置为/web/login，则管理器会包含发送到的所有内容的令牌 cookie/web/login 及其任何子路径，例如/web/login/help。它不包括发送到其他路径的请求的令牌，例如/web、或/web/order。

必需：否

类型：String

默认值：/

tokenRefreshDelaySec

用于背景刷新。后台令牌刷新之间的最长时间（以秒为单位）。

必需：否

类型：Integer

默认值：300（5 分钟）

允许的最小值：300（5 分钟）

允许的最大值：600（10 分钟）

Amazon WAF移动 SDK 的工作原理

移动软件开发工具包为您提供了一个可配置的令牌提供商，您可以使用它来检索和使用令牌。令牌提供商会验证您允许的请求是否来自合法客户。当您向所保护的Amazon资源发送请求时Amazon WAF，您可以将令牌包含在 Cookie 中以验证请求。您可以手动处理令牌 cookie，也可以让令牌提供商为您处理。

本节介绍移动 SDK 中包含的类、属性和方法之间的交互。有关 SDK 规范，请参阅[移Amazon WAF动 SDK 规范 \(p. 169\)](#)。

代币检索和缓存

在移动应用程序中创建令牌提供者实例时，您可以配置其管理令牌和令牌检索的方式。您的主要选择是如何维护有效的、未过期的令牌以用于应用程序的网络请求：

- 启用后台刷新-这是默认设置。令牌提供者自动在后台刷新令牌并将其缓存。启用后台刷新后，当您调用 `getToken()`，该操作将检索缓存的令牌。

令牌提供者以可配置的时间间隔执行令牌刷新，因此在应用程序处于活动状态时，未过期的令牌始终在缓存中可用。当您的应用程序处于非活动状态时，后台刷新会暂停。有关这方面的信息，请参见[在应用程序不活动后检索令牌 \(p. 172\)](#)。

- 禁用后台刷新-您可以禁用后台令牌刷新，然后仅按需检索令牌。按需检索的令牌不会被缓存，如果需要，您可以检索多个令牌。每个代币都独立于您检索的任何其他代币，并且每个代币都有自己的时间戳，用于计算到期时间。

禁用后台刷新时，您可以选择以下令牌检索：

- **`getToken()`**— 当您在禁用 `getToken()` 用后台刷新的情况下进行呼叫时，该呼叫会同步从中检索新令牌 Amazon WAF。这是一个潜在的阻塞调用，如果你在主线程上调用，可能会影响应用程序的响应能力。
- **`onTokenReady(WAFTokenResultCallback)`**— 此调用异步检索新令牌，然后在令牌准备就绪时在后台线程中调用提供的结果回调。

代币提供者如何重试失败的代币检索

检索失败时，令牌提供者会自动重试令牌检索。重试最初使用指数退避执行，起始重试等待时间为 100 ms。有关指数重试的信息，请参阅[中的错误重试和指数回退Amazon](#)。

当重试次数达到配置的次数时 `maxRetryCount`，令牌提供者要么停止尝试，要么切换到每 `maxErrorTokenRefreshDelayMsec` 毫秒重试一次，具体取决于令牌检索的类型：

- **`onTokenReady()`**— 令牌提供者在两次尝试之间切换到等待 `maxErrorTokenRefreshDelayMsec` 毫秒的状态，并继续尝试检索令牌。
- 后台刷新 — 令牌提供者在两次尝试之间切换到等待 `maxErrorTokenRefreshDelayMsec` 毫秒的状态，并继续尝试检索令牌。
- 禁用后台刷新时按需 **`getToken()`** 调用 — 令牌提供者停止尝试检索令牌并返回先前的令牌值，如果没有先前的令牌，则返回空值。

在应用程序不活动后检索令牌

仅当您的应用程序因您的应用程序类型处于活动状态时才会执行后台刷新：

- iOS-当应用程序处于前台时执行后台刷新。
- Android — 无论是在前台还是在后台，应用程序未关闭时都会执行后台刷新。

如果您的应用程序处于任何不支持后台刷新的状态的时间超过您配置的 `tokenRefreshDelaySec` 秒数，则令牌提供者会暂停后台刷新。例如，对于 iOS 应用程序，如果 `tokenRefreshDelaySec` 为 300 且该应用程序关闭或进入后台超过 300 秒，则令牌提供者会停止刷新令牌。当应用程序返回到活动状态时，令牌提供者会自动重新启动后台刷新。

当您的应用程序恢复到活动状态时，请致电 `onTokenReady()` 以便在令牌提供者检索并缓存新令牌时通知您。不要随便调用 `getToken()`，因为缓存可能还不包含当前有效的令牌。

为 Amazon WAF 移动 SDK 编写代码

本节提供使用移动 SDK 的代码示例。

初始化代币提供者并获取代币

您可以使用配置对象启动您的令牌提供者实例。然后，您可以使用可用操作检索令牌。下面说明了所需代码的基本组件。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
"Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
if let token = token {
//token available
}

if let error = error {
//error occurred after exhausting all retries
}
}

//getToken()
let token = tokenProvider.getToken()
```

Android

```
String applicationIntegrationURL = "Web ACL integration URL";
Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(domainName)
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
    if (wafToken != null) {
        // token available
    } else {
        // error occurred in token refresh
    }
};

// Add this callback to application creation or activity creation where token will be
used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
object
// if background refresh is disabled you can directly call getToken()(blocking call)
for new token
WAFToken token = tokenProvider.getToken();
```

允许 SDK 在您的 HTTP 请求中提供令牌 cookie

如果setTokenCookie是TRUE，则令牌提供商会在您向中指定的路径下的所有位置发出的 Web 请求中包含代币 cookieTokenCookiePath。默认情况下，setTokenCookie是TRUE，tokenCookiePath是/。

例如，您可以通过指定令牌 cookie 路径来缩小包含令牌 cookie 的请求的范围/web/login。如果您这样做，请检查您的Amazon WAF规则是否检查您发送到其他路径的请求中是否有令牌。使

用AWSManagedRulesATPRuleSet规则组时，需要配置登录路径，规则组会检查发送到该路径的请求中的令牌。有关更多信息，请参阅[将 ATP 托管规则组添加到您的 Web ACL \(p. 157\)](#)：

iOS

当setTokenCookie为TRUE时，令牌提供者将Amazon WAF令牌存储在HTTPCookieStorage.shared并自动将 cookie 包含在对您在中指定的域的请求中WAFConfiguration。

```
let request = URLRequest(url: URL(string: domainEndpointUrl!))
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error in
}.resume()
```

Android

如果setTokenCookie是TRUE，则令牌提供者将Amazon WAF令牌存储在应用程序范围内共享的CookieHandler实例中。令牌提供者会自动将 cookie 包含在对您在中指定的域的请求中WAFConfiguration。

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

如果您已经初始化了CookieHandler默认实例，则令牌提供者将使用它来管理 Cookie。否则，令牌提供者将使用该令Amazon WAF牌初始化一个新CookieManager实例，CookiePolicy.ACCEPT_ORIGINAL_SERVER然后将此新实例设置为中的默认实例CookieHandler。

以下代码显示了 Cookie 管理器和 Cookie 处理器在您的应用程序中不可用时，SDK 如何对其进行初始化。

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
    // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
    cookieManager = new CookieManager();
    CookieHandler.setDefault(cookieManager);
}
```

在您的 HTTP 请求中手动提供令牌 cookie

如果您设置为FALSE，则需要在setTokenCookie向受保护终端节点发送的请求中手动提供令牌 cookie，作为 Cookie HTTP 请求标头。以下代码演示了如何执行该操作。

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
"Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

```
URL url = new URL("Domain name");
```

```
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

CAPTCHA以及中的Challenge操作Amazon WAF

您可以将Amazon WAF规则配置为对符合规则检查标准的 Web 请求运行CAPTCHA或Challenge操作。

- CAPTCHA要求最终用户解开 CAPTCHA 难题以证明有人在发送请求。
- Challenge运行静默挑战，要求客户端会话验证它是浏览器而不是机器人。验证在后台运行，不涉及最终用户。这是一个不错的选择，可以验证您怀疑无效的客户端，同时又不会通过验证码拼图对最终用户体验产生负面影响。

Challenge规则操作类似于应用程序集成 SDK 中的挑战，如中所述[Amazon WAF 客户机应用程序集成 \(p. 164\)](#)。

Note

当您在其中一个规则中使用CAPTCHA或Challenge规则操作或在规则组中用作规则操作替代时，会向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

用户或客户端成功响应后，运行 CAPTCHA 或质询的脚本会自动使用更新后的令牌重新提交原始 Web 请求。

有关规则操作设置的描述，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

主题

- [什么是验证码拼图？ \(p. 175\)](#)
- [CAPTCHA和Challenge操作的工作原理 \(p. 177\)](#)
- [使用CAPTCHA和Challenge操作的最佳实践 \(p. 179\)](#)

什么是验证码拼图？

Amazon WAF提供标准的验证码功能，要求用户确认自己是人类。CAPTCHA 代表完全自动化的公共图灵测试，用于区分计算机和人类。CAPTCHA 拼图旨在验证是否有人在发送请求，并防止诸如网页抓取、证书填充和垃圾邮件之类的活动。

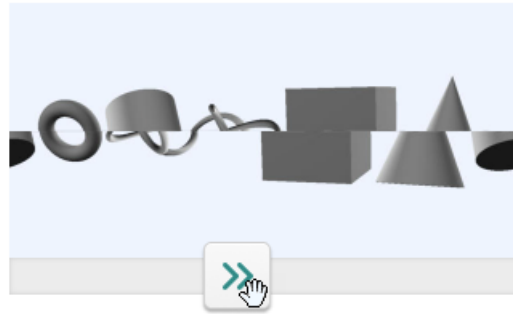
每个 CAPTCHA 谜题都包含一组标准控件，供最终用户申请新拼图、在音频和视觉谜题之间切换、访问其他说明以及提交拼图解决方案。所有谜题都支持屏幕阅读器、键盘控制和对比色。

CAPTCHA 拼图的书面说明以多种语言提供，包括阿拉伯语、德语、西班牙语、法语、意大利语、荷兰语、日语、葡萄牙语、土耳其语和中文（简体）。Amazon WAF CAPTCHA 使用客户端浏览器语言设置进行书面指令，并提供通过下拉菜单更改语言的选项。音频拼图的音频部分仅以英文提供。

典型的视觉拼图需要交互才能完成图像的特定部分，如以下屏幕截图所示。

Solve the puzzle

Slide the image to complete the donut



Solved: 0 Required: 3



English ▾

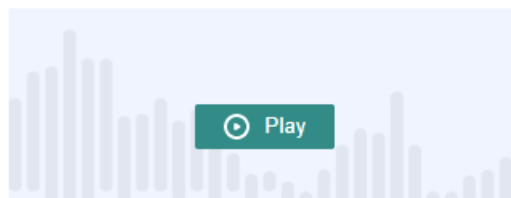
Submit

Amazon WAFCAPTCHA 拼图旨在直观地跨多个地理区域。默认谜题依赖于视觉元素和各种形式的计算机交互。Amazon WAFCAPTCHA 为视力障碍用户提供基于音频的替代谜题。这些拼图符合《网页内容可访问性指南》(WCAG) 的要求。有关信息，请参阅[万维网联盟 \(W3C\) 网站上的 Web 内容可访问性指南 \(WCAG\) 概述](#)。

音频拼图选项提供背景噪音，再加上有关用户应在文本框中键入的文本的英文说明。以下屏幕截图显示了音频拼图选项。

Solve the puzzle

Click play to listen to instructions



Keyboard audio toggle: alt + space

Enter your response

Answer

Solve by listening to the recording and typing your answer into the text box.



Submit

CAPTCHA 谜题旨在让人类相当容易快速地成功完成，计算机很难成功完成或以任何有意义的成功率随机完成。CAPTCHA 通常在封锁操作会阻止过多的合法请求时使用，但是让所有流量通过会导致不想要的请求（例如来自机器人的请求）的数量过高，令人无法接受。

CAPTCHA 无法清除所有不需要的请求。许多验证码谜题都是使用机器学习和人工智能解决的。为了避免 CAPTCHA，一些组织用人工干预来补充自动化技术。尽管如此，CAPTCHA 仍然是防止不太复杂的机器人流量和增加大规模操作所需资源的有用工具。

Amazon WAF随机生成其 CAPTCHA 谜题并在这些谜题中旋转，以确保向用户提供独特的挑战。Amazon WAF定期添加新的谜题类型和风格，以保持对抗自动化技术的效果。除了谜题外，Amazon WAF CAPTCHA 脚本还收集有关客户端的数据，以确保任务由人完成，并防止重播攻击。

CAPTCHA和Challenge操作的工作原理

Amazon WAF CAPTCHA 并且 Challenge 是标准的规则操作，因此它们相对容易实现。要使用其中任何一个，您需要为规则创建检查标准以确定要检查的请求，然后指定两个规则操作之一。有关规则操作选项的一般信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

主题

- [CAPTCHA和Challenge动作行为 \(p. 177\)](#)
- [CAPTCHA以及日志和指标中的Challenge操作 \(p. 178\)](#)

CAPTCHA和Challenge动作行为

当 Web 请求与带有 CAPTCHA 或 Challenge 操作的规则的检查标准相匹配时，将根据其令牌状态和豁免时间配置 Amazon WAF 确定如何处理该请求。Amazon WAF 还考虑请求是否可以处理 CAPTCHA 拼图或挑战脚本插页式广告。这些脚本旨在作为 HTML 内容进行处理，只有期待 HTML 内容的客户端才能正确处理它们。

Note

当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中用作规则操作替代时，会向您收取额外费用。有关更多信息，请参阅 [Amazon WAF 定价](#)。

该操作如何处理 Web 请求

Amazon WAF 将 CAPTCHA 或 Challenge 操作应用于 Web 请求，如下所示：

- 有效令牌 — Amazon WAF 处理此问题与 Count 操作类似。Amazon WAF 应用您为规则操作配置的所有标签和请求自定义设置，然后使用 Web ACL 中的其余规则继续评估请求。
- 令牌缺失、无效或已过期 — Amazon WAF 停止对请求的 Web ACL 评估，并阻止它到达预期目标。

Amazon WAF 根据规则操作类型，会生成一个响应，然后将其发送回客户端：

- Challenge— 在响应中 Amazon WAF 包括以下内容：
 - 值为 challenge 的标头 x-amzn-waf-action。
 - HTTP 状态代码 202 Request Accepted。
 - 如果请求包含值为 Accept 标头 text/html，则响应包含具有质询脚本的 JavaScript 页面插页式广告。
- CAPTCHA— 在响应中 Amazon WAF 包括以下内容：
 - 值为 captcha 的标头 x-amzn-waf-action。
 - HTTP 状态代码 405 Method Not Allowed。
 - 如果请求包含值为 Accept 标头 text/html，则响应包含带有 CAPTCHA 脚本的 JavaScript 页面插页式广告。

要在 Web ACL 或规则级别配置令牌到期时间，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)。

插页式广告的运用

当挑战插页式挑战运行时，在客户端成功响应之后，如果它还没有代币，插页式会为其初始化一个代币。然后它使用挑战解析时间戳更新代币。

当 CAPTCHA 插页式广告运行时，如果客户端还没有令牌，CAPTCHA 插页式会首先调用挑战脚本来挑战浏览器并初始化令牌。然后，插页式会运行其验证码谜题。当最终用户成功完成拼图时，插页式会使用验证码解析时间戳更新令牌。

无论哪种情况，在客户端成功响应且脚本更新令牌后，脚本都会使用更新的令牌重新提交原始 Web 请求。

您可以配置如何Amazon WAF处理令牌。有关信息，请参阅 [Amazon WAF网络请求令牌 \(p. 136\)](#)。

CAPTCHA以及日志和指标中的Challenge操作

CAPTCHA和Challenge操作可以是非终止的（例如Count），也可以是终止的（例如）Block。结果取决于请求是否具有具有操作类型的未过期时间戳的有效令牌。

- 有效令牌 — 当操作找到有效令牌但未阻止请求时，按如下方式Amazon WAF捕获指标和日志：
 - 增加和RequestsWithValidCaptchaToken或CaptchaRequestsChallengeRequests和的指标RequestsWithValidChallengeToken。
 - 将比赛记录为操作为CAPTCHA或的nonTerminatingMatchingRules条目Challenge。以下清单显示了与CAPTCHA操作进行此类匹配的日志部分。

```
"nonTerminatingMatchingRules": [  
  {  
    "ruleId": "captcha-rule",  
    "action": "CAPTCHA",  
    "ruleMatchDetails": [],  
    "captchaResponse": {  
      "responseCode": 0,  
      "solveTimestamp": 1632420429  
    }  
  }  
]
```

- 令牌@@ 缺失、无效或过期 — 当操作因令牌丢失或无效而阻止请求时，按如下方式Amazon WAF捕获指标和日志：
 - 增加CaptchaRequests或的指标ChallengeRequests。
 - 将匹配记录为带有 HTTP405 状态码的CaptchaResponse条目或带有 HTTP202 状态码的ChallengeResponse条目。日志显示请求是否缺少令牌或时间戳已过期。该日志还表明是Amazon WAF向客户端发送了 CAPTCHA 插页式页面，还是向客户端浏览器发送了静默质询。以下列表显示了与CAPTCHA操作进行此类匹配的日志部分。

```
"terminatingRuleId": "captcha-rule",  
"terminatingRuleType": "REGULAR",  
"action": "CAPTCHA",  
"terminatingRuleMatchDetails": [],  
...  
"responseCodeSent": 405,  
...  
"captchaResponse": {  
  "responseCode": 405,  
  "solveTimestamp": 0,  
  "failureReason": "TOKEN_MISSING"  
}
```

有关Amazon WAF日志的信息，请参见[记录 Web ACL 流量 \(p. 180\)](#)。

有关Amazon WAF指标的信息，请参阅[Amazon WAF 指标和维度 \(p. 502\)](#)。

有关规则操作选项的信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

使用CAPTCHA和Challenge操作的最佳实践

按照本节中的指导来计划和实施Amazon WAF CAPTCHA 或挑战。

规划您的验证码并挑战实施

根据你的网站使用情况、你想要保护的数据的敏感度以及请求的类型，确定在哪里放置验证码谜题或无声挑战。选择要应用验证码的请求，以便根据需要展示谜题，但请避免在无用且可能降低用户体验的地方提出这些请求。使用该Challenge操作运行静默挑战，这些挑战对最终用户的影响较小，但仍有助于验证请求是否来自 JavaScript 已启用的浏览器。

识别您不希望受验证码影响的请求，例如对 CSS 或图像的请求。仅在必要时使用验证码。例如，如果您计划在登录时进行验证码检查，并且用户总是直接从登录屏幕转到另一个屏幕，则可能不需要在第二个屏幕上进行验证码检查，并且可能会降低您的最终用户体验。

仅对GETtext/html请求使用Challenge和CAPTCHA操作。不要将它们用于POST其他请求类型，因为其他请求的浏览器行为可能会有所不同，可能无法正确处理插页式广告。

客户可能接受 HTML，但仍然无法处理验证码或挑战插页式广告。例如，带有小 iFrame 的网页上的小部件可能接受 HTML，但无法显示验证码或对其进行处理。避免为这些类型的请求设置规则操作，就像对不接受 HTML 的请求一样。

如何使用CAPTCHA和保护您的敏感的非 HTML 数据Challenge

您可以通过以下方法对敏感的非 HTML 数据（如 API）使用验证码和Challenge保护。

1. 识别接收 HTML 响应且在与敏感的非 HTML 数据请求附近运行的请求。
2. 编写CAPTCHA与 HTML 请求相匹配且与敏感数据请求匹配的Challenge规则。
3. 调整您的CAPTCHA和Challenge免疫时间设置，以便在正常的用户互动中，客户端从HTML请求中获得的令牌在请求您的敏感数据中可用且未过期。有关调整信息，请参见[时间戳到期：代币豁免时间 \(p. 137\)](#)。

当您的敏感数据请求与CAPTCHA或Challenge规则相匹配时，如果客户还有之前的谜题或挑战中的有效令牌，则该请求不会被阻止。如果令牌不可用或时间戳已过期，则访问您的敏感数据的请求将失败。有关规则操作的工作原理的更多信息，请参阅[CAPTCHA和Challenge动作行为 \(p. 177\)](#)。

使用验证码Challenge并调整您的现有规则

查看您的现有规则，看看是否要修改或添加这些规则。以下是需要考虑的一些常见情况。

- 如果您有基于速率的规则来屏蔽流量，但为了避免屏蔽合法用户，您将速率限制保持在相对较高的水平，请考虑在具有较低限制和/CAPTCHA 或Challenge操作的封锁规则之前添加第二条基于速率的规则。阻塞规则仍将阻止任何 IP 以过高的速率发送请求，而新规则将以更低的速率阻止大多数自动流量。有关基于速率的规则的信息，请参阅[基于速率的规则语句 \(p. 95\)](#)。
- 如果您有阻止请求的托管规则组，则可以将部分或全部规则的行为从切换Block到CAPTCHA或Challenge。为此，请在托管规则组配置中替代规则操作设置。有关替代规则操作的信息，请参阅[规则操作替代规则 \(p. 14\)](#)。

在部署之前测试您的验证码并对实现进行质疑

至于所有新功能，请按照中的指导进行操作[the section called “测试和调整您的保护措施” \(p. 200\)](#)。

在测试期间，查看您的令牌时间戳到期要求并设置 Web ACL 和规则级别免疫时间配置，以便在控制网站访问权限和为客户提供良好体验之间取得良好的平衡。有关信息，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)。

记录 Web ACL 流量

您可以启用日志记录以获取有关由您的 Web ACL 分析的流量的详细信息。记录的信息包括从您的 Amazon 资源 Amazon WAF 接收 Web 请求的时间、有关请求的详细信息以及有关请求匹配的规则的详细信息。您可以将日志发送到 Amazon Logs CloudWatch 日志组、Amazon Simple Storage Service (Amazon S3) 存储桶或 Amazon Kinesis Data Firehose。

主题

- [记录 Web ACL 流量信息的定价 \(p. 180\)](#)
- [Amazon WAF 记录目的地 \(p. 180\)](#)
- [管理 Web ACL 的日志记录 \(p. 187\)](#)
- [日志字段 \(p. 188\)](#)
- [日志示例 \(p. 192\)](#)

记录 Web ACL 流量信息的定价

根据与每种日志目标类型相关的成本，您需要为记录 Web ACL 流量信息付费。这些费用是使用费之外的费用 Amazon WAF。您的费用可能会有所不同，具体取决于您选择的目的地类型和记录的数据量等因素。

以下提供了指向每种日志目的地类型的定价信息的链接：

- CloudWatch 日志 — 费用用于出售的日志传输。参见 [亚马逊 CloudWatch 日志定价](#)。在“付费套餐”下，选择“日志”选项卡，然后在“Vended Logs”下，查看“交付到 CloudWatch 日志”的信息。
- Amazon S3 存储桶 — Amazon S3 的费用 CloudWatch 是指向 Amazon S3 存储桶传输日志和使用 Amazon S3 存储桶的总费用。
 - 有关 Amazon S3 的信息，请参阅 [Amazon S3 定价](#)。
 - 有关将 CloudWatch 日志出售到 Amazon S3 的信息，请参阅 [亚马逊 CloudWatch 日志定价](#)。在“付费套餐”下，选择“日志”选项卡，然后在“Vended Logs”下，查看有关交付到 S3 的信息
- Kinesis Data Firehose — 请参阅 [亚马逊 Kinesis Data Firehose](#)

有关 Amazon WAF 定价的信息，请参阅 [Amazon WAF 定价](#)。

Amazon WAF 记录目的地

本节介绍可以为日志选择 Amazon WAF 的日志记录目的地。每个部分都提供了有关配置目的地类型日志记录的指导，以及有关特定于目的地类型的任何行为的信息。配置日志记录目的地后，您可以向 Web ACL 日志记录配置提供其规范，以便开始对其进行登录。

主题

- [亚马逊 CloudWatch 日志 \(p. 180\)](#)
- [Amazon Simple Storage Service \(p. 182\)](#)
- [Amazon Kinesis Data Firehose \(p. 186\)](#)

亚马逊 CloudWatch 日志

本主题提供有关将 Web ACL 流量日志发送到 CloudWatch 日志日志组的信息。

Note

除了使用费用外，您还需要支付登录费用 Amazon WAF。有关信息，请参阅 [记录 Web ACL 流量信息的定价 \(p. 180\)](#)。

要向 Amazon CloudWatch Logs 发送日志，您需要创建 CloudWatch 日志日志组。启用登录时 Amazon WAF，您需要提供日志组 ARN。启用 Web ACL 的日志记录后，将日志以日志流形式 Amazon WAF CloudWatch 传送到 Logs 日志组。

使用 CloudWatch 日志时，可以在 Amazon WAF 控制台中浏览 Web ACL 的日志。在您的网页 ACL 页面中，选择“记录见解”选项卡。此选项是对通过 CloudWatch 控制台为日志提供的 CloudWatch 日志见解的补充。

在与 Amazon WAF Web ACL 相同的区域中配置 Web ACL 日志的日志组，并使用与管理 Web ACL 相同的帐户。有关配置 CloudWatch 日志组的信息，请参阅[使用日志组和日志流](#)。

日志组的配额

以下默认最大配额适用于 CloudWatch 日志组的空间和吞吐量限额。如果您对这些设置的登录要求过高，您将看到帐户 PutLogEvent 的限制指标。如果您看到限制迹象，则可以通过 Service Quotas 控制台的 Service Quotas 向两者 Amazon WAF 和 CloudWatch Logs 请求提高[限额](#)。

- 每个 Web ACL 的日志流数 — 35。您可以通过以下方式请求增加这笔的值 Amazon WAF。
- 每个日志流的吞吐量 — 每秒 5 MB。此设置是固定的。
- 一个账户的所有日志流的吞吐量 — 每秒 1,500 MB。您可以从 Logs 请求增加此 CloudWatch 值。

日志组命名

例如，您的日志组名称必须以您喜欢的任何后缀开头 aws-waf-logs- 和结尾 aws-waf-logs-testLogGroup2。

生成的 ARN 格式如下所示：

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

日志流的命名格式如下：

```
Region_web-acl-name_log-stream-number
```

日志流编号是一个正整数，小于或等于每个 Web ACL 的日志流数量 Amazon WAF 配额，如前所述。默认情况下，配额为 35。

以下显示了区域中 Web ACL TestWebACL 的示例日志流 us-east-1。

```
us-east-1_TestWebACL_19
```

将日志发布到 Logs 所需的权限 CloudWatch

为日志 CloudWatch 日志组配置 Web ACL 流量记录需要本节中描述的权限设置。这些权限是在您使用 Amazon WAF 完全访问管理策略之一时为您设置的，AWSWAFConsoleFullAccess 或者 AWSWAFFullAccess。如果您想更细致地管理对您的日志记录和 Amazon WAF 资源的访问权限，可以自己设置权限。有关管理权限的信息，请参阅 IAM 用户指南中的[Amazon 资源访问管理](#)。有关 Amazon WAF 托管策略的信息，请参阅[Amazon 适用于 Amazon WAF 的托管策略 \(p. 222\)](#)。

这些权限允许您更改 Web ACL 日志配置，为 CloudWatch 日志配置日志传输，以及检索有关您的日志组的信息。这些权限必须附加到您用来管理的用户 Amazon WAF。

```
{  
  "Version": "2012-10-17",  
}
```

```
"Statement":[
  {
    "Action":[
      "wafv2:PutLoggingConfiguration",
      "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource":[
      "*"
    ],
    "Effect":"Allow",
    "Sid":"LoggingConfigurationAPI"
  }
  {
    "Sid":"WebACLLoggingCWL",
    "Action":[
      "logs:CreateLogDelivery",
      "logs>DeleteLogDelivery",
      "logs:PutResourcePolicy",
      "logs:DescribeResourcePolicies",
      "logs:DescribeLogGroups"
    ],
    "Resource":[
      "*"
    ],
    "Effect":"Allow"
  }
]
```

当允许对所有Amazon资源执行操作时，策略中将指明"Resource"设置为"*"。这意味着允许对每个操作支持的所有Amazon资源执行操作。例如，该操作wafv2:PutLoggingConfiguration仅支持wafv2记录配置资源。

Amazon Simple Storage Service

本主题提供了有关将您的 Web ACL 流量日志发送到 Amazon S3 存储桶。

Note

除了使用费用外，您还需要支付登录费用Amazon WAF。有关信息，请参阅 [记录 Web ACL 流量信息的定价 \(p. 180\)](#)。

要将您的网络 ACL 流量日志发送到 Amazon S3，您需要为日志设置 Amazon S3 存储桶。启用登录时 Amazon WAF，您需要提供存储桶 ARN。有关创建日志记录桶的信息，请参阅 Amazon Simple Storage Service 用户指南中的[创建桶](#)。

Note

Amazon WAF支持使用 Amazon S3 存储桶对密钥类型 Amazon S3 密钥 (SSE-S3) 和Amazon Key Management Service (SSE-KMS) 进行加密Amazon KMS keys。 Amazon WAF不支持对由管理的 Amazon Key Management Service密钥进行加密Amazon。

您的 Web ACL 每隔 5 分钟将其日志文件发布到 Amazon S3 存储桶。每个日志文件包含在上一个 5 分钟期间内记录的流量的日志记录。

日志文件的最大文件大小为 75 MB。如果日志文件在 5 分钟期间内达到文件大小限制，则日志会停止向它添加记录，将其发布到 Amazon S3 存储桶，然后创建新的日志文件。

单个日志文件包含包含多条记录的交错条目。要查看 Web ACL 的所有日志文件，请查找按 Web ACL 名称、区域和您的账户 ID 汇总的条目。

命名要求和语法

用于 Amazon WAF 记录的存储段名称必须以您想要的任何后缀开头，aws-waf-logs- 并且可以以任何后缀结尾。例如，aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX。

存储段位置使用以下语法：

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

存储桶的 Amazon 资源名称 (ARN) 的格式如下：

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

在存储桶内，您的 Amazon WAF 日志写入一个文件夹结构，该结构由您的账户 ID、区域、Web ACL 名称以及日期和时间决定。

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

在文件夹内，日志文件名遵循类似的格式：

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

文件夹结构和日志文件名中使用的时间规范符合时间戳格式规范 YYYYMMddTHHmmZ。

下面显示了 Amazon S3 存储桶中的一个名为的存储桶的示例日志文件 DOC-EXAMPLE-BUCKET。Amazon Web Services 账户为 111111111111。网络 ACL 是 TEST-WEBACL，区域是 us-east-1。

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/1111111111/WAFLogs/us-east-1/  
TEST-WEBACL/2021/10/28/19/50/1111111111_waflogs_us-east-1_TEST-  
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

Note

用于 Amazon WAF 记录的存储段名称必须以您想要的任何后缀开头，aws-waf-logs- 并且可以以任何后缀结尾。

将日志发布到 Amazon S3 的权限

为 Amazon S3 存储桶进行以下权限设置。这些权限是在您使用 Amazon WAF 完全访问管理策略之一时为您设置的，AWSWAFConsoleFullAccess 或者 AWSWAFFullAccess。如果您想更细致地管理对您的日志记录和 Amazon WAF 资源的访问权限，可以自己设置这些权限。有关管理权限的信息，请参阅 IAM 用户指南中的 [Amazon 资源访问管理](#)。有关 Amazon WAF 托管策略的信息，请参阅 [Amazon 适用于 Amazon WAF 的托管策略 \(p. 222\)](#)。

以下权限允许您更改 Web ACL 日志配置和配置向 Amazon S3 存储桶传输日志。这些权限必须附加到您用来管理的用户 Amazon WAF。

Note

设置下面列出的权限时，您可能在 Amazon CloudTrail 日志中看到错误，表明访问被拒绝，但 Amazon WAF 登录的权限是正确的。

```
{
```



```
"Version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "wafv2:PutLoggingConfiguration",
      "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource": [
      "*"
    ],
    "Effect": "Allow",
    "Sid": "LoggingConfigurationAPI"
  },
  {
    "Sid": "WebACLLogDelivery",
    "Action": [
      "logs:CreateLogDelivery",
      "logs>DeleteLogDelivery"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Sid": "WebACLLoggingS3",
    "Action": [
      "s3:PutBucketPolicy",
      "s3:GetBucketPolicy"
    ],
    "Resource": [
      "arn:aws:s3::aws-waf-logs-example-bucket"
    ],
    "Effect": "Allow"
  }
]
```

当允许对所有Amazon资源执行操作时，策略中将指明"Resource"设置为"*"。这意味着允许对每个操作支持的所有Amazon资源执行操作。例如，该操作wafv2:PutLoggingConfiguration仅支持wafv2记录配置资源。

默认情况下，Amazon S3 Storage Service。只有存储桶所有者才能访问存储桶和其中存储的对象。但是，存储桶所有者可以通过编写访问策略来向其他资源和用户授予访问权限。

如果创建日志的用户拥有存储桶，则服务自动将以下策略附加到存储桶，以授予向它发布日志的日志权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::aws-waf-logs-example-bucket/AWSLogs/account-id/*",
    }
  ]
}
```



```
"Condition": {
  "StringEquals": {
    "s3:x-amz-acl": "bucket-owner-full-control",
    "aws:SourceAccount": ["account-id"]
  },
  "ArnLike": {
    "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
  }
},
{
  "Sid": "AWSLogDeliveryAclCheck",
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": "s3:GetBucketAcl",
  "Resource": "arn:aws:s3::aws-waf-logs-example-bucket",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": ["account-id"]
    },
    "ArnLike": {
      "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
    }
  }
}
]
```

Note

用于Amazon WAF记录的存储段名称必须以您想要的任何后缀开头，aws-waf-logs-并且可以以任何后缀结尾。

如果创建日志的用户不拥有存储桶，也没有存储桶的GetBucketPolicy和PutBucketPolicy权限，日志创建操作会失败。在这种情况下，存储桶所有者必须手动将上述策略添加到存储桶，并指定日志创建者的Amazon Web Services 账户 ID。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的[如何添加 S3 存储桶策略？](#) 如果存储桶从多个账户接收日志，则将Resource元素条目添加到每个账户的AWSLogDeliveryWrite策略声明。

例如，以下存储桶策略允许Amazon Web Services 账户111122223333将日志发布到名为的存储桶aws-waf-logs-doc-example：

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite20150319",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::aws-waf-logs-example-bucket/AWSLogs/111122223333/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["111122223333"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
        }
      }
    }
  ]
}
```

```
    }  
  },  
  {  
    "Sid": "AWSLogDeliveryAclCheck",  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "delivery.logs.amazonaws.com"  
    },  
    "Action": "s3:GetBucketAcl",  
    "Resource": "arn:aws:s3:::aws-waf-logs-example-bucket",  
    "Condition": {  
      "StringEquals": {  
        "aws:SourceAccount": ["111122223333"]  
      },  
      "ArnLike": {  
        "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]  
      }  
    }  
  }  
]  
}
```

Amazon S3 日志文件访问权限

除了必需的存储桶策略之外，Amazon S3 使用访问控制列表 (ACL) 管理对日志创建的日 Amazon WAF 日志文件的访问。默认情况下，存储桶所有者对每个日志文件具有 FULL_CONTROL 权限。如果日志传输拥有者与存储桶拥有者不同，则没有权限。日志传输账户具有 READ 和 WRITE 权限。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的[访问控制列表 \(ACL\) 概述](#)。

日志文件是压缩文件。如果您使用 Amazon S3 控制台打开这些文件，Amazon S3 会解压缩并显示这些记录。如果您下载日志文件，则必须对其进行解压才能查看记录。

Amazon Kinesis Data Firehose

本部分提供了有关将您的 Web ACL 流量日志发送到 Amazon Kinesis Data Firehose。

Note

除了使用费用外，您还需要支付登录费用 Amazon WAF。有关信息，请参阅[记录 Web ACL 流量信息的定价 \(p. 180\)](#)。

要将日志发送到 Amazon Kinesis Data Firehose，您需要将日志从网络 ACL 发送到已配置存储目标的 Amazon Kinesis Data Firehose。启用日志记录后，通过 Kinesis Data Firehose 的 HTTPS 端点将日志 Amazon WAF 传送到您的存储目的地。

有关如何创建 Amazon Kinesis Data Firehose 和查看存储日志的信息，请参阅[什么是 Amazon Kinesis Data Firehose？](#) 要了解您的 Kinesis Data Firehose 配置所需的权限，请参阅[使用 Amazon Kinesis Data Firehose 控制访问](#)。

您必须具有以下权限才能成功启用使用 Amazon Kinesis Data Firehose 的日志记录

- iam:CreateServiceLinkedRole
- firehose:ListDeliveryStreams
- wafv2:PutLoggingConfiguration

有关服务相关角色和 iam:CreateServiceLinkedRole 权限的信息，请参阅[将服务相关角色用于 Amazon WAF \(p. 226\)](#)。

有关创建传输流的更多信息，请参阅[创建 Amazon Kinesis Data Firehose 传输流](#)。

按如下方式为 Web ACL 配置 Amazon Kinesis Data Firehose 传输流。

- 使用与管理 Web ACL 相同的帐户创建它。
- 在与 Web ACL 相同的区域中创建它。如果您要为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）区域创建消防管 us-east-1。
- 为数据 firehose 指定一个以前缀开头的名称 aws-waf-logs-。例如，aws-waf-logs-us-east-2-analytics。
- 将其配置为直接输入，允许应用程序直接访问传输流。在 Amazon Kinesis Data Firehose 控制台中，对于传输流源设置，选择 Direct PUT 或其他来源。通过 API，将交付流属性设置 DeliveryStreamType 为 DirectPut。

Note

请勿使用 aKinesis stream 作为来源。

一条 Amazon WAF 日志等同于一条 Kinesis Data Firehose 记录。如果您通常每秒收到 10,000 个请求并且启用了完整日志，则在 Kinesis Data Firehose 中应设置每秒 10,000 条记录。如果您未正确配置 Kinesis Data Firehose，则 Amazon WAF 不会记录所有日志。有关更多信息，请参阅[Amazon Kinesis Data Firehose 配额](#)。

管理 Web ACL 的日志记录

您可以随时启用和禁用 Web ACL 的日志记录。

Note

除了使用费用外，您还需要支付登录费用 Amazon WAF。有关信息，请参阅[记录 Web ACL 流量信息的定价 \(p. 180\)](#)。

在 Web ACL 的日志配置中，您可以自定义 Amazon WAF 发送到日志的内容。

- 字段编辑-您可以删除日志记录中的某些字段。已编辑的字段显示 REDACTED 在日志中。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为 REDACTED。有关日志字段的列表，请参阅[日志字段 \(p. 188\)](#)。
- 日志筛选 — 您可以添加筛选，以指定哪些 Web 请求保留在日志中，哪些将丢弃的请求。您可以筛选在 Web 请求评估期间 Amazon WAF 适用的设置。您可以筛选以下设置：
 - 完全限定的标签 — 完全限定的标签具有前缀、可选命名空间和标签名称。前缀用于标识添加标签的规则规则组或 Web ACL 上下文。有关标签的信息，请参见[网络请求上的标签 \(p. 123\)](#)。
 - 规则操作-您可以根据任何常规规则操作设置进行筛选，也可以根据规则组规则的旧版 EXCLUDED_AS_COUNT 覆盖选项进行筛选。有关规则操作设置的信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。有关规则组规则的当前和旧版规则操作替代的信息，请参阅[规则组中的操作替代 \(p. 14\)](#)。
 - 普通规则操作筛选器适用于在规则中配置的操作，也适用于使用当前选项配置的用于覆盖规则组规则操作的操作。
 - EXCLUDED_AS_COUNT 日志过滤器与 Count 操作日志过滤器重叠。EXCLUDED_AS_COUNT 筛选当前和旧版选项，以便将规则组规则操作改写为 Count。

为 Web ACL 启用日志记录

此过程需要配置日志记录目标。有关您的目的地选择以及每个目的地的要求的信息，请参阅[Amazon WAF 记录目的地 \(p. 180\)](#)。

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。

2. 在导航窗格中，选择 Web ACL。
3. 选择要启用日志记录的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在 Logging (日志记录) 选项卡上，选择 Enable logging (启用日志记录)。
5. 选择日志目的地类型，然后选择您配置的日志记录目标。必须选择名称以开头的日志目的地aws-waf-logs-。
6. (可选) 如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 Add (添加)。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为REDACTED。
7. (可选) 如果您不想将所有请求发送到日志，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个过滤器，选择添加过滤器，然后选择您的筛选条件并指定要保留还是删除符合条件的请求。添加完过滤器后，如果需要，修改默认日志记录行为。
8. 选择启用日志记录。

Note

成功启用日志记录后，Amazon WAF将创建一个服务关联角色，该角色具有将日志写入日志记录目标所需的权限。有关更多信息，请参阅[将服务相关角色用于 Amazon WAF \(p. 226\)](#)：

禁用 Web ACL 的日志记录

1. 在导航窗格中，选择 Web ACL。
2. 选择要禁用其日志记录的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
3. 在 Logging (日志记录) 选项卡上，选择 Disable logging (禁用日志记录)。
4. 在对话框中，选择 Disable logging (禁用日志记录)。

日志字段

以下列表描述了可能的日志字段。

action

应用于请求的操作。Allow并Block正在终止规则操作。Count是非终止规则操作。CAPTCHA如果请求包含有效令牌，Challenge则为非终止；如果不包含有效令牌，则为终止。

args

查询字符串。

captchaResponse

对请求的验证码响应，在CAPTCHA操作导致 Web 请求检查终止时填充。当请求不包含令牌或令牌无效或过期时，该CAPTCHA操作将终止 Web 请求检查。此字段包含响应代码和失败原因。

质询响应

对请求的质询响应，在Challenge操作导致 Web 请求检查终止时填充。当请求不包含令牌或令牌无效或过期时，该Challenge操作将终止 Web 请求检查。此字段包含响应代码和失败原因。

clientIp

发送请求的客户端的 IP。

country

请求的源国家/地区。Amazon WAF如果无法确定原产国，则会将此字段设置为-。

excludedRules

仅用于规则组规则。规则组中您排除的规则列表。这些规则的操作设置为Count。

如果您使用覆盖规则操作选项将规则改写为计数，则此处不列出匹配项。它们被列为动作对action，overriddenAction。

exclusionType

一种表示排除的规则具有操作的类型Count。

ruleId

规则组中排除的规则的 ID。

formatVersion

日志的格式版本。

headers

标头的列表。

httpMethod

请求中的 HTTP 方法。

httpRequest

关于请求的元数据。

httpSourceId

关联资源的 ID：

- 对于亚马逊 CloudFront 发行版，ID 是*distribution-id* ARN 语法中的：

arn:partition:cloudfront::account-id:distribution/distribution-id

- 对于 Application Load Balancer，*load-balancer-id* ID 是 ARN 语法中的：

arn:partition:elasticloadbalancing:region:account-id:loadbalancer/app/load-balancer-name/load-balancer-id

- 对于 Amazon API Gateway REST API，*api-id* ID 是 ARN 语法中的：

arn:partition:apigateway:region:::/restapis/api-id/stages/stage-name

- 对于 Amazon AppSync GraphQL API 来说，ID 是*GraphQLApiId* ARN 语法中的：

arn:partition:appsync:region:account-id:apis/GraphQLApiId

- 对于 Amazon Cognito 用户池，ID 是*user-pool-id* ARN 语法中的：

arn:partition:cognito-idp:region:account-id:userpool/user-pool-id

- 对于 Amazon App Runner 服务，ID 是 ARN 语法中的：*apprunner-service-id*

arn:partition:apprunner:region:account-id:service/apprunner-service-name/apprunner-service-id

httpSourceName

请求的源。可能CF的值：亚马逊 CloudFront、APIGW亚马逊 Amazon API Gateway、ALB Application Load BalancerAmazon AppSync、COGNITOIDP Amazon Cognito 和APPRUNNER App Runner。APPSYNC

httpVersion

HTTP 版本。

labels

Web 请求上的标签。这些标签是由用于评估请求的规则应用的。Amazon WAF 记录前 100 个标签。

limitKey

表示 Amazon WAF 应使用哪个 IP 地址源来聚合基于速率的规则进行速率限制的请求。对于 Web 请求来源 IP，可能的值为 FORWARDED_IP，对于在请求标头中转发的 IP，可能的值为。

极限值

基于速率的规则用于聚合速率限制请求的 IP 地址。如果请求包含无效的 IP 地址，则 limitvalue 为 INVALID。

maxRateAllowed

在五分钟内允许的最大请求数，具有与所 limitKey 指定的字段相同的值。如果请求数超过了 maxRateAllowed 并且还满足规则中指定的其他谓词，则 Amazon WAF 将触发为此规则指定的操作。

nonTerminatingMatching规则

与请求匹配的非终止规则列表。

action

Amazon WAF 应用于请求的操作。这表示计数、验证码或挑战。当 Web 请求包含有效令牌时，CAPTCHA 和 Challenge 是非终止的。

OverriddenAct

仅用于在 Web ACL 中替换了规则操作的规则组规则。这是为规则组规则配置的操作，而不是应用于请求的操作。Amazon WAF 应用的操作就是 action 值。

ruleId

匹配请求且未终止的规则的 ID。

ruleMatchDetails

有关匹配请求的规则的信息。此字段仅针对 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。匹配规则可能需要匹配多个检查标准，因此这些匹配详细信息以匹配条件数组的形式提供。

超大字段

Web 请求中由 Web ACL 检查且超过 Amazon WAF 检查限制的字段列表。如果字段过大，但 Web ACL 未对其进行检查，则此处不会列出该字段。

此列表可以包含以下零个或多个值：REQUEST_BODY、REQUEST_JSON_BODY、REQUEST_HEADERS、和 REQUEST_COOKIES。有关超大字段的更多信息，请参阅[检查请求正文、标题和 Cookie \(p. 113\)](#)。

rateBasedRuleID

作用于请求的基于速率的规则 ID。如果这已终止请求，则 rateBasedRuleId 的 ID 与 terminatingRuleId 的 ID 相同。

rateBasedRule清单

对请求执行操作的基于速率的规则列表。

rateBasedRule姓名

根据请求执行的基于费率的规则的名称。

requestHeadersInserted

为处理自定义请求而插入的标头列表。

requestId

请求的 ID，由底层主机服务生成。对于 Application Load Balancer，这是跟踪 ID。对于所有其他人，这是请求 ID。

responseCodeSent

使用自定义响应发送的响应代码。

ruleGroupId

规则组的 ID。如果规则阻止了请求，则 ruleGroupId 的 ID 与 terminatingRuleId 的 ID 相同。

ruleGroupList

根据此请求执行操作的规则组列表，包含匹配信息。

terminatingRule

终止请求的规则。如果这是非空值，则它包含以下附加字段。

action

Amazon WAF 应用于请求的操作。这表示允许、阻止、验证码或质疑。当 Web 请求不包含有效令牌时，CAPTCHA 和 Challenge 操作将终止。

OverrideAct

仅用于在 Web ACL 中替换了规则操作的规则组规则。这是为规则组规则配置的操作，而不是应用于请求的操作。Amazon WAF 应用的操作就是 action 值。

ruleId

匹配请求的规则的 ID。

ruleMatchDetails

有关匹配请求的规则的信息。此字段仅针对 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。匹配规则可能需要匹配多个检查标准，因此这些匹配详细信息以匹配条件数组的形式提供。

terminatingRuleId

终止请求的规则的 ID。如果没有任何情况会终止请求，则值为 Default_Action。

terminatingRuleMatch 细节

有关与请求匹配的终止规则的详细信息。终止规则具有针对 Web 请求结束检查过程的操作。终止规则的可能操作包括 AllowBlock、CAPTCHA、和 Challenge。在检查 Web 请求期间，对于与请求匹配且具有终止操作的第一条规则，Amazon WAF 停止检查并应用操作。除了在日志中报告的匹配终止规则的威胁外，Web 请求可能包含其他威胁。

这仅适用于 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。匹配规则可能需要匹配多个检查标准，因此这些匹配详细信息以匹配条件数组的形式提供。

terminatingRuleType

终止请求的规则的类型。可能的值：RATE_BASED、REGULAR、GROUP 和 MANAGED_RULE_GROUP。

timestamp

时间戳，以毫秒为单位。

uri

请求的 URI。

webaclId

Web ACL 的 GUID。

日志示例

Example 在 SQLi 检测（终止）时触发的规则的日志输出

```
{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
  "terminatingRuleId": "STMTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "HIGH",
      "location": "HEADER",
      "matchedData": [
        "10",
        "AND",
        "1"
      ]
    }
  ],
  "httpSourceName": "-",
  "httpSourceId": "-",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "httpRequest": {
    "clientIp": "1.1.1.1",
    "country": "AU",
    "headers": [
      {
        "name": "Host",
        "value": "localhost:1989"
      },
      {
        "name": "User-Agent",
        "value": "curl/7.61.1"
      },
      {
        "name": "Accept",
        "value": "*/ *"
      },
      {
        "name": "x-stm-test",
        "value": "10 AND 1=1"
      }
    ],
    "uri": "/myUri",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "rid"
  },
  "labels": [
    {
      "name": "value"
```

```
    }  
  ]  
}
```

Example 在 SQLi 检测时触发的规则的日志输出（非终止）

```
{  
  "timestamp":1592357192516  
  ,"formatVersion":1  
  ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-  
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"  
  ,"terminatingRuleId":"Default_Action"  
  ,"terminatingRuleType":"REGULAR"  
  ,"action":"ALLOW"  
  ,"terminatingRuleMatchDetails":[]  
  ,"httpSourceName":"-"  
  ,"httpSourceId":"-"  
  ,"ruleGroupList":[]  
  ,"rateBasedRuleList":[]  
  ,"nonTerminatingMatchingRules":  
  [{  
    "ruleId":"TestRule"  
    ,"action":"COUNT"  
    ,"ruleMatchDetails":  
    [{  
      "conditionType":"SQL_INJECTION"  
      ,"sensitivityLevel": "HIGH"  
      ,"location":"HEADER"  
      ,"matchedData":[  
        "10"  
        ,"and"  
        ,"1"]  
      ]  
    }]  
  },  
  {"httpRequest":{  
    "clientIp":"3.3.3.3"  
    ,"country":"US"  
    ,"headers":[  
      {"name":"Host","value":"localhost:1989"}  
      ,{"name":"User-Agent","value":"curl/7.61.1"}  
      ,{"name":"Accept","value":"*//*"}  
      ,{"name":"myHeader","myValue":"10 AND 1=1"}  
    ]  
    ,"uri":"/myUri","args":""  
    ,"httpVersion":"HTTP/1.1"  
    ,"httpMethod":"GET"  
    ,"requestId":"rid"  
  },  
  "labels": [  
    {  
      "name": "value"  
    }  
  ]  
}
```

Example 在规则组内触发的多个规则的日志输出（Rulea-xss 终止，Rule-B 未终止）

```
{  
  "timestamp":1592361810888,  
  "formatVersion":1,  
  "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-  
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"  
  ,"terminatingRuleId":"RG-Reference"
```

```
, "terminatingRuleType": "GROUP"
, "action": "BLOCK",
"terminatingRuleMatchDetails":
[
  {
    "conditionType": "XSS"
    , "location": "HEADER"
    , "matchedData": ["<", "frameset"]
  }
]
, "httpSourceName": "-"
, "httpSourceId": "-"
, "ruleGroupList":
[
  {
    "ruleGroupId": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-world/c051b698-1f11-4m41-aef4-99a506d53f4b"
    , "terminatingRule": {
      "ruleId": "RuleA-XSS"
      , "action": "BLOCK"
      , "ruleMatchDetails": null
    }
    , "nonTerminatingMatchingRules":
    [
      {
        "ruleId": "RuleB-SQLi"
        , "action": "COUNT"
        , "ruleMatchDetails":
        [
          {
            "conditionType": "SQL_INJECTION"
            , "sensitivityLevel": "LOW"
            , "location": "HEADER"
            , "matchedData": [
              "10"
              , "and"
              , "1"
            ]
          }
        ]
      }
    ]
    , "excludedRules": null
  }
]
, "rateBasedRuleList": []
, "nonTerminatingMatchingRules": []
, "httpRequest": {
  "clientIp": "3.3.3.3"
  , "country": "US"
  , "headers":
  [
    { "name": "Host", "value": "localhost:1989" }
    , { "name": "User-Agent", "value": "curl/7.61.1" }
    , { "name": "Accept", "value": "*/*" }
    , { "name": "myHeader1", "value": "<frameset onload=alert(1)>" }
    , { "name": "myHeader2", "value": "10 AND 1=1" }
  ]
  , "uri": "/myUri"
  , "args": ""
  , "httpVersion": "HTTP/1.1"
  , "httpMethod": "GET"
  , "requestId": "rid"
}
, "labels": [
  {
    "name": "value"
  }
]
}
```

Example 为检查内容类型为 JSON 的请求正文而触发的规则的日志输出

Amazon WAF目前将 JSON 人体检查的位置报告为UNKNOWN。

```
{
  "timestamp": 1576280412771,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
  "terminatingRuleId": "STMTTest_SQLi_XSS",
  "terminatingRuleType": "REGULAR",
  "action": "BLOCK",
  "terminatingRuleMatchDetails": [
    {
      "conditionType": "SQL_INJECTION",
      "sensitivityLevel": "LOW",
      "location": "UNKNOWN",
      "matchedData": [
        "10",
        "AND",
        "1"
      ]
    }
  ],
  "httpSourceName": "ALB",
  "httpSourceId": "alb",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "1.1.1.1",
    "country": "AU",
    "headers": [],
    "uri": "",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "POST",
    "requestId": "null"
  },
  "labels": [
    {
      "name": "value"
    }
  ]
}
```

Example 针对带有有效的、未过期的验证码令牌的网络请求的 CAPTCHA 规则的日志输出

以下日志列表适用于将规则与CAPTCHA操作相匹配的 Web 请求。网络请求具有有效且未过期的 CAPTCHA 令牌，并且仅被标记为 CAPTCHA 匹配Amazon WAF，与Count操作的行为类似。此验证码匹配如下所示nonTerminatingMatchingRules。

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
```

```
{
  "ruleId": "captcha-rule",
  "action": "CAPTCHA",
  "ruleMatchDetails": [],
  "captchaResponse": {
    "responseCode": 0,
    "solveTimestamp": 1632420429
  }
}
],
"requestHeadersInserted": [
  {
    "name": "x-amzn-waf-test-header-name",
    "value": "test-header-value"
  }
],
"responseCodeSent": null,
"httpRequest": {
  "clientIp": "72.21.198.65",
  "country": "US",
  "headers": [
    {
      "name": "X-Forwarded-For",
      "value": "72.21.198.65"
    },
    {
      "name": "X-Forwarded-Proto",
      "value": "https"
    },
    {
      "name": "X-Forwarded-Port",
      "value": "443"
    },
    {
      "name": "Host",
      "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
    },
    {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
    },
    {
      "name": "cache-control",
      "value": "max-age=0"
    },
    {
      "name": "sec-ch-ua",
      "value": "\"Chromium\";v=\"94\"\", \"Google Chrome\";v=\"94\"\", \";Not A Brand\";v=
\\\"99\\\"\"
    },
    {
      "name": "sec-ch-ua-mobile",
      "value": "?0"
    },
    {
      "name": "sec-ch-ua-platform",
      "value": "\"Windows\""
    },
    {
      "name": "upgrade-insecure-requests",
      "value": "1"
    },
    {
      "name": "user-agent",
      "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.4606.54 Safari/537.36"
    }
  ]
}
```

```
    },
    {
      "name": "accept",
      "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
    },
    {
      "name": "sec-fetch-site",
      "value": "same-origin"
    },
    {
      "name": "sec-fetch-mode",
      "value": "navigate"
    },
    {
      "name": "sec-fetch-user",
      "value": "?1"
    },
    {
      "name": "sec-fetch-dest",
      "value": "document"
    },
    {
      "name": "referrer",
      "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-test/pets"
    },
    {
      "name": "accept-encoding",
      "value": "gzip, deflate, br"
    },
    {
      "name": "accept-language",
      "value": "en-US,en;q=0.9"
    },
    {
      "name": "cookie",
      "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/bS6YG0CJKAJqaRqDZ140ythKW0Zj9wKB208lSkYDRqf1y0NcVBFo5u0eYi0tvT4rtQCXsu+KanAardW8go4QSLw4yoED59lgV7oAhGyCa1AzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
    }
  ],
  "uri": "/pen-test/pets",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "GINMHHUgoAMFxug="
}
}
```

Example 针对没有 CAPTCHA 令牌的网络请求的 CAPTCHA 规则的日志输出

以下日志列表适用于将规则与CAPTCHA操作相匹配的 Web 请求。网络请求没有 CAPTCHA 令牌，已被阻止Amazon WAF。

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
}
```

```
"terminatingRuleMatchDetails": [],
"httpSourceName": "APIGW",
"httpSourceId": "123456789012:b34myvfw0b:pen-test",
"ruleGroupList": [],
"rateBasedRuleList": [],
"nonTerminatingMatchingRules": [],
"requestHeadersInserted": null,
"responseCodeSent": 405,
"httpRequest": {
  "clientIp": "72.21.198.65",
  "country": "US",
  "headers": [
    {
      "name": "X-Forwarded-For",
      "value": "72.21.198.65"
    },
    {
      "name": "X-Forwarded-Proto",
      "value": "https"
    },
    {
      "name": "X-Forwarded-Port",
      "value": "443"
    },
    {
      "name": "Host",
      "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
    },
    {
      "name": "X-Amzn-Trace-Id",
      "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
    },
    {
      "name": "sec-ch-ua",
      "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand\";v=
\\\"99\\\"\"
    },
    {
      "name": "sec-ch-ua-mobile",
      "value": "?0"
    },
    {
      "name": "sec-ch-ua-platform",
      "value": "\"Windows\""
    },
    {
      "name": "upgrade-insecure-requests",
      "value": "1"
    },
    {
      "name": "user-agent",
      "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.4606.54 Safari/537.36"
    },
    {
      "name": "accept",
      "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
    },
    {
      "name": "sec-fetch-site",
      "value": "cross-site"
    },
    {
      "name": "sec-fetch-mode",
      "value": "navigate"
    }
  ]
}
```



```
    },
    {
      "name": "sec-fetch-user",
      "value": "?1"
    },
    {
      "name": "sec-fetch-dest",
      "value": "document"
    },
    {
      "name": "accept-encoding",
      "value": "gzip, deflate, br"
    },
    {
      "name": "accept-language",
      "value": "en-US,en;q=0.9"
    }
  ],
  "uri": "/pen-test/pets",
  "args": "",
  "httpVersion": "HTTP/1.1",
  "httpMethod": "GET",
  "requestId": "GINKHEssoAMFsrg="
},
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
}
```

列出受基于速率的规则进行速率限制的 IP 地址

基于速率的规则将其规则操作应用于来自规则托管密钥列表中且与规则的范围缩小语句相匹配的 IP 地址的请求。当规则没有范围缩小语句时，它将操作应用于来自列表中 IP 地址的所有请求。该规则应用其规则操作来限制匹配请求的速率。该操作通常是，Block但可以是除以下之外的任何有效的规则操作Allow。单个基于速率的规则实例可以限制的最大 IP 地址数为 10,000。如果超过 10,000 个地址超过速率Amazon WAF限制，则限制速率最高的地址。有关基于速率的规则的信息，请参阅[基于速率的规则语句 \(p. 95\)](#)。

您可以使用 CLI、API 或任何 SDK 访问当前受基于速率的规则进行速率限制的 IP 地址列表。本主题介绍使用 CLI 和 API 进行访问。控制台目前不提供此功能。

对于Amazon WAF API，命令是[GetRateBasedStatementManagedKeys](#)。

对于Amazon WAF CLI，命令是 [get-rate-based-statement-managed-keys](#)。

以下显示了检索基于速率的规则的速率限制 IP 地址列表的语法，该规则在 Amazon CloudFront 发行版的 Web ACL 中使用。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLLOUDFRONT --region=us-east-1 --
web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

以下显示了区域应用程序、Amazon API Gateway REST API、Application Load Balancer、Amazon AppSync GraphQL API，Amazon Cognito 用户池或Amazon App Runner服务。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-
name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

Amazon WAF监控 Web 请求并独立管理 Web ACL、可选规则组和基于速率的规则的每个唯一组合的密钥。例如，如果在规则组内定义基于速率的规则，然后在 Web ACL 中使用该规则组，会Amazon WAF监控 Web

请求并管理该 Web ACL、规则组参考语句和基于速率的规则实例的密钥。如果您在第二个 Web ACL 中使用相同的规则组，则会 Amazon WAF 监控 Web 请求并管理第二次使用的密钥，与第一个 Web ACL 完全无关。

对于您在规则组内定义的基于速率的规则，除了 Web ACL 名称和规则组内基于速率的规则的名称外，还需要在请求中提供规则组参考语句的名称。以下显示了区域应用程序的语法，其中基于速率的规则在规则组内定义，规则组在 Web ACL 中使用。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-  
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupName --rule-  
name=RuleName
```

测试和调整您的 Amazon WAF 保护措施

我们建议您在将 Amazon WAF Web ACL 的所有更改应用到您的网站或 Web 应用程序流量之前，先对其进行测试和调整。

生产流量风险

在为生产流量部署 Web ACL 实现之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。然后使用生产流量在计数模式下测试和调整规则，然后再启用这些规则。

本节为测试和调整 Amazon WAF Web ACL、规则、规则组、IP 集和正则表达式模式集提供指导。

本节还提供了一般指导，用于测试您对由他人管理的规则组的使用情况。其中包括 Amazon 托管规则规则组、Amazon Web Services Marketplace 托管规则组以及其他账户与您共享的规则组。对于这些规则组，还要遵循规则组提供商提供的任何指导。

- 有关“机器人控制 Amazon 管理规则”规则组，另请参阅[测试和部署 Amazon WAF 机器人控制 \(p. 145\)](#)。
- 有关防止账户接管 Amazon 管理规则组的信息，另请参阅[测试和部署 ATP \(p. 159\)](#)。

更新期间出现暂时性不一致

创建或更改 Web ACL 或其他 Amazon WAF 资源时，更改需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。

下面是可能会看到变更传播过程中看到的临时不一致的示例：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，表明 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在使用 Web ACL 的某个区域生效，而在另一个区域无效。
- 更改规则操作设置后，可能会看到旧操作而是另一些地方看到新操作。
- 将 IP 地址添加到阻止规则中正在使用的 IP 集合后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

测试和调整高级步骤

本节提供测试您的 Web ACL 更改的步骤清单，包括其使用的任何规则或规则组。

Note

要遵循本节中的指导，您需要了解如何创建和管理 Web ACL、规则和规则组等 Amazon WAF 保护措施。本指南前面的部分中涵盖了该信息。

测试和调整您的网页 ACL

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 准备测试

准备好监控环境，将Amazon WAF保护切换到计数模式进行测试，并创建所需的任何资源关联。

请参阅[准备测试 \(p. 201\)](#)。

2. 监控和调整测试和生产环境

首先在测试或暂存环境中监控和调整您的Amazon WAF保护措施，然后在生产环境中监控和调整您的保护措施，直到您对它们能够根据您的需要处理流量感到满意。

请参阅[监控和优化 \(p. 202\)](#)。

3. 在生产中启用保护

当你对测试保护感到满意时，将其切换到生产模式，清理所有不必要的测试缺陷，然后继续监控。

请参阅[在生产中启用保护 \(p. 206\)](#)。

完成更改实施后，继续监控您的网络流量和生产环境中的保护措施，以确保它们按您的要求运行。网络流量模式可能会随着时间的推移而变化，因此您可能需要偶尔调整保护措施。

准备测试

本节介绍如何进行设置以测试和调整您的Amazon WAF保护措施。

Note

要遵循本节中的指导，您需要大致了解如何创建和管理 Web ACL、规则和规则组等Amazon WAF保护措施。本指南前面的部分中涵盖了该信息。

准备测试

1. 为网页 ACL 启用网页 ACL 日志记录、亚马逊 CloudWatch 指标和网络请求采样

使用日志、指标和采样来监控 Web ACL 规则与您的 Web 流量的交互。

- 日@@志-您可以配置Amazon WAF为记录 Web ACL 评估的 Web 请求。您可以将日志发送到日 CloudWatch 志、Amazon S3 存储桶或 Amazon Sinesis Data Firehose。您可以编辑字段并应用筛选。有关更多信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)：
- Amazon CloudWatch 指标 — 在您的 Web ACL 配置中，为要监控的所有内容提供指标规范。您可以通过Amazon WAF和 CloudWatch控制台查看指标。有关更多信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)：
- Web 请求采样 — 您可以查看 Web ACL 评估的所有 Web 请求的示例。有关 Web 请求采样的信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)。

2. 将保护设置为Count模式

在 Web ACL 配置中，将要测试的任何内容切换到计数模式。这使测试保护能够在不改变请求的处理方式的情况下记录与网络请求的匹配情况。您将能够在指标、日志和抽样请求中查看匹配结果，验证匹配标准并了解对您的网络流量可能产生的影响。无论规则操作如何，向匹配请求添加标签的规则都会添加标签。

- 在 Web ACL 中定义的规则-编辑 Web ACL 中的规则并将其操作设置为Count。
- 规则组-在 Web ACL 配置中，编辑规则组的规则语句，然后在规则窗格中打开“覆盖所有规则操作”下拉列表并选择Count。如果您在 JSON 中管理 Web ACL，请将规则添加到规则组参考语句中的RuleActionOverrides设置中，并将ActionToUse设置为Count。以下示例列表显示了“AWSManagedRulesAnonymousIpListAmazon托管规则”规则组中两个规则的替代项。

```
"ManagedRuleGroupStatement": {
```

```
"VendorName": "AWS",
"Name": "AWSManagedRulesAnonymousIpList",
"RuleActionOverrides": [
  {
    "ActionToUse": {
      "Count": {}
    },
    "Name": "AnonymousIpList"
  },
  {
    "ActionToUse": {
      "Count": {}
    },
    "Name": "HostingProviderIpList"
  }
],
"ExcludedRules": []
},
```

有关规则操作替代的更多信息，请参阅[覆盖规则组中的规则操作 \(p. 20\)](#)。

对于您自己的规则组，请勿修改规则组本身中的规则操作。带有Count操作的规则组规则不会生成测试所需的指标或其他工件。此外，更改规则组会影响所有使用该规则组的 Web ACL，而 Web ACL 配置内部的更改仅影响单个 Web ACL。

- Web ACL — 如果您正在测试新的 Web ACL，请将 Web ACL 的默认操作设置为允许请求。这使您可以试用 Web ACL，而不会以任何方式影响流量。

通常，计数模式生成的匹配次数多于生产模式。这是因为计算请求数的规则不会阻止 Web ACL 对请求的评估，因此稍后在 Web ACL 中运行的规则也可能与请求相匹配。当您将规则操作更改为其生产设置时，允许或阻止请求的规则将终止对与之匹配的请求的评估。因此，Web ACL 中检查匹配请求的规则通常较少。有关规则操作对 Web 请求总体评估的效果的更多信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。

使用这些设置，您的新保护不会改变 Web 流量，但会在指标、Web ACL 日志和请求样本中生成匹配信息。

3. 将 Web ACL 与资源相关联

如果 Web ACL 尚未与资源关联，请将其关联。

请参阅[将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)。

现在，您可以监控和调整 Web ACL 了。

监控和优化

本部分介绍如何监控和调整 Amazon WAF 保护措施。

Note

要遵循本节中的指导，您需要大致了解如何创建和管理 Web ACL、规则和规则组等 Amazon WAF 保护措施。本指南前面的部分中涵盖了该信息。

监控 Web 流量和规则匹配以验证 Web ACL 的行为。如果您发现问题，请调整规则以使其正确，然后进行监控以验证调整。

重复以下步骤，直到 Web ACL 根据需要管理您的 Web 流量。

进行监视和调谐

1. 监控流量和规则匹配情况

确保流量畅通，并且您的测试规则正在找到匹配的请求。

查找以下信息，了解您正在测试的保护措施：

- 日志 — 在日志中，与 Web 请求相匹配的测试规则如下所示：
 - Web ACL 中具有Count操作的规则列为nonTerminatingMatchingRules。
 - 规则组在ruleGroupId字段中标识。
 - 您Count通过 Web ACL 配置设置的规则组规则以以下两种方式之一显示ruleGroupList在的下方，具体取决于您配置Count替代的方式和时间：
 - 对于使用Count所选规则操作进行替换，匹配项列在action下方nonTerminatingMatchingRules，overriddenAction是，Count而是在规则组中为该规则配置的操作，通常为Block。规则操作覆盖是覆盖规则组规则操作的最新推荐选项，也是控制台向导提供的唯一选项。
 - 对于排除的规则，匹配项列在下方excludedRules。这是一个较旧的选项，已被替代选项所取代，不再可通过控制台使用。您在 2022 年 10 月 27 日之前通过控制台向导配置的 Web ACL 可能仍会使用它，您也可以通过 API 选择此选项。
 - Labels字段中列出了规则已应用于请求的标签。

有关日志记录内容的更多信息，请参阅[日志字段 \(p. 188\)](#)。

- 指标-与 Web 请求匹配的测试规则的指标显示如下：
 - Web ACL 中具有Count操作的规则被列为 Web ACL 的Count指标。
 - 对于您的规则组，您Count通过 Web ACL 配置设置为的规则列在规则组指标下。

Note

Amazon WAF不会为在规则组配置中使用Count操作配置的规则生成指标。它仅为您Count通过规则组参考语句的 Web ACL 配置替换的规则生成指标。

- 对于托管规则组，您Count通过 Web ACL 配置设置为的规则列在 Web ACL 指标下。只有规则组所有者才能查看规则组指标。

有关指标的更多信息，请参阅[查看 Web ACL 的指标 \(p. 204\)](#)。

- 抽样的 Web 请求 — 抽样请求提供与 Web 请求匹配的测试规则信息，如下所示：
 - 示例信息通过 Web ACL 中规则的指标名称识别匹配规则。对于规则组，该指标用于标识规则组参考语句。
 - 对于规则组内的规则，示例在中列出了匹配的规则名称RuleWithinRuleGroup。

有关索取样品的更多信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)。

2. 配置缓解措施以解决误报

如果您确定某条规则会产生误报，通过在不应该匹配的网络请求时进行匹配，则以下选项可以帮助您调整 Web ACL 保护以缓解误报。

更正规则检查标准

根据您的规则，您通常只需要调整用于检查网络请求的设置即可。示例包括更改正则表达式模式集中的规范、在检查之前调整应用于请求组件的文本转换，或者切换到使用转发的 IP 地址。请参阅下方有关导致问题的规则类型的指南[Amazon WAF 规则语句 \(p. 81\)](#)。

更正更复杂的问题

对于您无法控制的检查标准和一些复杂的规则，您可能需要进行其他更改，例如添加明确允许或阻止请求的规则，或者将请求排除在有问题的规则的评估范围之外。托管规则组通常需要这种类型的缓解措施，但其他规则也可以。示例包括基于速率的规则语句和 SQL 注入攻击规则语句。

为减少误报而采取的措施因您的使用案例而定。以下是常用方法：

- 添加缓解规则-添加一条在新规则之前运行的规则，该规则明确允许导致误报的请求。有关 Web ACL 中规则评估顺序的信息，请参阅[Web ACL 中规则和规则组的处理顺序 \(p. 13\)](#)。

使用这种方法，允许的请求将发送到受保护的资源，因此它们永远不会达到新的评估规则。如果新规则是付费管理规则组，则此方法还可以帮助控制使用该规则组的成本。

- 添加带有缓解规则的逻辑规则-使用逻辑规则语句将新规则与排除误报的规则相结合。下面列出了逻辑规则语句[规则语句列表 \(p. 82\)](#)。

例如，假设您要添加一个 SQL 注入攻击匹配语句，该语句会为一类请求生成误报。创建与这些请求匹配的规则，然后使用逻辑规则语句组合规则，这样您就只匹配不符合误报标准且与 SQL 注入攻击标准不匹配的请求。

- 添加范围缩小语句-对于基于速率的语句和托管规则组参考语句，通过在主语句中添加缩小范围语句，将导致误报的请求排除在评估之外。

与 scope-down 语句不匹配的请求永远不会到达规则组或基于速率的评估。有关范围缩小语句的信息，请参见[范围缩小声明 \(p. 110\)](#)。有关示例，请参阅[将 IP 范围排除在机器人管理之外 \(p. 154\)](#)。

- 添加标签匹配规则-对于使用标签的规则组，确定有问题的规则应用于请求的标签。添加与已确定的标签匹配的标签匹配规则，该规则位于规则组之后运行。在标签匹配规则中，您可以从要阻止的请求中筛选要允许的请求。

如果您使用此方法，则在完成测试后，在规则组中将有问题规则保持在计数模式，并保持自定义标签匹配规则不变。有关标签匹配语句的信息，请参见[标签匹配规则声明 \(p. 92\)](#)。有关示例，请参阅[允许特定被屏蔽的机器人 \(p. 149\)](#)和[ATP 示例：对丢失和泄露的凭据进行自定义处理 \(p. 162\)](#)。

- 更改托管规则组的版本-对于版本化的托管规则组，请更改您正在使用的版本。例如，您可以切换回您成功使用的最后一个静态版本。

这通常是临时修复。在继续在测试或暂存环境中测试最新版本的同时，或者在等待提供商提供更兼容的版本时，您可以更改生产流量的版本。有关托管规则组版本的信息，请参阅[托管规则组 \(p. 24\)](#)。

如果您对新规则按您的需要匹配请求感到满意，请转到测试的下一阶段并重复此过程。在生产环境中执行测试和调整的最后阶段。

查看 Web ACL 的指标

将 Web ACL 与一个或多个 Amazon 资源关联后，您可以在亚马逊 CloudWatch 图表中查看关联的结果指标。

有关 CloudWatch 指标的信息，请参阅[亚马逊 CloudWatch 用户指南](#)。有关 Amazon WAF 提供的指标列表，请参阅[Amazon WAF 指标和维度 \(p. 502\)](#)。

对于 Web ACL 中的每条规则以及关联资源转发给 Amazon WAF Web ACL 的所有请求，CloudWatch 允许您执行以下操作：

- 查看前一小时或之前三个小时的数据。
- 更改数据点之间的间隔。
- 更改对数据 CloudWatch 执行的计算，例如最大值、最小值、平均值或总和。

Note

Amazon WAF with CloudFront 是一项全球服务，只有当您在其中选择美国东部（弗吉尼亚北部）地区时，指标才可用 Amazon Web Services Management Console。如果您选择其他区域，则 CloudWatch 控制台中不会显示任何 Amazon WAF 指标。

查看 Web ACL 中规则的数据

1. 登录 Amazon Web Services Management Console 并打开 CloudWatch 主机，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 如果需要，可将区域更改为 Amazon 资源所在区域。对于 CloudFront，选择美国东部（弗吉尼亚北部）区域。
3. 在导航窗格的“指标”下，选择“所有指标”，然后在“浏览”选项卡下搜索 AWS::WAFv2。
4. 选中要查看其数据的 Web ACL 对应的复选框。
5. 更改适用的设置：

统计数据

选择对数据 CloudWatch 执行的计算。

时间范围

选择您要查看前一个小时还是前三个小时的数据。

周期

选择图表中的数据点之间的间隔。

规则

选择要查看其数据的规则。

请注意以下几点：

- 如果您最近将 Web ACL 与 Amazon 资源关联，您可能需要等待几分钟时间，数据才会显示在图表上，Web ACL 的指标才会显示在可用指标的列表中。
- 如果您将多个资源与 Web ACL 关联，则 CloudWatch 数据将包括对所有资源的请求。
- 您可以将光标悬停在数据点上以获取更多信息。
- 该图表不会自动自行刷新。要更新显示，请选择刷新 () 图标。

有关 CloudWatch 指标的更多信息，请参阅[监控 Amazon WAF、Amazon Firewall Manager 和 Amazon Shield Advanced \(p. 500\)](#)。

查看 Web 请求示例

在 Amazon WAF 控制台中，如果您启用了请求抽样，则可以查看 Amazon WAF 已检查、允许或阻止的请求的示例。对于每个示例请求，您可以查看关于该请求的详细数据，例如来源 IP 地址和请求中包含的标头。您还可以查看与请求匹配的规则以及规则操作设置。

请求样本包含最多 100 个与 Web ACL 中规则条件相匹配的请求，以及另外 100 个不匹配任何规则且应用了 Web ACL 默认操作的请求。示例中的请求来自在过去三个小时内收到您的内容请求的所有受保护资源。

当 Web 请求符合规则中的所有条件并且该规则的操作为 Count 时，Amazon WAF 继续使用 Web ACL 中的后续规则检查 Web 请求。因此，Web 请求可能会在抽样请求列表中多次出现。

查看受保护资源已转发到以Amazon WAF供检查的 Web 请求的示例

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，选择 Web ACL。
3. 选择要查看其请求的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在 Overview (概述) 选项卡中，Sampled requests (采样请求) 表显示每个请求的以下值：

指标名称

Web ACL 中与请求匹配的规则的 CloudWatch 指标名称。如果 Web 请求与 Web ACL 中的任何规则都不匹配，则此值为默认。

源 IP

发出请求的 IP 地址，或者如果查看器已使用 HTTP 代理或Application Load Balancer 发送请求，则为该代理或Application Load Balancer 的 IP 地址。

URI

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。

规则组内部规则

如果指标名称标识了规则组参考语句，则该语句将标识规则组内与请求匹配的规则。

操作

指示相应规则的操作是 Allow、Block 还是 Count。

Time

从受保护资源Amazon WAF收到请求的时间。

5. 要显示有关 Web 请求组件的其他信息，请在请求行中选择 URI 的名称。

在生产中启用保护

在生产环境中完成测试和调整的最后阶段后，请在生产模式下启用保护。

生产流量风险

在为生产流量部署 Web ACL 实现之前，请在测试环境中对其进行测试和调整，直到您对流量的潜在影响感到满意。在启用生产流量保护之前，还要在计数模式下使用生产流量对其进行测试和调整。

Note

要遵循本节中的指导，您需要大致了解如何创建和管理 Web ACL、规则和规则组等Amazon WAF 保护措施。本指南前面的部分中涵盖了该信息。

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

在生产中启用Amazon WAF保护

1. 切换到您的生产保护

更新您的 Web ACL 并切换生产设置。

- a. 删除您不需要的测试规则数

如果您添加了在生产中不需要的测试规则，请将其删除。如果您使用任何标签匹配规则来筛选托管规则组规则的结果，请务必将其保留在原处。

b. 切换为生产操作

将新规则的操作设置更改为预期的生产设置。

- 在 Web ACL 中定义的规则-编辑 Web ACL 中的规则并将其操作从更改Count为生产操作。
- 规则组 — 在规则组的 Web ACL 配置中，根据您的测试和调整活动的结果，切换规则以使用自己的操作或保留操作替换规则。Count如果您使用标签匹配规则来筛选规则组规则的结果，请务必保留该规则的覆盖范围。

要切换到使用规则的操作，请在您的 Web ACL 配置中编辑该规则组的规则语句并删除该规则的Count替换。如果您在 JSON 中管理 Web ACL，请在规则组参考语句中从RuleActionOverrides列表中删除该规则的条目。

- Web ACL — 如果您更改了测试的 Web ACL 默认操作，请将其切换到生产设置。

使用这些设置，您的新保护措施将按您的意图管理网络流量。

当您保存 Web ACL 时，与之关联的资源将使用您的生产设置。

2. 监视和调谐

为确保按照您的需要处理 Web 请求，请在启用新功能后密切监控您的流量。您将监控生产规则操作的指标和日志，而不是您在调整工作中监控的计数操作。继续监控并根据需要调整行为，以适应网络流量的变化。

如何Amazon WAF使用亚马逊 CloudFront 功能

创建 Web ACL 时，可以指定Amazon WAF要检查的一个或多个 CloudFront 发行版。Amazon WAF根据您在 Web ACL 中确定的标准，开始检查和管理针对这些发行版的 Web 请求。CloudFront 提供了一些增强 Amazon WAF功能的功能。本章介绍几种可以配置的方法，CloudFront 以便 CloudFront 更好地协同Amazon WAF工作。

主题

- [Amazon WAF与 CloudFront 自定义错误页面一起使用 \(p. 207\)](#)
- [对于在您自己的 HTTP 服务器上运行的应用程序，将 Amazon WAF 与 CloudFront 结合使用 \(p. 208\)](#)
- [选择 CloudFront 响应的 HTTP 方法 \(p. 208\)](#)

Amazon WAF与 CloudFront 自定义错误页面一起使用

默认情况下，当根据您指定的条件Amazon WAF阻止 Web 请求时，它会将 HTTP 状态代码403 (Forbidden)返回 CloudFront，并将该状态代码 CloudFront 返回给查看者。然后，查看器显示简要且采用稀疏格式的默认消息，如下所示：

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

您可以通过定义自定义响应来替换Amazon WAF Web ACL 规则中的此行为。有关使用Amazon WAF规则自定义响应行为的更多信息，请参阅[对Block操作的自定义响应 \(p. 120\)](#)。

Note

您使用Amazon WAF规则自定义的响应优先于您在 CloudFront 自定义错误页面中定义的任何响应规范。

如果您希望通过 CloudFront 显示自定义错误消息（可能使用与网站其他部分相同的格式），则可以配置为 CloudFront 向查看器返回包含自定义错误消息的对象（例如，HTML 文件）。

Note

CloudFront 无法区分您的源返回的 HTTP 状态码 403 和请求被阻止 Amazon WAF 时返回的 HTTP 状态码 403。这意味着，您无法根据 HTTP 状态代码 403 的不同原因返回不同的自定义错误页面。

有关 CloudFront 自定义错误页面的更多信息，请参阅亚马逊 CloudFront 开发者指南中的[生成自定义错误响应](#)。

对于在您自己的 HTTP 服务器上运行的应用程序，将 Amazon WAF 与 CloudFront 结合使用

Amazon WAF 使用时 CloudFront，您可以保护在任何 HTTP Web 服务器上运行的应用程序，无论是在亚马逊弹性计算云 (Amazon EC2) 中运行的 Web 服务器还是您私下管理的 Web 服务器。您也可以配置 CloudFront 为要求在 CloudFront 和您自己的 Web 服务器之间以及查看者之间使用 HTTPS CloudFront。

需要在 CloudFront 和你自己的网络服务器之间使用 HTTPS

要要求在 CloudFront 和您自己的 Web 服务器之间使用 HTTPS，您可以使用 CloudFront 自定义源功能并为特定来源配置原始协议策略和原始域名设置。在您的 CloudFront 配置中，您可以指定服务器的 DNS 名称以及您在从源中获取对象时 CloudFront 希望使用的端口和协议。您还应确保自定义源服务器上的 SSL/TLS 证书与您已配置的源域名匹配。当您在外部使用自己的 HTTP Web 服务器时 Amazon，您必须使用由受信任的第三方证书颁发机构 (CA)（例如，Comodo 或 Symantec）签署的证书。DigiCert 有关需要 HTTPS 才能在 CloudFront 与您自己的 Web 服务器之间进行通信的更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的[“需要 HTTPS 才能 CloudFront 与您的自定义源进行通信”](#)主题。

需要在查看者和之间使用 HTTPS CloudFront

要要求在查看器和之间使用 HTTPS，您可以更改 CloudFront 分发中一个或多个缓存行为的查看器协议策略。CloudFront 有关在观众和之间使用 HTTPS 的更多信息 CloudFront，请参阅亚马逊 CloudFront 开发者指南中的[“需要 HTTPS 才能 CloudFront 在查看者之间进行通信”](#)主题。您也可以自带 SSL 证书，这样观众就可以使用您自己的域名（例如 <https://www.mysite.com>）通过 HTTPS 连接到您的 CloudFront 发行版。有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的[配置备用域名和 HTTPS](#)主题。

选择 CloudFront 响应的 HTTP 方法

在创建 Amazon CloudFront Web 发行版时，您可以选择要处理并转发 CloudFront 到源的 HTTP 方法。可从以下选项中进行选择：

- **GET, HEAD**— 您 CloudFront 只能使用从源中获取对象或获取对象标头。
- **GETHEAD, OPTIONS**— 您 CloudFront 只能使用从源获取对象、获取对象标头或检索源服务器支持的选项列表。
- **GET、HEAD、OPTIONS、PUT、POST、PATCH、DELETE**— 您可以使用获 CloudFront 取、添加、更新和删除对象，以及获取对象标头。此外，您可以执行其他 POST 操作，例如从 Web 表格提交数据。

您还可以使用 Amazon WAF 字节匹配规则语句来允许或阻止基于 HTTP 方法的请求，如[字符串匹配规则语句 \(p. 100\)](#) 中所述。如果您想使用 CloudFront 支持的方法组合，例如 GET 和 HEAD，则无需配置 Amazon WAF 为阻止使用其他方法的请求。如果您想允许组合使用 CloudFront 不支持的方法，例如 GETHEADPOST、和，则可以配置 CloudFront 为响应所有方法，然后使用 Amazon WAF 来阻止使用其他方法的请求。

有关选择 CloudFront 响应方法的更多信息，请参阅《亚马逊 CloudFront 开发者指南》中[“您在创建或更新 Web 发行版时指定的值”](#)主题中的[“允许的 HTTP 方法”](#)。

您使用 Amazon WAF 服务的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

Note

本节为您提供使用 Amazon WAF 服务及其 Amazon 资源（例如 Amazon WAF Web ACL 和规则组）提供标准 Amazon 安全指导。

有关使用保护 Amazon 资源的信息 Amazon WAF，请参阅 Amazon WAF 指南的其余部分。

安全性是 Amazon 和您的共同责任。[责任共担模型](#)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 Web Services 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，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Amazon WAF 的合规性计划，请参阅[合规性计划范围内的 Amazon 服务](#)。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Amazon WAF 时应用责任共担模式。以下主题说明如何配置 Amazon WAF 以实现您的安全性和合规性目标。您还会了解如何使用其它 Amazon 服务以帮助您监控和保护 Amazon WAF 资源。

主题

- [Amazon WAF 中的数据保护 \(p. 209\)](#)
- [适用于 Amazon WAF 的 Identity and Access Management \(p. 210\)](#)
- [Amazon WAF 中的日志记录和监控 \(p. 228\)](#)
- [Amazon WAF 的合规性验证 \(p. 229\)](#)
- [Amazon WAF 中的故障恢复能力 \(p. 230\)](#)
- [Amazon WAF 中的基础设施安全性 \(p. 230\)](#)

Amazon WAF 中的数据保护

Amazon [责任共担模式](#) 适用于 Amazon WAF 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）。这包括使用控制台、API、Amazon CLI 或 Amazon SDK 处理 Amazon WAF 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。

Amazon WAF 实体（例如 Web ACL、规则组和 IP 集）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

正在删除 Amazon WAF 资源

您可以删除您在中创建的资源 Amazon WAF。请参阅以下部分中每种资源类型的指南。

- [删除 Web ACL \(p. 23\)](#)
- [删除规则组 \(p. 79\)](#)
- [删除 IP 集 \(p. 116\)](#)
- [删除正则表达式模式集 \(p. 118\)](#)

适用于 Amazon WAF 的 Identity and Access Management

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）来使用 Amazon WAF 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- [受众 \(p. 210\)](#)
- [使用身份进行身份验证 \(p. 211\)](#)
- [使用策略管理访问 \(p. 212\)](#)
- [Amazon WAF 如何与 IAM 协同工作 \(p. 213\)](#)
- [适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)
- [Amazon 适用于 Amazon WAF 的托管策略 \(p. 222\)](#)
- [对 Amazon WAF 身份和访问进行故障排除 \(p. 225\)](#)
- [将服务相关角色用于 Amazon WAF \(p. 226\)](#)

受众

使用 Amazon Identity and Access Management (IAM) 的方式因您可以在 Amazon WAF 中执行的操作而异。

服务用户 – 如果使用 Amazon WAF 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Amazon WAF 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Amazon WAF 中的功能，请参阅 [对 Amazon WAF 身份和访问进行故障排除 \(p. 225\)](#)。

服务管理员 – 如果您在公司负责管理 Amazon WAF 资源，则您可能具有 Amazon WAF 的完全访问权限。您有责任确定您的服务用户应访问哪些 Amazon WAF 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon WAF 搭配使用的更多信息，请参阅 [Amazon WAF 如何与 IAM 协同工作 \(p. 213\)](#)。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Amazon WAF 的访问权限的详细信息。要查看您可在 IAM 中使用的 Amazon WAF 基于身份的策略示例，请参阅 [适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅 Amazon 一般参考中的 [签名版本 4 签名流程](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的 [在 Amazon 中使用多重身份验证 \(MFA\)](#)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 Amazon Account Management 参考指南中的 [需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

IAM 用户和组

[IAM 用户](#) 是 Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 [对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#) 是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的 [何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

[IAM 角色](#) 是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过 [切换角色](#)，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以担任角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南中的 [使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access (联合用户访问) – 要向联合身份分配权限, 请创建角色并为角色定义权限。当联合身份进行身份验证时, 该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色信息, 请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色, 以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人 (可信主体) 访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是, 对于某些 Amazon Web Services, 您可以将策略直接附加到资源 (而不是使用角色作为代理)。要了解用于跨账户访问的角色和基于资源的策略之间的差别, 请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 – 某些 Amazon Web Services 使用其它 Amazon Web Services 中的功能。例如, 当您在某个服务中进行调用时, 该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
 - 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时, 您将被视为主体。策略向主体授予权限。使用某些服务时, 您可能会执行一个操作, 此操作然后在不同服务中触发另一个操作。在这种情况下, 您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作, 请参阅服务授权参考中的[Amazon WAFV2 的操作、资源和条件键](#)。
 - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 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](#)。
 - 服务相关角色 – 服务相关角色是与 Amazon Web Service 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中, 并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用, 您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色, 并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息, 请参阅 IAM 用户指南中的[使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户, 请参阅 IAM 用户指南中的[何时创建 IAM 角色 \(而不是用户 \)](#)。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源, 以控制 Amazon 中的访问。策略是 Amazon 中的对象; 在与身份或资源相关联时, 策略定义它们的权限。在主体 (用户、根用户或角色会话) 发出请求时, Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息, 请参阅 IAM 用户指南中的[JSON 策略概览](#)。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说, 哪个主体 可以对什么资源 执行操作, 以及在什么条件 下执行。

默认情况下, 用户和角色没有权限。要授予用户对所需资源执行操作的权限, IAM 管理员可以创建 IAM 策略。然后, 管理员可以向角色添加 IAM 策略, 并且用户可以代入角色。

IAM policy 定义操作的权限, 无关乎您使用哪种方法执行操作。例如, 假设您有一个允许 iam:GetRole 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份 (如 IAM 用户、用户组或角色) 的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略, 请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括

Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的[在托管式策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 Amazon 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Simple Storage Service (Amazon S3)、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的[访问控制列表 \(ACL\) 概览](#)。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的[IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 Amazon Web Services 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的[SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

Amazon WAF 如何与 IAM 协同工作

在使用 IAM 管理对 Amazon WAF 的访问之前，您应该了解哪些 IAM 功能可用于 Amazon WAF。

您可以与 Amazon WAF 搭配使用的 IAM 功能

IAM 功能	Amazon WAF 支持
基于身份的策略 (p. 214)	是

IAM 功能	Amazon WAF 支持
基于资源的策略 (p. 214)	否
策略操作 (p. 215)	是
策略资源 (p. 215)	是
策略条件键 (特定于服务) (p. 216)	是
ACL (p. 217)	否
ABAC (策略中的标签) (p. 217)	部分
临时凭证 (p. 217)	是
委托人权限 (p. 217)	是
服务角色 (p. 218)	是
服务相关角色 (p. 218)	是

要大致了解 Amazon WAF 和其他 Amazon 服务如何与大多数 IAM 功能一起使用，请参阅《IAM 用户指南》中的[与 IAM 一起使用的 Amazon 服务](#)。

适用于 Amazon WAF 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

要查看 Amazon WAF 基于身份的策略的示例，请参阅[适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)。

Amazon WAF 内基于资源的策略

支持基于资源的策略。	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。

适用于 Amazon WAF 的策略操作

支持策略操作	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

要查看Amazon WAF操作列表，请参阅服务授权参考中 [Amazon WAFV2 定义的操作](#)。

Amazon WAF 中的策略操作在操作前使用以下前缀：

```
wafv2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
    "wafv2:action1",
    "wafv2:action2"
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以开头的所有操作List，请包括以下操作：Amazon WAF

```
"Action": "wafv2:List*"
```

要查看 Amazon WAF 基于身份的策略的示例，请参阅 [适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)。

Amazon WAF 的策略资源

支持策略资源	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN \)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看Amazon WAF资源类型及其 ARN 的列表，请参阅服务授权参考Amazon WAF中的 [V2 定义的资源](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Amazon WAFV2 定义的操作](#)。要允许或拒绝对 Amazon WAF 资源子集的访问权限，请在策略的 resource 元素中包含资源的 ARN。

Amazon WAFwafv2资源的 ARN 具有以下格式：

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

有关 ARN 规范的一般信息，请参阅 [Amazon Web Services 一般参考中的 Amazon Resource Name \(ARN\)](#)。

以下列出了特定于wafv2资源 ARN 的要求：

- **##**：对于用于保护亚马逊 CloudFront 发行版的Amazon WAF资源，请将其设置为us-east-1。否则，请将其设置为与受保护的区域资源一起使用的区域。
- **##**：将范围设置global为与亚马逊 CloudFront 发行版一起使用或regional与Amazon WAF支持的任何区域资源一起使用。这些区域资源是 Amazon API Gateway REST API、GraphQL API、Amazon AppSync GraphQL API、Amazon Cognito 用户池和一项Amazon App Runner服务。
- **####**：指定以下值之一：webacl、rulegroup、ipsetregexpatternset、或managedruleset。
- **####**：指定您为Amazon WAF资源提供的名称，或指定通配符 (*) 以表示满足 ARN 中其他规范的所有资源。您必须指定资源名称和资源 ID，或者为两者都指定通配符。
- **##ID**：指定Amazon WAF资源的 ID，或指定通配符 (*) 以表示满足 ARN 中其他规范的所有资源。您必须指定资源名称和资源 ID，或者为两者都指定通配符。

例如，以下 ARN 指定区域 us-west-1 中具有账户 111122223333 的区域作用域的所有 Web ACL：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

以下 ARN 为区域111122223333中的账户指定了MyIPManagementRuleGroup以全局作用域命名的规则组us-east-1：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

要查看 Amazon WAF 基于身份的策略的示例，请参阅 [适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)。

Amazon WAF 的策略条件键

支持特定于服务的策略条件键	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。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](#)。

Amazon支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 [Amazon 全局条件上下文键](#)。

要查看Amazon WAF条件键的列表，请参阅《服务授权参考》[Amazon WAF中的 V2 的条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅 [Amazon WAFV2 定义的操作](#)。

要查看 Amazon WAF 基于身份的策略的示例，请参阅 [适用于 Amazon WAF 的基于身份的策略示例 \(p. 218\)](#)。

Amazon WAF 中的 ACL

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体 (账户成员、用户或角色) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带有 Amazon WAF 的 ABAC

支持 ABAC (策略中的标签)	部分

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体 (用户或角色) 以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes (是)。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial (部分)。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的 [什么是 ABAC ?](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的 [使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证用于 Amazon WAF

支持临时凭证	是

某些 Amazon Web Services 在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon Web Services 与临时凭证配合使用，请参阅 IAM 用户指南中的 [使用 IAM 的 Amazon Web Services](#)。

如果您不使用用户名和密码而用其它方法登录到 Amazon Web Services Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录 (SSO) 链接访问 Amazon 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 [切换到角色 \(控制台\)](#)。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 [IAM 中的临时安全凭证](#)。

Amazon WAF 的跨服务主体权限

支持委托人权限	是

当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关操作，请参阅服务授权参考中的 [Amazon WAFV2 的操作、资源和条件键](#)。

Amazon WAF 的服务角色

支持服务角色	是

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](#)。

Warning

更改服务角色的权限可能会破坏 Amazon WAF 功能。仅当 Amazon WAF 提供相关指导时才编辑服务角色。

Amazon WAF 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与 Amazon Web Service 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Amazon WAF 服务相关角色的详细信息，请参阅 [将服务相关角色用于 Amazon WAF \(p. 226\)](#)。

适用于 Amazon WAF 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Amazon WAF 资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要用户用户在其需要的资源上执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 [创建 IAM policy](#)。

有关定义的操作和资源类型的详细信息 Amazon WAF，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 [Amazon WAFV2 的操作、资源和条件键](#)。

主题

- [策略最佳实践 \(p. 218\)](#)
- [使用 Amazon WAF 控制台 \(p. 219\)](#)
- [允许用户查看他们自己的权限 \(p. 219\)](#)
- [向 Amazon WAF、CloudFront 和授予只读访问权限 CloudWatch \(p. 220\)](#)
- [授予 Amazon WAF、CloudFront 和的完全访问权限 CloudWatch \(p. 220\)](#)
- [授予单个访问权限 Amazon Web Services 账户 \(p. 221\)](#)
- [授予对指定的 Web ACL 和规则组的访问权限 \(p. 221\)](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon WAF 资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户中找到这些策略。我们建议通

过定义特定于您的使用场景的 Amazon 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon 托管策略](#)或[工作职能的 Amazon 托管策略](#)。

- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy 语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM Access Analyzer 策略验证](#)。
- Require multi-factor authentication (MFA) [需要多重身份验证 (MFA)] – 如果您所处的场景要求您的 Amazon Web Services 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 [配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用 Amazon WAF 控制台

要访问 Amazon WAF 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 Amazon Web Services 账户中的 Amazon WAF 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色可以使用 Amazon WAF 控制台，还应将 Amazon WAFAWSWAFConsoleReadOnlyAccessAmazon 托管策略至少附加到实体。有关此托管策略的信息，请参阅 [Amazon 托管策略：AWSWAFConsoleReadOnlyAccess \(p. 222\)](#)。有关将托管策略附加到用户的更多信息，请参阅 IAM 用户指南中的向用户 [添加权限](#)。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",

```



```
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

向Amazon WAF、CloudFront和授予只读访问权限 CloudWatch

以下策略授予用户对Amazon WAF资源、亚马逊 CloudFront 网络分配和亚马逊 CloudWatch 指标的只读访问权限。对于需要权限查看 Amazon WAF 条件、规则和 Web ACL 中的设置、了解与 Web ACL 关联的分发以及在 CloudWatch 中监控指标和请求示例的用户，这十分有用。这些用户无法创建、更新或删除 Amazon WAF 资源：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:Get*",
        "wafv2:List*",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeRegions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

授予Amazon WAF、CloudFront和的完全访问权限 CloudWatch

以下策略允许用户执行任何Amazon WAF操作、对 CloudFront Web 发行版执行任何操作，以及监控中的指标和请求示例 CloudWatch。它对作为 Amazon WAF 管理员的用户十分有用：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "wafv2:*",
        "cloudfront:CreateDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront>DeleteDistribution",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeRegions"
      ]
    }
  ]
}
```

```
    ],  
    "Effect": "Allow",  
    "Resource": "*"    
  }  
]  
}
```

强烈建议您为拥有管理权限的用户配置 Multi-Factor Authentication (MFA)。有关更多信息，请参阅 IAM 用户指南Amazon中的[使用Multi-Factor Authentication \(MFA\) 设备](#)。

授予单个访问权限Amazon Web Services 账户

此策略向账户 444455556666 授予以下权限：

- 对所有 Amazon WAF 操作和资源的完全访问权限。
- 读取和更新对所有 CloudFront 发行版的访问权限，这允许您关联 Web ACL 和 CloudFront 发行版。
- 读取所有 CloudWatch 指标和指标统计数据的访问权限，这样您就可以在Amazon WAF控制台中查看 CloudWatch 数据和请求示例。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "wafv2:*"  
      ],  
      "Resource": [  
        "arn:aws:wafv2:us-east-1:444455556666:*"  
      ]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "cloudfront:GetDistribution",  
        "cloudfront:GetDistributionConfig",  
        "cloudfront:ListDistributions",  
        "cloudfront:ListDistributionsByWebACLId",  
        "cloudfront:UpdateDistribution",  
        "cloudwatch:ListMetrics",  
        "cloudwatch:GetMetricStatistics",  
        "ec2:DescribeRegions"  
      ],  
      "Resource": [  
        "*"    
      ]  
    }  
  ]  
}
```

授予对指定的 Web ACL 和规则组的访问权限

以下策略允许用户对账户中的特定 Web ACL 和特定规则组执行任何Amazon WAF操作444455556666。

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "wafv2:*"  
      ]  
    }  
  ]  
}
```

```
    ],
    "Resource": [
      "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/test123/112233d7c-86b2-458b-af83-51c51example",
      "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/test123rulegroup/555555555-6666-1234-abcd-00d11example"
    ]
  }
]
```

Amazon适用于 Amazon WAF 的托管策略

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 Web Services 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 Web Services 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，服务最有可能更新 Amazon 托管策略。服务不会从 Amazon 托管策略中删除权限，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，ViewOnlyAccess Amazon 托管策略提供对许多 Amazon Web Services 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：AWSWAFReadOnlyAccess

此策略授予只读权限，该权限允许用户访问 Amazon WAF 资源但不能对其进行修改。您可以将此策略附加到您的 IAM 身份。Amazon WAF 还将此策略附加到服务角色，该角色允许 Amazon WAF 代表您执行操作。

有关此策略的详细信息，请参阅 IAM 控制台 [AWSWAFReadOnlyAccess](#) 中的。

Amazon托管策略：AWSWAFFullAccess

此策略授予对 Amazon WAF 资源的完全访问权限。您可以将此策略附加到您的 IAM 身份。Amazon WAF 还将此策略附加到服务角色，该角色允许 Amazon WAF 代表您执行操作。

有关此策略的详细信息，请参阅 IAM 控制台 [AWSWAFFullAccess](#) 中的。

Amazon托管策略：AWSWAFConsoleReadOnlyAccess

此策略向控制台授予只读权限，Amazon WAF 控制台包括集成服务的资源 Amazon WAF 和用于集成服务的资源，例如亚马逊、Amazon API Gateway CloudFront、Application Load Balancer Amazon AppSync、Amazon Cognito 和 Amazon App Runner。您可以将此策略附加到您的 IAM 身份。Amazon WAF 还将此策略附加到服务角色，该角色允许 Amazon WAF 代表您执行操作。

有关此策略的详细信息，请参阅 IAM 控制台 [AWSWAFConsoleReadOnlyAccess](#) 中的。

Amazon托管策略：AWSWAFConsoleFullAccess

该策略授予对控制台的完全访问权限，Amazon WAF 控制台包括集成服务的资源，例如亚马逊 Amazon WAF、亚马逊 Amazon API Gateway CloudFront、Application Load Balancer Amazon AppSync、Amazon Cognito 和 Amazon App Runner。您可以将此策略附加到您的 IAM 身份。Amazon WAF 还将此策略附加到服务角色，该角色允许 Amazon WAF 代表您执行操作。

有关此策略的详细信息，请参阅 IAM 控制台 [AWSWAFConsoleFullAccess](#) 中的。

对 Amazon 托管式策略的 Amazon WAF 更新

查看有关 Amazon WAF 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）。有关此页面更改的自动提示，请订阅 Amazon WAF 文档历史记录页面上的 RSS 源 [文档历史记录 \(p. 525\)](#)。

策略	变更描述	日期
AWSWAFFullAccess 此策略 Amazon WAF 允许您在集成服务中 Amazon WAF 和集成服务中代表您管理 Amazon 资源。 IAM 控制台中的详细信息： AWSWAFFullAccess 。	扩展了权限，可以向可以保护的资源类型添加 Amazon App Runner 服务 Amazon WAF。	2023 年 3 月 30 日
AWSWAFReadOnlyAccess 此策略 Amazon WAF 允许您在集成服务中 Amazon WAF 和集成服务中代表您管理 Amazon 资源。 IAM 控制台中的详细信息： AWSWAFReadOnlyAccess 。	扩展了权限，可以向可以保护的资源类型添加 Amazon App Runner 服务 Amazon WAF。	2023 年 3 月 30 日
AWSWAFConsoleFullAccess 此策略 Amazon WAF 允许您在集成服务中和集成服务中 Amazon WAF 代表您管理 Amazon 控制台 Amazon 资源和其他资源。 IAM 控制台中的详细信息： AWSWAFConsoleFullAccess 。	扩展了权限，可以向可以保护的资源类型添加 Amazon App Runner 服务 Amazon WAF。	2023 年 3 月 30 日
AWSWAFConsoleReadOnlyAccess 此策略 Amazon WAF 允许您在集成服务中和集成服务中 Amazon WAF 代表您管理 Amazon 控制台 Amazon 资源和其他资源。 IAM 控制台中的详细信息： AWSWAFConsoleReadOnlyAccess 。	扩展了权限，可以向可以保护的资源类型添加 Amazon App Runner 服务 Amazon WAF。	2023 年 3 月 30 日
AWSWAFFullAccess 此策略 Amazon WAF 允许您在集成服务中 Amazon WAF 和集成服务中代表您管理 Amazon 资源。 IAM 控制台中的详细信息： AWSWAFFullAccess 。	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中 Amazon WAF。	2022 年 8 月 25 日
AWSWAFReadOnlyAccess	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中 Amazon WAF。	2022 年 8 月 25 日

策略	变更描述	日期
此策略Amazon WAF允许您在集成服务中Amazon WAF和集成服务中代表您管理Amazon资源。 IAM 控制台中的详细信息：AWSWAFReadOnlyAccess。		
AWSWAFConsoleFullAccess 此策略Amazon WAF允许您在集成服务中和集成服务中Amazon WAF代表您管理Amazon控制台Amazon资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleFullAccess。	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中Amazon WAF。	2022 年 8 月 25 日
AWSWAFConsoleReadOnlyAccess 此策略Amazon WAF允许您在集成服务中和集成服务中Amazon WAF代表您管理Amazon控制台Amazon资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleReadOnlyAccess。	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中Amazon WAF。	2022 年 8 月 25 日
AWSWAFFullAccess 此策略Amazon WAF允许您在集成服务中Amazon WAF和集成服务中代表您管理Amazon资源。 IAM 控制台中的详细信息：AWSWAFFullAccess。	更正了 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs 的日志传输 此更改解决了在日志配置期间发生的访问被拒绝的错误。有关记录 Web ACL 流量的信息，请参阅记录 Web ACL 流量 (p. 180)。	2022 年 1 月 11 日
AWSWAFConsoleFullAccess 此策略Amazon WAF允许您在集成服务中和集成服务中Amazon WAF代表您管理Amazon控制台Amazon资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleFullAccess。	更正了 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs 的日志传输 此更改解决了在日志配置期间发生的访问错误。有关记录 Web ACL 流量的信息，请参阅记录 Web ACL 流量 (p. 180)。	2022 年 1 月 11 日
AWSWAFFullAccess 此策略Amazon WAF允许您在集成服务中Amazon WAF和集成服务中代表您管理Amazon资源。 IAM 控制台中的详细信息：AWSWAFFullAccess。	为扩展日志选项添加了新权限。 此更改允许Amazon WAF访问 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs。有关记录 Web ACL 流量的信息，请参阅记录 Web ACL 流量 (p. 180)。	2021 年 8 月 15 日

策略	变更描述	日期
AWSWAFConsoleFullAccess 此策略Amazon WAF允许您在集成服务中和集成服务中Amazon WAF代表您管理Amazon控制台Amazon资源和其他资源。 IAM 控制台中的详细信息： AWSWAFConsoleFullAccess 。	为扩展日志选项添加了新权限。 此更改允许Amazon WAF访问 Amazon Simple Storage Service (Amazon S3) 和 Amazon CloudWatch Logs。有关记录 Web ACL 流量的信息，请参阅 记录 Web ACL 流量 (p. 180) 。	2021 年 8 月 15 日
Amazon WAF 已开启跟踪更改	Amazon WAF 为其 Amazon 托管策略开启了跟踪更改。	2021-3-01

对 Amazon WAF 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Amazon WAF 和 IAM 时可能遇到的常见问题。

主题

- [我无权在 Amazon WAF 中执行操作 \(p. 225\)](#)
- [我无权执行 iam : PassRole \(p. 225\)](#)
- [我希望允许我的 Amazon Web Services 账户以外的人访问我的 Amazon WAF 资源 \(p. 226\)](#)

我无权在 Amazon WAF 中执行操作

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 wafv2:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
wafv2:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 wafv2:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon WAF。

有些 Amazon Web Services 允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon WAF 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我希望允许我的 Amazon Web Services 账户以外的人访问我的 Amazon WAF 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon WAF 是否支持这些功能，请参阅 [Amazon WAF 如何与 IAM 协同工作 \(p. 213\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的[为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方 Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的 Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的[为经过外部身份验证的用户（联合身份验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的 [IAM 角色与基于资源的策略有何不同](#)。

将服务相关角色用于 Amazon WAF

Amazon WAF 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 Amazon WAF 直接相关。服务相关角色由 Amazon WAF 预定义，并包含该服务代表您调用其他 Amazon 服务所需的一切权限。

服务相关角色使 Amazon WAF 的设置更轻松，因为您不必手动添加必要的权限。Amazon WAF 定义其服务相关角色的权限，除非另行定义，否则仅 Amazon WAF 可以代入其角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这将保护您的 Amazon WAF 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅[使用 IAM 的 Amazon 服务](#)并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

Amazon WAF 的服务相关角色权限

Amazon WAF 使用服务相关角色 `AWSServiceRoleForWAFV2Logging`。

Amazon WAF 使用此服务相关角色将日志写入 Amazon Kinesis Data Firehose。仅当您在 Amazon WAF 中启用日志记录时，才会使用此角色。有关更多信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)：

`AWSServiceRoleForWAFV2Logging` 服务相关角色信任 `wafv2.amazonaws.com` 服务来代入角色。

角色的权限策略允许 Amazon WAF 对指定的资源完成以下操作：

- 操作：`firehose:PutRecord`以及名称以“aws-waf-logs-”开头的 `Amazfirehose:PutRecordBatch` on Kinesis Data Firehose 数据流资源。例如，`aws-waf-logs-us-east-2-analytics`。

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](#)。

为 Amazon WAF 创建服务相关角色

无需手动创建服务相关角色。如果您在 Amazon Web Services Management Console 中启用 Amazon WAF 日志记录，或者在 Amazon WAF CLI 或 Amazon WAF API 中发出 `PutLoggingConfiguration` 请求，Amazon WAF 会为您创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

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。当您启用 Amazon WAF 日志记录时，Amazon WAF 再次为您创建服务相关角色。

为 Amazon WAF 编辑服务相关角色

Amazon WAF 不允许您编辑 `AWSServiceRoleForWAFV2Logging` 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。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 Amazon WAF 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，您必须先清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 Amazon WAF 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。

删除 `AWSServiceRoleForWAFV2Logging` 所用的 Amazon WAF 资源

1. 在 Amazon WAF 控制台中，删除所有 Web ACL 的日志记录。有关更多信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)：
2. 使用 API 或 CLI，为已启用日志记录的每个 Web ACL 提交 `DeleteLoggingConfiguration` 请求。有关更多信息，请参阅[Amazon WAF API 参考](#)。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 `AWSServiceRoleForWAFV2Logging` 服务相关角色。有关更多信息，请参阅 IAM 用户指南的[删除服务相关角色](#)。

Amazon WAF 服务相关角色的受支持区域

Amazon WAF 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 WAF 终端节点和配额](#)。

Amazon WAF 中的日志记录和监控

监控是保持 Amazon WAF 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。应从 Amazon 解决方案的所有部分收集监控数据，以便更轻松地调试出现的多点故障。Amazon 提供了多种工具来监视 Amazon WAF 资源并对潜在的事件做出响应：

亚马逊 CloudWatch 警报

使用 CloudWatch 警报，可以观看单个指标在指定时间段内的变化。如果指标超过给定阈值，CloudWatch 会向 Amazon SNS 主题或 Amazon Auto Scaling 策略发送通知。有关更多信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)：

Amazon CloudTrail 日志

CloudTrail 提供了用户、角色或 Amazon 服务在中所执行操作的记录 Amazon WAF。通过使用收集的信息 CloudTrail，您可以确定向发出了什么请求 Amazon WAF、发出请求的 IP 地址、请求的发出时间以及其他详细信息。有关更多信息，请参阅[使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)：

Amazon WAF Web ACL 流量记录

Amazon WAF 为您的 Web ACL 分析的流量提供日志记录。这些日志包含从受保护 Amazon 资源 Amazon WAF 收到请求的时间、请求的详细信息以及请求所匹配的规则的操作设置等。有关更多信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)：

Amazon WAF 的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审核员将评估 Amazon WAF 的安全性和合规性，例如 SOC、PCI、FedRAMP、HIPAA 和其他计划。

有关特定合规性计划范围内的 Amazon 服务的列表，请参阅[合规性计划范围内的 Amazon 服务](#)。有关一般信息，请参阅[Amazon 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[下载 Amazon Artifact 中的报告](#)。

您在使用 Amazon WAF 时的合规性责任由您数据的敏感性、您组织的合规性目标以及适用的法律法规决定。如果您对 Amazon WAF 的使用需遵守 HIPAA、PCI 或 FedRAMP 等标准，Amazon 提供了以下实用资源：

- [《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 上部署基于安全性和合规性的基准环境的步骤。
- [Amazon Web Services 上的 HIPAA 安全性和合规性架构设计](#) — 此技术白paper 介绍了公司 Amazon 如何使用创建符合 HIPAA 标准的应用程序。
- [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](#) – 此 Amazon 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 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。
- [Amazon Well-Architected 的框架](#) — Amazon Well-Architected 的框架可帮助您构建安全的云应用程序。

Amazon WAF 中的故障恢复能力

Amazon 全球基础设施围绕 Amazon Web Services 区域和可用区构建。Amazon Web Services 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。

有关 Amazon Web Services 区域 和可用区的更多信息，请参阅 [Amazon 全球基础设施](#)。

Amazon WAF 中的基础设施安全性

作为一项托管服务 Amazon WAF，由 [Amazon Web Services：安全流程概述中所述的 Amazon 全球网络安全程序提供](#) 保护。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon WAF。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 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，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [Amazon Security Token Service](#) (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon WAF 配额

Note

这是最新版本的 Amazon WAF。有关“Amazon WAF 经典”，请参阅 [Amazon WAF Classic \(p. 238\)](#)。

Amazon WAF 受以下配额（以前称为限制）所限。这些配额与提供了 Amazon WAF 的所有区域的配额相同。每个区域分别受这些配额的约束。配额不会跨区域累积。

Amazon WAF 对每个账户可以具有的最大实体数施加了默认配额。您可以 [请求提高](#) 这些配额。

资源	每个区域每个账户的默认配额
网络 ACL 的最大数量	100
最大规则组数	100
每个 Web ACL 的最大 Web ACL 容量单位 (WCU)	1500
每个规则组的最大 WCU	1500
最大 IP 集数	100
每个 Web ACL 每秒的最大请求数量	25000
每个 Web ACL 或规则组的最大自定义请求标头数	100
每个 Web ACL 或规则组的自定义响应标头的最大数量	100
每个 Web ACL 或规则组的自定义响应正文的最大数量	50

资源	每个区域每个账户的默认配额
每个 Web ACL 的最大 Amazon Logs CloudWatch 日志流数，用于将 Web ACL 流量记录到 CloudWatch 日志日志组	35

Amazon WAF 在 CloudFront 允许的最大每秒请求数 (RPS) 由 [《CloudFront 开发者指南》](#) 设置 CloudFront 和说明。

Amazon WAF 针对每个区域、每个账户对以下实体设置具有固定的配额。无法更改这些配额。

资源	每区域每账户的配额
每个规则组对 IP 集和正则表达式模式集的最大引用数	50
每个 Web ACL 对 IP 集、正则表达式模式集和规则组的最大引用数	50
每个 IP 集合的 CIDR 表示法中的 IP 地址的最大数量	10000
每个 Web ACL 基于速率的规则的最大数量	10
每个规则组基于速率的规则的最大数量	4
根据基于速率的规则，可以阻止的最长唯一 IP 地址数	10000
字符串匹配语句中的最大字符数	200
每个正则表达式模式中的最大字符数	200
每个正则表达式集合的唯一正则表达式模式的最大数量	10
正则表达式集合的最大数量	10
可以检查的 Web 请求正文的最大大小	8 KB
可为基于速率的规则定义的最小请求速率	100
每个规则语句的最大文本转换次数	3
单个自定义响应定义的最大自定义响应正文内容的最大大小	4 KB
单个自定义响应定义的最大自定义标头数	10
单个自定义请求定义的最大自定义标头数	10
单个规则组或单个 Web ACL 的所有响应正文内容的最大组合大小	50 KB

Amazon WAF 针对每个区域、每个账户对调用有以下固定配额。这些配额适用于通过任何可用方式（包括控制台、CLI、Amazon CloudFormation、REST API 和开发工具包）对服务的总调用次数。无法更改这些配额。

调用类型	每区域每账户的配额
调用 AssociateWebACL 的最大次数	每 2 秒一个请求
调用 DisassociateWebACL 的最大次数	每 2 秒一个请求

调用类型	每区域每账户的配额
调用 GetWebACLForResource 的最大次数	每秒一个请求
调用 ListResourcesForWebACL 的最大次数	每秒一个请求
对任何单个 Get 或 List 操作的最大调用次数 (如果未为其定义其他配额)	每秒五个请求
对任何单个 Create、Put 或 Update 操作的最大调用次数 (如果未为其定义其他配额)	每秒一个请求

将您的Amazon WAF经典资源迁移到Amazon WAF

本节提供将您的规则和 Web ACL 从 CAmazon WAF lassic 迁移到的指导Amazon WAF。Amazon WAF 于 2019 年 11 月发布。如果您使用 CAmazon WAF lassic 创建了规则和 Web ACL 等资源，则需要使用 CAmazon WAF lassic 来处理这些资源，或者将它们迁移到最新版本。

在开始迁移工作之前，请通读 [Amazon WAF \(p. 5\)](#) 熟悉 Amazon WAF。

主题

- [为什么要迁移到 Amazon WAF ? \(p. 232\)](#)
- [迁移的工作原理 \(p. 233\)](#)
- [迁移注意事项和限制 \(p. 233\)](#)
- [将 Web ACL 从Amazon WAF经典版迁移到Amazon WAF \(p. 234\)](#)

为什么要迁移到 Amazon WAF ?

与前一版本相比，Amazon WAF 的最新版本提供了许多改进，同时保留了您习惯的大多数概念和术语。

以下列表介绍 Amazon WAF 最新版本中的主要更改。在继续迁移之前，请花一些时间查看此列表并熟悉 Amazon WAF 指南的其余内容。

- Amazon的托管规则Amazon WAF — 现在可通过Amazon托管规则访问的规则组提供针对常见网络威胁的保护。这些规则组中的大多数都是免费包含的Amazon WAF。有关更多信息[Amazon托管规则规则组列表 \(p. 32\)](#)，请参阅博客文章《[宣布的Amazon托管规则](#)》[Amazon WAF](#)。
- 新Amazon WAF API — 新 API 允许您使用一组 API 配置所有Amazon WAF资源。为了区分区域和全球应用程序，新 API 包括一个 scope 设置。有关 API 的更多信息，请参阅 [AmazonWAFV2 操作](#)和 [AmazonWAFV2 数据类型](#)。

在 API、SDK、CLI 和Amazon CloudFormation Classic 中，CAmazon WAF lassic 保留其命名方案 Amazon WAF，在引用最新版本时添加了V2或v2，具体视上下文而定。

- 简化的服务配额 (限制) —Amazon WAF 现在允许每个 Web ACL 有更多规则，并允许您表达更长的正则表达式模式。有关更多信息，请参阅[Amazon WAF 配额 \(p. 230\)](#)：
- Web ACL 限制现在基于计算需求 ——Web ACL 限制现在以 Web ACL 容量单位 (WCU) 为基础。Amazon WAF根据运行规则所需的操作能力计算规则的 WCU。Web ACL 的 WCU 是 Web ACL 中所有规则和规则组的 WCU 之和。

有关 WCU 的一般信息，请参阅[Amazon WAF 的工作原理 \(p. 6\)](#)。有关每条规则的 WCU 使用情况的信息，请参阅[规则语句列表 \(p. 82\)](#)。

- 基于文档的规则编写-您现在可以以 JSON 格式编写和表达规则、规则组和 Web ACL。您不再需要使用单独的 API 调用来创建不同的条件，然后将条件与规则相关联。这极大地简化了编写和维护代码的方式。在

查看 Web ACL 时，您可以通过控制台访问 Web ACL 的 JSON 格式，方法是选择 Download web ACL as JSON (将 Web ACL 下载为 JSON)。创建自己的规则时，可以通过选择 Rule JSON editor (规则 JSON 编辑器) 来访问其 JSON 表示形式。

- 规则嵌套和完整的逻辑操作支持-您可以使用逻辑规则语句和使用嵌套来编写复杂的组合规则。您可以创建语句，如 [A AND NOT(B OR C)]。有关更多信息，请参阅[规则语句列表 \(p. 82\)](#)：
- IP 集的可变 CIDR 范围支持 — IP 集规范现在在 IP 范围中具有更大的灵活性。对于 IPv4，Amazon WAF 支持 /1 到 /32。对于 IPv6，Amazon WAF 支持 /1 到 /128。有关 IP 集的更多信息，请参阅[IP 集匹配规则语句 \(p. 91\)](#)。
- 可链接的文本转换 —Amazon WAF 可以在检查 Web 请求内容之前对其进行多次文本转换。有关更多信息，请参阅[文本转换 \(p. 107\)](#)：
- 改善了控制台体验-新Amazon WAF控制台具有可视化规则生成器和更直观的控制台设计。
- Firewall ManagerAmazon WAF 策略的扩展选项-在Amazon WAF Web ACL 的Firewall Manager 管理中，您现在可以创建一组先Amazon WAF处理的规则组和一组最后Amazon WAF处理的规则组。应用 Amazon WAF 策略后，本地账户所有者可以添加自己的规则组，供 Amazon WAF 在这两个组之间进行处理。有关Firewall ManagerAmazon WAF 策略的更多信息，请参阅[Amazon WAF 策略 \(p. 444\)](#)。
- Amazon CloudFormation支持所有规则语句类型 —Amazon WAFAmazon CloudFormation 支持Amazon WAF控制台和 API 支持的所有规则语句类型。此外，您可以轻松地将您以 JSON 格式编写的规则转换为 YAML 格式。

迁移的工作原理

自动迁移会延续您的大部分Amazon WAF经典 Web ACL 配置，剩下一些需要手动处理的事情。

以下列出了迁移 Web ACL 的概要步骤。

1. 自动迁移会读取与现有 Web ACL 相关的所有内容，而无需修改或删除 Amazon WAF classic 中的任何内容。它创建 Web ACL 及其相关资源的表示形式，与 Amazon WAF 兼容。它为新的 Web ACL 生成一个 Amazon CloudFormation模板并将其存储在 Amazon S3 存储桶。
2. 您可以将此模板部署到 Amazon CloudFormation 中，以便在 Amazon WAF 中重新创建 Web ACL 和相关资源。
3. 您可以查看 Web ACL 并手动完成迁移，同时确保您的新 Web ACL 充分利用最新 Amazon WAF 的功能。
4. 您可以手动将受保护的资源切换到新的 Web ACL。

迁移注意事项和限制

迁移不会延续你的所有设置，就像你在Amazon WAF Classic 中的设置一样。有些事物（如托管规则）不会在两个版本之间确切地映射。其他设置，例如 Web ACL 与受保护Amazon资源的关联，最初在新版本中处于禁用状态，因此您可以在准备就绪时添加它们。

以下列表介绍迁移的注意事项，并说明您可能要采取的任何应对步骤。使用此概览来规划迁移。稍后的详细迁移步骤将指导您完成建议的迁移步骤。

- 单一账户 — 您只能将任何账户的Amazon WAF经典资源迁移到同一账户的Amazon WAF资源。
- 托管规则 — 迁移不会带来Amazon Web Services Marketplace卖家的任何托管规则。某些 Amazon Web Services Marketplace 卖家对于 Amazon WAF 具有同等的托管规则，您可以再次订阅它们。在执行此操作之前，请查看最新版本提供的Amazon托管规则Amazon WAF。其中大多数对Amazon WAF用户是免费的。有关托管规则的信息，请参阅[托管规则组 \(p. 24\)](#)。
- Web ACL 关联 — 迁移不会导致 Web ACL 和受保护资源之间的任何关联。这是设计使然，目的是避免影响生产工作负载。验证所有内容都已正确迁移后，请将新的 Web ACL 与您的资源关联。

- 日志记录-默认情况下，已迁移的 Web ACL 的日志记录处于禁用状态。这是设计使然。当您准备好从 Amazon WAF Classic 切换到时启用日志记录 Amazon WAF。
- Amazon Firewall Manager 规则组-迁移不处理由 Firewall Manager 管理的规则组。您可以迁移由 Firewall Manager 管理的 Web ACL，但迁移不会带来规则组。与其为这些 Web ACL 使用迁移工具，不如在 Firewall Manager Amazon WAF 中为新的 ACL 重新创建策略。

Note

Firewall Manager 为 Amazon WAF Classic 管理的规则组是 Firewall Manager 规则组。对于新版本的 Amazon WAF，规则组是 Amazon WAF 规则组。在功能上，它们是一样的。

- Amazon WAF 安全自动化 — 不要尝试迁移任何 [Amazon WAF 安全自动化](#)。迁移不会转换自动化过程可能正在使用的 Lambda 函数。当新的 Amazon WAF Security Automations 解决方案可用且与最新 Amazon WAF 版本兼容时，请重新部署该解决方案。

将 Web ACL 从 Amazon WAF 经典版迁移到 Amazon WAF

要迁移 Web ACL 并切换到它，请执行自动迁移，然后完成一系列手动步骤。

主题

- [迁移 Web ACL：自动迁移 \(p. 234\)](#)
- [迁移 Web ACL：手动后续操作 \(p. 235\)](#)
- [迁移 Web ACL：其他注意事项 \(p. 236\)](#)
- [迁移 Web ACL：切换 \(p. 237\)](#)

迁移 Web ACL：自动迁移

自动将 Web ACL 配置从 Amazon WAF 经典版迁移到 Amazon WAF

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 选择“切换到 Amazon WAF 经典”并查看 Web ACL 的配置设置。记下这些设置，同时考虑到前一节 [迁移注意事项和限制 \(p. 233\)](#) 中介绍的注意事项和限制。
3. 在顶部的信息对话框中，找到以 Migrate Web ACL 开头的句子，然后选择迁移向导的链接。这将启动迁移向导。

如果您没有看到信息对话框，则可能是自启动 Amazon WAF Classic 主机以来就关闭了该对话框。在导航栏中，选择“切换到新”，Amazon WAF 然后选择“切换到 Amazon WAF 经典”，信息对话框应该会重新出现。

4. 选择要迁移的 Web ACL。
5. 对于迁移配置，请提供用于模板的 Amazon S3 存储桶。您需要为迁移 API 正确配置的 Amazon S3 存储桶来存储其生成的 Amazon CloudFormation 模板。
 - 如果存储桶已加密，则加密必须使用 Amazon S3 (SSE-S3) 密钥。迁移不支持使用 Amazon Key Management Service (SSE-KMS) 密钥。
 - 存储桶名称必须以 aws-waf-migration- 开头。例如，aws-waf-migration-my-web-acl。
 - 存储桶必须位于您要部署此模板的区域中。例如，对于中的 Web ACL us-west-2，您必须在中使用 Amazon S3 存储桶，us-west-2 并且必须将模板堆栈部署到 us-west-2。
6. 对于 S3 bucket policy (S3 存储桶策略)，我们建议选择 Auto apply the bucket policy required for migration (自动应用迁移所需的存储桶策略)。或者，如果您想自行管理存储桶，则必须手动应用以下存储桶策略：

- 对于全球亚马逊 CloudFront 应用程序 (waf) :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "apiv2migration.waf.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/*"
    }
  ]
}
```

- 对于区域 Amazon API Gateway 或 Application Load Balancer 应用程序 (waf-regional) :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "apiv2migration.waf-regional.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/*"
    }
  ]
}
```

7. 在 Choose how to handle rules that cannot be migrated (选择如何处理无法迁移的规则) 中, 选择排除无法迁移的规则或选择停止迁移。有关无法迁移的规则的信息, 请参阅[迁移注意事项和限制 \(p. 233\)](#)。
8. 选择下一步。
9. 对于创建 Amazon CloudFormation 模板, 验证您的设置, 然后选择开始创建 Amazon CloudFormation 模板以开始迁移过程。这可能需要几分钟时间, 具体取决于 Web ACL 的复杂性。
10. 在“创建并运行 Amazon CloudFormation 堆栈以完成迁移”中, 您可以选择前往 Amazon CloudFormation 控制台从模板创建堆栈, 创建新的 Web ACL 及其资源。为此, 请选择创建 Amazon CloudFormation 堆栈。

自动迁移过程完成后, 您可以继续执行手动后续步骤。请参阅[迁移 Web ACL : 手动后续操作 \(p. 235\)](#)。

迁移 Web ACL : 手动后续操作

自动迁移完成后, 请查看新创建的 Web ACL 并填入迁移过程未带入的组件。以下过程介绍迁移未处理的 Web ACL 管理的各个方面。有关列表, 请参阅[迁移注意事项和限制 \(p. 233\)](#)。

完成基本迁移 - 手动步骤

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机, [网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 控制台应自动使用 Amazon WAF 的最新版本。要验证这一点, 请在导航窗格中查看是否可以找到“切换到 Amazon WAF 经典”选项。如果您看到“切换到新版本”Amazon WAF, 请选择该选项以切换到最新版本。
3. 在导航窗格中, 选择 Web ACL。

4. 在 Web ACL 页面中，在创建新 Web ACL 的区域的列表中找到新的 Web ACL。选择 Web ACL 的名称以显示 Web ACL 的设置。
5. 根据您的之前的 Amazon WAF 经典 Web ACL 查看新 Web ACL 的所有设置。默认情况下，日志记录和受保护的资源关联处于禁用状态。您可以在准备好进行切换时启用这些功能。
6. 如果您的 Amazon WAF 经典 Web ACL 具有基于速率的规则和条件，则迁移时不会出现该条件。您可以在新的 Web ACL 中向规则添加条件。
 - a. 在 Web ACL 设置页面中，选择 Rules (规则) 选项卡。
 - b. 在列表中找到基于速率的规则，选择该规则，然后选择 Edit (编辑)。
 - c. 对于 Criteria to count request towards rate limit (将请求计入速率限制的标准)，选择 Only consider requests that match the criteria in a rule statement (仅考虑与规则语句中的标准匹配的请求)，然后提供附加标准。您可以使用任何可嵌套的规则语句（包括逻辑语句）添加标准。有关选择的信息，请参阅[规则语句列表 \(p. 82\)](#)。
7. 如果您的 Amazon WAF 经典 Web ACL 有托管规则组，则在迁移过程中不会包含规则组。您可以将托管规则组添加到新的 Web ACL 中。查看有关托管规则组的信息，包括新版本中可用的 Amazon 托管规则列表 Amazon WAF，请访问[托管规则组 \(p. 24\)](#)。要添加托管规则组，请执行以下操作：
 - a. 在 Web ACL 设置页面中，选择 Web ACL Rules (规则) 选项卡。
 - b. 选择 Add rules (添加规则)，然后选择 Add managed rule groups (添加托管规则组)。
 - c. 展开您选择的供应商的列表，然后选择要添加的规则组。对于 Amazon Web Services Marketplace 卖家，您可能需要订阅规则组。有关在 Web ACL 中使用托管规则组的更多信息，请参阅[托管规则组 \(p. 24\)](#)和[Web ACL 规则和规则组评估 \(p. 12\)](#)。

完成基本迁移过程后，我们建议您查看您的需求并考虑其他选项，以确保新配置尽可能高效并使用最新的可用安全选项。请参阅[迁移 Web ACL：其他注意事项 \(p. 236\)](#)。

迁移 Web ACL：其他注意事项

查看您的新 Web ACL，并考虑新 Amazon WAF 版本中提供的选项，以确保配置尽可能高效并使用最新的可用安全选项。

其他 Amazon 托管规则

考虑在 Web ACL 中实施额外的 Amazon 托管规则，以提高应用程序的安全状况。这些都包含 Amazon WAF 在内，不会产生额外的成本。Amazon 托管规则包含以下类型的规则组：

- 基准规则组针对各种常见威胁提供了一般保护，例如阻止已知错误输入进入应用程序并防止访问管理页面。
- 使用案例特定的规则组为许多不同的使用案例和环境提供增量保护。
- IP 信誉列表基于客户端的源 IP 提供威胁情报。

有关更多信息，请参阅[Amazon 的托管规则 Amazon WAF \(p. 32\)](#)：

规则优化和清理

重新访问旧规则，并考虑通过重写它们或删除过时的规则来优化它们。例如，如果您过去部署了 OWASP 十大 Web 应用程序漏洞、《[为使用 OWASP 十大 Web 应用程序漏洞做好准备](#)》Amazon WAF 和《[我们的新白皮书](#)》的技术 paper 文中的 Amazon CloudFormation 模板，则应考虑将其替换为 Amazon 托管规则。虽然文档中的概念仍然适用，可以帮助您编写自己的规则，但模板创建的规则已在很大程度上被 Amazon 托管规则所取代。

Amazon CloudWatch 指标和告警

重新访问您的亚马逊 CloudWatch 指标并根据需要设置警报。迁移不会带入 CloudWatch 警报，并且您的指标名称可能并不符合您需要。

与您的应用程序团队一起审核

与您的应用程序团队合作并检查安全状况。找出应用程序经常解析哪些字段，并添加规则以相应地清理输入。如果应用程序的业务逻辑无法处理边缘案例，请检查是否存在任何边缘案例，并添加规则以捕获这些案例。

规划切换

与您的应用程序团队一起规划切换的时间。从旧的 Web ACL 关联切换到新的 Web ACL 关联可能需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。在此期间，一些请求将由旧的 Web ACL 处理，而其他请求将由新的 Web ACL 处理。在整个交换过程中，您的资源将受到保护，但是在切换过程中，您可能会注意到请求处理中的不一致性。

准备好切换时，请按照[迁移 Web ACL：切换 \(p. 237\)](#)中的步骤操作。

迁移 Web ACL：切换

验证新的 Web ACL 设置后，就可以开始使用它来代替 Amazon WAF 传统的 Web ACL 了。

开始使用新的 Amazon WAF Web ACL

1. 按照[将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)中的指导，将 Amazon WAF Web ACL 与要保护的资源关联。这会自动断开资源与旧 Web ACL 的关联。

交换机的传播可能需要几秒钟到几分钟。在此期间，有些请求可能由旧的 Web ACL 处理，而另一些请求可能由新的 Web ACL 处理。在整个交换过程中，您的资源将受到保护，但是在交换完成之前，您可能会注意到请求处理中的不一致性。

2. 按照[记录 Web ACL 流量 \(p. 180\)](#)中的指导为新的 Web ACL 配置日志记录。
3. (可选) 如果您的 Amazon WAF 经典 Web ACL 不再与任何资源关联，请考虑将其完全从 Amazon WAF Classic 中删除。有关信息，请参阅[删除 Web ACL \(p. 291\)](#)。

Amazon WAF Classic

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon WAFClassic 是一种 Web 应用程序防火墙，可用于监控转发到 Amazon API Gateway API (Amazon) 的 HTTP 和 HTTPS 请求。CloudFront 或是 Application Load Balancer。Amazon WAFClassic 还让您控制对您的内容的访问。根据指定的条件 (如请求源自的 IP 地址或查询字符串的值)，API Gateway, CloudFront 或是使 Application Load Balancer 请求的内容或使用 HTTP 状态代码 403 (禁止) 来响应请求。你也可以配置 CloudFront 在请求被阻止时返回自定义错误页面。

主题

- [设置Amazon WAF经典 \(p. 238\)](#)
- [怎么样Amazon WAF经典作品 \(p. 240\)](#)
- [Amazon WAF经典定价 \(p. 242\)](#)
- [入Amazon WAF入 \(p. 242\)](#)
- [创建和配置 Web 访问控制列表 \(Web ACL\) \(p. 252\)](#)
- [使用Amazon WAF与结合使用的经典规则组Amazon Firewall Manager \(p. 295\)](#)
- [开始使用Amazon Firewall Manager启用Amazon WAF经典规则 \(p. 297\)](#)
- [教程：创建Amazon Firewall Manager具有分层规则的策略 \(p. 300\)](#)
- [记录 Web ACL 流量信息 \(p. 302\)](#)
- [列出根据基于速率的规则而阻止的 IP 地址 \(p. 306\)](#)
- [操作方法Amazon WAFClassic CloudFront 功能 \(p. 307\)](#)
- [Amazon WAF经典版中的安全性 \(p. 308\)](#)
- [Amazon WAF经典配额 \(p. 326\)](#)

设置Amazon WAF经典

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

本主题介绍一些初步步骤，例如创建用户帐户，以便您为使用Amazon WAF Classic 做好准备。您无需无需无需这些。您只需为使用的 Amazon 服务付费。

Note

如果您是新用户，请不要按照这些Amazon WAF Classic的设置步骤进行操作。Amazon WAF相反，请按照 [设置 \(p. 3\)](#) 中 Amazon WAF 的最新版本的对应步骤操作。

完成这些步骤后，请参阅[入Amazon WAF入 \(p. 242\)](#)继续开始使用Amazon WAF Classic。

Note

Amazon Shield Standard 包含在 Amazon WAF Classic 中，不需要额外设置。有关更多信息，请参阅 [Amazon Shield 的工作原理 \(p. 330\)](#)：

如果您使用 Amazon WAF Classic 或 Amazon Shield Advanced 首次使用，请完成本节中的步骤。

主题

- [注册一个 Amazon Web Services 账户 \(p. 3\)](#)
- [保护 IAM 用户 \(p. 3\)](#)
- [Download tools \(p. 239\)](#)

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) 来保护您的管理员用户。有关说明，请参阅 IAM 用户指南中的 [为 IAM 用户启用虚拟 MFA 设备 \(控制台\)](#)。

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](#)
- [基于 IAM 身份的策略示例](#)

Download tools

Amazon Web Services Management Console 包括 Amazon WAF Classic 控制台，但如果您想以编程方式访问 Amazon WAF Classic，请参阅以下内容：

- 如果您要调用 Amazon WAF API 而不必处理低级别详细信息（例如汇编原始 HTTP 请求），那么您可以使用 SAMzaDK。Amazon 开发工具包提供用于封装 Amazon WAF Classic 和其他 Amazon 服务的功能的函数和数据类型。要下载 Amazon 开发工具包，请参阅还包括先决条件和安装说明的适用页面：
 - [Java](#)

- [JavaScript](#)
- [.NET](#)
- [Node.js](#)
- [PHP](#)
- [Python](#)
- [Ruby](#)

有关开发工具Amazon包的完整列表，请参阅[用于Amazon Web Services 的工具](#)。

- [如果您正在使用Amazon未提供软件DAmazon WAF K。Amazon WAF](#)
- Amazon Command Line Interface(Amazon CLI) 支持Amazon WAF经典。利用 Amazon CLI，您可以从命令行控制多个 Amazon 服务并通过脚本自动执行这些服务。有关更多信息，请参阅[Amazon Command Line Interface](#)：
- Amazon Tools for Windows PowerShell支持Amazon WAF经典。有关更多信息，请参阅 [Amazon Tools for PowerShellCmdlet](#)。

怎么样Amazon WAF经典作品

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。

对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

你用Amazon WAF控制 API Gateway 的经典方式，亚马逊 CloudFront 或者应用 Application Load Balancer 响应 Web 请求。您首先需创建条件、规则和 Web 访问控制列表 (Web ACL)。您需要定义条件、将条件合并为规则并将规则合并为 Web ACL。

Note

您还可以使用Amazon WAFClassic Elastic Container Service (Amazon ECS) 容器中托管的应用程序。Amazon ECS 是一项高度可扩展的快速容器管理服务，它可轻松运行、停止和管理群集上的 Docker 容器。要使用此选项，您可以将 Amazon ECS 配置为使用Amazon WAFClassic 启用 Application Load Balancer，可以在您的服务中跨任务保护 HTTP/HTTPS（第 7 层）流量。有关更多信息，请参阅主题[服务负载均衡](#)中的Amazon Elastic Container Service 开发人员。

条件

条件定义您希望的基本特征Amazon WAF在 Web 请求中需要注意的 Classic:

- 可能是恶意的脚本。攻击者会嵌入可以利用 Web 应用程序漏洞的脚本。这称为跨站点脚本。
- 请求源自的 IP 地址或地址范围。
- 请求源自的国家/地区或地理位置。
- 请求的指定部分的长度 (如查询字符串)。
- 可能是恶意的 SQL 代码。攻击者会尝试通过在 Web 请求中嵌入恶意 SQL 代码从数据库提取数据。这称为 SQL 注入。
- 请求中出现的字符串，例如，在 User-Agent 标头中出现的值或是在查询字符串中出现的文本字符串。您还可以使用正则表达式 (regex) 指定这些字符串。

某些条件采用多个值。例如，您可以在 IP 条件中指定最多 10,000 个 IP 地址或 IP 地址范围。

规则

您可将条件合并为规则，以精确锁定要允许、阻止或计数的请求。Amazon WAFClassic 提供两种类型的规则：

常规规则

常规规则仅使用条件来锁定特定请求。例如，根据您发现的来自某个攻击者的最近请求，您可以创建一个规则，其中包含以下条件：

- 请求来自 192.0.2.44。
- 请求在 User-Agent 标头中包含值 BadBot。
- 请求表现为在查询字符串中包含类似 SQL 的代码。

当一个规则包括多个条件时，如本例所示，Amazon WAFClassic 查找符合所有条件的请求，也就是说，它AND是条件在一起。

将至少一个条件添加到常规规则。没有条件的常规规则无法匹配任何请求，因此永远不会触发规则的操作（允许、计数或阻止）。

基于速率的规则

基于速率的规则就像常规规则一样，具有额外的速率限制。基于速率的规则计算从满足规则条件的 IP 地址到达的请求。如果来自 IP 地址的请求在五分钟内超过速率限制，则该规则可能会触发操作。操作可能需要一两分钟的时间才能触发。

对于基于速率的规则而言，条件是可选的。如果未在基于速率的规则中添加任何条件，则速率限制适用于所有 IP 地址。如果将条件与速率限制组合在一起，则速率限制适用于与条件匹配的 IP 地址。

例如，基于您发现的来自某个攻击者的最近请求，您可以创建一个基于速率的规则，包含如下条件：

- 请求来自 192.0.2.44。
- 请求在 User-Agent 标头中包含值 BadBot。

在此基于速率的规则中，您还定义了一个速率限制。在本例中，假设您创建了速率限制 1000。当请求既符合上述两个条件又超过每 5 分钟 1000 个请求的速率限制时，将触发在 Web ACL 中定义的该规则的操作（阻止或计数）。

不符合这两个条件的请求不计入速率限制，也不受此规则的影响。

又如，假设您希望将请求限定为网站上特定页面的请求。为此，您可以向基于速率的规则中添加以下字符串匹配条件：

- Part of the request to filter on 是 URI。
- Match Type (匹配类型) 是 Starts with。
- Value to match 是 login。

还要将 RateLimit 指定为 1000。

通过向 Web ACL 中添加此基于速率的规则，您可以将请求限制在登录页面，而不影响网站其余部分。

Web ACL

在您将条件合并为规则之后，您可将规则合并为 Web ACL。在其中可定义每个规则的操作（允许、阻止或计数）以及默认操作：

每个规则的操作

当 Web 请求匹配一个规则中的所有条件时，Amazon WAFClassic 可以阻止请求，或是允许将请求转发到 API Gateway API，CloudFront 分配或应用程序负载均衡器。您可以指定所需的操作 Amazon WAF对每个规则执行 Classic。

Amazon WAFClassic 会按照规则列出的顺序，将请求与 Web ACL 中的规则进行比较。Amazon WAFClassic 随后执行与请求匹配的最后一个规则关联的操作。例如，如果某个 Web 请求与允许请求

的一个规则以及阻止请求的另一个规则匹配，Amazon WAFClassic 会根据先列出的规则允许或阻止该请求。

如果您希望先测试新规则，然后再开始使用它，则还可以配置Amazon WAFClassic (Classic) 可计数满足规则中所有条件的请求。与允许或阻止请求的规则一样，对请求进行计数的规则受其在 Web ACL 的规则列表中的位置的影响。例如，如果一个 Web 请求匹配允许请求的规则，同时又匹配另一个对请求进行计数的规则，那么如果允许请求的规则先列出，则不对请求进行计数。

默认操作

默认操作决定是否Amazon WAFClassic 允许或阻止不匹配 Web ACL 中任何规则中的所有条件的请求。例如，假设您创建一个 Web ACL，并仅添加您在前面定义的规则：

- 请求来自 192.0.2.44。
- 请求在 User-Agent 标头中包含值 BadBot。
- 请求表现为在查询字符串中包含恶意 SQL 代码。

如果某个请求不满足规则的所有三个条件，并且默认操作是否为ALLOW、Amazon WAFClassic 将请求转发到 API Gateway，CloudFront 或使用 Application Load Balancer，服务会使用请求的对象进行响应。

如果您向 Web ACL 中添加两个或更多规则，Amazon WAF仅当有请求不满足任何规则的所有条件时，Classic 才执行默认操作。例如，假设您添加另一个只包含一个条件的规则：

- 在 User-Agent 标头中包含值 BIGBadBot 的请求。

Amazon WAF仅当有请求既不满足第一个规则的所有三个条件，也不满足第二个规则的一个条件时，Classic 才执行默认操作。

在某些情况下，Amazon WAF可能会遇到内部错误，该错误会延迟对 Amazon API Gateway、Amazon 的响应。CloudFront 或有关允许还是阻止请求的 Application Load Balancer。在这些情况下，CloudFront 通常会允许请求或提供内容。API 网关和 Application Load Balancer 通常会拒绝请求，不提供内容。

Amazon WAF经典定价

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

与Amazon WAFClassic，您只需为您创建的 Web ACL 和规则以及为其中的 HTTP 请求数付费。Amazon WAFClassic 检查。有关更多信息，请参阅 [Amazon WAF经典定价](#)。

入Amazon WAF入

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

本教程展示如何使用Amazon WAF Classic 来执行以下任务：

- 设置Amazon WAF经典。
- 使用Amazon WAF经典控制台创建 Web 访问控制列表 (Web ACL)，并指定要用来筛选 Web 请求的条件。例如，您可以指定请求的来源 IP 地址以及请求中仅由攻击者使用的值。
- 向规则中添加条件。规则使您可以确定要阻止或允许的目标 Web 请求。Web 请求必须匹配规则中的所有条件，然后Amazon WAF Classic 会根据您指定的条件阻止或允许请求。
- 向 Web ACL 中添加规则。可以在其中指定基于添加到每个规则的条件阻止还是允许 Web 请求。
- 指定默认操作 (阻止或允许)。这是Amazon WAF Classic 在 Web 请求与您的任何规则均不匹配时采取的操作。
- 选择您希望Amazon WAF Classic 检查网络请求的亚马逊 CloudFront 发行版。本教程仅涵盖的步骤，但 Application Load Balancer 和 Amazon API Gateway API 的过程本质上是相同的。Amazon WAF经典版 CloudFront 适用于所有人Amazon Web Services 区域。Amazon WAF与 API Gateway 或 Application Load Balancer 一起使用的经典版本在[Amazon服务端点](#)列出的区域中可用。

Note

对于在本教程中创建的资源，Amazon 向您收取的费用通常少于每日 0.25 美元。当您完成本教程时，建议您删除资源以避免产生不必要的费用。

主题

- [步骤 1：设置Amazon WAF经典 \(p. 243\)](#)
- [步骤 2：创建 Web ACL \(p. 243\)](#)
- [步骤 3：创建 IP 匹配条件 \(p. 244\)](#)
- [步骤 4：创建地理匹配条件 \(p. 244\)](#)
- [步骤 5：创建字符串匹配条件 \(p. 245\)](#)
- [步骤 5A：创建正则表达式条件 \(可选\) \(p. 246\)](#)
- [步骤 6：创建 SQL 注入匹配条件 \(p. 247\)](#)
- [步骤 7：\(可选\) 创建其他条件 \(p. 248\)](#)
- [步骤 8：创建规则并添加条件 \(p. 248\)](#)
- [步骤 9：将规则添加 Web ACL \(p. 249\)](#)
- [步骤 10：清除资源 \(p. 250\)](#)

步骤 1：设置Amazon WAF经典

如果您尚未按照中的常规设置步骤操作[设置Amazon WAF经典 \(p. 238\)](#)，请立即执行此操作。

步骤 2：创建 Web ACL

Amazon WAFClassic 控制台指导您完成配置 CAamazon WAF lassic 根据指定的条件 (如请求源自的 IP 地址或请求中的值) 来阻止或允许 Web 请求。在此步骤中，您将创建一个 Web ACL。

创建 Web ACL

1. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。

如果您在导航窗格中看到“切换到Amazon WAF经典”，请将其选中。

2. 如果这是您第一次使用“Amazon WAF经典”，请选择“转到Amazon WAF经典”，然后选择“配置 Web ACL”。

如果您之前使用过 Amazon WAF 经典版，请在导航窗格中选择 Web ACL，然后选择创建 Web ACL。

- 在 Name web ACL (命名 web ACL) 页面上，对于 Web ACL name (Web ACL 名称)，输入一个名称。

Note

Web ACL 在创建之后无法更改名称。

- 对于 CloudWatch metric name (&CW; 指标名称)，输入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9)，且不能包含空格。

Note

Web ACL 在创建之后无法更改名称。

- 对于 Region (亚马逊云科技区域)，选择一个区域。如果要将此 Web ACL 与 CloudFront 分配相关联，请选择全局 (CloudFront)。
- 对于 Amazon resource to associate，选择要与您的 Web ACL 关联的资源，然后选择 Next。

步骤 3：创建 IP 匹配条件

IP 匹配条件指定请求的来源 IP 地址或 IP 地址范围。在此步骤中，您将创建一个 IP 匹配条件。在后面的步骤中，您会指定是允许还是阻止源自指定 IP 地址的请求。

Note

有关 IP 匹配条件的更多信息，请参阅[使用 IP 匹配条件 \(p. 258\)](#)。

创建 IP 匹配条件

- 在 Create conditions (创建条件) 页面上，对于 IP match conditions (IP 匹配条件)，选择 Create condition (创建条件)。
- 在 Create IP match condition (创建 IP 匹配条件) 对话框中，对于 Name (名称)，输入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 或以下特殊字符：_!@#%&*}.,/。
- 对于 Address (地址)，输入 192.0.2.0/24。此 IP 地址范围 (采用 CIDR 表示法指定) 包含从 192.0.2.0 到 192.0.2.255 的 IP 地址。(192.0.2.0/24 IP 地址范围保留供示例使用，因此不会有 Web 请求源自这些 IP 地址。)

Amazon WAFClassic 支持以下 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。Amazon WAFClassic 支持以下 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。(要指定一个 IP 地址，如 192.0.2.44，请输入 192.0.2.44/32。) 不支持其他范围。

有关 CIDR 表示法的更多信息，请参阅维基百科条目 [Classless Inter-Domain Routing](#)。

- 选择 Create (创建)。

步骤 4：创建地理匹配条件

地理匹配条件指定请求源自的一个或多个国家/地区。在此步骤中，您将创建一个地理匹配条件。在后面的步骤中，您会指定是允许还是阻止源自指定国家/地区的请求。

Note

有关地理匹配条件的更多信息，请参阅[使用地理匹配条件 \(p. 260\)](#)。

创建地理匹配条件

- 在 Create conditions 页面上，对于 Geo match conditions，选择 Create condition。

2. 在 Create geo match condition (创建地理匹配条件) 对话框中，对于 Name (名称)，输入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 或以下特殊字符：_!@#%&*},./。
3. 选择位置类型和国家/地区。目前，Location type (位置类型) 只能是 Country (国家/地区)。
4. 选择 Add location。
5. 选择 Create (创建)。

步骤 5：创建字符串匹配条件

字符串匹配条件标识您希望 Amazon WAF Classic 在请求中搜索的字符串，例如标头或查询字符串中的指定值。字符串通常由可打印 ASCII 字符组成，但您可以指定从十六进制 0x00 到 0xFF (十进制 0 到 255) 的任何字符。在此步骤中，您将创建一个字符串匹配条件。在后面的步骤中，您将指定是允许还是阻止包含指定字符串的请求。

Note

有关字符串匹配条件的更多信息，请参阅[使用字符串匹配条件 \(p. 270\)](#)。

创建字符串匹配条件

1. 在 Create conditions (创建条件) 页面上，对于 String and regex match conditions (字符串和正则表达式匹配条件)，选择 Create condition (创建条件)。
2. 在 Create string match condition (创建字符串匹配条件) 对话框中，输入下列值：

名称

输入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 或以下特殊字符：_!@#%&*},./。

类型

选择 String match。

Part of the request to filter on

选择您希望 Amazon WAF Classic 在其中检查指定字符串的 Web 请求中哪部分。

对于此示例，选择 Header。

Note

如果您选择 Body 作为要筛选的请求部分的值，Amazon WAF Classic 将仅检查前 8192 字节 (8 KB)，因为只会 CloudFront 转发前 8192 字节进行检查。要允许或阻止正文超过 8192 字节的请求，您可以创建大小约束条件。(Amazon WAF Classic 从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)：

Header (在“Part of the request to filter on”为“Header”时是必需的)

由于您要筛选的部分请求选择了标题，因此必须指定希望 Amazon WAF Classic 检查哪个标头。输入 User-Agent (用户代理)。(此值不区分大小写。)

Match type

选择指定字符串必须出现在 User-Agent 标头中的何处，例如，字符串开头、末尾还是其他什么地方。

在此示例中，选择“完全匹配”，这表示 Amazon WAF Classic 会检查 Web 请求中是否存在与您指定的值相同的标头值。

Transformation

为了避开 Amazon WAF Classic，攻击者在 Web 请求中使用不寻常的格式，例如，通过添加空格或对部分或全部请求进行 URL 编码。转换会通过删除空格、通过对请求进行 URL 解码或是通过执行可消除攻击者常用的许多不寻常格式的其他操作，将 Web 请求转换为更标准的格式。

您只能指定一个类型的文本转换。

对于此示例，选择 None。

Value is base64 encoded

当您在 Value to match (要匹配的值) 中输入的值已进行了 base64 编码时，选中此复选框。

对于此示例，不要选中此复选框。

Value to match

指定您希望 Amazon WAF Classic 在其中指定进行筛选的 Web 请求部分中搜索的值。

在此示例中，输入 BadBot。Amazon WAF Classic 将检查 Web 请求中的 User-Agent 标题以获取该值 BadBot。

Value to match 的最大长度是 50 个字符。如果您要指定 base64 编码值，您可以提供最多 50 个字符（编码前）。

3. 如果您希望 Amazon WAF Classic 检查 Web 请求中是否有多个值，例如包含的 User-Agent 标头 BadBot 和包含的查询字符串 BadParameter，则有两种选择：

- 如果您希望仅当 Web 请求同时包含两个值 (AND) 时才允许或阻止请求，则为每个值创建一个字符串匹配条件。
- 如果您希望在 Web 请求包含任意一个值或同时包含两个值 (OR) 时允许或阻止请求，则将两个值添加到同一个字符串匹配条件。

对于此示例，选择 Create。

步骤 5A：创建正则表达式条件（可选）

正则表达式条件是一种字符串匹配条件，其类似之处在于它标识了您希望 Amazon WAF Classic 在请求中搜索的字符串，例如标头或查询字符串中的指定值。主要区别是使用正则表达式 (regex) 来指定您希望 Amazon WAF Classic 搜索的字符串模式。在此步骤中，您将创建一个正则表达式匹配条件。在后面的步骤中，您会指定是允许还是阻止包含指定字符串的请求。

Note

有关正则表达式匹配条件的更多信息，请参阅 [使用正则表达式匹配条件 \(p. 275\)](#)。

创建正则表达式匹配条件

1. 在 Create conditions (创建条件) 页面上，对于 String match and regex conditions (字符串匹配和正则表达式条件)，选择 Create condition (创建条件)。
2. 在 Create string match condition (创建字符串匹配条件) 对话框中，输入下列值：

名称

输入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 或以下特殊字符：_!@#%&*},./。

类型

选择 Regex match。

Part of the request to filter on

选择您希望 Amazon WAF Classic 在其中检查指定字符串的 Web 请求中哪部分。

对于此示例，选择 Body。

Note

如果您选择 `Body` 作为要筛选的请求部分的值，CAmazon WAF classic 将仅检查前 8192 字节 (8 KB)，因为只会 CloudFront 转发前 8192 字节进行检查。要允许或阻止正文超过 8192 字节的请求，您可以创建大小约束条件。(Amazon WAFClassic 从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)：

Transformation

为了避开 Amazon WAF Classic，攻击者在 Web 请求中使用不寻常的格式，例如，通过添加空格或对部分或全部请求进行 URL 编码。转换会通过删除空格、通过对请求进行 URL 解码或是通过执行可消除攻击者常用的许多不寻常格式的其他操作，将 Web 请求转换为更标准的格式。

您只能指定一个类型的文本转换。

对于此示例，选择 `None`。

与请求匹配的正则表达式模式

选择 `Create regex pattern set`。

新模式集名称

输入名称，然后指定您希望 CAmazon WAF classic 搜索的正则表达式模式。

接下来，输入正则表达式 `I[a@] mAb[a@] dReques t`。Amazon WAFClassic 将检查 Web 请求中的 `User-Agent` 标题中的值：

- `iaMaBadRequest`
- `IamAB@dRequest`
- 我 @mABadRequest
- `I@mAB@dRequest`

3. 选择 `Create pattern set and add filter`。
4. 选择 `Create ( 创建 )`。

步骤 6：创建 SQL 注入匹配条件

SQL 注入匹配条件指定您希望 Amazon WAF Classic 检查恶意 SQL 代码的 Web 请求部分（例如，标头或查询字符串）。攻击者使用 SQL 查询从数据库中提取数据。在此步骤中，您将创建一个 SQL 注入匹配条件。在后面的步骤中，您会指定是允许还是阻止表现为包含恶意 SQL 代码的请求。

Note

有关字符串匹配条件的更多信息，请参阅[使用 SQL 注入匹配条件 \(p. 266\)](#)。

创建 SQL 注入匹配条件

1. 在 `Create conditions` 页面上，对于 `SQL injection match conditions`，选择 `Create condition`。
2. 在 `Create SQL injection match condition (创建 SQL 注入匹配条件)` 对话框中，输入下列值：

名称

输入名称。

Part of the request to filter on

选择您希望 Amazon WAF Classic 在其中检查恶意 SQL 代码的 Web 请求部分。

对于此示例，选择 `Query string`。

Note

如果您选择 Body 作为要筛选的请求部分的值，CAmazon WAF classic 将仅检查前 8192 字节 (8 KB)，因为只会 CloudFront 转发前 8192 字节进行检查。要允许或阻止正文超过 8192 字节的请求，您可以创建大小约束条件。(Amazon WAFClassic 从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)：

Transformation

对于此示例，选择 URL decode。

攻击者使用异常格式 (例如 URL 编码) 来绕过 Amazon WAF 经典格式。在 CAmazon WAF classic 检查请求之前，URL 解码选项消除了 Web 请求中的一些格式。

您只能指定一个类型的文本转换。

3. 选择 Create (创建)。
4. 选择 Next (下一步)。

步骤 7：(可选) 创建其他条件

Amazon WAF 经典版包括其他条件，包括以下条件：

- 大小约束条件-指定您希望 Amazon WAF Classic 检查长度的 Web 请求部分 (例如，标头或查询字符串)。有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)：
- 跨站点脚本匹配条件-指定您希望检查恶意脚本的 Web 请求中您希望 Amazon WAF 检查是否存在恶意脚本的部分。有关更多信息，请参阅[使用跨站点脚本匹配条件 \(p. 253\)](#)：

您可以选择现在创建这些条件，也可以跳到[步骤 8：创建规则并添加条件 \(p. 248\)](#)。

步骤 8：创建规则并添加条件

您可以创建规则来指定希望 Amazon WAF Classic 在 Web 请求中搜索的条件。如果您向规则添加多个条件，则 Web 请求必须与规则中的所有条件相匹配，Amazon WAFClassic 才能允许或阻止基于该规则的请求。

Note

有关规则的更多信息，请参阅[使用规则 \(p. 280\)](#)。

创建规则并添加条件

1. 在 Create rules 页面上，选择 Create rule。
2. 在 Create rule (创建规则) 对话框中，键入下列值：

名称

输入名称。

CloudWatch 指标名称

输入 Amazon WAF Classic 将创建并与规则关联的 CloudWatch 指标的名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9)，且不能包含空格。

Rule type

选择 Regular rule (常规规则) 或 Rate-based rule (基于速率的规则)。基于速率的规则与常规规则基本相同，但还考虑到任何五分钟时段来自标识的 IP 地址的请求数。有关这些规则类型的更多信息，请参阅[怎么样 Amazon WAF 经典作品 \(p. 240\)](#)。对于此示例，请选择 Regular rule。

Rate limit

对于基于速率的规则，请输入与规则条件匹配的 IP 地址在任何五分钟内允许的最大请求数。

3. 对于要添加到规则的第一个条件，指定以下设置：

- 根据 Web 请求与条件中的设置是否匹配，选择是让 CAmazon WAF classic 允许还是阻止请求。

对于此示例，选择 does。

- 选择您要添加到规则的条件的类型：IP 匹配集条件、字符串匹配集条件或 SQL 注入匹配集条件。

对于此示例，选择 originate from IP addresses in。

- 选择要添加到规则的条件。

对于此示例，选择您在前面的任务中创建的 IP 匹配条件。

4. 选择 Add condition (添加条件)。

5. 添加您之前创建的地理匹配条件。指定以下值：

- When a request does
- originate from a geographic location in
- 选择您的地理匹配条件。

6. 选择 Add another condition。

7. 添加您之前创建的字符串匹配条件。指定以下值：

- When a request does
- match at least one of the filters in the string match condition
- 选择您的字符串匹配条件。

8. 选择 Add condition (添加条件)。

9. 添加您之前创建的 SQL 注入匹配条件。指定以下值：

- When a request does
- match at least one of the filters in the SQL injection match condition
- 选择您的 SQL 注入匹配条件。

10. 选择 Add condition (添加条件)。

11. 添加您之前创建的大小约束条件。指定以下值：

- When a request does
- match at least one of the filters in the size constraint condition
- 选择您的大小约束条件。

12. 如果您创建任何其他条件 (如正则表达式条件)，以类似方式添加这些条件。

13. 选择 Create (创建)。

14. 对于 Default action，选择 Allow all requests that don't match any rules。

15. 选择 Review and create。

步骤 9：将规则添加 Web ACL

向 Web ACL 中添加规则时，您可指定以下设置：

- 您希望 Amazon WAF Classic 对符合规则中所有条件的 Web 请求执行的操作：允许、阻止请求或对请求计数。
- Web ACL 的默认操作。这是您希望 Amazon WAF Classic 对不符合规则中所有条件的 Web 请求执行的操作：允许或阻止请求。

Amazon WAFClassic 开始阻止符合以下所有条件（以及您可能添加的任何其他条件）的 CloudFront Web 请求：

- User-Agent 标头的值是 BadBot
- (如果您创建并添加了正则表达式条件) Body 的值是四个字符串中与模式 I[a@]mAB[a@]dRequest 匹配的任一个字符串
- 请求源自 192.0.2.0-192.0.2.255 范围中的 IP 地址
- 请求源自您在地理匹配条件中所选的国家/地区
- 请求表现为在查询字符串中包含恶意 SQL 代码

Amazon WAFClassic CloudFront 允许响应任何不符合所有这三个条件的请求。

步骤 10：清除资源

现在您已成功完成了教程。为了防止您的账户产生额外的 Amazon WAF Classic 费用，您希望清理创建的 Amazon WAF Classic 对象。或者，您可以更改配置以便与您确实要进行允许、阻止和计数的 Web 请求匹配。

Note

对于在本教程中创建的资源，Amazon 向您收取的费用通常少于每日 0.25 美元。完成后，建议您删除资源以防止产生不必要的费用。

删除 CAmazon WAF lassic 收费的对象

1. 取消您的 Web ACL 与您的 CloudFront 发行版的关联：
 - a. 登录 Amazon Web Services Management Console 并打开 Amazon WAF 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。

如果您在导航窗格中看到“切换到 Amazon WAF 经典”，请将其选中。
 - b. 选择要删除的 Web ACL 的名称。这将在右侧窗格中打开一个包含 Web ACL 详细信息的页面。
 - c. 在右窗格的“规则”选项卡上，使用此 Web ACL 部分转到 Amazon 资源。对于与 Web ACL 关联的 CloudFront 分配，请在“类型”列中选择 x。
2. 从规则中删除条件：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择在教程中创建的规则。
 - c. 选择 Edit rule。
 - d. 选择每个条件标题右侧的 x。
 - e. 选择 Update (更新)。
3. 从 Web ACL 中删除规则，然后删除 Web ACL：
 - a. 在导航窗格中，选择 Web ACL。
 - b. 选择您在教程中创建的 Web ACL 的名称。这将在右侧窗格中打开一个包含 Web ACL 详细信息的页面。
 - c. 在 Rules 选项卡上，选择 Edit web ACL。
 - d. 选择规则标题右侧的 x。
 - e. 选择 Actions，然后选择 Delete web ACL。
4. 删除规则：
 - a. 在导航窗格中，选择 Rules (规则)。

- b. 选择在教程中创建的规则。
- c. 选择 Delete (删除)。
- d. 在 Delete 对话框中，再次选择 Delete 以确认。

Amazon WAFClassic 不对条件收费，但如果您想完成清理，请执行以下步骤从条件中移除过滤器并删除条件。

删除筛选条件和条件

1. 删除 IP 匹配条件中的 IP 地址范围，然后删除 IP 匹配条件：
 - a. 在 Amazon WAF 经典控制台的导航窗格中，选择 IP 地址。
 - b. 选择在教程中创建的 IP 匹配条件。
 - c. 选中您添加的 IP 地址范围的复选框。
 - d. 选择 Delete IP address or range。
 - e. 在 IP match conditions 窗格中，选择 Delete。
 - f. 在 Delete 对话框中，再次选择 Delete 以确认。
2. 删除 SQL 注入匹配条件中的筛选条件，然后删除 SQL 注入匹配条件：
 - a. 在导航窗格中，选择 SQL injection。
 - b. 选择在教程中创建的 SQL 注入匹配条件。
 - c. 选中您添加的筛选条件的复选框。
 - d. 选择 Delete filter。
 - e. 在 SQL injection match conditions 窗格中，选择 Delete。
 - f. 在 Delete 对话框中，再次选择 Delete 以确认。
3. 删除字符串匹配条件中的筛选条件，然后删除字符串匹配条件：
 - a. 在导航窗格中，选择 String and regex matching。
 - b. 选择在教程中创建的字符串匹配条件。
 - c. 选中您添加的筛选条件的复选框。
 - d. 选择 Delete filter。
 - e. 在 String match conditions 窗格中，选择 Delete。
 - f. 在 Delete 对话框中，再次选择 Delete 以确认。
4. 如果您创建了一个，请删除正则表达式匹配条件中的筛选条件，然后删除正则表达式匹配条件：
 - a. 在导航窗格中，选择 String and regex matching。
 - b. 选择在教程中创建的正则表达式匹配条件。
 - c. 选中您添加的筛选条件的复选框。
 - d. 选择 Delete filter。
 - e. 在 Regex match conditions 窗格中，选择 Delete。
 - f. 在 Delete 对话框中，再次选择 Delete 以确认。
5. 删除大小约束条件中的筛选条件，然后删除大小约束条件：
 - a. 在导航窗格中，选择 Size constraints。
 - b. 选择在教程中创建的大小约束条件。
 - c. 选中您添加的筛选条件的复选框。
 - d. 选择 Delete filter。
 - e. 在 Size constraint conditions 窗格中，选择 Delete。
 - f. 在 Delete 对话框中，再次选择 Delete 以确认。

创建和配置 Web 访问控制列表 (Web ACL)

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

Web 访问控制列表 (Web ACL) 使您可以精细地控制您的亚马逊 API G (Amazon API Gateway) 的 Web 请求 CloudFront 分发或应 Application Load Balancer 响应。您可以允许或阻止以下类型的请求：

- 源自某个 IP 地址或 IP 地址范围
- 源自一个特定国家/地区或多个国家/地区
- 请求的特定部分中包含指定字符串或与正则表达式 (regex) 模式匹配
- 超过指定长度
- 似乎包含恶意 SQL 代码 (称为 SQL 注入)
- 似乎包含恶意脚本 (称为跨站点脚本)

您还可以对这些规则的任意组合进行测试，或阻止、统计不仅满足指定条件，还在任何 5 分钟周期内超过指定请求数的 Web 请求。

要选择希望允许或阻止访问您的内容的请求，请执行以下任务：

1. 为与您指定的任何条件都不匹配的 Web 请求选择默认操作 (允许或阻止)。有关更多信息，请参阅[确定 Web ACL 的默认操作 \(p. 287\)](#)。
2. 指定要用于允许或阻止请求的条件：
 - 要基于请求是否表现为包含恶意脚本允许或阻止请求，请创建跨站点脚本匹配条件。有关更多信息，请参阅[使用跨站点脚本匹配条件 \(p. 253\)](#)。
 - 要基于请求源自的 IP 地址允许或阻止请求，请创建 IP 匹配条件。有关更多信息，请参阅[使用 IP 匹配条件 \(p. 258\)](#)。
 - 要基于请求源自的国家/地区允许或阻止请求，请创建地理匹配条件。有关更多信息，请参阅[使用地理匹配条件 \(p. 260\)](#)。
 - 要基于请求是否超过指定长度允许或阻止请求，请创建大小约束条件。有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)。
 - 要基于请求是否表现为包含恶意 SQL 代码允许或阻止请求，请创建 SQL 注入匹配条件。有关更多信息，请参阅[使用 SQL 注入匹配条件 \(p. 266\)](#)。
 - 要基于出现在请求中的字符串允许或阻止请求，请创建字符串匹配条件。有关更多信息，请参阅[使用字符串匹配条件 \(p. 270\)](#)。
 - 要基于出现在请求中的正则表达式模式允许或阻止请求，请创建正则表达式匹配条件。有关更多信息，请参阅[使用正则表达式匹配条件 \(p. 275\)](#)。
3. 将条件添加到一个或多个规则。如果您将多个条件添加到同一个规则，则 Web 请求必须与所有条件匹配，Amazon WAF 这样，您可以根据规则允许或阻止任何请求。有关更多信息，请参阅[使用规则 \(p. 280\)](#)。(可选) 您可以使用基于速率的规则而不是常规规则来限制来自满足条件的任何 IP 地址的请求数。
4. 将规则添加到 Web ACL。对于每个规则，指定是否需要 Amazon WAFClassic (经典) 可基于添加到规则的条件允许或阻止请求。如果将多个规则添加到 Web ACL，则 Amazon WAFClassic 按规则在 Web ACL 中列出的顺序来评估规则。有关更多信息，请参阅[使用 Web ACL \(p. 286\)](#)。

添加新规则或更新现有规则时，最多可能需要一分钟这些更改才能显示并在 Web ACL 和资源中生效。

主题

- [使用条件 \(p. 253\)](#)
- [使用规则 \(p. 280\)](#)
- [使用 Web ACL \(p. 286\)](#)

使用条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

在希望允许或阻止请求时指定的条件。

- 要基于请求是否表现为包含恶意脚本允许或阻止请求，请创建跨站点脚本匹配条件。有关更多信息，请参阅[使用跨站点脚本匹配条件 \(p. 253\)](#)。
- 要基于请求源自的 IP 地址允许或阻止请求，请创建 IP 匹配条件。有关更多信息，请参阅[使用 IP 匹配条件 \(p. 258\)](#)。
- 要基于请求源自的国家/地区允许或阻止请求，请创建地理匹配条件。有关更多信息，请参阅[使用地理匹配条件 \(p. 260\)](#)。
- 要基于请求是否超过指定长度允许或阻止请求，请创建大小约束条件。有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)。
- 要基于请求是否表现为包含恶意 SQL 代码允许或阻止请求，请创建 SQL 注入匹配条件。有关更多信息，请参阅[使用 SQL 注入匹配条件 \(p. 266\)](#)。
- 要基于出现在请求中的字符串允许或阻止请求，请创建字符串匹配条件。有关更多信息，请参阅[使用字符串匹配条件 \(p. 270\)](#)。
- 要基于出现在请求中的正则表达式模式允许或阻止请求，请创建正则表达式匹配条件。有关更多信息，请参阅[使用正则表达式匹配条件 \(p. 275\)](#)。

主题

- [使用跨站点脚本匹配条件 \(p. 253\)](#)
- [使用 IP 匹配条件 \(p. 258\)](#)
- [使用地理匹配条件 \(p. 260\)](#)
- [使用大小约束条件 \(p. 262\)](#)
- [使用 SQL 注入匹配条件 \(p. 266\)](#)
- [使用字符串匹配条件 \(p. 270\)](#)
- [使用正则表达式匹配条件 \(p. 275\)](#)

使用跨站点脚本匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

攻击者有时会将脚本插入到 Web 请求中，以试图利用 Web 应用程序中的漏洞。您可以创建一个或多个跨站点脚本匹配条件，确定应对 Web 请求部分（如 URI 或查询字符串）。Amazon WAF检查是否有恶意脚本的经

脚本。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止表现为包含恶意脚本的请求。

主题

- [创建跨站点脚本匹配条件 \(p. 254\)](#)
- [创建或编辑跨站点脚本匹配条件时指定的值 \(p. 254\)](#)
- [在跨站点脚本匹配条件中添加和删除筛选条件 \(p. 257\)](#)
- [删除跨站点脚本匹配条件 \(p. 257\)](#)

创建跨站点脚本匹配条件

当您创建跨站点脚本匹配条件时，可以指定筛选条件。这些筛选条件指示您想要的 Web 请求部分。Amazon WAFClassic (经典) 可检查是否存在恶意脚本，如 URI 或查询字符串。您可以将多个筛选条件添加到跨站点脚本匹配条件，也可以为每个筛选条件创建单独条件。下面是每种配置影响的方式Amazon WAF经典行为：

- 每个跨站点脚本匹配条件多个筛选条件（推荐）— 将包含多个筛选条件的跨站点脚本匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求只能与跨站脚本匹配条件中的一个筛选条件匹配，Amazon WAFClassic 可根据该条件允许或阻止请求。

例如，假设您创建一个跨站点脚本匹配条件并且该条件包含两个筛选条件。一个过滤器指示Amazon WAF在 URI 中检查是否存在恶意脚本的 Classic，另一个指示Amazon WAF检查查询字符串的典型。Amazon WAF如果请求表现为包含恶意脚本，则经典允许或阻止请求或者在 URI 中要么在查询字符串中。

- 每个跨站点脚本匹配条件的筛选条件— 将单独的跨站点脚本匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求必须与所有条件匹配，Amazon WAF这样，您可以根据条件允许或阻止任何请求。

假设您创建两个条件，每个条件包含前面示例中的两个筛选条件中的一个。将这两个条件添加到同一个规则并将该规则添加到 Web ACL 时，Amazon WAF仅当 URI 和查询字符串都表现为包含恶意脚本时，Classic 才会允许或阻止请求。

Note

将跨站点脚本匹配条件添加到规则时，您还可以将配置。Amazon WAF经典允许或阻止网络请求不要似乎包含恶意脚本。

创建跨站点脚本匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。
如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。
2. 在导航窗格中，选择 Cross-site scripting。
3. 选择 Create condition (创建条件)。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑跨站点脚本匹配条件时指定的值 \(p. 254\)](#)。
5. 选择 Add another filter。
6. 如果要添加其他筛选条件，请重复步骤 4 和 5。
7. 添加完筛选条件后，选择 Create。

创建或编辑跨站点脚本匹配条件时指定的值

创建或更新跨站点脚本匹配条件时，需要指定以下值：

名称

跨站点脚本匹配条件的名称。

该名称只能包含字符 A-Z、a-z、0-9 和特殊字符：_! " # ' + * } , . /。条件的名称在创建后不可更改。

Part of the request to filter on

选择应对每个 Web 请求的部分。Amazon WAF 经典来检查恶意脚本：

标头

指定的请求标头，例如 User-Agent 或 Referer 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查询字符串

URL 中在 ? 字符之后出现的部分 (如果有)。

Note

对于跨站点脚本匹配条件，建议您选择：所有查询参数 (仅限值) 而不是查询字符串为了 Part of the request to filter on。

URI

例如，请求的 URI 路径，用于标识资源，/images/daily-ad.jpg。这包括 URI 的查询字符串或片段组件。想要了解有关信息，请参阅[统一资源标识符 \(URI\)：通用语法](#)。

除非指定了 Transformation (转换)，否则 URI 不会被标准化，并且会被检查，就像 Amazon 是作为请求的一部分从客户端收到它一样。Transformation (转换) 将按指定方式重新设置 URI 的格式。

Body

请求中包含要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据 (如表单数据) 的部分。

Note

如果选择 Body 对于的价值 Part of the request to filter on，Amazon WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。(Amazon WAF Classic 会从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)。

单一查询参数 (仅限值)

您已定义为查询字符串的一部分的任何参数。例如，如果 URL 为“www.xyz.com?UserName=abc&SalesRegion=seattle”，您可以向 UserName 或 SalesRegion 参数添加一个筛选条件。

如果您选择 Single query parameter (value only) (单一查询参数 (仅限值))，您还将指定 Query parameter name (查询参数名称)。这是查询字符串中您将检查的参数，如 UserName 或 SalesRegion。Query parameter name (查询参数名称) 的最大长度为 30 个字符。Query parameter name (查询参数名称) 不区分大小写。例如，如果您指定 UserName 作为 Query parameter name (查询参数名称)，这将匹配 UserName 的所有变体，如 username 和 UsERName。

所有查询参数 (仅限值)

与单一查询参数 (仅限值)，而不是检查单个参数的值，Amazon WAF Classic 检查查询字符串中的所有参数值是否可能存在恶意脚本。例如，如果 URL 是“www.xyz.com/USERNAME=ABC &

SalesRegion = 西雅图”，然后选择所有查询参数（仅限值）、Amazon WAF如果任一值，则经典将触发比赛UserName要么SalesRegion包含可能包含恶意脚本。

标头

如果你选择了标头为了Part of the request to filter on，则从常见标头列表中选择标头，或输入应选择标头的名称。Amazon WAF经典来检查恶意脚本。

Transformation

转换之前重新格式化 Web 请求Amazon WAFClassic 会检查请求。这可消除一些不寻常的格式，可防范攻击者在 Web 请求中使用它们以试图绕过。Amazon WAFClassic。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

None（无）

Amazon WAFClassic 在针对中的字符串检查 Web 请求之前，不会对它执行任何文本转换。Value to match.

Convert to lowercase

Amazon WAF将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

Amazon WAFClassic 将 HTML 编码的字符替换为未编码的字符：

- 将 " 替换为 &
- 将 替换为不间断空格
- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符
- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

规范化空格

Amazon WAFClassic 将以下字符替换为空格字符（十进制 32）：

- \f，换页符，十进制 12
- \t，制表符，十进制 9
- \n，换行符，十进制 10
- \r，回车符，十进制 13
- \v，垂直制表符，十进制 11
- 不间断空格，十进制 160

此外，此选项将多个空格替换为一个空格。

Simplify command line

对于包含操作系统命令行命令的请求，使用此选项可执行以下转换：

- 删除以下字符：\ " ' ^
- 删除以下字符之前的空格：/ (
- 将以下字符替换为空格：, ;
- 将多个空格替换为一个空格
- 将大写字母 (A-Z) 转换为小写字母 (a-z)

URL decode

解码 URL 编码的请求。

在跨站点脚本匹配条件中添加和删除筛选条件

您可以在跨站点脚本匹配条件中添加或删除筛选条件。要更改筛选条件，请添加一个新筛选条件并删除旧条件。

在跨站点脚本匹配条件中添加或删除筛选条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Cross-site scripting。
3. 选择要在其中添加或删除筛选条件的条件。
4. 要添加筛选条件，请执行以下步骤：
 - a. 选择 Add filter。
 - b. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑跨站点脚本匹配条件时指定的值 \(p. 254\)](#)。
 - c. 选择 Add (添加)。
5. 要删除筛选条件，请执行以下步骤：
 - a. 选择要删除的筛选条件。
 - b. 选择 Delete filter。

删除跨站点脚本匹配条件

如果要删除某个跨站点脚本匹配条件，则必须先删除该条件中的所有筛选条件，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除跨站点脚本匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Cross-site scripting。
3. 在 Cross-site scripting match conditions 窗格中，选择要删除的跨站点脚本匹配条件。
4. 在右窗格中，选择 Associated rules 选项卡。

如果使用此跨站点脚本匹配条件的规则的列表为空，请转到步骤 6。如果列表中包含任何规则，则记下这些规则，然后继续执行步骤 5。

5. 要从使用跨站点脚本匹配条件的规则中删除它，请执行以下步骤：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的跨站点脚本匹配条件的规则的名称。
 - c. 在右窗格中，选择要从规则中删除的跨站点脚本匹配条件，然后选择 Remove selected condition。
 - d. 对使用要删除的跨站点脚本匹配条件的所有其余规则重复步骤 b 和 c。
 - e. 在导航窗格中，选择 Cross-site scripting。
 - f. 在 Cross-site scripting match conditions 窗格中，选择要删除的跨站点脚本匹配条件。

6. 选择 Delete 删除所选条件。

使用 IP 匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要基于请求源自的 IP 地址允许或阻止 Web 请求，请创建一个或多个 IP 匹配条件。IP 匹配条件可列出请求源自的最多 10,000 个 IP 地址或 IP 地址范围。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止来自这些 IP 地址的请求。

主题

- [创建 IP 匹配条件 \(p. 258\)](#)
- [编辑 IP 匹配条件 \(p. 259\)](#)
- [删除 IP 匹配条件 \(p. 259\)](#)

创建 IP 匹配条件

如果要基于请求源自的 IP 地址允许某些 Web 请求并阻止其他请求，请为要允许的 IP 地址创建一个 IP 匹配条件，并为要阻止的 IP 地址创建另一个 IP 匹配条件。

Note

将 IP 匹配条件添加到规则时，您还可以对其进行配置。Amazon WAF经典允许或阻止网络请求不要源自您在条件中指定的 IP 地址。

创建 IP 匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 IP addresses。
3. 选择 Create condition (创建条件)。
4. 在 Name (名称) 字段中输入名称。

该名称只能包含字母数字字符 (A-Z、0-9) 以及以下特殊字符：_! " # \$ % & ' * + , - . / : ; [\] ^ _ { | } ~ 。条件的名称在创建后不可更改。

5. 选择正确的 IP 版本并使用 CIDR 表示法指定 IP 地址或 IP 地址范围。下面是一些示例：

- 要指定 IPv4 地址 192.0.2.44，请键入 192.0.2.44/32。
- 要指定 IPv6 地址 0:0:0:0:ffff:c000:22c，请键入 0:0:0:0:ffff:c000:22c/128。
- 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请键入 192.0.2.0/24。
- 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。

Amazon WAFClassic 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。Amazon WAF经典版支持 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。有关 CIDR 表示法的更多信息，请参阅维基百科条目[无类域间路由](#)。

6. 选择 Add another IP address or range。

7. 如果要添加其他 IP 地址或范围，请重复步骤 5 和 6。
8. 添加完值后，选择 Create IP match condition。

编辑 IP 匹配条件

您可以将 IP 地址范围添加到 IP 匹配条件或删除范围。要更改范围，请添加新范围并删除旧范围。

编辑 IP 匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 IP addresses。
3. 在 IP match conditions 窗格中，选择要编辑的 IP 匹配条件。
4. 添加 IP 地址范围：
 - a. 在右窗格中，选择 Add IP address or range。
 - b. 选择正确的 IP 版本并使用 CIDR 表示法输入 IP 地址范围。下面是一些示例：
 - 要指定 IPv4 地址 192.0.2.44，请输入 192.0.2.44/32。
 - 要指定 IPv6 地址 0:0:0:0:ffff:c000:22c，请输入 0:0:0:0:ffff:c000:22c/128。
 - 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请输入 192.0.2.0/24。
 - 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。

Amazon WAFClassic 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。Amazon WAF经典版支持 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。有关 CIDR 表示法的更多信息，请参阅维基百科条目[无类域间路由](#)。

- c. 要添加更多 IP 地址，请选择 Add another IP address (添加其他 IP 地址) 并输入值。
 - d. 选择 Add (添加)。
5. 删除 IP 地址或范围：
 - a. 在右窗格中，选择要删除的值。
 - b. 选择 Delete IP address or range。

删除 IP 匹配条件

如果要删除某个 IP 匹配条件，则必须先删除该条件中的所有 IP 地址和范围，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除 IP 匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 IP addresses。
3. 在 IP match conditions 窗格中，选择要删除的 IP 匹配条件。
4. 在右窗格中，选择 Rules 选项卡。

如果使用此 IP 匹配条件的规则的列表为空，请转到步骤 6。如果列表中包含任何规则，则记下这些规则，然后继续执行步骤 5。

5. 要从使用某个 IP 匹配条件的规则中删除该条件，请执行以下步骤：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的 IP 匹配条件的规则的名称。
 - c. 在右窗格中，选择要从规则中删除的 IP 匹配条件，然后选择 Remove selected condition。
 - d. 对使用要删除的 IP 匹配条件的所有其余规则重复步骤 b 和 c。
 - e. 在导航窗格中，选择 IP match conditions。
 - f. 在 IP match conditions 窗格中，选择要删除的 IP 匹配条件。
6. 选择 Delete 删除所选条件。

使用地理匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要基于请求源自的国家/地区允许或阻止 Web 请求，请创建一个或多个地理匹配条件。地理匹配条件列出了您的请求源自的国家/地区。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止来自这些国家/地区的请求。

您可以将地理匹配条件用于其他条件Amazon WAF构建复杂筛选的经典条件或规则。例如，如果您要阻止某些国家/地区，但仍然允许来自该国家/地区的特定 IP 地址，则可以创建包含地理匹配条件和 IP 匹配条件的规则。配置规则以阻止源自该国家/地区且与已批准的 IP 地址不匹配的请求。再举一个例子，如果您希望为特定国家/地区中的用户设置资源优先级，则可以在两个不同的基于速率的规则中包括地理匹配条件。为首选国家/地区中的用户设置较高的速率限制，并为所有其他用户设置较低的速率限制。

Note

如果使用 CloudFront 地理限制功能可阻止某个国家/地区访问您的内容，则会阻止来自该国家/地区的任何请求，并且不会将Amazon WAFClassic。因此，如果应基于地理位置以及其他请求允许或阻止请求，则Amazon WAF经典条件，你应该不使用 CloudFront 地理限制功能。您可以改为使用 Amazon WAF经典的地理匹配条件。

主题

- [创建地理匹配条件 \(p. 260\)](#)
- [编辑地理匹配条件 \(p. 261\)](#)
- [删除地理匹配条件 \(p. 261\)](#)

创建地理匹配条件

如果要基于请求源自的国家/地区允许某些 Web 请求并阻止其他请求，请为要允许的国家/地区创建一个地理匹配条件，并为要阻止的国家/地区创建另一个地理匹配条件。

Note

将地理匹配条件添加到规则时，您还可以对其进行配置。Amazon WAF经典允许或阻止网络请求不要源自您在条件中指定的国家/地区。

创建地理匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Geo match。
3. 选择 Create condition (创建条件)。
4. 在 Name (名称) 字段中输入名称。

该名称只能包含字母数字字符 (A-Z、0-9) 以及以下特殊字符：_! " # ' + * } , . / 。条件的名称在创建后不可更改。

5. 选择区域。
6. 选择位置类型和国家/地区。Location type (位置类型) 目前只能是 Country (国家/地区)。
7. 选择 Add location。
8. 选择 Create (创建) 。

编辑地理匹配条件

您可以向地理匹配条件中添加国家/地区或从地理匹配条件中删除国家/地区。

编辑地理匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Geo match。
3. 在 Geo match conditions 窗格中，选择要编辑的地理匹配条件。
4. 要添加国家/地区，请按照下列步骤操作：
 - a. 在右窗格中，选择 Add filter。
 - b. 选择位置类型和国家/地区。Location type (位置类型) 目前只能是 Country (国家/地区)。
 - c. 选择 Add (添加) 。
5. 要删除国家/地区，请按照下列步骤操作：
 - a. 在右窗格中，选择要删除的值。
 - b. 选择 Delete filter。

删除地理匹配条件

如果要删除某个地理匹配条件，则必须先删除该条件中的所有国家/地区，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除地理匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 从使用某个地理匹配条件的规则中删除该条件：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的地理匹配条件的规则的名称。
 - c. 在右窗格中，选择 Edit rule。

- d. 选择要删除的条件旁边的 X。
 - e. 选择 Update (更新)。
 - f. 对使用要删除的地理匹配条件的所有其余规则重复这些步骤。
3. 从要删除的条件中删除筛选条件：
 - a. 在导航窗格中，选择 Geo match。
 - b. 选择要删除的地理匹配条件的名称。
 - c. 在右窗格中，选中 Filter 旁边的复选框来选择所有筛选条件。
 - d. 选择 Delete filter。
4. 在导航窗格中，选择 Geo match。
5. 在 Geo match conditions 窗格中，选择要删除的地理匹配条件。
6. 选择 Delete 删除所选条件。

使用大小约束条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要基于请求指定部分的长度允许或阻止 Web 请求，请创建一个或多个大小约束条件。大小约束条件确定 Web 请求中您希望的部分。Amazon WAF经典来看，你想要的字节数Amazon WAF要查找的经典和运算符，如大于 (>) 或小于 (<)。例如，您可以使用大小约束条件来查找长度超过 100 个字节的查询字符串。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是基于这些设置允许还是阻止请求。

请注意，如果你配置Amazon WAFClassic (经典) 可检查请求正文，例如，通过在正文中搜索指定字符串，Amazon WAFClassic 只检查前 8192 个字节 (8 KB)。如果 Web 请求的请求正文不会超过 8192 个字节，则可以创建一个大小约束条件并阻止请求正文大于 8192 个字节的请求。

主题

- [创建大小约束条件 \(p. 262\)](#)
- [创建或编辑大小约束条件时指定的值 \(p. 263\)](#)
- [在大小约束条件中添加和删除筛选条件 \(p. 265\)](#)
- [删除大小约束条件 \(p. 266\)](#)

创建大小约束条件

创建大小约束条件时，需要指定筛选条件以确定应对的 Web 请求部分。Amazon WAF经典来评估长度。您可以将多个筛选条件添加到大小约束条件，也可以为每个筛选条件创建单独的条件。下面是每种配置影响的方式Amazon WAF经典行为：

- 每个大小约束条件的筛选条件— 将单独的大小约束条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求必须与所有条件匹配，Amazon WAF这样，您可以根据条件允许或阻止任何请求。

例如，假设您创建两个条件。一个条件与查询字符串大于 100 个字节的 Web 请求匹配。另一个条件与请求正文大于 1024 个字节的 Web 请求匹配。将这两个条件添加到同一个规则并将该规则添加到 Web ACL 时，Amazon WAF只有在两个条件都为真时，经典才允许或阻止请求。

- 每个大小约束条件有多个筛选条件数— 将包含多个筛选条件的大小约束条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求只需与大小约束条件中的一个筛选条件匹配，Amazon WAFClassic 可根据该条件允许或阻止请求。

假设您创建一个而不是两个条件，并且这一个条件包含与前面示例相同的两个筛选条件。Amazon WAF 如果查询字符串大于 100 个字节或请求正文大于 1024 个字节，则 Classic 会允许或阻止请求。

Note

将大小约束条件添加到规则时，您还可以将配置。Amazon WAF 经典允许或阻止网络请求不要匹配条件中的值。

创建大小约束条件

1. 登录到 Amazon Web Services Management Console 打开 Amazon WAF 控制台 <https://console.aws.amazon.com/wafv2/>。

如果您看到切换到 Amazon WAF Classic 在导航窗格中，选择它。

2. 在导航窗格中，选择 Size constraints。
3. 选择 Create condition (创建条件)。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑大小约束条件时指定的值 \(p. 263\)](#)。
5. 选择 Add another filter。
6. 如果要添加其他筛选条件，请重复步骤 4 和 5。
7. 添加完筛选器后，选择 Create size constraint condition。

创建或编辑大小约束条件时指定的值

创建或更新大小约束条件时，需要指定以下值：

名称

为大小约束条件输入名称。

该名称只能包含字母数字字符 (A-Z、0-9) 以及以下特殊字符：_! " # + *}, ./。条件的名称在创建后不可更改。

Part of the request to filter on

选择应对每个 Web 请求的部分：Amazon WAF 经典来评估长度：

标头

指定的请求标头，例如 User-Agent 或 Referer 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查询字符串

URL 中在 ? 字符之后出现的部分 (如果有)。

URI

例如，请求的 URI 路径，用于标识资源，/images/daily-ad.jpg。这包括 URI 的查询字符串或片段组件。想要了解有关信息，请参阅 [统一资源标识符 \(URI\)：通用语法](#)。

除非指定了 Transformation (转换)，否则 URI 不会被标准化，并且会被检查，就像 Amazon 是作为请求的一部分从客户端收到它一样。Transformation (转换) 将按指定方式重新设置 URI 的格式。

Body

请求中包含要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据 (如表单数据) 的部分。

单一查询参数 (仅限值)

您已定义为查询字符串的一部分的任何参数。例如, 如果 URL 为“www.xyz.com?UserName=abc&SalesRegion=seattle”, 您可以向 UserName 或 SalesRegion 参数添加一个筛选条件。

如果您选择 Single query parameter (value only) (单一查询参数 (仅限值)), 您还将指定 Query parameter name (查询参数名称)。这是查询字符串中您将检查的参数, 如 UserName。Query parameter name (查询参数名称) 的最大长度为 30 个字符。Query parameter name (查询参数名称) 不区分大小写。例如, 如果您指定 UserName 作为 Query parameter name (查询参数名称), 这将匹配 UserName 的所有变体, 如 username 和 UsERName。

所有查询参数 (仅限值)

与相似单一查询参数 (仅限值), 而不是检查单个参数的价值, Amazon WAFClassic 将检查查询字符串中所有参数的值, 以确定是否有大小约束条件。例如, 如果 URL 是“www.xyz.comUSERNAME=ABC & SalesRegion = 西雅图”, 然后选择所有查询参数 (仅限值)、Amazon WAFClassic 将触发一个匹配值, 如果任何一个UserName要么SalesRegion超过指定的大小。

Header (仅当“Part of the request to filter on”是“Header”时)

如果你选择了标头为了Part of the request to filter on, 则从常见标头列表中选择标头, 或键入应使用的标头的名称Amazon WAF经典来评估长度。

比较运算符

选择自己想要的方式Amazon WAFClassic (经典) 按照为指定的值评估 Web 请求中的查询字符串的长度。Size。

例如, 如果您选择大于为了比较运算符然后键入100为了Size、Amazon WAFClassic 评估 Web 请求中是否存在长度超过 100 个字节的查询字符串。

Size

输入应对应的长度 (以字节为单位) Amazon WAF应在查询字符串中监视的经典。

Note

如果选择 URI 作为 Part of the request to filter on 的值, 则 URI 中的 / 算作一个字符。例如, URI 路径/logo.jpg长度是 9 个字符。

Transformation

转换之前重新格式化 Web 请求Amazon WAFClassic 会评估请求中指定部分的长度。这可消除一些不寻常的格式, 可防范攻击者在 Web 请求中使用它们以试图绕过。Amazon WAFClassic。

Note

如果选择Body为了Part of the request to filter on, 你无法配置Amazon WAFClassic (经典) 执行转换, 因为只转发前 8192 个字节进行检查。但是, 您仍可以基于 HTTP 请求正文的大小来筛选流量并指定转换。None (无)。(Amazon WAFClassic 会从请求标头获取正文的长度。)

您只能指定一个类型的文本转换。

转换可以执行以下操作:

None (无)

Amazon WAF在检查长度之前, Classic 不会对 Web 请求执行任何文本转换。

Convert to lowercase

Amazon WAF将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

Amazon WAFClassic 将 HTML 编码的字符替换为未编码的字符：

- 将 " 替换为 &
- 将 替换为不间断空格
- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符
- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

规范化空格

Amazon WAFClassic 将以下字符替换为空格字符（十进制 32）：

- \f, 换页符, 十进制 12
- \t, 制表符, 十进制 9
- \n, 换行符, 十进制 10
- \r, 回车符, 十进制 13
- \v, 垂直制表符, 十进制 11
- 不间断空格, 十进制 160

此外, 此选项将多个空格替换为一个空格。

Simplify command line

对于包含操作系统命令行命令的请求, 使用此选项可执行以下转换：

- 删除以下字符：\ " ' ^
- 删除以下字符之前的空格：/ (
- 将以下字符替换为空格：, ;
- 将多个空格替换为一个空格
- 将大写字母 (A-Z) 转换为小写字母 (a-z)

URL decode

解码 URL 编码的请求。

在大小约束条件中添加和删除筛选条件

您可以在大小约束条件中添加或删除筛选条件。要更改筛选条件, 请添加一个新筛选条件并删除旧条件。

在大小约束条件中添加或删除筛选条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中, 选择它。

2. 在导航窗格中, 选择 Size constraint。
3. 选择要在其中添加或删除筛选条件的条件。
4. 要添加筛选条件, 请执行以下步骤：
 - a. 选择 Add filter。
 - b. 指定适用的筛选条件设置。有关更多信息, 请参阅 [创建或编辑大小约束条件时指定的值 \(p. 263\)](#)。

- c. 选择 Add (添加)。
5. 要删除筛选条件，请执行以下步骤：
 - a. 选择要删除的筛选条件。
 - b. 选择 Delete filter。

删除大小约束条件

如果要删除某个大小约束条件，需要先删除该条件中的所有筛选条件，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除大小约束条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Size constraints。
3. 在 Size constraint conditions 窗格中，选择要删除的大小限制条件。
4. 在右窗格中，选择 Associated rules 选项卡。

如果使用此大小约束条件的规则的列表为空，请转到步骤 6。如果列表中包含任何规则，则记下这些规则，然后继续执行步骤 5。

5. 要从使用某个大小约束条件的规则中将其删除，请执行以下步骤：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的大小约束条件的规则的名称。
 - c. 在右窗格中，选择要从规则中删除的大小约束条件，然后选择 Remove selected condition。
 - d. 对使用要删除的大小约束条件的所有其余规则重复步骤 b 和 c。
 - e. 在导航窗格中，选择 Size constraint。
 - f. 在 Size constraint conditions 窗格中，选择要删除的大小限制条件。
6. 选择 Delete 删除所选条件。

使用 SQL 注入匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

攻击者有时会将恶意 SQL 代码插入到 Web 请求中，以试图从数据库提取数据。要允许或阻止表现为包含恶意 SQL 代码的 Web 请求，请创建一个或多个 SQL 注入匹配条件。SQL 注入匹配条件确定应对 Web 请求部分 (如 URI 路径或查询字符串)。Amazon WAF经典检查。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止表现为包含恶意 SQL 代码的请求。

主题

- [创建 SQL 注入匹配条件 \(p. 267\)](#)
- [创建或编辑 SQL 注入匹配条件时指定的值 \(p. 267\)](#)
- [在 SQL 注入匹配条件中添加和删除筛选条件 \(p. 269\)](#)
- [删除 SQL 注入匹配条件 \(p. 270\)](#)

创建 SQL 注入匹配条件

创建 SQL 注入匹配条件时，需要指定筛选条件，它们指示应对 Web 请求的部分。Amazon WAFClassic (经典) 可检查是否存在恶意 SQL 代码，如 URI 或查询字符串。您可以将多个筛选条件添加到 SQL 注入匹配条件，也可以为每个筛选条件创建单独的条件。下面是每种配置影响的方式Amazon WAF经典行为：

- 每个 SQL 注入匹配条件多个过滤器（推荐）— 将包含多个筛选条件的 SQL 注入匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求只需与 SQL 注入匹配条件中的一个筛选条件匹配，Amazon WAFClassic 可根据该条件允许或阻止请求。

例如，假设您创建一个 SQL 注入匹配条件，并且该条件包含两个筛选条件。一个过滤器指示Amazon WAF在 URI 中检查是否存在恶意 SQL 代码的 Classic，另一个指示Amazon WAF检查查询字符串的典型。Amazon WAF如果请求表现为包含恶意 SQL 代码，则经典允许或阻止请求。或者在 URI 中要么在查询字符串中。

- 每个 SQL 注入匹配条件的筛选条件— 将单独的 SQL 注入匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求必须与所有条件匹配，Amazon WAF这样，您可以根据条件允许或阻止任何请求。

假设您创建两个条件，每个条件包含前面示例中的两个筛选条件中的一个。将这两个条件添加到同一个规则并将该规则添加到 Web ACL 时，Amazon WAF仅当 URI 和查询字符串都表现为包含恶意 SQL 代码时，Classic 才会允许或阻止请求。

Note

将 SQL 注入匹配条件添加到规则时，您还可以将配置。Amazon WAF经典允许或阻止网络请求不要似乎包含恶意 SQL 代码。

创建 SQL 注入匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 SQL injection。
3. 选择 Create condition (创建条件)。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑 SQL 注入匹配条件时指定的值 \(p. 267\)](#)。
5. 选择 Add another filter。
6. 如果要添加其他筛选条件，请重复步骤 4 和 5。
7. 添加完筛选器后，选择 Create。

创建或编辑 SQL 注入匹配条件时指定的值

创建或更新 SQL 注入匹配条件时，需要指定以下值：

名称

SQL 注入匹配条件的名称。

该名称只能包含字母数字字字字字字字字字 (A-Z、0-9) 以及以下特殊字符：_! " # \$ % & ' () * + , - . / : ; [\] ^ _ { | } ~ 。条件的名称在创建后不可更改。

Part of the request to filter on

选择应对每个 Web 请求的部分。Amazon WAF检查是否有恶意 SQL 代码的经典：

标头

指定的请求标头，例如 User-Agent 或 Referer 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查询字符串

URL 中在 ? 字符之后出现的部分 (如果有)。

Note

对于 SQL 注入匹配条件，建议您选择所有查询参数 (仅限值) 而不是查询字符串作为 Part of the request to filter on。

URI

例如，请求的 URI 路径，用于标识资源，/images/daily-ad.jpg。这包括 URI 的查询字符串或片段组件。想要了解有关信息，请参阅[统一资源标识符 \(URI\)：通用语法](#)。

除非指定了 Transformation (转换)，否则 URI 不会被标准化，并且会被检查，就像 Amazon 是作为请求的一部分从客户端收到它一样。Transformation (转换) 将按指定方式重新设置 URI 的格式。

Body

请求中包含要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据 (如表单数据) 的部分。

Note

如果选择 Body 作为 Part of the request to filter on，Amazon WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。(Amazon WAF Classic 会从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)。

单一查询参数 (仅限值)

您已定义为查询字符串的一部分的任何参数。例如，如果 URL 为 "www.xyz.com?UserName=abc&SalesRegion=seattle"，您可以向 UserName 或 SalesRegion 参数添加一个筛选条件。

如果您选择 Single query parameter (value only) (单一查询参数 (仅限值))，您还将指定 Query parameter name (查询参数名称)。这是查询字符串中您将检查的参数，如 UserName 或 SalesRegion。Query parameter name (查询参数名称) 的最大长度为 30 个字符。Query parameter name (查询参数名称) 不区分大小写。例如，如果您指定 UserName 作为 Query parameter name (查询参数名称)，这将匹配 UserName 的所有变体，如 username 和 UsERName。

所有查询参数 (仅限值)

与相似单一查询参数 (仅限值)，而不是检查单个参数的价值，Amazon WAF Classic 将检查查询字符串中所有参数的值，以确定是否有恶意 SQL 代码。例如，如果 URL 是 "www.xyz.comUSERNAME=ABC & SalesRegion = 西雅图"，然后选择所有查询参数 (仅限值)、Amazon WAF 如果两者的值之一，Classic 将触发匹配 UserName 要么 SalesRegion 包含可能包含恶意 SQL 代码。

标头

如果你选择了标头作为 Part of the request to filter on，则从常见标头列表中选择标头，或输入应选择标头的名称。Amazon WAF 检查是否有恶意 SQL 代码的经典版本。

Transformation

转换之前重新格式化 Web 请求 Amazon WAF Classic 会检查请求。这可消除一些不寻常的格式，可防范攻击者在 Web 请求中使用它们以试图绕过。Amazon WAF Classic。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

None (无)

Amazon WAFClassic 在针对中的字符串检查 Web 请求之前，不会对它执行任何文本转换。Value to match.

Convert to lowercase

Amazon WAF将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

Amazon WAFClassic 将 HTML 编码的字符替换为未编码的字符：

- 将 " 替换为 &
- 将 替换为不间断空格
- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符
- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

规范化空格

Amazon WAFClassic 将以下字符替换为空格字符 (十进制 32)：

- \f, 换页符, 十进制 12
- \t, 制表符, 十进制 9
- \n, 换行符, 十进制 10
- \r, 回车符, 十进制 13
- \v, 垂直制表符, 十进制 11
- 不间断空格, 十进制 160

此外，此选项将多个空格替换为一个空格。

Simplify command line

对于包含操作系统命令行命令的请求，使用此选项可执行以下转换：

- 删除以下字符：\ " ' ^
- 删除以下字符之前的空格：/ (
- 将以下字符替换为空格：, ;
- 将多个空格替换为一个空格
- 将大写字母 (A-Z) 转换为小写字母 (a-z)

URL decode

解码 URL 编码的请求。

在 SQL 注入匹配条件中添加和删除筛选条件

您可以在 SQL 注入匹配条件中添加或删除筛选条件。要更改筛选条件，请添加一个新筛选条件并删除旧条件。

在 SQL 注入匹配条件中添加或删除筛选条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 SQL injection。
3. 选择要在其中添加或删除筛选条件的条件。
4. 要添加筛选条件，请执行以下步骤：
 - a. 选择 Add filter。
 - b. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑 SQL 注入匹配条件时指定的值 \(p. 267\)](#)。
 - c. 选择 Add (添加)。
5. 要删除筛选条件，请执行以下步骤：
 - a. 选择要删除的筛选条件。
 - b. 选择 Delete filter。

删除 SQL 注入匹配条件

如果要删除某个 SQL 注入匹配条件，需要先删除该条件中的所有筛选条件，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除 SQL 注入匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 SQL injection。
3. 在 SQL injection match conditions 窗格中，选择要删除的 SQL 注入匹配条件。
4. 在右窗格中，选择 Associated rules 选项卡。

如果使用此 SQL 注入匹配条件的规则的列表为空，请转到步骤 6。如果列表中包含任何规则，则记下这些规则，然后继续执行步骤 5。

5. 要从使用某个 SQL 注入匹配条件的规则中将其删除，请执行以下步骤：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的 SQL 注入匹配条件的规则的名称。
 - c. 在右窗格中，选择要从规则中删除的 SQL 注入匹配条件，然后选择 Remove selected condition。
 - d. 对使用要删除的 SQL 注入匹配条件的所有其余规则重复步骤 b 和 c。
 - e. 在导航窗格中，选择 SQL injection。
 - f. 在 SQL injection match conditions 窗格中，选择要删除的 SQL 注入匹配条件。
6. 选择 Delete 删除所选条件。

使用字符串匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要基于出现在请求中的字符串允许或阻止 Web 请求，请创建一个或多个字符串匹配条件。字符串匹配条件确定要搜索的字符串，以及应搜索的 Web 请求部分 (如指定标头或查询字符串)。Amazon WAF经典来检查字符串。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止包含该字符串的请求。

主题

- [创建字符串匹配条件 \(p. 271\)](#)
- [创建或编辑字符串匹配条件时指定的值 \(p. 271\)](#)
- [在字符串匹配条件中添加和删除筛选条件 \(p. 274\)](#)
- [删除字符串匹配条件 \(p. 275\)](#)

创建字符串匹配条件

创建字符串匹配条件时，需要指定筛选条件以确定要搜索的字符串以及应对 Web 请求的部分。Amazon WAFClassic (经典) 可检查该字符串，如 URI 或查询字符串。您可以将多个筛选条件添加到字符串匹配条件，也可以为每个筛选条件创建单独的字符串匹配条件。下面是每种配置影响的方式Amazon WAF经典行为：

- 每个字符串匹配条件一个筛选— 将单独的字符串匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求必须与所有条件匹配，Amazon WAF这样，您可以根据条件允许或阻止任何请求。

例如，假设您创建两个条件。一个条件与 User-Agent 标头中包含值 BadBot 的 Web 请求匹配。另一个条件与查询字符串中包含值 BadParameter 的 Web 请求匹配。将这两个条件添加到同一个规则并将该规则添加到 Web ACL 时，Amazon WAF仅当请求包含两个值时，Classic 才允许或阻止请求。

- 每个字符串匹配条件有多个筛选条件— 将包含多个筛选条件的字符串匹配条件添加到一个规则并将该规则添加到一个 Web ACL 时，Web 请求只需与字符串匹配条件中的一个筛选条件匹配，Amazon WAF这样，您可以根据一个条件允许或阻止请求。

假设您创建一个而不是两个条件，并且这一个条件包含与前面示例相同的两个筛选条件。Amazon WAF如果包含 Classic 允许或阻止请求或者 BadBot中的User-Agent标题要么 BadParameter在查询字符串中。

Note

将字符串匹配条件添加到规则时，您还可以将配置。Amazon WAF经典允许或阻止网络请求不要匹配条件中的值。

创建字符串匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 String and regex matching。
3. 选择 Create condition (创建条件)。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑字符串匹配条件时指定的值 \(p. 271\)](#)。
5. 选择 Add filter。
6. 如果要添加其他筛选条件，请重复步骤 4 和 5。
7. 添加完筛选器后，选择 Create。

创建或编辑字符串匹配条件时指定的值

创建或更新字符串匹配条件时，需要指定以下值：

名称

为字符串匹配条件输入名称。该名称只能包含字母数字字字字字字字字字 (A-Z、0-9) 以及以下特殊字符：_! " # + *}, ./。条件的名称在创建后不可更改。

类型

选择 String match。

Part of the request to filter on

选择应对每个 Web 请求的部分。Amazon WAF 检查您在中指定的字符串的 Classic Value to match：标头

指定的请求标头，例如 User-Agent 或 Referer 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查询字符串

URL 中在 ? 字符之后出现的部分 (如果有)。

URI

例如，请求的 URI 路径，用于标识资源，/images/daily-ad.jpg。这包括 URI 的查询字符串或片段组件。想要了解有关信息，请参阅[统一资源标识符 \(URI\)：通用语法](#)。

除非指定了 Transformation (转换)，否则 URI 不会被标准化，并且会被检查，就像 Amazon 是作为请求的一部分从客户端收到它一样。Transformation (转换) 将按指定方式重新设置 URI 的格式。

Body

请求中包含要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据 (如表单数据) 的部分。

Note

如果选择 Body 对于的价值 Part of the request to filter on，Amazon WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。(Amazon WAF Classic 会从请求标头获取正文的长度。) 有关更多信息，请参阅[使用大小约束条件 \(p. 262\)](#)。

单一查询参数 (仅限值)

您已定义为查询字符串的一部分的任何参数。例如，如果 URL 为“www.xyz.com?UserName=abc&SalesRegion=seattle”，您可以向 UserName 或 SalesRegion 参数添加一个筛选条件。

如果查询字符串中出现重复的参数，求出的值将为“OR”。也就是说，任一个值都将触发匹配。例如，在 URL“www.xyz.com?SalesRegion=boston&SalesRegion=seattle”中，Value to match (要匹配的值) 中无论是“boston”还是“seattle”，都会触发匹配。

如果您选择 Single query parameter (value only) (单一查询参数 (仅限值))，您还将指定 Query parameter name (查询参数名称)。这是查询字符串中您将检查的参数，如 UserName 或 SalesRegion。Query parameter name (查询参数名称) 的最大长度为 30 个字符。Query parameter name (查询参数名称) 不区分大小写。例如，如果您指定 UserName 作为 Query parameter name (查询参数名称)，这将匹配 UserName 的所有变体，如 username 和 UsERName。

所有查询参数 (仅限值)

与相似单一查询参数 (仅限值)，而不是检查单个参数的价值，Amazon WAF Classic 检查查询字符串中所有参数的值，以获取 Value to match。例如，如果 URL 是“www.xyz.com?USERNAME=ABC & SalesRegion = 西雅图”，然后选择所有查询参数 (仅限值)、Amazon WAF 如果两者的值之一，Classic 将触发匹配 UserName 要么 SalesRegion 被指定为 Value to match。

Header (仅当“Part of the request to filter on”是“Header”时)

如果你选择了标头来自的 Part of the request to filter on 列表中，从常见标头列表中选择标头，或输入应选择标头的名称。Amazon WAF 经典检查。

Match type

在您想要的请求部分内容中Amazon WAF经典来检查，选择字符串的位置Value to match必须看起来与此过滤器匹配：

Contains

字符串在请求的指定部分中的任何位置出现。

Contains word

Web 请求的指定部分必须包含 Value to match，并且 Value to match 必须仅包含字母数字字符或下划线 (A-Z、a-z、0-9 或 `_`)。此外，Value to match 必须是单词，这表示以下一种情况：

- Value to match 与 Web 请求的指定部分的值精确匹配，如标头的值。
- Value to match 处于 Web 请求的指定部分的开头，并且后跟字母数字字符或下划线 (`_`) 之外的字符 (例如，BadBot;)。
- Value to match 处于 Web 请求的指定部分的末尾，并且前面是字母数字字符或下划线 (`_`) 之外的字符 (例如，;BadBot)。
- Value to match 处于 Web 请求的指定部分的中间，并且前面和后面是字母数字字符或下划线 (`_`) 之外的字符 (例如，-BadBot;)。

Exactly matches

字符串和请求的指定部分的值是相同的。

从开始

字符串出现在请求的指定部分的开头。

Ends with

字符串出现在请求的指定部分的末尾。

Transformation

转换之前重新格式化 Web 请求Amazon WAFClassic 会检查请求。这可消除一些不寻常的格式，可防范攻击者在 Web 请求中使用它们以试图绕过。Amazon WAFClassic。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

None (无)

Amazon WAFClassic 在针对中的字符串检查 Web 请求之前，不会对它执行任何文本转换。Value to match.

Convert to lowercase

Amazon WAF将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

Amazon WAFClassic 将 HTML 编码的字符替换为未编码的字符：

- 将 `"` 替换为 `&`
- 将 ` ` 替换为不间断空格
- 将 `<` 替换为 `<`
- 将 `>` 替换为 `>`
- 将以十六进制格式表示的字符 `&#xhhhh`；替换为对应字符
- 将以十进制格式表示的字符 `&#nnnn`；替换为对应字符

规范化空格

Amazon WAFClassic 将以下字符替换为空格字符 (十进制 32)：

- \f, 换页符, 十进制 12
- \t, 制表符, 十进制 9
- \n, 换行符, 十进制 10
- \r, 回车符, 十进制 13
- \v, 垂直制表符, 十进制 11
- 不间断空格, 十进制 160

此外, 此选项将多个空格替换为一个空格。

Simplify command line

如果您担心攻击者注入操作系统命令行命令并使用异常格式伪装部分或所有命令, 使用此选项可执行以下转换:

- 删除以下字符: \ " ' ^
- 删除以下字符之前的空格: / (
- 将以下字符替换为空格: , ;
- 将多个空格替换为一个空格
- 将大写字母 (A-Z) 转换为小写字母 (a-z)

URL decode

解码 URL 编码的请求。

Value is base64 encoded

如果 Value to match 中的值进行了 base64 编码, 则选中此复选框。使用 base64 编码可指定攻击者在其请求中包含的不可打印的字符 (如制表符和换行符)。

Value to match

指定您想要的值Amazon WAF在 Web 请求中搜索的经典。最大长度为 50 个字节。如果要对值进行 base64 编码, 则 50 字节的最大长度适用于编码之前的值。

在字符串匹配条件中添加和删除筛选条件

您可以将筛选条件添加到字符串匹配条件或删除筛选条件。要更改筛选条件, 请添加一个新筛选条件并删除旧条件。

在字符串匹配条件中添加或删除筛选条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中, 选择它。

2. 在导航窗格中, 选择 String and regex matching。
3. 选择要在其中添加或删除筛选条件的条件。
4. 要添加筛选条件, 请执行以下步骤:
 - a. 选择 Add filter。
 - b. 指定适用的筛选条件设置。有关更多信息, 请参阅 [创建或编辑字符串匹配条件时指定的值 \(p. 271\)](#)。
 - c. 选择 Add (添加)。
5. 要删除筛选条件, 请执行以下步骤:
 - a. 选择要删除的筛选条件。
 - b. 选择 Delete Filter。

删除字符串匹配条件

如果要删除某个字符串匹配条件，需要先删除该条件中的所有筛选条件，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除字符串匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 从使用某个字符串匹配条件的规则中删除该条件：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的字符串匹配条件的规则的名称。
 - c. 在右窗格中，选择 Edit rule。
 - d. 选择要删除的条件旁边的 X。
 - e. 选择 Update (更新)。
 - f. 对使用要删除的字符串匹配条件的所有其余规则重复这些步骤。
3. 从要删除的条件中删除筛选条件：
 - a. 在导航窗格中，选择 String and regex matching。
 - b. 选择要删除的字符串匹配条件的名称。
 - c. 在右窗格中，选中 Filter 旁边的复选框来选择所有筛选条件。
 - d. 选择 Delete filter。
4. 在导航窗格中，选择 String and regex matching。
5. 在 String and regex match conditions 窗格中，选择要删除的字符串匹配条件。
6. 选择 Delete 删除所选条件。

使用正则表达式匹配条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要基于出现在请求中的与正则表达式 (regex) 模式匹配的字符串允许或阻止 Web 请求，请创建一个或多个正则表达式匹配条件。正则表达式匹配条件是一种字符串匹配条件，它确定要搜索的模式，以及应对 Web 请求的部分 (如指定标头或查询字符串)。Amazon WAF经典来检查模式。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止包含该模式的请求。

主题

- [创建正则表达式匹配条件 \(p. 275\)](#)
- [创建或编辑时指定的值 RegEx 匹配条件 \(p. 276\)](#)
- [编辑正则表达式匹配条件 \(p. 278\)](#)

创建正则表达式匹配条件

在创建正则表达式匹配条件时，指定标识您要搜索的字符串 (使用正则表达式) 的模式集。然后，将这些模式集添加到指定所需 Web 请求部分的筛选条件中。Amazon WAFClassic (经典) 可检查该模式集，如 URI 或查询字符串。

您可以将多个正则表达式添加到单个模式集中。如果您这样做，这些表达式将使用 OR 进行组合。也就是说，如果请求的适当部分与列出的任何表达式匹配，则 Web 请求将与模式集匹配。

将正则表达式匹配条件添加到规则时，您还可以对其进行配置。Amazon WAF 经典允许或阻止网络请求不要匹配条件中的值。

Amazon WAF 经典支持大多数[标准 Perl 兼容正则表达式 \(PCRE\)](#)。不过，不支持以下各种：

- 反向引用和捕获子表达式
- 任意零宽度断言
- 子例程引用和递归模式
- 条件模式
- 回溯控制动词
- \C 单字节指令
- \R 换行符匹配指令
- 匹配重置指令的 \K 开头
- 标注和嵌入式代码
- 原子分组和占有式限定符

创建正则表达式匹配条件

1. 登录到 Amazon Web Services Management Console 打开 Amazon WAF 控制台 <https://console.aws.amazon.com/wafv2/>。

如果您看到切换到 Amazon WAF Classic 在导航窗格中，选择它。

2. 在导航窗格中，选择 String and regex matching。
3. 选择 Create condition (创建条件)。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑时指定的值 RegEx 匹配条件 \(p. 276\)](#)。
5. 选择 Create pattern set and add filter (如果您创建新的模式集) 或 Add filter (如果您使用现有模式集)。
6. 选择 Create (创建)。

创建或编辑时指定的值 RegEx 匹配条件

创建或更新正则表达式匹配条件时，需要指定以下值：

名称

为正则表达式匹配条件输入名称。该名称只能包含字母数字字符 (A-Z、0-9) 以及以下特殊字符：_! " # \$ % & ' * + , - . / : ; < = > ? [\] ^ _ { | } ~ 。条件的名称在创建后不可更改。

类型

选择 Regex match。

Part of the request to filter on

选择应对每个 Web 请求的部分。Amazon WAF 经典来检查您在中指定的模式 Value to match：

标头

指定的请求标头，例如 User-Agent 或 Referer 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST 和 PUT。

查询字符串

URL 中在 ? 字符之后出现的部分 (如果有)。

URI

例如, 请求的 URI 路径, 用于标识资源, /images/daily-ad.jpg. 这包括 URI 的查询字符串或片段组件。想要了解有关信息, 请参阅[统一资源标识符 \(URI\) : 通用语法](#)。

除非指定了 Transformation (转换), 否则 URI 不会被标准化, 并且会被检查, 就像 Amazon 是作为请求的一部分从客户端收到它一样。Transformation (转换) 将按指定方式重新设置 URI 的格式。

Body

请求中包含要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据 (如表单数据) 的部分。

Note

如果选择Body对于的价值Part of the request to filter on、Amazon WAFClassic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求, 可以创建大小约束条件。(Amazon WAFClassic 会从请求标头获取正文的长度。) 有关更多信息, 请参阅[使用大小约束条件 \(p. 262\)](#)。

单一查询参数 (仅限值)

您已定义为查询字符串的一部分的任何参数。例如, 如果 URL 为“www.xyz.com?UserName=abc&SalesRegion=seattle”, 您可以向 UserName 或 SalesRegion 参数添加一个筛选条件。

如果查询字符串中出现重复的参数, 求出的值将为“OR”。也就是说, 任一个值都将触发匹配。例如, 在 URL“www.xyz.com?SalesRegion=boston&SalesRegion=seattle”中, 与 Value to match (要匹配的值) 中的“boston”或“seattle”匹配的模式会触发匹配。

如果您选择 Single query parameter (value only) (单一查询参数 (仅限值)), 您还将指定 Query parameter name (查询参数名称)。这是查询字符串中您将检查的参数, 如 UserName 或 SalesRegion。Query parameter name (查询参数名称) 的最大长度为 30 个字符。Query parameter name (查询参数名称) 不区分大小写。例如, 如果您指定 UserName 作为 Query parameter name (查询参数名称), 这将匹配 UserName 的所有变体, 如 username 和 UsERName。

所有查询参数 (仅限值)

与相似单一查询参数 (仅限值), 而不是检查单个参数的价值, Amazon WAFClassic Classic 将针对中指定的模式检查查询字符串中所有参数的值。Value to match. 例如, 在 URL“www.xyz.com?UserName=abc&SalesRegion=seattle”中, Value to match (要匹配的值) 中与 UserName 或 SalesRegion 匹配的模式会触发匹配。

Header (仅当“Part of the request to filter on”是“Header”时)

如果你选择了标头来自的Part of the request to filter on列表中, 从常见标头列表中选择标头, 或输入应选择标头的名称。Amazon WAF经典检查。

Transformation

转换之前重新格式化 Web 请求Amazon WAFClassic 会检查请求。这可消除一些不寻常的格式, 可防范攻击者在 Web 请求中使用它们以试图绕过。Amazon WAFClassic。

您只能指定一个类型的文本转换。

转换可以执行以下操作:

None (无)

Amazon WAFClassic 在针对中的字符串检查 Web 请求之前, 不会对它执行任何文本转换。Value to match.

Convert to lowercase

Amazon WAF将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

Amazon WAFClassic 将 HTML 编码的字符替换为未编码的字符：

- 将 " 替换为 &
- 将 替换为不间断空格
- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符
- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

规范化空格

Amazon WAFClassic 将以下字符替换为空格字符（十进制 32）：

- \f, 换页符, 十进制 12
- \t, 制表符, 十进制 9
- \n, 换行符, 十进制 10
- \r, 回车符, 十进制 13
- \v, 垂直制表符, 十进制 11
- 不间断空格, 十进制 160

此外, 此选项将多个空格替换为一个空格。

Simplify command line

如果您担心攻击者注入操作系统命令行命令并使用异常格式伪装部分或所有命令, 使用此选项可执行以下转换：

- 删除以下字符：\ " ' ^
- 删除以下字符之前的空格：/ (
- 将以下字符替换为空格：, ;
- 将多个空格替换为一个空格
- 将大写字母 (A-Z) 转换为小写字母 (a-z)

URL decode

解码 URL 编码的请求。

与请求匹配的正则表达式模式

您可以选择现有的模式集或创建新的模式集。如果您创建新的模式集, 请指定以下内容：

新模式集名称

输入名称, 然后指定所需的正则表达式模式。Amazon WAF搜索的经典。

如果您将多个正则表达式添加到模式集中, 这些表达式将使用 OR 进行组合。也就是说, 如果请求的适当部分与列出的任何表达式匹配, 则 Web 请求将与模式集匹配。

Value to match 的最大长度是 70 个字符。

编辑正则表达式匹配条件

您可以对现有正则表达式匹配条件进行以下更改：

- 从现有模式集中删除模式
- 向现有模式集中添加模式
- 从现有的正则表达式匹配条件中删除筛选条件

- 向现有的正则表达式匹配条件中添加筛选条件（正则表达式匹配条件中只能具有一个筛选条件。因此，要添加筛选条件，您必须首先删除现有的筛选条件。）
- 删除现有的正则表达式匹配条件

Note

您无法从现有的筛选条件中添加或删除模式集。您必须编辑模式集，或删除筛选条件并使用新的模式集创建新的筛选条件。

从现有模式集中删除模式

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 String and regex matching。
3. 选择 View regex pattern sets。
4. 选择要编辑的模式集的名称。
5. 选择 Edit (编辑)。
6. 选择要删除的模式旁边的 X。
7. 选择 Save (保存)。

向现有模式集中添加模式

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 String and regex matching。
3. 选择 View regex pattern sets。
4. 选择要编辑的模式集的名称。
5. 选择 Edit (编辑)。
6. 输入新的正则表达式模式。
7. 选择新模式旁边的 +。
8. 选择 Save (保存)。

从现有的正则表达式匹配条件中删除筛选条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 String and regex matching。
3. 选择具有要删除的筛选条件的条件的名称。
4. 选中要删除的筛选条件旁边的框。
5. 选择 Delete filter。

删除正则表达式匹配条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 从正则表达式条件中删除筛选条件。有关执行此操作的说明，请参阅[从现有的正则表达式匹配条件中删除筛选条件 \(p. 279\)](#)。
3. 从使用某个正则表达式匹配条件的规则中删除该条件：
 - a. 在导航窗格中，选择 Rules (规则)。
 - b. 选择使用要删除的正则表达式匹配条件的规则的名称。
 - c. 在右窗格中，选择 Edit rule。
 - d. 选择要删除的条件旁边的 X。
 - e. 选择 Update (更新)。
 - f. 对使用要删除的正则表达式匹配条件的所有其余规则重复这些步骤。
4. 在导航窗格中，选择 String and regex matching。
5. 选择要删除的条件旁边的按钮。
6. 请选择 Delete (删除)。

向现有的正则表达式匹配条件中添加筛选条件或更改其中的筛选条件

正则表达式匹配条件中只能具有一个筛选条件。如果要添加或更改筛选条件，您必须首先删除现有的筛选条件。

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 从要更改的正则表达式条件中删除筛选条件。有关执行此操作的说明，请参阅[从现有的正则表达式匹配条件中删除筛选条件 \(p. 279\)](#)。
3. 在导航窗格中，选择 String and regex matching。
4. 选择要更改的条件名称。
5. 选择 Add filter。
6. 为新的筛选条件输入适当的值，然后选择 Add。

使用规则

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

规则可以让您准确确定目标所需的 Web 请求，Amazon WAF通过指定所需的确切条件允许或阻止 ClassicAmazon WAF经典值得注意。例如，Amazon WAFClassic 可以检查请求源自的 IP 地址和、请求包含的字符串和字符串出现的位置以及请求是否表现为包含恶意 SQL 代码。

主题

- [创建规则并添加条件 \(p. 281\)](#)
- [在规则中添加和删除条件 \(p. 282\)](#)
- [删除规则 \(p. 283\)](#)
- [Amazon Web Services Marketplace 规则组 \(p. 283\)](#)

创建规则并添加条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果将多个条件添加到一个规则，则 Web 请求必须匹配所有条件。Amazon WAF这样，您可以根据该规则允许或阻止任何请求。

创建规则并添加条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Rules (规则)。
3. 选择 Create rule (创建规则)。
4. 输入以下值：

名称

输入名称。

CloudWatch 指标名称

输入的名称 CloudWatch 指标Amazon WAFClassic 将创建并与规则关联。该名称只能包含字母数字字符 (A-Z、a-z、0-9)，最大长度为 128 和最小长度为 1。它不能包含空格或为预留的指标名称。Amazon WAF经典版，包括 “All” 和 “Default_Action”。

Rule type

选择 Regular rule 或 Rate-based rule。基于速率的规则与常规规则基本相同，但还考虑到五分钟时段来自 IP 地址的请求数。有关这些规则类型的详细信息，请参阅[怎么样Amazon WAF经典作品 \(p. 240\)](#)。

Rate limit

对于基于速率的规则，请输入与规则条件匹配的 IP 地址在任何五分钟内允许的最大请求数。速率限制必须至少为 100。

您可以单独指定速率限制，也可以指定速率限制和条件。如果您仅指定速率限制，Amazon WAF 会对所有 IP 地址设置限制。如果您指定速率限制和条件，Amazon WAF 会对与条件匹配的 IP 地址设置限制。

当 IP 地址达到速率限制阈值时，Amazon WAF 会尽快应用指定的操作 (阻止或计数)，通常在 30 秒内。一旦操作到位，如果五分钟没有来自 IP 地址的请求，则 Amazon WAF 会将计数器重置为零。

5. 要将条件添加到规则，请指定以下值：

When a request does/does not

如果要Amazon WAF如果需要基于条件中的筛选条件允许或阻止请求，则选择。请参阅。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且需要。Amazon WAFClassic 要允许或阻止来自这些 IP 地址的请求，请选择请参阅。

如果要Amazon WAFClassic (经典) 要基于条件中的筛选器的反向条件允许或阻止请求，请选择。不。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且需要。Amazon WAF允许或阻止符合以下条件的请求不要来自那些 IP 地址，请选择不。

match/originate from

选择要添加到规则的条件的类型：

- 跨站点脚本匹配条件 — 选择在跨站点脚本匹配条件中匹配至少一个筛选条件
- IP 匹配条件 — 选择源自于中的 IP 地址
- 地理匹配条件 — 选择originate from a geographic location in
- 大小约束条件 — 选择match at least one of the filters in the size constraint condition
- 选择 SQL 注入匹配条件 — 选择match at least one of the filters in the SQL injection match condition
- 字符串匹配条件 — 选择match at least one of the filters in the string match condition
- 正则表达式匹配条件 — 选择在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的条件。列表仅显示在上一步选择的类型的条件。

6. 要将另一个条件添加到规则中，请选择 Add another condition，然后重复步骤 4 和 5。请注意以下几点：
 - 如果您添加多个条件，则 Web 请求必须与每个条件中的至少一个筛选条件匹配，Amazon WAF 经典：允许或阻止基于该规则的请求。
 - 如果将两个 IP 匹配条件添加到同一规则中，Amazon WAFClassic (经典) 只允许或阻止源自在两个 IP 匹配条件中同时出现的 IP 地址的请求
7. 添加完条件后，选择 Create。

在规则中添加和删除条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

可以通过添加或删除条件来更改规则。

在规则中添加或删除条件

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Rules (规则)。
3. 选择要在其中添加或删除条件的规则的名称。
4. 选择 Add rule。
5. 要添加条件，请选择 Add condition 并指定以下值：

When a request does/does not

如果要Amazon WAFClassic (经典) 要基于条件中的筛选条件允许或阻止请求 (例如源自 IP 地址范围 192.0.2.0/24 的 Web 请求)，请选择请参阅。

如果要Amazon WAFClassic (经典) 要基于条件中的筛选器的反向条件允许或阻止请求，请选择。不。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且需要。Amazon WAF允许或阻止符合以下条件的请求不要来自那些 IP 地址，请选择不。

match/originate from

选择要添加到规则的条件的类型：

- 跨站点脚本匹配条件 — 选择在跨站点脚本匹配条件中匹配至少一个筛选条件
- IP 匹配条件 — 选择源自于中的 IP 地址
- 地理匹配条件 — 选择originate from a geographic location in
- 大小约束条件 — 选择match at least one of the filters in the size constraint condition
- 选择 SQL 注入匹配条件 — 选择match at least one of the filters in the SQL injection match condition
- 字符串匹配条件 — 选择match at least one of the filters in the string match condition
- 正则表达式匹配条件 — 选择在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的的条件。列表仅显示在上一步选择的类型的条件。

6. 要删除条件，请选择条件名称右侧的 X
7. 选择 Update (更新)。

删除规则

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

如果要删除某个规则，需先从使用该规则的 Web ACL 中将其删除，然后删除该规则中包含的条件。

删除一项规则

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 要从使用某个规则的 Web ACL 中将其删除，请对每个 Web ACL 执行以下步骤：
 - a. 在导航窗格中，选择 Web ACL。
 - b. 选择使用待删除规则的 Web ACL 的名称。
 - c. 选择 Rules 选项卡。
 - d. 选择 Edit web ACL。
 - e. 选择X在要删除的规则右侧，然后选择更新。
3. 在导航窗格中，选择 Rules (规则)。
4. 选择要删除的规则的名称。
5. 请选择 Delete (删除)。

Amazon Web Services Marketplace 规则组

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
有关最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

Amazon WAF经典提供Amazon Web Services Marketplace规则组以帮助您保护资源。Amazon Web Services Marketplace规则组是预定义的、 ready-to-use 由编写和更新的规则Amazon和Amazon合作伙伴公司。

一段时间Amazon Web Services Marketplace设计规则组旨在帮助保护特定类型的 Web 应用程序，如 WordPress、Joomla 或 PHP。其他Amazon Web Services Marketplace规则组可提供广泛的保护功能以应对已知威胁或常见的 Web 应用程序漏洞，例如[OWASP 前 10](#)。

您可以安装一个Amazon Web Services Marketplace来自首选的规则组Amazon您也可以添加自己的定制Amazon WAF加强保护的经典规则。如果您需要符合监管合规性（如 PCI 或 HIPAA），或许可以使用Amazon Web Services Marketplace规则组以满足 Web 应用程序防火墙要求。

Amazon Web Services Marketplace 规则组不需要签订长期合同即可使用，也没有最低费用限制。当您订阅规则组时，将按月收取费用（按小时比例）和根据数量收取持续请求费用。有关更多信息，请参阅[Amazon WAF经典定价](#)以及每个人的描述Amazon Web Services Marketplace打开规则组Amazon Web Services Marketplace。

自动更新

随时了解不断变化的威胁情形会非常耗时且成本高昂。Amazon Web Services Marketplace当您实施和使用规则组时，规则组可以帮助您节省时间。Amazon WAFClassic。另一个好处是Amazon而且我们的Amazon合作伙伴自动更Amazon Web Services Marketplace当出现在新的漏洞和威胁时，规则组。

我们的许多合作伙伴会在新漏洞公开披露之前收到通知。他们可以在新威胁广为人知之前更新其规则组并为您部署它们。许多合作伙伴还拥有威胁研究团队，可调查和分析最近出现的威胁，以便编写最相关的规则。

访问中的规则Amazon Web Services Marketplace规则组

每个 Amazon Web Services Marketplace 规则组都提供了旨在防护的攻击和漏洞类型的全面描述。为了保护规则组提供商的知识产权，您将无法查看规则组中的单个规则。此限制还有助于避免恶意用户设计专门避开已发布规则的威胁。

因为您无法查看Amazon Web Services Marketplace规则组中，您也无法编辑Amazon Web Services Marketplace规则组。但是，您可以从规则组中排除特定规则。这称为“规则组例外”。排除规则不会删除这些规则。相反，它将规则的操作更改为 COUNT。因此，与已排除规则匹配的请求会计入总数，但不会受到阻止。您将收到每个排除规则的 COUNT 指标。

在对意外阻止流量的规则组进行故障排除时，排除规则会很有用（误报）。一种故障排除技术是识别规则组中阻止所需流量的特定规则，然后禁用（排除）该特定规则。

除了排除特定规则外，您还可以通过启用或禁用整个规则组以及选择要执行的规则组操作来优化保护。有关更多信息，请参阅[使用Amazon Web Services Marketplace规则组 \(p. 284\)](#)。

配额

您只能启用一个Amazon Web Services Marketplace规则组。您还可以启用使用 Amazon Firewall Manager 创建的一个自定义规则组。这些规则组计入每个 Web ACL 10 个规则的最大配额。因此，您可以有一个Amazon Web Services Marketplace单个 Web ACL 中的规则组、一个自定义规则组和最多八个自定义规则。

定价

适用于Amazon Web Services Marketplace规则组定价，请参阅[Amazon WAF经典定价](#)以及每个人的描述Amazon Web Services Marketplace打开规则组Amazon Web Services Marketplace。

使用Amazon Web Services Marketplace规则组

您可以订阅和取消订阅Amazon Web Services Marketplace上的规则组Amazon WAF经典控制台。您还可以从规则组中排除特定规则。

订阅和使用Amazon Web Services Marketplace规则组

1. 登录到Amazon Web Services Management Console然后打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Marketplace。
3. 在可用 Marketplace 产品部分中，选择规则组的名称以查看详细信息和定价信息。
4. 如果您要订阅规则组，请选择继续。

Note

如果您不想订阅此规则组，只需在您的浏览器中关闭此页面。

5. 选择设置您的账户。
6. 将规则组添加到 Web ACL 中，就像您添加单个规则一样。有关更多信息，请参阅 [创建 Web ACL \(p. 287\)](#) 或 [编辑 Web ACL \(p. 291\)](#)。

Note

往 Web ACL 中添加规则组时，您为规则组设置的操作（无覆盖或覆盖以计数）称为规则组覆盖操作。有关更多信息，请参阅 [规则组覆盖 \(p. 286\)](#)。

取消订阅Amazon Web Services Marketplace规则组

1. 登录到Amazon Web Services Management Console然后打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 从所有 Web ACL 中删除规则组。有关更多信息，请参阅 [编辑 Web ACL \(p. 291\)](#)。
3. 在导航窗格中，选择 Marketplace。
4. 选择 Manage your subscriptions。
5. 选择您想取消订阅的规则组旁边的取消订阅。
6. 选择是，取消订阅。

从规则组中排除规则（规则组例外）

1. 登录到Amazon Web Services Management Console然后打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 如果尚未启用，请启用Amazon WAF经典日志记录。有关更多信息，请参阅 [记录 Web ACL 流量信息 \(p. 302\)](#)。使用Amazon WAF标识要排除的规则 ID。这些规则通常是阻止合法请求的规则。
3. 在导航窗格中，选择 Web ACL。
4. 选择要编辑的 Web ACL 的名称。此操作将打开一个页面，其中包含右窗格中的 Web ACL 详细信息。

Note

在您可以从该规则组中排除规则之前，您要编辑的规则组必须与 Web ACL 相关联。

5. 在右窗格中的 Rules 选项卡上，选择 Edit web ACL。
6. 在 Rule group exceptions (规则组例外) 部分中，展开您要编辑的规则组。
7. 选择要排除的规则旁边的 X。可以使用Amazon WAFClassic 日志。
8. 选择 Update (更新)。

排除规则不会从规则组中删除这些规则。相反，它将规则的操作更改为 COUNT。因此，与已排除规则匹配的请求会计入总数，但不会受到阻止。您将收到每个排除规则的 COUNT 指标。

Note

您可以使用相同的过程从您在 Amazon Firewall Manager 中创建的自定义规则组中排除规则。但是，除了使用这些步骤从自定义规则组中排除规则之外，您还可以使用[从添加和删除规则 Amazon WAF 经典规则组 \(p. 296\)](#)中描述的步骤编辑自定义规则组。

规则组覆盖

Amazon Web Services Marketplace 规则组有两个可能的操作：没有覆盖和覆盖以计数。如果您要测试规则组，请将操作设置为覆盖以计数。此规则组操作会覆盖该规则组中包含的单个规则指定的任何数据块操作。也就是说，如果规则组的操作设置为覆盖以计数，这些请求则不会阻止基于单个规则操作的匹配请求，而会被进行计数。相反，如果您把规则组的操作设置为无覆盖，则会使用该规则组中单个规则的操作。

Amazon Web Services Marketplace 规则组问题排查

如果你发现那个 Amazon Web Services Marketplace 规则组正阻止合法流量，请执行以下步骤。

Amazon Web Services Marketplace 规则组故障排除

1. 排除阻止合法流量的特定规则。可以使用 Amazon WAF Classic 日志。有关排除规则的更多信息，请参阅[从规则组中排除规则（规则组例外） \(p. 285\)](#)。
2. 如果排除特定规则无法解决问题，则可以将 Amazon Web Services Marketplace 规则组的操作从 No override (无覆盖) 更改为 Override to count (覆盖以计数)。这会允许 Web 请求通过，而不管规则组中的各个规则操作是什么。这还为您提供了亚马逊 CloudWatch 规则组的指标。
3. 在将 Amazon Web Services Marketplace 规则组操作设置为 Override to count (覆盖以计数) 之后，联系规则组提供商的客户支持团队来进一步对问题进行排查。有关联系信息，请参阅 Amazon Web Services Marketplace 产品列表页面上的规则组列表。

联系客户支持

对于有关的问题 Amazon WAF Classic 或由托管规则组 Amazon，联系 Amazon Web Services Support。有关管理的规则组的问题 Amazon 请联系该合作伙伴的客户支持团队。若要查找合作伙伴联系信息，请参阅 Amazon Web Services Marketplace 上的合作伙伴列表。

创建和销售 Amazon Web Services Marketplace 规则组

如果你想出售 Amazon Web Services Marketplace 打开规则组 Amazon Web Services Marketplace 请参阅[如何在销售软件 Amazon Web Services Marketplace](#)。

使用 Web ACL

Note

这是 Amazon WAF Classic 文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。对于最新版本的 Amazon WAF 请参阅[Amazon WAF \(p. 5\)](#)。

将规则添加到 Web ACL 时，您可指定是否需要 Amazon WAF Classic (经典) 可基于规则中的条件允许或阻止请求。如果将多个规则添加到 Web ACL，则 Amazon WAF Classic (Classic) 按照在 Web ACL 中列出规则的

顺序，评估每个请求。如果 Web 请求与规则中的所有条件匹配，Amazon WAFClassic 会立即执行对应操作（允许或阻止），不会针对 Web ACL 中的其余规则（如果有）评估请求。

如果 Web 请求不与 Web ACL 中的任何规则匹配，Amazon WAFClassic 将执行您为 Web ACL 指定的默认操作。有关更多信息，请参阅 [确定 Web ACL 的默认操作 \(p. 287\)](#)。

如果要在开始使用某个规则允许或阻止请求之前测试它，可以将 Amazon WAF 对与规则中的条件匹配的 Web 请求进行计数。有关更多信息，请参阅 [测试 Web ACL \(p. 292\)](#)。

主题

- [确定 Web ACL 的默认操作 \(p. 287\)](#)
- [创建 Web ACL \(p. 287\)](#)
- [将 Web ACL 与 Amazon API Gateway API API 关联或取消关联，CloudFront 分配或应用程序负载均衡器 \(p. 290\)](#)
- [编辑 Web ACL \(p. 291\)](#)
- [删除 Web ACL \(p. 291\)](#)
- [测试 Web ACL \(p. 292\)](#)

确定 Web ACL 的默认操作

Note

这是 Amazon WAFClassic 文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。
对于最新版本的 Amazon WAF 请参阅[Amazon WAF \(p. 5\)](#)。

创建和配置 Web ACL 时，必须制定的第一个并且最重要的决策是，是否应该针对 Amazon WAF 经典用于允许 Web 请求或阻止 Web 请求。默认操作指示你想要什么 Amazon WAFClassic（经典）在针对您指定的所有条件检查了 Web 请求，并且 Web 请求不符合其中任一条件时，应执行的操作：

- Allow（允许）允许如果要允许大多数用户访问您的网站，但是阻止其请求源自指定 IP 地址或其请求表现为包含恶意 SQL 代码或指定值的攻击者进行访问，请选择 Allow（允许）对于默认操作。
- Block（阻止）阻止如果要阻止大多数准用户访问您的网站，但是允许其请求源自指定 IP 地址或其请求包含指定值的用户进行访问，请选择 Block（阻止）对于默认操作。

在确定默认操作之后制定的许多决策取决于您是要允许还是阻止大多数 Web 请求。例如，如果要允许大多数请求，则创建的匹配条件通常应指定要阻止的 Web 请求，如以下这些条件：

- 源自进行数量不合理的请求的 IP 地址的请求
- 源自您不在其中开展业务或是频繁攻击源的国家/地区的请求
- 在 User-Agent 标头中包含伪造值的请求
- 表现为包含恶意 SQL 代码的请求

创建 Web ACL

Note

这是 Amazon WAFClassic 文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。
对于最新版本的 Amazon WAF 请参阅[Amazon WAF \(p. 5\)](#)。

创建 Web ACL

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>.

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 如果这是您首次使用Amazon WAF选择 Classic转到Amazon WAFClassic然后配置 Web ACL. 如果你用过Amazon WAF之前经典，请选择Web ACL在导航窗格中选择，然后选择创建 Web ACL.
3. 适用于Web ACL 名，输入一个名称。

Note

Web ACL 在创建之后无法更改名称。

4. 适用于CloudWatch 指标名称，更改默认名称（如果适用）。该名称只能包含字母数字字符（A-Z、a-z、0-9），最大长度为 128 和最小长度为 1。它不能包含空格或为预留的指标名称。Amazon WAF经典版，包括“All”和“Default_Action”。

Note

Web ACL 在创建之后无法更改名称。

5. 对于 Region（亚马逊云科技区域），选择一个区域。
6. 对于 Amazon resource，选择要与此 Web ACL 关联的资源，然后选择 Next。
7. 如果你已经创建了你想要的条件Amazon WAF经典用于检查 Web 请求，请选择下一步，然后继续下一步。

如果尚未创建条件，请创建条件。有关更多信息，请参阅以下主题：

- [使用跨站点脚本匹配条件 \(p. 253\)](#)
- [使用 IP 匹配条件 \(p. 258\)](#)
- [使用地理匹配条件 \(p. 260\)](#)
- [使用大小约束条件 \(p. 262\)](#)
- [使用 SQL 注入匹配条件 \(p. 266\)](#)
- [使用字符串匹配条件 \(p. 270\)](#)
- [使用正则表达式匹配条件 \(p. 275\)](#)

8. 如果您已经创建了规则或规则组（或订阅了Amazon Web Services Marketplace规则组）您希望添加到此 Web ACL，请将这些规则添加到 Web ACL：
 - a. 在 Rules 列表中，选择一个规则。
 - b. 选择 Add rule to web ACL。
 - c. 重复步骤 a 和 b，添加所有要添加到此 Web ACL 的规则。
 - d. 前往步骤 10。
9. 如果尚未创建规则，现在可以添加规则：
 - a. 请选择 Create rule (创建规则)。
 - b. 输入以下值：

名称

输入名称。

CloudWatch 指标名称

输入的名称 CloudWatch 指标Amazon WAFClassic 将创建并与规则关联。该名称只能包含字母数字字符（A-Z、a-z、0-9），最大长度为 128 和最小长度为 1。它不能包含空格或为预留的指标名称。Amazon WAF经典版，包括“All”和“Default_Action”。

Note

创建规则之后，无法更改指标名称。

- c. 要将条件添加到规则，请指定以下值：

When a request does/does not

如果要Amazon WAFClassic (经典) 要基于条件中的筛选条件允许或阻止请求 (例如源自 IP 地址范围 192.0.2.0.2.0/24 的 Web 请求)，请选择请参阅。

如果要Amazon WAFClassic (经典) 要基于条件中的筛选器的反向条件允许或阻止请求，请选择。不。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0.2.0/24 并且需要Amazon WAF允许或阻止符合以下条件的请求不要来自那些 IP 地址，请选择不。

match/originate from

选择要添加到规则的条件的类型：

- 跨站点脚本匹配条件 — 选择在跨站点脚本匹配条件中匹配至少一个筛选条件
- IP 匹配条件 — 选择源自于中的 IP 地址
- 地理匹配条件 — 选择originate from a geographic location in
- 大小约束条件 — 选择match at least one of the filters in the size constraint condition
- 选择 SQL 注入匹配条件 — 选择match at least one of the filters in the SQL injection match condition
- 字符串匹配条件 — 选择match at least one of the filters in the string match condition
- 正则表达式匹配条件 — 选择在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的条件。列表仅显示您在前面列表中选择类型的条件。

- d. 要将另一个条件添加到规则，请选择 Add another condition (添加另一个条件)，然后重复步骤 b 和 c。请注意以下几点：

- 如果您添加多个条件，则 Web 请求必须与每个条件中的至少一个筛选条件匹配，Amazon WAF 这样，您可以根据该规则允许或阻止任何请求。
- 如果将两个 IP 匹配条件添加到同一规则中，Amazon WAFClassic (经典) 只允许或阻止源自在两个 IP 匹配条件中同时出现的 IP 地址的请求。

- e. 重复步骤 9，创建要添加到此 Web ACL 的所有规则。

- f. 选择 Create (创建)。

- g. 继续执行步骤 10。

10. 对于 Web ACL 中的每个规则或规则组，选择所需的管理类型。Amazon WAF经典提供，如下所示：

- 对于每个规则，选择是否需要Amazon WAFClassic (经典) 可基于规则中的条件允许、阻止或计数 Web 请求：
 - Allow (允许) — API Gateway，CloudFront 或使用应 Application Load Balancer 响应请求的对象。对于 CloudFront，如果对象不在边缘缓存中，CloudFront 将请求转发到源。
 - Block (阻止) — API Gateway，CloudFront 或应用 Application Load Balancer 使用 HTTP 403 (禁止) 状态代码响应请求。CloudFront 还可以使用自定义错误页面进行响应。有关更多信息，请参阅 [使用Amazon WAF经典搭配 CloudFront 自定义错误页面 \(p. 307\)](#)。
 - 计数—Amazon WAFClassic 使与规则中的条件匹配的请求计数器递增，然后继续基于 Web ACL 中的其余规则检查 Web 请求。

有关在开始使用 Web ACL 允许或阻止 Web 请求之前，使用 Count (计数) 测试 Web ACL 的信息，请参阅 [对与 Web ACL 中的规则匹配的 Web 请求计数 \(p. 292\)](#)。

- 对于每个规则组，为其设置覆盖操作：
 - 没有覆盖—使使用规则组中各个规则的操作。

- 覆盖要计数—覆盖组中各个规则指定的所有阻止操作，以便仅对所有匹配的请求进行计数。

有关更多信息，请参阅 [规则组覆盖 \(p. 286\)](#)。

11. 如果需要更改 Web ACL 中的规则顺序，请使用 Ordercolumn.Amazon WAF Classic (Classic) 基于规则出现在 Web ACL 中的顺序来检查 Web 请求。
12. 如果要删除添加到 Web ACL 的规则，请在规则所在行中选择 x。
13. 选择 Web ACL 的默认操作。这就是这样的行动 Amazon WAF 当 Web 请求不与此 Web ACL 中的任何规则中的条件匹配时，Classic (经典)。有关更多信息，请参阅 [确定 Web ACL 的默认操作 \(p. 287\)](#)。
14. 选择 Review and create。
15. 查看 Web ACL 的设置，然后选择 Confirm and create。

将 Web ACL 与 Amazon API Gateway API API API 关联或取消关联，CloudFront 分配或应用程序负载均衡器

Note

这是 Amazon WAF Classic 文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅 [将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。

对于最新版本的 Amazon WAF 请参阅 [Amazon WAF \(p. 5\)](#)。

要关联或取消关联 Web ACL，请执行适用的过程。请注意，您还可以将 Web ACL 与 CloudFront 分配时创建或更新分配。有关更多信息，请参阅 [使用 Amazon WAF 控制对您的内容的访问的经典](#) 中的亚马逊 CloudFront 开发人员指南。

当关联 Web ACL 时，以下限制将适用：

- 每个 API Gateway API、Application Load Balancer 和 CloudFront 分配只能与一个 Web ACL 相关联。
- 与 CloudFront 分配不能与应用 Application Load Balancer 或 API Gateway API 相关联。但是，Web ACL 可以与其他 ACL 相关联。CloudFront 分配。

要将 Web ACL 与 API Gateway API 相关联，请执行以下操作：CloudFront Application Load Balancer

1. 登录到 Amazon Web Services Management Console 打开 Amazon WAF 控制台 <https://console.aws.amazon.com/wafv2/>。
如果您看到切换到 Amazon WAF Classic 在导航窗格中，选择它。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与 API Gateway API API 关联的 Web ACL 的名称，CloudFront 分配或 Application Load Balancer。这将在右窗格中打开一个页面，其中包含 Web ACL 的详细信息。
4. 在存储库的 Rule 选项卡，下 Amazon 使用此 Web ACL 的资源，选择添加关联。
5. 系统提示时，请使用资源列表以选择要将此 Web ACL 与之关联的 API Gateway API、CloudFront 分配或 Application Load Balancer。如果选择应用程序负载均衡器，还必须指定区域。
6. 选择 Add (添加)。
7. 要将此 Web ACL 与其他 API Gateway API 关联，CloudFront 分配或其他 Application Load Balancer，请重复步骤 4 到 6。

要从 API Gateway API 取消关联 Web ACL，请执行以下操作：CloudFront Application Load Balancer

1. 登录到 Amazon Web Services Management Console 打开 Amazon WAF 控制台 <https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Web ACL。
3. 选择要从 API Gateway API 取消关联的 Web ACL 的名称， CloudFront 分配或 Application Load Balancer。这将在右窗格中打开一个页面，其中包含 Web ACL 的详细信息。
4. 在存储库的Rule选项卡，下Amazon使用此 Web ACL 的资源，选择x对于每个 API Gateway API， CloudFront 要从中取消与此 Web ACL 的关联的分配或 Application Load Balancer。

编辑 Web ACL

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

要对 Web ACL 添加或删除规则，或是更改默认操作，请执行以下过程。

编辑 Web ACL

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL 的名称。这将在右窗格中打开一个页面，其中包含 Web ACL 的详细信息。
4. 在右窗格中的 Rules 选项卡上，选择 Edit web ACL。
5. 要将规则添加到 Web ACL，请执行以下步骤：
 - a. 在 Rules 列表中，选择要添加的规则。
 - b. 选择 Add rule to web ACL。
 - c. 重复步骤 a 和 b，添加所有所需的规则。
6. 如果需要更改 Web ACL 中的规则顺序，请使用Ordercolumn.Amazon WAF Classic (Classic) 基于规则出现在 Web ACL 中的顺序来检查 Web 请求。
7. 要从 Web ACL 中删除规则，请选择该规则所在行右侧的x。这不会从中删除规则Amazon WAF它只是从此 Web ACL 删除规则。
8. 要更改规则的操作或 Web ACL 的默认操作，请选择首选选项。

Note

为规则组或设置操作时Amazon Web Services Marketplace规则组 (与单个规则组相对)，您为规则组设置的操作 (任何一个规则组)。没有覆盖要么覆盖要计数) 被称为覆盖操作。有关更多信息，请参阅[规则组覆盖 \(p. 286\)](#)。

9. 选择 Save changes (保存更改)。

删除 Web ACL

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。

对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

要删除 Web ACL，必须先删除 Web ACL 中包含的规则并取消关联所有规则。CloudFront 分配和 Application Load Balancer来自 Web ACL。请执行以下过程。

删除 Web ACL

1. 登录到Amazon Web Services Management Console打开Amazon WAF控制台<https://console.aws.amazon.com/wafv2/>。

如果您看到切换到Amazon WAFClassic在导航窗格中，选择它。

2. 在导航窗格中，选择 Web ACL。
3. 选择要删除的 Web ACL 的名称。这将在右窗格中打开一个页面，其中包含 Web ACL 的详细信息。
4. 在右窗格中的 Rules 选项卡上，选择 Edit web ACL。
5. 要从 Web ACL 中删除所有规则，请选择每个规则所在行右侧的 x。这不会从中删除规则Amazon WAF 它只是从此 Web ACL 删除规则。
6. 选择 Update (更新)。
7. 取消 Web ACL 与所有 ACL 的关联 CloudFront 分配和Application Load Balancer. 在存储库的Rule选项卡，下Amazon使用此 Web ACL 的资源，选择x对于每个 API Gateway API，CloudFront 分配或 Application Load Balancer。
8. 在 Web ACLs 页面上，确认已选择要删除的 Web ACL，然后选择 Delete。

测试 Web ACL

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

为了确保您不会意外配置Amazon WAFClassic 用于阻止要允许的请求或允许的请求，建议您在网站或 Web 应用程序中开始使用 Web ACL 之前先对其进行全面测试。

主题

- [对与 Web ACL 中的规则匹配的 Web 请求计数 \(p. 292\)](#)
- [查看 API Gateway 的 Web 请求的采样 CloudFront 或已将Application Load Balancer 转发给的Amazon WAFClassic \(p. 294\)](#)

对与 Web ACL 中的规则匹配的 Web 请求计数

在向 Web ACL 添加规则时，需指定您希望Amazon WAFClassic：对与该规则中所有条件匹配的 Web 请求进行允许、阻止或计数。建议您首先进行以下配置：

- 将 Web ACL 中的所有规则配置为对 Web 请求计数
- 将 Web ACL 的默认操作设置为允许请求

在此配置中，Amazon WAFClassic 会根据第一个规则中的条件检查每个 Web 请求。如果 Web 请求与该规则中的所有条件都匹配，Amazon WAFClassic 会增加该规则的计数器。那么Amazon WAFClassic 会根据下一个规则中的条件检查 Web 请求。如果请求与该规则中的所有条件都匹配，Amazon WAFClassic 会增加规则的计数器。这种情况一直持续到Amazon WAFClassic 已根据所有规则中的条件检查完请求进行检查。

在将 Web ACL 中的所有规则配置为对请求计数并将 Web ACL 与一个 Amazon API Gateway API Gateway API 关联后，CloudFront 分配或 Application Load Balancer，您可以在 Amazon 中查看结果计数 CloudWatch 图表。对于 Web ACL 中的每个规则以及 API Gateway 的所有请求，CloudFront 或者一个 Application Load Balancer 转发给 Amazon WAF Web ACL 的 Classic CloudWatch 让您可以：

- 查看前一个小时或前三个小时的数据
- 更改数据点之间的间隔
- 更改计算 CloudWatch 对数据执行，如最大值、最小值、平均值或求和

Note

Amazon WAF Classic CloudFront 是一种全局性服务和指标，仅当您选择美国东部（弗吉尼亚州北部）区域中的 Amazon Web Services Management Console。如果您选择其他区域，Amazon WAF Classic 指标将显示在 CloudWatch 控制台。

查看 Web ACL 中规则的数据

1. 登录 Amazon Web Services Management Console 打开 CloudWatch 控制台位于 <https://console.aws.amazon.com/cloudwatch/>。
2. 在导航窗格的 Metrics 下，选择 WAF。
3. 选中要查看其数据的 Web ACL 对应的复选框。
4. 更改适用的设置：

统计数据

选择符合以下条件的计算 CloudWatch 对数据执行。

时间范围

选择您要查看前一个小时还是前三个小时的数据。

周期

选择图表中的数据点之间的间隔。

规则

选择要查看其数据的规则。

请注意以下几点：

- 如果您刚刚将 Web ACL 与一个 API Gateway API 关联，CloudFront 分配或 Application Load Balancer，您可能需要等待几分钟时间，数据才会显示在图表上，Web ACL 的指标才会显示在可用指标的列表中。
 - 如果您关联了多个 API Gateway API，CloudFront 使用 Web ACL 的 Application Load Balancer CloudWatch 数据将包含与该 Web ACL 关联的所有分配的所有请求。
 - 您可以将鼠标光标悬停在数据点上方，以获取更多信息。
 - 该图表不会自动自行刷新。要更新显示，请选择刷新 () 图标。
5. (可选) 查看 API Gateway 的各个请求的详细信息 CloudFront 或已将 Application Load Balancer 转发给的 Amazon WAF Classic。有关更多信息，请参阅 [查看 API Gateway 的 Web 请求的采样 CloudFront 或已将 Application Load Balancer 转发给的 Amazon WAF Classic \(p. 294\)](#)。
 6. 如果您确定规则正在截获您不想截获的请求，请更改相应设置。有关更多信息，请参阅 [创建和配置 Web 访问控制列表 \(Web ACL\) \(p. 252\)](#)。

如果您对所有规则只截获正确的请求感到满意，则将每个规则的操作改为 Allow 或 Block。有关更多信息，请参阅 [编辑 Web ACL \(p. 291\)](#)。

查看 API Gateway 的 Web 请求的采样 CloudFront 或已将 Application Load Balancer 转发给的 Amazon WAFClassic

在 Amazon WAFClassic 控制台，您可以查看 API Gateway 的请求的采样 CloudFront 或已将 Application Load Balancer 转发给的 Amazon WAF 经典，用于检查。对于每个示例请求，您可以查看关于该请求的详细数据，例如来源 IP 地址和请求中包含的标头。您还可以查看请求匹配哪个规则，以及该规则配置为允许还是阻止请求。

请求采样包含多达 100 个与每个规则中的所有条件都匹配的请求，还有用于默认操作的 100 个请求，该默认操作适用于未与任何规则中的所有条件匹配的请求。示例中的请求来自所有 API Gateway API，CloudFront 在前 15 分钟内收到内容请求的边缘站点或 Application Load Balancer。

查看 API Gateway 的 Web 请求的采样；CloudFront 或已将 Application Load Balancer 转发给的 Amazon WAFClassic

1. 登录 Amazon Web Services Management Console 打开 Amazon WAF 控制台位于 <https://console.aws.amazon.com/wafv2/>.

如果您看到切换到 Amazon WAFClassic 在导航窗格中，选择它。

2. 在导航窗格中，选择要查看其请求的 Web ACL。
3. 在右窗格中，选择 Requests 选项卡。

Sampled requests 表显示每个请求的下列值：

源 IP

该请求来自的 IP 地址或 (如果查看者使用 HTTP 代理或 Application Load Balancer 发送请求) 代理或 Application Load Balancer 的 IP 地址。

URI

请求的 URI 路径，用于标识资源，例如 /images/daily-ad.jpg。这包括查询字符串或 URI 的片段组件。想要了解有关信息，请参阅 [统一资源标识符 \(URI\)：通用语法](#)。

Matches rule

确定 Web ACL 中 Web 请求匹配其所有条件的第一个规则。如果 Web 请求与 Web ACL 中任何规则的所有条件均不匹配，则 Matches rule 的值为 Default。

请注意，当 Web 请求匹配某规则中的所有条件并且用于该规则的操作是计数、Amazon WAFClassic 将根据 Web ACL 中的后续规则继续检查 Web 请求。在此情况下，一个 Web 请求会在采样的请求列表中出现两次；一次是出于具有 Count 操作的规则，一次是出于后续规则或默认操作。

操作

指示相应规则的操作是 Allow、Block 还是 Count。

Time

那个时候 Amazon WAFClassic 收到了来自 API Gateway 的请求，CloudFront 或您的 Application Load Balancer。

4. 要显示有关请求的更多信息，请选择位于该请求的 IP 地址左侧的箭头。Amazon WAFClassic 将显示以下信息：

源 IP

与表中 Source IP 列的值相同的 IP 地址。

国家/地区

请求来源国家/地区的双字母国家/地区代码。如果查看者使用 HTTP 代理或Application Load Balancer 发送请求，则为 HTTP 代理或Application Load Balancer 所在国家/地区的双字母国家/地区代码。

有关双字母国家/地区代码及其对应的国家/地区名称的列表，请参阅维基百科条目 [ISO 3166-1 alpha-2](#)。

方法

请求的 HTTP 请求方法：GET、HEAD、OPTIONS、PUT、POST、PATCH 或 DELETE。

URI

与表中 URI 列的值相同的 URI。

Request headers

请求中的请求标头和标头值。

5. 要刷新示例请求列表，请选择 Get new samples。

使用Amazon WAF与结合使用的经典规则组Amazon Firewall Manager

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

网络 ACL 和安全组都允许（因此可到达您的实例）的发起 ping 的Amazon WAFClassic规则组是您添加到的一组规则。Amazon WAFClassicAmazon Firewall Manager政策。您可以创建自己的规则组，也可以从 Amazon Web Services Marketplace 购买托管规则组。

Important

如果要添加Amazon Web Services Marketplace规则组到您的 Firewall Manager 策略，您组织中的每个账户都必须先订阅该规则组。在所有账户都已订阅后，您可以将该规则组添加到某个策略。有关更多信息，请参阅[Amazon Web Services Marketplace 规则组 \(p. 283\)](#)。

主题

- [创建Amazon WAF经典规则组 \(p. 295\)](#)
- [从中添加和删除规则Amazon WAF经典规则组 \(p. 296\)](#)

创建Amazon WAF经典规则组

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

当您创建时Amazon WAF要与之配合使用的经典规则组Amazon Firewall Manager，请指定要添加到组的规则。

创建规则组 (控制台)

1. 登录到Amazon Web Services Management Console使用Amazon Firewall Manager在先决条件中设置的管理员账户，然后通过以下网址打开 Firewall Manager 控制台：<https://console.amazonaws.cn/wafv2/fms>.

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 Amazon Firewall Manager 管理员账户 \(p. 404\)](#)。

2. 在导航窗格中，选择切换到Amazon WAFClassic.
3. 在Amazon WAF经典导航窗格，选择规则组.
4. 选择 Create rule group (创建规则组)。

Note

您不能将基于速率的规则添加到规则组。

5. 如果您已创建要添加到规则组的规则，请选择 Use existing rules for this rule group (对此规则组使用现有规则)。如果您要创建要添加到规则组的新规则，请选择 Create rules and conditions for this rule group (为此规则组创建规则和条件)。
6. 请选择 Next (下一步)。
7. 如果您选择创建规则，请按照[创建规则并添加条件 \(p. 281\)](#)中的步骤创建规则。

Note

使用Amazon WAF创建规则的经典控制台。

创建所有需要的规则后，请转到下一步。

8. 键入规则组名称。
9. 要将规则添加到规则组，请选择规则，然后选择 Add rule (添加规则)。选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。有关选项的更多信息，请参阅[怎么样Amazon WAF经典作品 \(p. 240\)](#)。
10. 在添加完规则后，请选择 Create (创建)。

可通过将规则组添加到 Amazon WAF WebACL 并将 WebACL 操作设置为 Override to Count (覆盖以计数) 来测试规则组。此操作将覆盖您为组中包含的规则选择的任何操作，并且仅对匹配的请求计数。有关更多信息，请参阅[创建 Web ACL \(p. 287\)](#)。

从中添加和删除规则Amazon WAF经典规则组

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

您可以在Amazon WAF经典规则组。

从规则组中删除规则不会删除规则本身，而只会将该规则从规则组移除。

在规则组中添加或删除规则 (控制台)

1. 登录到Amazon Web Services Management Console使用Amazon Firewall Manager在先决条件中设置的管理员账户，然后通过以下网址打开 Firewall Manager 控制台：<https://console.amazonaws.cn/wafv2/fms>.

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 Amazon Firewall Manager 管理员账户 \(p. 404\)](#)。

2. 在导航窗格中，选择切换到Amazon WAFClassic.
3. 在Amazon WAF经典导航窗格，选择规则组。
4. 选择要编辑的规则组。
5. 选择 Edit rule group (编辑规则组)。
6. 要添加规则，请执行以下步骤：
 - a. 选择一个规则，然后选择 Add rule to rule group (将规则添加到规则组)。选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。有关选项的更多信息，请参阅[怎么样Amazon WAF经典作品 \(p. 240\)](#)。重复操作以将更多规则添加到规则组。

Note

您不能将基于速率的规则添加到规则组。

- b. 选择 Update (更新)。
7. 要删除规则，请执行以下步骤：
 - a. 选择要删除的规则旁的 X。重复操作以从规则组中删除更多规则。
 - b. 选择 Update (更新)。

开始使用Amazon Firewall Manager启用Amazon WAF经典规则

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

您可以使用Amazon Firewall Manager启用Amazon WAF规则，Amazon WAF经典规则，Amazon Shield Advanced保护和 Amazon VPC 安全组。每一项的设置步骤略有不同。

- 若要使用 Firewall Manager 启用规则，请使用最新版本的Amazon WAF，不要使用此主题。请按照[Amazon Firewall ManagerAmazon WAF政策入门 \(p. 408\)](#)中的步骤操作。
- 使用 Firewall Manager 启用Amazon Shield Advanced保护，请按照中的步骤操作[开始使用Amazon Firewall Manager Amazon Shield Advanced策略 \(p. 410\)](#)。
- 要使用 Firewall Manager 启用 Amazon VPC 安全组，请按照中的步骤操作[开始使用Amazon Firewall ManagerAmazon VPC 安全组策略 \(p. 413\)](#)。

使用 Firewall Manager 启用Amazon WAF经典规则，请按顺序执行以下步骤。

主题

- [第 1 步：完成先决条件 \(p. 298\)](#)
- [第 2 步：创建规则 \(p. 298\)](#)
- [第 3 步：创建规则组 \(p. 298\)](#)
- [第 4 步：创建并应用Amazon Firewall ManagerAmazon WAF经典策略 \(p. 299\)](#)

第 1 步：完成先决条件

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager先决条件 \(p. 403\)](#)介绍了这些步骤。在继续执行[第 2 步：创建规则 \(p. 298\)](#)之前，请满足所有先决条件后。

第 2 步：创建规则

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

在本步骤中，您将使用创建规则。Amazon WAFClassic。如果您已有Amazon WAF要与之配合使用的经典规则Amazon Firewall Manager，请跳过此步骤然后转到[第 3 步：创建规则组 \(p. 298\)](#)。

Note

使用Amazon WAF创建规则的经典控制台。

创建Amazon WAF经典规则（控制台）

- 创建您的规则，然后将您的条件添加到规则。有关更多信息，请参阅[创建规则并添加条件 \(p. 281\)](#)。

您现在已准备好转到[第 3 步：创建规则组 \(p. 298\)](#)。

第 3 步：创建规则组

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

规则组是一系列规则，用于定义在满足特定的一组条件时要执行的操作。您可以使用 Amazon Web Services Marketplace 中的托管规则组，也可以创建自己的规则组。有关托管规则组的信息，请参阅[Amazon Web Services Marketplace 规则组 \(p. 283\)](#)。

要创建您自己的规则组，请执行以下步骤。

创建规则组（控制台）

- 登录到Amazon Web Services Management Console使用Amazon Firewall Manager在先决条件中设置的管理员账户，然后通过以下网址打开 Firewall Manager 控制台：<https://console.amazonaws.cn/wafv2/fms>。
- 在导航窗格中，选择 Security policies (安全策略)。
- 如果您未满足先决条件，控制台会显示有关如何解决任何问题的说明。按照这些说明操作，然后再次开始本步骤（创建规则组）。如果您已满足先决条件，请选择 Close (关闭)。

4. 选择 Create policy (创建策略)。

对于 Policy type (策略类型)，选择 Amazon WAF Classic。

5. 选择创建Amazon Firewall Manager策略并添加新规则组。
6. 选择一个Amazon Web Services 区域然后选择下一步。
7. 由于您已创建规则，因此无需创建条件。请选择 Next (下一步)。
8. 由于您已创建规则，因此无需创建规则。请选择 Next (下一步)。
9. 选择 Create rule group (创建规则组)。
10. 对于 Name (名称)，输入一个易于理解的名称。
11. 输入名称的 CloudWatch 指标指标Amazon WAFClassic Classic 将创建并与规则组关联。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 或以下特殊字符：_! " # + * } , . / 。且不能包含空格。
12. 选择规则，然后选择 Add rule (添加规则)。规则具有一项操作设置，可让您选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。在本教程中，请选择 Count (计数)。重复添加规则，直到您已将所需的所有规则添加到规则组。
13. 选择 Create (创建)。

您现在已准备好转到[第 4 步：创建并应用Amazon Firewall ManagerAmazon WAF经典策略 \(p. 299\)](#)。

第 4 步：创建并应用Amazon Firewall ManagerAmazon WAF经典策略

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

在创建规则组后，您将创建 Amazon Firewall Manager Amazon WAF 策略。Firewall ManagerAmazon WAF 策略包含您要应用于资源的规则组。

创建 Firewall ManagerAmazon WAF策略 (控制台)

1. 在您创建规则组 (上一个过程[第 3 步：创建规则组 \(p. 298\)](#)中的最后一步) 后，控制台会显示 Rule group summary (规则组摘要) 页面。请选择 Next (下一步)。
2. 对于 Name (名称)，输入一个易于理解的名称。
3. 对于 Policy type (策略类型)，选择 WAF。
4. 适用于区域，选择Amazon Web Services 区域。为了保护亚马逊 CloudFront 选择资源，选择服务全球。

为了保护多个区域中的资源 (而不是 CloudFront 资源)，您必须为每个区域创建单独的 Firewall Manager 策略。

5. 选择要添加的规则组，然后选择 Add rule group (添加规则组)。
6. 策略有两个可能的操作：按规则组设置的操作和计数。如果您要测试策略和规则组，请将操作设置为 Count (计数)。此操作会覆盖该策略中包含的规则组指定的任何阻止 操作。即，如果将策略的操作设置为 Count (计数)，则只会对这些请求进行计数而不会阻止它们。相反，如果将策略的操作设置为 Action set by rule group (由规则组设置的操作)，则会使用该策略中规则组的操作。在本教程中，请选择 Count (计数)。
7. 请选择 Next (下一步)。
8. 如果您希望仅在策略中包含特定账户，或者仅从策略中排除特定账户，请选择 Select accounts to include/exclude from this policy (optional) (选择要在此策略中包含/排除的账户 (可选))。选择 Include only these accounts in this policy (仅在此策略中包含这些账户) 或 Exclude these accounts from this

policy (仅从此策略中排除这些账户)。您只能选择一个选项。选择 Add (添加)。选择要包含或排除的账号，然后选择 OK (确定)。

Note

如果您不选择此选项，Firewall Manager 会将策略应用于您组织中的所有账户 Amazon Organizations。如果您将新账户添加到组织，Firewall Manager 会将该策略自动应用于该账户。

9. 选择要保护的资源的类型。
10. 如果您只想保护带特定标签的资源，或者排除带特定标签的资源，请选择 Use tags to include/exclude resources (使用标签来包含/排除资源)，输入标签，然后选择 Include (包含) 或 Exclude (排除)。您只能选择一个选项。

如果您输入了多个标签 (以逗号分隔)，并且某个资源带有任一这些标签，则会将该资源视为匹配项。

有关标签的更多信息，请参阅[使用标签编辑器](#)。

11. 选择 Create and apply this policy to existing and new resources (创建此策略并将其应用于现有资源和新资源)。

此选项在 Amazon Organizations 中为组织内的每个适用账户创建一个 Web ACL，并将 Web ACL 与账户中的指定资源关联。此选项还将策略应用于符合上述条件 (资源类型和标签) 的所有新资源。或者，如果你选择创建此策略但不将策略应用于现有资源或新资源，Firewall Manager 会在组织内的每个适用账户中创建一个 Web ACL，但不会将 Web ACL 应用于任何资源。您稍后必须将策略应用于资源。

12. 在默认设置中保留对 Replace existing associated web ACLs (替换现有关联 Web ACL) 的选择。

选择此选项后，Firewall Manager 会从范围内资源中删除所有现有 Web ACL 关联，然后再将新策略的 Web ACL 与资源关联。

13. 请选择 Next (下一步)。
14. 查看新策略。要进行任何更改，请选择 Edit (编辑)。若您满意所创建的策略，请选择 Create policy (创建策略)。

教程：创建Amazon Firewall Manager具有分层规则的策略

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

与Amazon Firewall Manager，您可以创建和应用Amazon WAFClassic包含分层规则的保护策略。也就是说，您可以集中创建和实施某些规则，但将特定于账户的规则创建和维护委派给其他人。您可以监控集中应用 (常见) 的规则，以防止意外删除或误操作，从而确保一致地应用它们。特定于账户的规则可根据各个团队的需求添加进一步的保护。

Note

最新版本的 Amazon WAF 中内置了此功能，不需要进行任何特殊处理。如果您尚未使用Amazon WAF经典版本，请改为使用最新版本的。请参阅[为 Amazon WAF 创建Amazon Firewall Manager策略 \(p. 423\)](#)。

以下教程介绍如何创建一组分层的保护规则。

主题

- [第 1 步：指定 Firewall Manager 管理员账户 \(p. 301\)](#)

- [第 2 步：使用 Firewall Manager 管理员账户创建规则组 \(p. 301\)](#)
- [第 3 步：创建 Firewall Manager 策略并附加通用规则组 \(p. 301\)](#)
- [第 4 步：添加特定于账户的规则 \(p. 301\)](#)
- [结论 \(p. 302\)](#)

第 1 步：指定 Firewall Manager 管理员账户

使用 Amazon Firewall Manager，您必须在组织中指定一个账户作为 Firewall Manager 管理员账户。该账户可以是管理账户，也可以是组织中的成员账户。

您可以使用 Firewall Manager 管理员账户来创建一组通用规则，以便应用于组织中的其他账户。组织中的其他账户无法更改这些集中应用的规则。

要将账户指定为 Firewall Manager 管理员账户并完成使用 Firewall Manager 的其他先决条件，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。如果您已经完成了先决条件，则可以跳到本教程的步骤 2。

在本教程中，我们将管理员账户称为 **Firewall-Administrator-Account**。

第 2 步：使用 Firewall Manager 管理员账户创建规则组

接下来，使用 **Firewall-Administrator-Account** 创建规则组。此规则组包含您将应用于由您在下一步中创建的策略控制的所有成员账户的通用规则。仅 **Firewall-Administrator-Account** 可以对这些规则和容器规则组进行更改。

在本教程中，我们将此容器规则组称为 **Common-Rule-Group**。

要创建规则组，请参阅 [创建 Amazon WAF 经典规则组 \(p. 295\)](#) 中的说明。请记住使用 Firewall Manager 管理员账户登录控制台 (**Firewall-Administrator-Account**) 在遵循这些说明时。

第 3 步：创建 Firewall Manager 策略并附加通用规则组

使用 **Firewall-Administrator-Account**，创建 Firewall Manager 策略。在创建此策略时，您必须执行以下操作：

- 将 **Common-Rule-Group** 添加到新策略。
- 在组织中包含您希望 **Common-Rule-Group** 应用到的所有账户。
- 添加您希望 **Common-Rule-Group** 应用到的所有资源。

有关创建策略的说明，请参阅 [创建 Amazon Firewall Manager 策略 \(p. 422\)](#)。

这将在每个指定的账户中创建一个 Web ACL，并将 **Common-Rule-Group** 添加到每个这些 Web ACL 中。创建策略后，此 Web ACL 和通用规则将部署到所有指定的账户。

在本教程中，我们将此 Web ACL 称为 **Administrator-Created-ACL**。现在，组织的每个指定成员账户中都存在唯一的 **Administrator-Created-ACL**。

第 4 步：添加特定于账户的规则

组织中的每个成员账户现在都可以将自己的特定于账户的规则添加到其账户中存在的 **Administrator-Created-ACL**。已经在 **Administrator-Created-ACL** 中的通用规则连同新的特定于账户的规则会继续应用。Amazon WAF 根据规则在 Web ACL 中的出现顺序检查 Web 请求。这适用于 **Administrator-Created-ACL** 和特定于账户的规则。

要向 **Administrator-Created-ACL** 中添加规则，请参阅 [编辑 Web ACL \(p. 19\)](#)。

结论

您现在拥有一个 Web ACL，其中包含由 Firewall Manager 管理员账户管理的通用规则以及每个成员账户维护的特定于账户的规则。

每个账户中的 **Administrator-Created-ACL** 都引用单个 **Common-Rule-Group**。因此，Firewall Manager 管理员账户在未来对 **Common-Rule-Group** 将立即在每个成员账户中生效。

成员账户无法更改或删除 **Common-Rule-Group** 中的通用规则。

特定于账户的规则不影响其他账户。

记录 Web ACL 流量信息

Note

这是 Amazon WAF 经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。
有关的最新版本 Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

您可以启用日志记录以获取有关 Web ACL 分析的流量的详细信息。日志中包含的信息包括 Amazon WAF Classic 从 Amazon 资源收到请求的时间，以及每个请求所匹配的规则的操作。

要开始使用，您需要设置 Amazon Kinesis Data Firehose。在这个过程中，您需要选择用于存储日志的目标。接下来，选择您要启用日志记录的 Web ACL。启用日志记录后，通过 firehose 将日志 Amazon WAF 传送到您的存储目的地。

有关如何创建 Amazon Kinesis Firehose 和查看存储的日志相关信息，请参阅[什么是 Amazon Kinesis Data Firehose ?](#)。要了解您的 Kinesis Data Firehose 所需的权限，请参阅[使用 Amazon Kinesis Data Firehose 控制访问](#)。

您必须拥有以下权限才能成功启用日志记录：

- iam:CreateServiceLinkedRole
- firehose:ListDeliveryStreams
- waf:PutLoggingConfiguration

有关服务相关角色以及 iam:CreateServiceLinkedRole 权限的更多信息，请参阅[将服务相关角色用于 Amazon WAF Classic \(p. 321\)](#)。

为 Web ACL 启用日志记录

1. 使用以前缀“aws-waf-logs-”开头的名称创建 Amazon Kinesis Data Firehose 例如，aws-waf-logs-us-east-2-analytics。使用 PUT 源，在您执行操作的区域中创建 Data Firehose。如果您要为亚马逊捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）创建消防管。有关更多信息，请参阅[创建 Amazon Kinesis Data Firehose 传输流](#)。

Important

请勿选择 Kinesis stream 作为源。

一条 Amazon WAF 经典日志等同于一条 Kinesis Data Firehose 记录。如果您通常每秒收到 10,000 个请求并且启用了完整日志，则在 Kinesis Data Firehose 中应设置每秒 10,000 条记

录。如果您没有正确配置 Kinesis Data Firehose，Amazon WAFClassic 将无法记录所有日志。有关更多信息，请参阅 [Amazon Kinesis Data Firehose 配额](#)。

2. 登录Amazon Web Services Management Console并打开Amazon WAF主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。

如果您在导航窗格中看到“切换到Amazon WAF经典”，请将其选中。

3. 在导航窗格中，选择 Web ACL。
4. 选择要为其启用日志记录的 Web ACL 的名称。这将在右侧窗格中打开一个包含 Web ACL 详细信息的页面。
5. 在 Logging (日志记录) 选项卡上，选择 Enable logging (启用日志记录)。
6. 选择您在第一步中创建的 Kinesis Data Firehose。您必须选择以“aws-waf-logs-”开头的消防管。
7. (可选) 如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 Add (添加)。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 cookie 字段，则日志中的 cookie 字段将为 REDACTED。
8. 选择启用日志记录。

Note

成功启用日志记录后，Amazon WAFClassic 将创建一个具有向 Amazon Kinesis Data Firehose 写入日志所需的权限的服务关联角色。有关更多信息，请参阅[将服务相关角色用于Amazon WAF Classic \(p. 321\)](#)：

禁用 Web ACL 的日志记录

1. 在导航窗格中，选择 Web ACL。
2. 选择要禁用其日志记录的 Web ACL 的名称。这将在右侧窗格中打开一个包含 Web ACL 详细信息的页面。
3. 在 Logging (日志记录) 选项卡上，选择 Disable logging (禁用日志记录)。
4. 在对话框中，选择 Disable logging (禁用日志记录)。

Example 示例日志

```
{
  "timestamp":1533689070589,
  "formatVersion":1,
  "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
  "terminatingRuleId":"Default_Action",
  "terminatingRuleType":"REGULAR",
  "action":"ALLOW",
  "httpSourceName":"CF",
  "httpSourceId":"i-123",
  "ruleGroupList":[
    {
      "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
      "terminatingRule":null,
      "nonTerminatingMatchingRules":[
        {
          "action": "COUNT",
          "ruleId": "4659b169-2083-4a91-bbd4-08851a9aaf74"}
      ],
      "excludedRules":
      [
        {
          "exclusionType":
            "EXCLUDED_AS_COUNT",
            "ruleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"}
      ]
    }
  ]
}
```



```
    ]
  },
  ],
  "rateBasedRuleList": [
    {
      "rateBasedRuleId": "7c968ef6-32ec-4fee-96cc-51198e412e7f",
      "limitKey": "IP",
      "maxRateAllowed": 100
    },
    {
      "rateBasedRuleId": "462b169-2083-4a93-bbd4-08851a9aaf30",
      "limitKey": "IP",
      "maxRateAllowed": 100
    }
  ],
  "nonTerminatingMatchingRules": [
    {
      "action": "COUNT",
      "ruleId": "4659b181-2011-4a91-bbd4-08851a9aaf52"
    }
  ],
  "httpRequest": {
    "clientIp": "192.10.23.23",
    "country": "US",
    "headers": [
      {
        "name": "Host",
        "value": "127.0.0.1:1989"
      },
      {
        "name": "User-Agent",
        "value": "curl/7.51.2"
      },
      {
        "name": "Accept",
        "value": "*/*"
      }
    ],
    "uri": "REDACTED",
    "args": "username=abc",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "cloud front Request id"
  }
}
```

下面是对这些日志中列出的各个项的说明：

timestamp

时间戳，以毫秒为单位。

formatVersion

日志的格式版本。

webaclId

Web ACL 的 GUID。

terminatingRuleId

终止请求的规则 ID。如果没有任何情况会终止请求，则值为 Default_Action。

terminatingRuleType

终止请求的规则的类型。可能的值：基于费率、常规和群组。

action

操作。终止规则的可能值为：ALLOW 和 BLOCK。COUNT 不是终止规则的有效值。

terminatingRuleMatch细节

有关与请求匹配的终止规则的详细信息。终止规则具有针对 Web 请求结束检查过程的操作。终止规则的可能操作是 ALLOW 和 BLOCK。这仅适用于 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。与所有用于检查多个事物的规则语句一样，Amazon WAF 对第一个匹配应用操作并停止检查 Web 请求。除了日志中报告的威胁之外，具有终止操作的 Web 请求还可能包含其他威胁。

httpSourceName

请求的源。可能的值：CF（如果源是亚马逊 CloudFront）、APIGW（如果源是 Amazon API Gateway）和 ALB（如果源是 Application Load Balancer）。

httpSourceId

源 ID。此字段显示关联亚马逊 CloudFront 发行版的 ID、API Gateway 的 REST API 或 Application Load Balancer 名称。

ruleGroupList

对此请求进行操作的规则组的列表。在前面的代码示例中，只有一个。

ruleGroupId

规则组的 ID。如果规则阻止了请求，则 ruleGroupId 的 ID 与 terminatingRuleId 的 ID 相同。

terminatingRule

规则组中终止了请求的规则。如果这是非空值，它还会包含 ruleId 和 action。在这种情况下，操作将始终为 BLOCK。

nonTerminatingMatching规则

规则组中与请求匹配的规则列表。这些规则将始终为 COUNT 规则（匹配的非终止规则）。

操作（nonTerminatingMatching规则组）

它将始终为 COUNT（匹配的非终止规则）。

ruleId（nonTerminatingMatching规则组）

规则组中与请求匹配并且为非终止规则的 ID。即 COUNT 规则。

excludedRules

规则组中您排除的规则列表。这些规则的操作设置为 COUNT。

exclusionType（excludedRules 组）

一种类型，指示排除的规则具有操作 COUNT。

ruleId（excludedRules 组）

规则组中排除的规则 ID。

rateBasedRule清单

对请求执行操作的基于速率的规则列表。

rateBasedRuleId

作用于请求的基于速率的规则 ID。如果这已终止请求，则 rateBasedRuleId 的 ID 与 terminatingRuleId 的 ID 相同。

limitKey

Amazon WAF 用于确定请求是否来自单个原因而需要受速率监控的字段。可能的值：IP。

maxRateAllowed

在五分钟内允许的最大请求数，具有与 limitKey 所指定的字段相同的值。如果请求数超过了 maxRateAllowed 并且还满足规则中指定的其他谓词，则 Amazon WAF 将触发为此规则指定的操作。

httpRequest

关于请求的元数据。

clientIp

发送请求的客户端的 IP。

country

请求的源国家/地区。Amazon WAF 如果无法确定原产国，则会将此字段设置为 -。

headers

标头的列表。

uri

请求的 URI。上述代码示例演示在编辑了此字段时应具有的值。

args

查询字符串。

httpVersion

HTTP 版本。

httpMethod

请求中的 HTTP 方法。

requestId

请求的 ID。

列出根据基于速率的规则而阻止的 IP 地址

Note

这是 Amazon WAF Classic 文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。对于最新版本的 Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon WAF Classic 提供根据基于速率的规则而阻止的 IP 地址。

查看根据基于速率的规则阻止的地址

1. 登录到 Amazon Web Services Management Console 然后打开 Amazon WAF 控制台<https://console.aws.amazon.com/wafv2/>。

如果你明白切换到 Amazon WAF Classic 在导航窗格中，选择它。

2. 在导航窗格中，选择 Rules (规则)。
3. 在 Name 列中，选择一个基于速率的规则。

列表显示该规则当前阻止的 IP 地址。

操作方法Amazon WAFClassic CloudFront 功能

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

在创建 Web ACL 时，您可以指定一个或多个 CloudFront 你想要的发行版Amazon WAFClassicAmazon WAF Classic 便开始根据您在 Web ACL 中确定的条件来允许、阻止对于这些分配的 Web 请求或对 Web 请求计数。CloudFront 提供了一些功能来增强功能Amazon WAF经典功能。本章介绍了几种用于配置的方法。CloudFront 要做 CloudFront 和Amazon WAFClassic 可以更好地协作。

主题

- [使用Amazon WAF经典搭配 CloudFront 自定义错误页面 \(p. 307\)](#)
- [使用Amazon WAF经典搭配 CloudFront对于在您自己的 HTTP 服务器上运行的应用程序 \(p. 307\)](#)
- [选择 CloudFront 响应的 HTTP 方法 \(p. 308\)](#)

使用Amazon WAF经典搭配 CloudFront 自定义错误页面

何时Amazon WAFClassic 会根据您指定的条件阻止 Web 请求，它会将 HTTP 状态代码 403 (Forbidden) 返回给 CloudFront。下一步：CloudFront 会将该状态代码返回给查看器。然后，查看器显示简要且采用稀疏格式的默认消息，如下所示：

Forbidden: You don't have permission to access /myfilename.html on this server.

如果您更愿意显示自定义错误消息，可能与您网站其他部分使用相同的格式设置，则您可以配置 CloudFront 会将包含自定义错误消息的对象 (例如，HTML 文件) 返回给查看器。

Note

CloudFront 无法区分由您的源返回的 HTTP 状态代码 403 与由返回的 HTTP 状态代码 403Amazon WAFClassic 表示请求被阻止。这意味着，您无法根据 HTTP 状态代码 403 的不同原因返回不同的自定义错误页面。

有关的更多信息 CloudFront 自定义错误页面，请参阅[自定义错误响应](#)中的亚马逊 CloudFront 开发人员指南。

使用Amazon WAF经典搭配 CloudFront对于在您自己的 HTTP 服务器上运行的应用程序

当您使用以下应用程序时：Amazon WAF经典搭配 CloudFront，则您可以保护运行在任意 HTTP webserver 上的应用程序，不论这是在 Amazon Elastic Compute Cloud (Amazon EC2) 中运行的 webserver 还是您私下管理的 webserver。您也可以配置 CloudFront 要求在之间使用 HTTPS CloudFront和您自己的 webserver，以及在查看器和之间使用 CloudFront。

要求 HTTPS CloudFront 和您自己的Webserver

要求在以下时间之间使用 HTTP CloudFront 和您自己的 webserver，您可以使用 CloudFront 自定义原点功能并配置源协议策略和源域名特定来源的设置。在您的 CloudFront 配置时，您可以指定服务器的 DNS 名称，并指定所需的端口和协议。CloudFront 在从源中提取对象时使用。您还应确保自定义源服务器上的 SSL/TLS 证书与您已配置的源域名匹配。当您在外部使用自己的 HTTP Web 服务器时，Amazon 则您必须使用由信任的第三方证书颁发机构 (CA) (例如，Comodo) 签署的证书。DigiCert，或赛门铁克。有关要求是在之间使用 HTTPS 进行通信 CloudFront 和你自己的 web 服务器，请参阅主题 [要求在之间使用 HTTPS 进行通信 CloudFront 和您的自定义源](#) 中的亚马逊 CloudFront 开发人员指南。

要求在查看器和 之间使用 HTTPS CloudFront

要求在查看器和之间使用 HTTPS CloudFront，您可以更改查看器协议策略对于您的中的一个或多个缓存行为 CloudFront 分配。有关在查看器和之间使用 HTTPS CloudFront，请参阅主题 [要求在查看器和之间使用 HTTPS 进行通信 CloudFront](#) 中的亚马逊 CloudFront 开发人员指南。您也可以自带 SSL 证书，这样查看器可以连接到您的 CloudFront 例如，使用您自己的域名通过 HTTPS 进行分发 [https://www.mysite.com](#)。有关更多信息，请参阅主题 [配置备用域名和 HTTPS](#) 中的亚马逊 CloudFront 开发人员指南。

选择 CloudFront 响应的 HTTP 方法

当你创建亚马逊时 CloudFront Web 分配，您可以选择您希望的 HTTP 方法 CloudFront 处理并转发到您的源。可从以下选项中进行选择：

- GET、HEAD— 您可以使用 CloudFront 只能从源获取对象或获取对象标头。
- GET、HEAD、选项— 您可以使用 CloudFront 只能从源获取对象、获取对象标头或检索您的源服务器支持的选项的列表。
- GET、HEAD、OPTIONS、PUT、POST、补丁、删除— 您可以使用 CloudFront 获取、添加、更新和删除对象，并获取对象标头。此外，您可以执行其他 POST 操作，例如从 Web 表格提交数据。

您还可以使用 Amazon WAF 经典字符串匹配条件，如中所述。 [使用字符串匹配条件 \(p. 270\)](#)。如果你想使用多种方法的组合 CloudFront 支持，例如 GET 和 HEAD，则您不需要配置 Amazon WAF Classic 用于阻止使用其他方法的请求。如果你想允许使用以下方法的组合 CloudFront 不支持，例如 GET、HEAD、和 POST，你可以配置 CloudFront 响应所有方法，然后使用 Amazon WAF Classic 用于阻止使用其他方法的请求。

有关选择 CloudFront 响应，请参阅 [允许的 HTTP 方法](#) 在主题中 [您创建或更新 Web 分配时指定的值](#) 中的亚马逊 CloudFront 开发人员指南。

Amazon WAF 经典版中的安全性

Note

这是 Amazon WAF 经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅 [将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。有关的最新版本 Amazon WAF，请参阅 [Amazon WAF \(p. 5\)](#)。

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业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。 [责任共担模型](#) 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 Web Services 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，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Amazon WAF Classic 的合规性计划，请参阅 [合规性计划范围内的 Amazon 服务](#)。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Amazon WAF Classic 时应用责任共担模式。以下主题说明如何配置 Amazon WAF Classic 以实现您的安全性和合规性目标。您还将了解如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon WAF Classic 资源。

主题

- [中的 Amazon WAF 数据保护保护保护保护保护保护 \(p. 309\)](#)
- [Amazon WAF Classic 的身份和访问管理 \(p. 310\)](#)
- [中的日志记录和监控 Amazon WAF Classic \(p. 324\)](#)
- [的合规性验证 Amazon WAF Classic \(p. 325\)](#)
- [中的故障恢复能力 Amazon WAF Classic \(p. 326\)](#)
- [中的基础设施安全性 Amazon WAF Classic \(p. 326\)](#)

中的 Amazon WAF 数据保护保护保护保护保护保护保护

Note

这是 Amazon WAF 经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。有关的最新版本 Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon [共享责任模型](#) 适用于 Amazon WAF 经典中的数据保护。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（例如您客户的电子邮件地址）放入标签或自由格式文本字段（例如名称字段）。这包括当您使用控制台、API 或 Amazon SDK Amazon Web Services 使用 CA Amazon WAF Classic 或其他设备时。Amazon CLI 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。

Amazon WAF 传统实体（例如 Web ACL、规则和条件）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

删除 Amazon WAF 经典资源

您可以删除您按照标准说明创建的 Amazon WAF 资源。请参阅以下部分中每种资源类型的指南。

- [删除 Web ACL \(p. 291\)](#)
- [从中添加和删除规则 Amazon WAF 经典规则组 \(p. 296\)](#)

- [删除规则 \(p. 283\)](#)

Amazon WAFClassic 的身份和访问管理

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）来使用 Amazon WAF Classic 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- [受众 \(p. 210\)](#)
- [使用身份进行身份验证 \(p. 211\)](#)
- [使用策略管理访问 \(p. 212\)](#)
- [Amazon WAF经典如何与 IAM 配合使用 \(p. 313\)](#)
- [适用于Amazon WAF Classic 的基于身份的策略示例 \(p. 318\)](#)
- [对Amazon WAF传统身份和访问进行故障排除 \(p. 320\)](#)
- [将服务相关角色用于Amazon WAF Classic \(p. 321\)](#)

受众

使用Amazon Identity and Access Management (IAM) 的方式因您可以在Amazon WAF Classic 中执行的操作而异。

服务用户-如果您使用Amazon WAF Classic 服务来完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多Amazon WAF经典功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问Amazon WAF Classic 中的功能，请参阅[对Amazon WAF传统身份和访问进行故障排除 \(p. 320\)](#)。

服务管理员 — 如果您在公司负责管理Amazon WAF Classic 资源，则您可能具有Amazon WAF Classic 的完全访问权限。您有责任确定您的服务用户应访问哪些Amazon WAF Classic 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与Amazon WAF Classic 搭配使用的更多信息，请参阅[Amazon WAF经典如何与 IAM 配合使用 \(p. 313\)](#)。

IAM 管理员 — 如果您是 IAM 管理员，您可能希望了解有关您可以如何编写策略以管理对Amazon WAF Classic 的访问的详细信息。要查看您可在 IAM 中使用的Amazon WAF经典基于身份的策略示例，请参阅[适用于Amazon WAF Classic 的基于身份的策略示例 \(p. 318\)](#)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅 Amazon 一般参考中的[签名版本 4 签名流程](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 Amazon Account Management 参考指南 中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

IAM 用户和组

[IAM 用户](#)是 Amazon Web Services 账户内对某个人或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

[IAM 角色](#)是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以担任角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的[使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 – 某些 Amazon Web Services 使用其它 Amazon Web Services 中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

- 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关[操作](#)，请参阅《服务授权参考》中的 [Access、资源和条件键](#)。Amazon WAFAmazon WAF
- 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 [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](#)。
- 服务相关角色 – 服务相关角色是与 Amazon Web Service 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的[何时创建 IAM 角色（而不是用户）](#)。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的[JSON 策略概览](#)。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 iam:GetRole 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的[在托管式策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 Amazon 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体 (账户成员、用户或角色) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Simple Storage Service (Amazon S3) 、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的 [访问控制列表 \(ACL\) 概览](#)。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体 (IAM 用户或角色) 授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 [IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体 (包括每个 Amazon Web Services 账户根用户) 的权限。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 [SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的 [会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的 [策略评估逻辑](#)。

Amazon WAF经典如何与 IAM 配合使用

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL) ，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

在使用 IAM 管理对Amazon WAF Classic 的访问权限之前，您应该了解哪些 IAM 功能可用于Amazon WAF Classic。

您可以与Amazon WAF Clastic 配合使用的 IAM 功能

IAM 功能	Amazon WAF经典支持
基于身份的策略 (p. 314)	是
基于资源的策略 (p. 314)	否
策略操作 (p. 314)	是
策略资源 (p. 315)	是
策略条件键 (特定于服务) (p. 316)	是

IAM 功能	Amazon WAF经典支持
ACL (p. 317)	否
ABAC (策略中的标签) (p. 317)	部分
临时凭证 (p. 317)	是
委托人权限 (p. 318)	是
服务角色 (p. 318)	是
服务相关角色 (p. 318)	是

要大致了解Amazon WAF Classic 和其他Amazon服务如何与大多数 IAM 功能一起使用，请参阅《[IAM 用户指南](#)》中的与 [IAM 一起使用的Amazon服务](#)。

适用于Amazon WAF Classic 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素引用](#)。

要查看基于身份Amazon WAF的策略的示例，请参阅[适用于Amazon WAF Classic 的基于身份的策略示例 \(p. 318\)](#)。

Amazon WAF经典中的基于资源的策略

支持基于资源的策略。	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 角色与基于资源的策略有何不同](#)。

Amazon WAFClassic 的政策行动

支持策略操作	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

[要查看Amazon WAF经典操作列表，请参阅服务授权参考中的Amazon WAF区域定义的操作Amazon WAF和区域定义的操作。](#)

Amazon WAFClassic 中的策略操作在操作前使用以下前缀：

```
waf
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
  "waf:action1",
  "waf:action2"
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定Amazon WAF Classic 中以开头的所有操作List，包括以下操作，包括以下操作：

```
"Action": "waf:List*"
```

要查看基于身份Amazon WAF的策略的示例，请参阅[适用于Amazon WAF Classic 的基于身份的策略示例 \(p. 318\)](#)。

Amazon WAF经典版的政策资源

支持策略资源	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN \)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

[要查看Amazon WAF经典资源类型及其 ARN 的列表，请参阅服务授权参考中的资源Amazon WAF和Amazon WAF区域定义的资源。](#)要了解您可以使用哪些操作指定每个资源的 ARN，请参阅[由区域定义的操作Amazon WAF和Amazon WAF区域定义的操作](#)。要允许或拒绝访问Amazon WAF经典资源的子集，请在策略的resource元素中包含该资源的 ARN。

在“Amazon WAF经典”中，资源是 Web ACL 和规则。Amazon WAFClassic 还支持字节匹配、IP 匹配和大小限制等条件。

这些资源和条件关联有唯一 Amazon 资源名称 (ARN)，如下表所示。

Amazon WAF 控制台中的名称	Amazon WAF SDK/CLI 中的名称	ARN 格式	
Web ACL	WebACL	arn:aws:waf:: <i>account</i> :webacl/ <i>ID</i>	
规则	Rule	arn:aws:waf:: <i>account</i> :rule/ <i>ID</i>	
字符串匹配条件	ByteMatchSet	arn:aws:waf:: <i>account</i> :bytematchset/ <i>ID</i>	
SQL 注入匹配条件	SqlInjectionMatchSet	arn:aws:waf:: <i>account</i> :sqlinjectionset/ <i>ID</i>	
大小约束条件	SizeConstraintSet	arn:aws:waf:: <i>account</i> :sizeconstraintset/ <i>ID</i>	
IP 匹配条件	IPSet	arn:aws:waf:: <i>account</i> :ipset/ <i>ID</i>	
跨站点脚本匹配条件	XssMatchSet	arn:aws:waf:: <i>account</i> :xssmatchset/ <i>ID</i>	

要允许或拒绝访问 Amazon WAF 经典资源的子集，请在策略的 `resource` 元素中包含该资源的 ARN。Amazon WAF Classic 的 ARN 采用以下格式：

```
arn:aws:waf::account:resource/ID
```

将 *account*、*resource* 和 *ID* 变量替换为有效值。有效值如下：

- *##*：您的 IDAmazon Web Services 账户。您必须指定值。
- *##*：Amazon WAF 经典资源的类型。
- *ID*：Amazon WAF 经典资源的 ID，或通配符 (*)，用于表示与指定类型关联的所有资源 Amazon Web Services 账户。

例如，以下 ARN 指定账户 111122223333 的所有 Web ACL：

```
arn:aws:waf::111122223333:webacl/*
```

Amazon WAF 经典的策略条件键

支持特定于服务的策略条件键	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用 [条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。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](#)。

Amazon 支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 [Amazon 全局条件上下文键](#)。

要查看 Amazon WAF 经典条件密钥列表，请参阅服务授权参考中的 [条件密钥 Amazon WAF](#) 和 [Amazon WAF 区域定义的资源](#)。要了解您可以对哪些操作和资源使用条件键，请参阅区域 [定义的操作](#)，Amazon WAF 以及 [Amazon WAF 区域定义的操作](#)。

要查看基于身份 Amazon WAF 的策略的示例，请参阅 [适用于 Amazon WAF Classic 的基于身份的策略示例 \(p. 318\)](#)。

Amazon WAF 经典版中的 ACL

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体 (账户成员、用户或角色) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 以 Amazon WAF 经典版

支持 ABAC (策略中的标签)	部分

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体 (用户或角色) 以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes (是)。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial (部分)。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的 [什么是 ABAC ?](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的 [使用基于属性的访问控制 \(ABAC\)](#)。

在 Amazon WAF 经典版中使用临时凭证

支持临时凭证	是

某些 Amazon Web Services 在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon Web Services 与临时凭证配合使用，请参阅 IAM 用户指南中的 [使用 IAM 的 Amazon Web Services](#)。

如果您不使用用户名和密码而用其它方法登录到 Amazon Web Services Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录 (SSO) 链接访问 Amazon 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 [切换到角色 \(控制台\)](#)。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 [IAM 中的临时安全凭证](#)。

Amazon WAFClassic 的跨服务主体权限

支持委托人权限	是

当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其他相关[操作](#)，请参阅《服务授权参考》中的 [Access 资源](#)和[条件键](#)。Amazon WAFAmazon WAF

Amazon WAF经典版的服务角色

支持服务角色	是

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](#)。

Warning

更改服务角色的权限可能会破坏 Amazon WAF Classic 的功能。仅当 Amazon WAF Classic 提供相关指导时才编辑服务角色。

Amazon WAFClassic 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与 Amazon Web Service 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Amazon WAF 经典服务相关角色的详细信息，请参阅[将服务相关角色用于 Amazon WAF Classic \(p. 321\)](#)。

适用于 Amazon WAF Classic 的基于身份的策略示例

Note

这是 Amazon WAF 经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的 Amazon WAF 经典资源迁移到 Amazon WAF \(p. 232\)](#)。有关的最新版本 Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

默认情况下，用户和角色没有创建或修改 Amazon WAF 经典资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要用户用户在其需要的资源上执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

有关 Amazon WAF Classic 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的[操作、资源和条件键](#)。Amazon WAFAmazon WAF

主题

- [策略最佳实践 \(p. 319\)](#)
- [使用Amazon WAF经典控制台 \(p. 319\)](#)
- [允许用户查看他们自己的权限 \(p. 319\)](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的Amazon WAF经典资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon 托管策略](#)或[工作职能的 Amazon 托管策略](#)。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM Access Analyzer 策略验证](#)。
- Require multi-factor authentication (MFA) [需要多重身份验证 (MFA)] – 如果您所处的场景要求您的 Amazon Web Services 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的[配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用Amazon WAF经典控制台

要访问Amazon WAF Classic 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的中的Amazon WAF Classic 资源的详细信息Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

可以访问和使用Amazon控制台的用户也可以访问Amazon WAF经典控制台。无需额外权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
```

```
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
```

对Amazon WAF传统身份和访问进行故障排除

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

使用以下信息可帮助您诊断和修复在使用Amazon WAF Classic 和 IAM 时可能遇到的常见问题。

主题

- [我无权在Amazon WAF Classic 中执行操作 \(p. 320\)](#)
- [我无权执行 iam : PassRole \(p. 321\)](#)
- [我希望允许我的以外的人访问我Amazon Web Services 账户的Amazon WAF Classic 资源 \(p. 321\)](#)

我无权在Amazon WAF Classic 中执行操作

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 waf:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
waf:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 waf:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一个错误，表明您无权执行操作，则iam:PassRole必须更新策略以允许您将角色传递给 Amazon WAF Classic。

有些 Amazon Web Services 允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在Amazon WAF Classic 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我希望允许我的以外的人访问我Amazon Web Services 账户的Amazon WAF Classic 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解Amazon WAF Classic 是否支持这些功能，请参阅[Amazon WAF经典如何与 IAM 配合使用 \(p. 313\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的[为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的[为经过外部身份验证的用户（联合身份验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的[IAM 角色与基于资源的策略有何不同](#)。

将服务相关角色用于Amazon WAF Classic

Note

这是Amazon WAF经典文档。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源（例如规则和 Web ACL），但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
有关的最新版本Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon WAF经典版使用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Amazon WAF Classic 直接相关。服务相关角色由Amazon WAF Classic 预定义，并包含服务代表您调用其他Amazon服务所需的所有权限。

服务相关角色可让您更轻松地设置Amazon WAF Classic，因为您不必手动添加必要的权限。Amazon WAFClassic 定义其服务相关角色的权限，除非另外定义，否则只有Amazon WAF Classic 可以代入该角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这将保护您的Amazon WAF经典资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅[使用 IAM 的 Amazon 服务](#)并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

Amazon WAFClassic 的服务相关角色权限

Amazon WAFClassic 使用以下服务相关角色：

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

Amazon WAFClassic 使用这些服务相关角色将日志写入 Amazon Kinesis Data Firehose。仅当您在 Amazon WAF 中启用日志记录时，才会使用这些角色。有关更多信息，请参阅[记录 Web ACL 流量信息 \(p. 302\)](#)：

`AWSServiceRoleForWAFLogging`和`AWSServiceRoleForWAFRegionalLogging`服务相关角色信任以下服务以代入该角色：

- `waf.amazonaws.com`
`waf-regional.amazonaws.com`

角色的权限策略允许 Amazon WAF Classic 对指定资源完成以下操作：

- 操作：`firehose:PutRecord`以及名称以“aws-waf-logs-”开头的 `Amazfirehose:PutRecordBatch` on Kinesis Data Firehose 数据流资源。例如，`aws-waf-logs-us-east-2-analytics`。

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 CAmazon WAF lassic 的服务相关角色

无需手动创建服务相关角色。当您在上启用 Amazon WAF 经典登录或在 Amazon Web Services Management Console 经典 CLI 或 Amazon WAF 经 Amazon WAF 典 API 中 `PutLoggingConfiguration` 发出请求时，CAmazon WAF lassic 会为您创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

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。当您启用 Amazon WAF Classic 日志记录时，Amazon WAFClassic 将再次为您创建服务相关角色。

编辑 Amazon WAF Classic 的服务相关角色

Amazon WAFClassic 不允许您编辑 `AWSServiceRoleForWAFLogging` 和 `AWSServiceRoleForWAFRegionalLogging` 与服务相关的角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。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 Amazon WAF Classic 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，您必须先清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 CAmazon WAF lassic 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。

删除AWSServiceRoleForWAFLogging和使用的Amazon WAF经典资源AWSServiceRoleForWAFRegionalLogging

1. 在Amazon WAF经典控制台上，从每个 Web ACL 中删除日志记录。有关更多信息，请参阅[记录 Web ACL 流量信息 \(p. 302\)](#)：
2. 使用 API 或 CLI，为已启用日志记录的每个 Web ACL 提交 DeleteLoggingConfiguration 请求。有关更多信息，请参阅[Amazon WAFClassic API 参考](#)。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除AWSServiceRoleForWAFLogging和AWSServiceRoleForWAFRegionalLogging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](#)。

Amazon WAF传统服务相关角色的受支持区域

Amazon WAFClassic 支持在以下情况下使用服务关联角色Amazon Web Services 区域。

区域名称	区域标识	Amazon WAF经典版Support
美国东部（弗吉尼亚州北部）	us-east-1	是
美国东部（俄亥俄州）	us-east-2	是
美国西部（北加利福尼亚）	us-west-1	是
美国西部（俄勒冈州）	us-west-2	是
亚太地区（孟买）	ap-south-1	是
亚太地区（大阪）	ap-northeast-3	是
亚太地区（首尔）	ap-northeast-2	是
亚太地区（新加坡）	ap-southeast-1	是
亚太地区（悉尼）	ap-southeast-2	是
亚太地区（东京）	ap-northeast-1	是
加拿大（中部）	ca-central-1	是
欧洲（法兰克福）	eu-central-1	是
欧洲（爱尔兰）	eu-west-1	是
欧洲（伦敦）	eu-west-2	是
欧洲（巴黎）	eu-west-3	是
南美洲（圣保罗）	sa-east-1	是
中国（北京）	cn-north-1	否

中的日志记录和监控Amazon WAFClassic

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

监控是维护可靠性、可用性和性能的重要环节Amazon WAF经典和你的Amazon解决方案。你应该从你的所有部分收集监控数据Amazon解决方案，以便更轻松地调试出现的多点故障。Amazon提供了多种用于监控Amazon WAF经典资源和应对潜在事件：

亚马逊 CloudWatch Alarms

使用 CloudWatch 警报，您可以观看单个指标在指定时间段内的变化。如果指标超出给定阈值，CloudWatch 发送通知到 Amazon SNS 主题或Amazon Auto Scaling政策。有关更多信息，请参阅[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。

Amazon CloudTrail 日志

CloudTrail 提供了用户、角色或用户所执行操作的记录。Amazon服务Amazon WAFClassic。通过使用 CloudTrail 收集的信息，可以确定已对发出的请求Amazon WAFClassic、发出请求的源 IP 地址、请求方、发出请求的时间以及其他详细信息。有关更多信息，请参阅[使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)。

的合规性验证Amazon WAFClassic

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。对于最新版本的Amazon WAF请参阅[Amazon WAF \(p. 5\)](#)。

第三方审计员评估的安全性和合规性Amazon WAF经典作为多个组成部分Amazon合规性计划，如 SOC、PCI、FedRAMP、HIPAA 及其他计划。

有关特定合规性计划范围内的Amazon服务的列表，请参阅[合规性计划范围内的Amazon服务](#)。有关一般信息，请参阅[Amazon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[下载 Amazon Artifact 中的报告](#)。

使用时的合规责任Amazon WAFClassic 由您数据的敏感性、您组织的合规性目标以及适用的法律法规决定。如果你使用Amazon WAFClassic 需遵守 HIPAA、PCI 或 FedRAMP 等标准，Amazon提供了以下实用资源：

- [《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上部署基于安全性和合规性的基准环境的步骤。
- [设计符合 HIPAA 安全性和合规性要求的架构白皮书](#) – 此白皮书介绍公司如何使用 Amazon 创建符合 HIPAA 标准的应用程序。
- [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](#) – 此Amazon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 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。
- [Amazon架构完善的框架](#)— 该Amazon架构完善的框架可帮助您构建安全的云应用程序。

中的故障恢复能力Amazon WAFClassic

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF请参阅，[Amazon WAF \(p. 5\)](#)。

Amazon全球基础设施围绕Amazon Web Services 区域和可用区构建。Amazon Web Services 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。

有关Amazon Web Services 区域和可用区的更多信息，请参阅[Amazon全球基础设施](#)。

中的基础设施安全性Amazon WAFClassic

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

作为托管服务，Amazon WAF经典受Amazon中描述的全局网络安全程序[Amazon Web Services : 概述安全过程](#)白皮书。

你用Amazon访问发布的 API 调用Amazon WAF经典通过网络。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 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，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用[Amazon Security Token Service](#) (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon WAF经典配额

Note

这是Amazon WAFClassic文档中)。仅当 2019 年 11 月之前在 Amazon WAF 中创建了 Amazon WAF 资源 (例如规则和 Web ACL)，但尚未将这些资源迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅[将您的Amazon WAF经典资源迁移到Amazon WAF \(p. 232\)](#)。
对于最新版本的Amazon WAF，请参阅[Amazon WAF \(p. 5\)](#)。

Amazon WAFClassic 受以下配额 (以前称为限制) 所限。

Amazon WAFClassic 对每个区域、每个账户的实体数施加了默认配额。您可以[请求提高](#)这些配额。

资源	每个区域每个账户的默认配额
Web ACL	50
规则	100

资源	每个区域每个账户的默认配额
基于费率的规则	5
每区域每 账户的条件数	对于除了正则表达式匹配和地理匹配之外的所有条件，每种条件类型为 100 个。例如，100 个大小约束条件和 100 个 IP 匹配条件。有关正则表达式和地理匹配条件，请参阅下表。
每秒请求数	每个 web ACL 25,000 个*

* 此配额仅适用于Amazon WAFApplication Load Balancer 上的经典。每秒请求数 (RPS) 配额Amazon WAFCloudFront 上的经典与 RPS 配额支持相同 CloudFront 这在[CloudFront 开发人员](#)。

无法更改 Amazon WAF Classic 实体的以下配额。

资源	每区域每账户的配额
每个 Web ACL 的规则组数	2：客户创建的 1 个规则组和 1 个 Amazon Web Services Marketplace 规则组
每个 Web ACL 的规则数	10
每个规则的条件数	10
每个 IP 匹配条件的 IP 地址范围数 (以 CIDR 表示法显示)	10000 您最多可以一次更新 1000 个地址。API 调用UpdateIPSet在一个请求中最多可接受 1000 个地址。
根据基于速率的规则而阻止的 IP 地址	10000
每 5 分钟周期内基于速率规则的最小速率限制	100
每个跨站点脚本匹配条件的筛选条件数	10
每个大小约束条件的筛选条件数	10
每个 SQL 注入匹配条件的筛选条件数	10

资源	每区域每账户的配额
每个字符串匹配条件的筛选条件数	10
在字符串匹配条件中，HTTP 标头名中的字符数 (如果您已将配置完成配置)Amazon WAFCClassic 用于检查 Web 请求中的标头以获取指定值	40
在字符串匹配条件中，您需要的值中的字符数Amazon WAF经典搜索	50
正则表达式匹配条件	10
在正则表达式匹配条件中，您需要的模式中的字符数Amazon WAF经典搜索	70
在正则表达式匹配条件中，每个模式集的模式数	10
在正则表达式匹配条件中，每个正则表达式条件的模式集数	1
模式集	5
地理匹配条件	50
每个地理匹配条件的位置	50

Amazon WAFCClassic 对每个区域、每个账户的调用有以下固定配额。这些配额适用于通过任何可用方式（包括控制台、CLI、Amazon CloudFormation、REST API 和开发工具包）对服务的总调用次数。无法更改这些配额。

调用类型	每区域每账户的配额
调用 AssociateWebACL 的最大次数	每 2 秒 1 个请求
调用 DisassociateWebACL 的最大次数	每 2 秒 1 个请求
调用 GetWebACLForResource 的最大次数	每秒 1 个请求
调用 ListResourcesForWebACL 的最大次数	每秒 1 个请求
调用 CreateWebACLMigrationStack 的最大次数	每秒 1 个请求
调用 GetChangeToken 的最大次数	每秒 10 个请求
调用 GetChangeTokenStatus 的最大次数	每秒 1 个请求
对任何单个 List 操作的最大调用次数 (如果未为其定义其他配额)	每秒 5 个请求
对任何单个 Create、Put、Get 或 Update 操作的最大调用次数 (如果未为其定义其他配额)	每秒 1 个请求

Amazon Shield

对于面向 Internet 的应用程序而言，防范分布式拒绝服务 (DDoS) 攻击是至关重要的。在上构建应用程序时 Amazon，您可以利用这些保护 Amazon 提供没有额外费用。此外，您还可以使用 Amazon Shield Advanced 托管威胁防护服务，通过额外的 DDoS 检测、缓解和响应功能来改善您的安全状况。

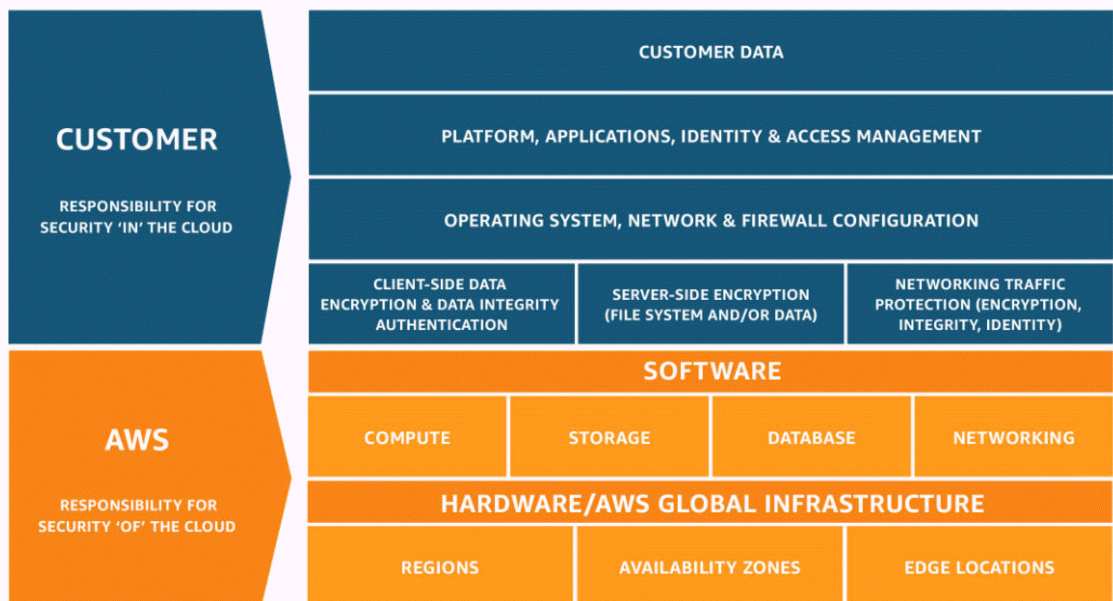
Amazon 致力于为您提供工具、最佳实践和服务，以帮助确保高可用性、安全性和弹性，防御互联网上的坏行为者。提供本指南旨在帮助 IT 决策者和安全工程师了解如何使用 Shield 和 Shield Advanced 更好地保护其应用程序免受 DDoS 攻击和其他外部威胁的侵害。

在上构建应用程序时 Amazon，您可以获得自动保护 Amazon 针对常见的体积 DDoS 攻击向量，例如 UDP 反射攻击和 TCP SYN 洪水。您可以利用这些保护措施来确保运行的应用程序的可用性 Amazon 通过设计和配置您的体系结构以实现 DDoS 弹性。

本指南提供了可帮助您设计、创建和配置应用程序架构以实现 DDoS 弹性的建议。遵循本指南中提供的最佳实践的应用程序在受到更大规模的 DDoS 攻击以及更广泛的 DDoS 攻击媒介的目标时，可以从更好的可用性连续性中受益。此外，本指南向您展示了如何使用 Shield Advanced 为关键应用程序实施优化的 DDoS 防护状态。这些应用程序包括您保证向客户提供一定级别的可用性的应用程序以及那些需要来自运营支持的应用程序 Amazon 在 DDoS 活动期间。

安全性是 Amazon 和您的共同责任。[责任共担模型](#) 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 Web Services 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，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Shield Advanced 的合规性计划，请参阅 [Amazon 合规性计划范围内的服务](#)。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。



Amazon Shield 的工作原理

Amazon Shield Standard 和 Amazon Shield Advanced 并为网络层和传输层（第 3 层和第 4 层）以及应用层（第 7 层）的 Amazon 资源提供保护，使其免受分布式拒绝服务 (DDoS) 攻击。DDoS 攻击是指多个受感染的系统试图向目标充斥流量的攻击。DDoS 攻击可以阻止合法的最终用户访问目标服务，并可能由于流量过大而导致目标崩溃。

Amazon Shield 提供保护，抵御各种已知的 DDoS 攻击媒介和零日攻击媒介。Shield 检测和缓解旨在提供针对威胁的覆盖范围，即使在检测时服务尚未明确知道威胁也是如此。

Shield 检测到的攻击类别包括以下几类：

- 网络容量攻击（第 3 层）— 这是基础设施层攻击向量的子类别。这些向量试图使目标网络或资源的容量饱和，从而拒绝向合法用户提供服务。
- 网络协议攻击（第 4 层）— 这是基础设施层攻击向量的子类别。这些向量滥用协议拒绝向目标资源提供服务。网络协议攻击的一个常见示例是 TCP SYN 泛洪，它会耗尽服务器、负载均衡器或防火墙等资源上的连接状态。网络协议攻击也可以是大规模的。例如，较大的 TCP SYN 泛洪可能意图使网络容量饱和，同时耗尽目标资源或中间资源的状态。
- 应用层攻击（第 7 层）— 此类攻击向量试图通过向应用程序充斥对目标有效的查询（例如 Web 请求泛洪）来拒绝向合法用户提供服务。

目录

- [Amazon Shield Standard 概览 \(p. 330\)](#)
- [Amazon Shield Advanced 概览 \(p. 331\)](#)
 - [Amazon Shield Advanced 受保护资源 \(p. 331\)](#)
 - [Amazon Shield Advanced 功能和选项 \(p. 332\)](#)
 - [决定是否订阅 Amazon Shield Advanced 和应用额外保护 \(p. 333\)](#)
- [DDoS 攻击示例 \(p. 333\)](#)
- [如何 Amazon Shield 检测事件 \(p. 334\)](#)
 - [基础设施层威胁的检测逻辑 \(p. 334\)](#)
 - [应用层威胁的检测逻辑 \(p. 335\)](#)
 - [应用程序中多个资源的检测逻辑 \(p. 336\)](#)
- [如何 Amazon Shield 缓解事件 \(p. 336\)](#)
 - [防范 \(p. 337\)](#)
 - [Amazon Shield CloudFront 和 Route 53 的缓解逻辑 \(p. 337\)](#)
 - [Amazon Shield Amazon 区域的缓解逻辑 \(p. 338\)](#)
 - [Amazon Shield Amazon Global Accelerator 标准加速器的缓解逻辑 \(p. 338\)](#)
 - [Amazon Shield Advanced 弹性 IP 的缓解逻辑 \(p. 339\)](#)
 - [Amazon Shield Advanced Web 应用程序的缓解逻辑 \(p. 339\)](#)

Amazon Shield Standard 概览

Amazon Shield 是一项托管威胁防护服务，可保护应用程序的边界。周边是来自 Amazon 网络外部的应用程序流量的第一个入口点。

要确定您的应用程序边界在哪里，请考虑用户如何从互联网访问您的应用程序。如果第一个入口点位于某个 Amazon 区域，则应用程序边界是您的 Amazon Virtual Private Cloud (VPC)。如果用户通过 Amazon Route 53 定向到您的应用程序，并首先使用 Amazon CloudFront 或 Amazon Global Accelerator 访问该应用程序，则应用程序边界从 Amazon 网络边缘开始。

Shield 为所有正在运行的应用程序提供 DDoS 检测和缓解优势，但是您在设计应用程序架构时做出的决定将影响您的 DDoS 弹性水平。AmazonDDoS 弹性是指您的应用程序在攻击期间继续在预期参数内运行的能力。

所有Amazon客户均可享受Shield Standard的自动保护，无需额外付费。Shield Standard 可防御针对您的网站或应用程序的最常见、最频繁发生的网络和传输层 DDoS 攻击。虽然 Shield Standard 有助于保护所有Amazon客户，但您可以从亚马逊 Route 53 托管区域、亚马逊 CloudFront 分发和Amazon Global Accelerator标准加速器中获得特别的好处。这些资源获得全面的可用性保护，可抵御所有已知的网络和传输层攻击。

Amazon Shield Advanced 概览

Amazon Shield Advanced是一项托管服务，可帮助您保护应用程序免受外部威胁，例如 DDoS 攻击、容量机器人和漏洞利用尝试。要获得更高级别的攻击防护，您可以订购 Amazon Shield Advanced。有关 Shield 高级版定价的信息，请参阅[Amazon Shield Advanced定价](#)。

Note

对于作为Amazon Organizations组织成员的账户，无论付款人账户本身是否已订阅，都将Shield Advanced订阅Amazon账单记入该组织的付款人账户。

当您订阅 Shield Advanced 并为您的资源添加保护时，Shield Advanced 会为这些资源提供扩展的 DDoS 攻击保护。您从 Shield Advanced 获得的保护可能会因您的架构和配置选择而异。使用本指南中的信息使用 Shield Advanced 构建和保护弹性应用程序，并在需要专家帮助时进行升级。

主题

- [Amazon Shield Advanced受保护资源 \(p. 331\)](#)
- [Amazon Shield Advanced功能和选项 \(p. 332\)](#)
- [决定是否订阅Amazon Shield Advanced和应用额外保护 \(p. 333\)](#)

Amazon Shield Advanced受保护资源

Note

Shield Advanced 保护仅适用于您在 Shield Advanced 中明确指定的资源或通过 Amazon Firewall Manager 策略保护的资源。Shield Advanced 不会自动保护您的资源。

您可以使用 Shield Advanced 对以下资源类型进行高级监控和保护：

- 亚马逊 CloudFront 发行。对于 CloudFront 持续部署，Shield Advanced 可保护与受保护的主发行版关联的任何暂存发行版。
- Amazon Route 53 托管区域
- Amazon Global Accelerator标准加速器。
- Amazon EC2 弹性 IP 地址。Shield Advanced 保护与受保护的弹性 IP 地址关联的资源。
- Amazon EC2 实例，通过关联Amazon EC2 弹性 IP 地址。
- 以下弹性Load Balancing (ELB) Load Balancer (ELB)
 - Application
 - 经典负载均衡器。
 - 网络负载均衡器，通过与 Amazon EC2 弹性 IP 地址的关联。

有关保护这些资源类型的更多信息，请参阅[Amazon Shield Advanced按资源类型划分的保护 \(p. 352\)](#)。

Amazon Shield Advanced功能和选项

Amazon Shield Advanced订阅包括以下功能和选项。它们补充了您已经获得的 DDoS 检测和缓解功能 Amazon。

- Amazon WAF集成 — Shield Advanced 使用Amazon WAF Web ACL、规则和规则组作为其应用层保护的一部分。您的 Shield Advanced 订阅涵盖了网络 ACL、规则和网络请求的基本Amazon WAF费用。

有关 Amazon WAF 的更多信息，请参阅 [Amazon WAF 的工作原理 \(p. 6\)](#)。有关基本Amazon WAF费用的信息，请参阅[Amazon WAF定价](#)。您对 Shield Advanced 的订阅不包括任何额外Amazon WAF费用，例如 Bot Control 的可选智能威胁缓解功能或规则操作的费用，CAPTCHA以及Challenge。有关 Shield 高级版定价的信息，请参阅[Amazon Shield Advanced定价](#)。

- 自动应用层 DDoS 缓解 — 您可以将 Shield Advanced 配置为自动响应，以缓解针对受保护资源的应用程序层（第 7 层）攻击。借助自动缓解功能，Shield Advanced 通过为您的受保护资源创建、评估和部署自定义Amazon WAF规则来响应检测到的 DDoS 攻击。您可以配置自动缓解以计数或阻止作为攻击一部分的 Web 请求。

有关更多信息，请参阅 [Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

- 基于运行状况的检测 — 您可以将 Amazon Route 53 运行Health 检查与 Shield Advanced 结合使用，为事件检测和缓解提供信息。运行Health 检查会根据您的规格监控应用程序，在满足您的规格时报告运行状况良好，不符合规格时报告运行状况。在 Shield Advanced 中使用运行状况检查有助于防止误报，并在受保护资源不健康时提供更快检测和缓解措施。您可以对除 Route 53 托管区域以外的任何资源类型使用基于运行状况的检测。Shield Advanced 主动参与仅适用于启用了基于生命值的检测的资源。

有关更多信息，请参阅 [使用运行状况检查配置基于健康的检测 \(p. 358\)](#)。

- 保护组-您可以使用保护组创建受保护资源的逻辑分组，以增强对整个群组的检测和缓解。您可以定义保护组的成员资格标准，以便自动包括新保护的资源。受保护资源可归属于多个保护组。

有关更多信息，请参阅 [Amazon Shield Advanced保护 \(p. 368\)](#)。

- 增强对 DDoS 事件和攻击的可见性 — Shield Advanced 使您可以访问高级实时指标和报告，以全面了解针对受保护Amazon资源的事件和攻击。您可以通过 Shield Advanced API 和控制台以及亚马逊 CloudWatch 指标访问这些信息。

有关更多信息，请参阅 [对 DDoS 事件的可见性 \(p. 369\)](#)。

- 通过以下方式集中管理 Shield Advanced 保护Amazon Firewall Manager — 您可以使用 Firewall Manager 自动将 Shield Advanced 保护应用于您的新帐户和资源，并将Amazon WAF规则部署到您的 Web ACL。Shield Advanced 客户可免费使用Firewall Manager Shield 高级保护策略。您还可以使用带有 Amazon Simple Notification Service (SNS) 主题的 Firewall Manager 来集中管理账户的 Shield Advanced 监控活动，或者Amazon Security Hub。

有关在 Shield Advanced 中使用Firewall Manager 更多信息，请参阅[Amazon Firewall Manager \(p. 403\)](#)和[Amazon Shield Advanced 策略 \(p. 449\)](#)。有关Firewall Manager 定价的信息，请参阅[Amazon Firewall Manager定价](#)。

- AmazonShield Response Team (SRT) — SRT 在保护Amazon Amazon.com 及其子公司方面拥有丰富的经验。作为Amazon Shield Advanced客户，在影响应用程序可用性的 DDoS 攻击期间，您可以随时联系 SRT 寻求帮助。您还可以与 SRT 合作，为您的资源创建和管理自定义缓解措施。要使用SRT的服务，您还必须订阅[业务Support 计划](#)或[企业Support 计划](#)。

有关更多信息，请参阅 [Shield 响应小组 \(SRT\) 支持 \(p. 348\)](#)。

- 主动参与 — 通过主动参与，如果您与受保护资源关联的 Amazon Route 53 运行状况检查在 Shield Advanced 检测到的事件中变得不正常，Shield Response Team (SRT) 会直接与您联系。当您的应用程序的可用性可能受到可疑攻击的影响时，这样可以更快地与专家接触。

有关更多信息，请参阅 [配置主动参与操作 \(p. 350\)](#)。

- 成本保护机会 — Shield Advanced 可提供一些成本保护，以防您的Amazon账单激增，这可能是由于针对受保护资源的 DDoS 攻击而导致的。

有关更多信息，请参阅 [在申请服务抵扣金额Amazon Shield Advanced \(p. 381\)](#)。

决定是否订阅Amazon Shield Advanced和应用额外保护

查看本节中的场景，以帮助决定订阅哪些账户Amazon Shield Advanced以及在哪里应用额外保护。使用 Shield Advanced，您需要为在整合账单账户下创建的所有账户支付月度订阅费，外加根据传出的数据量 GB 支付使用费。有关 Shield 高级版定价的信息，请参阅[Amazon Shield Advanced定价](#)。

Note

对于作为Amazon Organizations组织成员的账户，无论付款人账户本身是否已订阅，都将Shield Advanced订阅Amazon账单记入该组织的付款人账户。

要使用 Shield Advanced 保护应用程序及其资源，您需要将管理该应用程序的账户订阅到 Shield Advanced，然后为应用程序的资源添加保护。有关订阅账户和保护资源的信息，请参阅[Amazon Shield Advanced 入门 \(p. 343\)](#)。

确定要保护的应用程序

考虑为需要以下任何一项的应用程序实施 Shield Advanced 保护：

- 保证应用程序用户的可用性。
- 如果应用程序受到 DDoS 攻击的影响，可以快速联系 DDoS 缓解专家。
- 意识到应用程序可能受Amazon到 DDoS 攻击的影响，以及来自您的安全或运营团队的攻击通知Amazon和攻击升级通知。
- 云成本的可预测性，包括 DDoS 攻击何时影响您对Amazon服务的使用。

如果应用程序或其资源需要上述任何一项，请考虑为相关帐户创建订阅。

确定要保护的资源

对于每个订阅的账户，考虑为具有以下任何特征的每种资源添加 Shield Advanced 保护：

- 该资源为互联网上的外部用户提供服务。
- 该资源暴露在互联网上，也是关键应用程序的一部分。考虑所有暴露的资源，无论你是否打算让互联网上的用户访问这些资源。
- 资源受Amazon WAF Web ACL 保护。

要了解有关为资源创建和管理保护功能的更多信息，请参[中的资源保护Amazon Shield Advanced \(p. 351\)](#)阅

此外，请遵循本指南中的建议，以帮助确保为实现 DDoS 弹性架构应用程序，并正确配置了 Shield Advanced 的功能以实现最佳保护。

DDoS 攻击示例

Amazon Shield Advanced 针对多种类型的攻击提供大范围的保护。

以下列表描述了一些常见的攻击类型：

用户数据报协议 (UDP) 反射攻击

在 UDP 反射攻击中，攻击者可以伪造请求源并使用 UDP 从服务器获得大量响应。流向受欺骗、受攻击的 IP 地址的额外网络流量可能会减慢目标服务器的速度，并阻止合法的最终用户访问所需的资源。

TCP SYN 泛载

TCP SYN 泛洪攻击的目的是使连接处于半开状态，从而耗尽系统的可用资源。当用户连接到 Web 服务器等 TCP 服务时，客户端会发送 TCP SYN 数据包。服务器将返回确认，客户端将返回自己的确认，完成三次握手。在 TCP SYN 泛洪中，永远不会返回第三条确认消息，服务器只能等待响应。这会使其他用户无法连接到服务器。

DNS 查询泛洪

在 DNS 查询洪水中，攻击者使用多个 DNS 查询来耗尽 DNS 服务器的资源。Amazon Shield Advanced 可以帮助防御 Route 53 DNS 服务器上的 DNS 查询泛洪攻击。

HTTP 泛洪/缓存清除 (第 7 层) 攻击

通过 HTTP 洪水 (包括 GET/POST 洪水)，攻击者发送多个 HTTP 请求，这些请求似乎来自 Web 应用程序的真实用户。缓存清除攻击是一种 HTTP 泛洪，它在 HTTP 请求的查询字符串中使用禁止使用的位于边缘的缓存内容的变体，并强制从源 Web 服务器提供内容，从而导致对源 Web 服务器造成附加的、可能具有破坏性的压力。

如何Amazon Shield检测事件

Amazon 为 Amazon 网络和单个 Amazon 服务运行服务级别的检测系统，以确保它们在 DDoS 攻击期间保持可用。此外，资源级检测系统会监控每个单独 Amazon 的资源，以确保流向该资源的流量保持在预期参数范围内。这种组合通过应用缓解措施来保护目标 Amazon 资源和 Amazon 服务，这些缓解措施包括丢弃已知的错误数据包、突出潜在的恶意流量以及对来自最终用户的流量进行优先排序。

检测到的事件在 Shield Advanced 事件摘要、攻击详情和亚马逊 CloudWatch 指标中显示为 DDoS 攻击向量的名称，或者好 Volumetric 像评估基于流量而不是签名一样。有关 DDoS Detected CloudWatch 指标中可用的攻击向量维度的更多信息，请参阅 [Amazon Shield Advanced 指标和警报 \(p. 506\)](#)

主题

- [基础设施层威胁的检测逻辑 \(p. 334\)](#)
- [应用层威胁的检测逻辑 \(p. 335\)](#)
- [应用程序中多个资源的检测逻辑 \(p. 336\)](#)

基础设施层威胁的检测逻辑

用于保护目标 Amazon 资源免受基础设施层 (第 3 层和第 4 层) 的 DDoS 攻击的检测逻辑取决于资源类型以及资源是否受保护 Amazon Shield Advanced。

检测亚马逊 CloudFront 和亚马逊 Route 53

当您使用 CloudFront 和 Route 53 为 Web 应用程序提供服务时，发往应用程序的所有数据包都将由全内联 DDoS 缓解系统进行检查，该系统不会引入任何可观察到的延迟。实时缓解了针对 CloudFront 分布和 Route 53 托管区域的 DDoS 攻击。无论您是否使用，这些保护措施都适用 Amazon Shield Advanced。

遵循最佳实践，尽可能使用 CloudFront Route 53 作为 Web 应用程序的入口点，以最快地检测和缓解 DDoS 事件。

检测Amazon Global Accelerator和区域服务

资源级检测可保护在 Amazon 区域中启动的 Amazon Global Accelerator 标准加速器和资源，例如经典负载均衡器、应用程序负载均衡器和弹性 IP 地址 (EIP)。这些资源类型会受到监控，以防流量升高可能表明存在需要缓解的 DDoS 攻击。每分钟都会评估每种 Amazon 资源的流量。如果资源的流量增加，则会进行额外的检查以衡量资源的容量。

Shield 执行以下标准检查：

- Amazon Elastic Compute Cloud (Amazon EC2) 实例，附加到 Amazon EC2 实例的 EIP，Shield Advanced 从受保护资源中检索容量。容量取决于目标的实例类型、实例大小和其他因素，例如实例是否使用增强联网。
- 经典负载均衡器和 Application Load Balancer 从目标负载均衡器节点检索容量。
- 连接到网络负载均衡器的 EIP — Shield 从目标负载均衡器检索容量。容量与目标负载均衡器的组配置无关。
- Amazon Global Accelerator 标准加速器 — Shield 根据端点配置检索容量。

这些评估涉及网络流量的多个维度，例如端口和协议。如果超过目标资源的容量，Shield 会发出 DDoS 缓解措施。Shield 采取的缓解措施将减少 DDoS 流量，但可能不会消除 DDoS 流量。如果在与已知的 DDoS 攻击向量一致的流量维度上超过资源容量的一小部分，Shield 也可以采取缓解措施。Shield 将这种缓解设置为有限的生存时间 (TTL)，只要攻击持续进行，它就会延长生存时间 (TTL)。

Note

Shield 采取的缓解措施将减少 DDoS 流量，但可能无法消除 DDoS 流量。您可以使用诸如 Amazon Network Firewall 主机防火墙之类的解决方案来增强 Shield，iptables 以防止您的应用程序处理对您的应用程序无效或不是由合法最终用户生成的流量。

Shield Advanced 保护为现有的 Shield 检测活动增加了以下内容：

- 较低的检测阈值 — Shield Advanced 将缓解设置为计算容量的一半。这可以更快地缓解缓慢加剧的攻击，并缓解容量特征更加模糊的攻击。
- 间歇性攻击保护 — Shield Advanced 根据攻击的频率和持续时间将缓解措施的生存时间 (TTL) 呈指数级增长。当资源经常成为攻击目标和短时间内发生攻击时，这可以延长缓解措施的有效期。
- 基于运行状况的检测 — 当您为 Route 53 Health 检查与 Shield Advanced 保护的资源关联时，将在检测逻辑中使用运行状况检查的状态。在检测到的事件期间，如果运行状况检查正常，Shield Advanced 需要在采取缓解措施之前更加确信该事件是攻击。相反，如果健康检查不健康，Shield Advanced 可能会在信心建立之前就采取缓解措施。此功能有助于避免误报，并可更快地应对影响应用程序的攻击。有关使用 Shield Advanced 进行健康检查的信息，请参阅 [使用运行状况检查配置基于健康的检测 \(p. 358\)](#)。

应用层威胁的检测逻辑

Amazon Shield Advanced 为受保护的 Amazon CloudFront 发行版和应用程序负载均衡器提供 Web 应用程序层检测。使用 Shield Advanced 保护这些资源类型时，可以将 Amazon WAF Web ACL 与您的保护相关联，以启用 Web 应用程序层检测。Shield Advanced 消耗关联的 Web ACL 的请求数据，并为您的应用程序建立流量基线。Web 应用程序层检测依赖于 Shield Advanced 和之间的原生集成 Amazon WAF。要了解有关应用层保护的更多信息，包括将 Amazon WAF Web ACL 关联到 Shield Advanced 保护资源，请参阅 [Amazon Shield Advanced 应用层 \(第 7 层\) 保护 \(p. 353\)](#)。

对于 Web 应用程序层检测，Shield Advanced 监控应用程序流量并将其与历史基线进行比较，寻找异常。这种监控涵盖总流量和交通构成。在 DDoS 攻击期间，我们预计流量的数量和构成都会发生变化，Shield Advanced 要求两者都存在统计学上的显著偏差才能声明事件。

Shield Advanced 根据历史时间窗执行测量。这种方法可以减少来自流量合法变化或与预期模式相匹配的流量变化（例如每天同时进行的销售）产生的误报通知。

Note

让 Shield Advanced 有时间建立代表正常、合法流量模式的基准，从而避免 Shield Advanced 保护中的误报。在任何可能导致 Web 流量异常模式的计划事件发生前至少 24 小时将 Web ACL 与您的受保护资源关联。Shield Advanced Web 应用程序层检测在观察 30 天的正常流量时最为准确。

Shield Advanced 检测事件所需的时间受其观察到的流量变化的影响。对于较小的流量变化，Shield Advanced 会更长时间地观察流量，以建立对事件正在发生的信心。对于更高的音量变化，Shield Advanced 可以更快地检测和报告事件。

Note

您可以构建应用程序，使其能够根据流量或负载的增加进行扩展，从而确保它不受较小请求泛洪的影响。使用 Shield Advanced，您的受保护资源将受到成本保护。这有助于保护您免受 DDoS 攻击可能导致的云账单意外增加。要了解有关 Shield Advanced 成本保护的更多信息，请参阅[在申请服务抵扣金额Amazon Shield Advanced \(p. 381\)](#)。

应用程序中多个资源的检测逻辑

您可以使用 Amazon Shield Advanced 保护组创建属于同一应用程序的受保护资源集合。您可以选择将哪些受保护资源放入一个组中，也可以指定应将相同类型的所有资源视为一个组。例如，您可以创建一组所有应用程序负载均衡器。创建保护组时，Shield Advanced 检测会聚合该组内受保护资源的所有流量。如果您有许多资源，每个资源的流量都很小，但聚合量很大，这很有用。对于在受保护资源之间传输流量的蓝绿色部署，您也可以使用保护组来保留应用程序基线。

您可以选择通过以下方式之一聚合保护组中的流量：

- Sum — 此聚合合并了保护组中资源间的所有流量。您可以使用此聚合来确保新创建的资源具有现有基准并降低检测灵敏度，这有助于防止误报。
- 均值 — 此聚合使用保护组中所有流量的平均值。您可以将此聚合用于资源间流量统一的应用程序，例如负载均衡器。
- Max — 此聚合使用保护组中所有资源中最高的流量。当保护组中有多个应用程序层时，您可以使用此聚合。例如，您可能有一个保护组，其中包括 CloudFront 分配、其 Application Load Balancer 来源和应用程序负载均衡器的 Amazon EC2 实例目标。

对于针对多个面向互联网的 Elastic IP 或 Amazon Global Accelerator 标准加速器的攻击，您还可以使用保护组来提高 Shield Advanced 放置缓解措施的速度。当保护组中的一个资源成为目标时，Shield Advanced 会建立对群组中其他资源的信心。这会使 Shield Advanced 检测处于警戒状态，可以缩短创建额外缓解措施所需的时间。

要了解有关保护组的更多信息，请参阅[Amazon Shield Advanced 保护 \(p. 368\)](#)。

如何 Amazon Shield 缓解事件

保护应用程序的缓解逻辑可能因应用程序架构而异。当您使用 Amazon CloudFront 和 Amazon Route 53 保护 Web 应用程序时，您将受益于特定于 Web 和 DNS 用例的缓解措施，这些缓解措施可以保护服务的所有流量。当您的应用程序的入口点是在某个 Amazon 区域中运行的资源时，缓解逻辑会因服务、资源类型和您的使用情况而异 Amazon Shield Advanced。

Amazon DDoS 缓解系统由 Shield 工程师开发，与 Amazon 服务紧密集成。工程师会考虑您的架构的各个方面，例如目标资源的容量和运行状况。Shield 工程师持续监控 DDoS 缓解系统的效率和性能，并能够在发现或预计到新的威胁时快速做出响应。

您可以构建应用程序，使其能够根据流量或负载的增加进行扩展，从而帮助确保它不受较小请求洪水的影响。如果您使用 Shield Advanced 来保护您的资源，您将获得保障，以防因 DDoS 攻击而导致云账单意外增加。

基础设施防范

对于基础设施层攻击，Amazon Shield DDoS 缓解系统存在于 Amazon 网络边界和 Amazon 边缘位置。在整个 Amazon 基础架构中设置多个级别的安全控制可 defense-in-depth 为您的云应用程序提供帮助。

Shield 在互联网的所有入口处维护 DDoS 缓解系统。当 Shield 检测到 DDoS 攻击时，它会为每个入口点重新路由流量，通过位于同一位置的 DDoS 缓解系统。这不会带来任何可观察到的额外延迟，并且在所有 Amazon 区域和所有边缘站点提供超过 TeraBits 每秒 100 (Tbps) 的缓解容量。Shield 可以保护您的资源可用性，而无需将流量重新路由到外部或远程清理中心，这可能会增加延迟。

- 在Amazon网络边界，对于任何Amazon服务或资源，DDoS 缓解系统都能缓解来自互联网的基础设施层攻击。当Shield 探测器或Shield 响应小组 (SRT) 的工程师发出信号时，系统会执行缓解措施。
- 在Amazon边缘站点，DDoS 缓解系统会持续检查转发到 Amazon CloudFront 分配和 Amazon Route 53 托管区域的每个数据包，无论其来源如何。必要时，系统会应用专为 Web 和 DNS 流量设计的缓解措施。使用亚马逊 CloudFront 和亚马逊 Route 53 保护您的 Web 应用程序的另一个好处是，可以立即缓解 DDoS 攻击，无需从 Shield 检测发出信号。

应用层缓解措施

Shield Advanced 为已启用 Shield Advanced 保护的亚马逊 CloudFront 发行版和应用程序负载均衡器提供 Web 应用程序层缓解措施。启用保护时，将Amazon WAF Web ACL 与资源关联，以启用 Web 应用程序层检测。此外，您可以选择启用自动应用层缓解，这会指示 Shield Advanced 在 DDoS 攻击期间为您管理保护。

Shield 仅提供针对已启用 Shield Advanced 和自动应用层缓解的资源的应用层攻击的缓解措施。借助自动缓解功能，Shield Advanced 可通过Amazon WAF保护措施自动缓解攻击，然后在不再需要缓解措施时将其删除。有关此类缓解措施的详细信息，请参阅[Shield Advanced 如何管理自动 \(p. 355\)](#)。

防范

Amazon ShieldDDoS 缓解的主要功能如下：

- 数据包验证-这可确保每个被检查的数据包都符合预期的结构，并且对其协议有效。支持的协议验证包括 IP、TCP (包括标头和选项)、UDP、ICMP、DNS 和 NTP。
- 访问控制列表 (ACL) 和整形器 — ACL 根据特定属性评估流量，然后丢弃匹配的流量或将其映射到整形器。整形器限制匹配流量的数据包速率，丢弃多余的数据包以控制到达目的地的流量。Amazon Shield检测和Shield 响应小组 (SRT) 工程师可以为预期流量提供专用的速率分配，并为具有与已知 DDoS 攻击向量匹配的属性的流量提供更严格的速率分配。ACL 可以匹配的属性包括端口、协议、TCP 标志、目标地址、源国家/地区以及数据包负载中的任意模式。
- 怀疑分数 — 利用Shield对预期流量的了解来对每个数据包进行分数。对符合已知正常流量模式的数据包的怀疑分数较低。观察已知的不良流量属性可能会增加数据包的怀疑分数。当需要对数据包进行速率限制时，Shield 会首先丢弃怀疑分数较高的数据包。这有助于 Shield 缓解已知和零日 DDoS 攻击，同时避免误报。
- TCP SYN 代理 — 这通过发送 TCP SYN cookie 来挑战新连接，然后再允许它们传递给受保护的服务，从而防御 TCP SYN 泛洪攻击。Shield DDoS 缓解提供的 TCP SYN 代理是无状态的，这使它能够在不耗尽状态的情况下缓解已知最大的 TCP SYN 洪水攻击。这是通过与Amazon服务集成以传递连接状态而不是在客户端和受保护服务之间维护连续代理来实现的。TCP SYN 代理目前在亚马逊 CloudFront 和亚马逊 Route 53 上可用。
- 速率分布 — 这会根据流向受保护资源的流入模式持续调整每个位置的整形器值。这样可以防止对可能无法均匀进入Amazon网络的客户流量进行速率限制。

Amazon Shield CloudFront 和 Route 53 的缓解逻辑

Shield DDoS 缓解措施会持续检查 Route 53 的 CloudFront 流量。这些服务在全球分布的Amazon边缘站点网络上运行，使您可以广泛访问Shield的DDoS缓解能力，并从离最终用户更近的基础设施中交付应用程序。

- CloudFront— Shield DDoS 缓解措施仅允许对 Web 应用程序有效的流量传递到服务。这可以自动防范许多常见的 DDoS 向量，例如 UDP 反射攻击。

CloudFront 保持与您的应用程序源站的持续连接，通过与 Shield TCP SYN 代理功能的集成自动缓解 TCP SYN 洪水，传输层安全 (TLS) 在边缘终止。这些组合功能可确保您的应用程序源仅接收格式正确的 Web 请求，并保护其免受低层 DDoS 攻击、连接泛洪和 TLS 滥用。

CloudFront 结合使用 DNS 流量方向和任播路由。这些技术通过缓解靠近源头的攻击、提供故障隔离以及确保访问容量来缓解已知规模最大的攻击，从而提高应用程序的弹性。

- Route 53 — Shield 缓解措施仅允许有效的 DNS 请求到达服务。Shield 使用可疑评分来缓解 DNS 查询泛滥，该评分会优先考虑已知的正常查询，并取消包含可疑或已知 DDoS 攻击属性的查询的优先级。

Route 53 使用随机分片，为 IPv4 和 IPv6 的每个托管区域提供一组唯一的四个解析器 IP 地址。每个 IP 地址对应 Route 53 位置的不同子集。每个位置子集都由权威的 DNS 服务器组成，这些服务器仅部分与任何其他子集中的基础设施重叠。这样可以确保如果用户查询因任何原因失败，则重试时将成功提供查询。

Route 53 使用任播路由，根据网络邻近度将 DNS 查询定向到最近的节点。Anycast 还将 DDoS 流量分散到许多边缘站点，从而防止攻击集中在单个位置。

除了缓解速度外，CloudFront Route 53 还提供了对 Shield 全球分布式容量的广泛接入。要利用这些功能，请使用这些服务作为动态或静态 Web 应用程序的入口点。

要了解有关使用 CloudFront 和 Route 53 保护 Web 应用程序的更多信息，请参阅[如何使用亚马逊 CloudFront 和亚马逊 Route 53 帮助保护动态 Web 应用程序免受 DDoS 攻击](#)。要了解有关 Route 53 故障隔离的更多信息，请参阅[全局故障隔离案例研究](#)。

Amazon ShieldAmazon 区域的缓解逻辑

在 Amazon 区域中启动的资源受到 Shield 资源级检测放置的 Amazon Shield DDoS 缓解系统的保护。区域资源包括弹性 IP (EIP)、经典负载均衡器和应用程序负载均衡器。

在采取缓解措施之前，Shield 会识别目标资源及其容量。Shield 使用容量来确定其缓解措施应允许转发到资源的最大总流量。缓解措施中的访问控制列表 (ACL) 和其他调整器可能会减少某些流量的允许流量，例如与已知 DDoS 攻击向量匹配或预计不会出现大量流量的流量。这进一步限制了缓解措施允许进行 UDP 反射攻击或带有 TCP SYN 或 FIN 标志的 TCP 流量的流量。

Shield 决定容量，每种资源类型的缓解效果也不同。

- 对于 Amazon EC2 实例或连接到 Amazon EC2 实例的 EIP，Shield 根据实例类型和其他实例属性（例如该实例是否启用了增强联网）来计算容量。
- 对于 Application Load Balancer 或 Classic Load Balancer，Shield 会单独计算负载均衡器的每个目标节点的容量。这些资源的 DDoS 攻击缓解由 Shield DDoS 缓解措施和负载均衡器的自动扩展相结合。当 Shield Response Team (SRT) 对 Application Load Balancer 或 Classic Load Balancer 资源进行攻击时，他们可能会加速扩展作为一项额外的保护措施。
- Shield 根据底层 Amazon 基础设施的可用容量计算某些 Amazon 资源的容量。这些资源类型包括网络负载均衡器 (NLB) 和通过网关负载均衡器或路由流量的资源 Amazon Network Firewall。

Note

通过附加受 Shield Advanced 保护的 EIP 来保护您的网络负载均衡器。您可以与 SRT 合作，根据底层应用程序的预期流量和容量构建自定义缓解措施。

当 Shield 进行缓解时，Shield 在缓解逻辑中定义的初始速率限制将同样应用于每个 Shield DDoS 缓解系统。例如，如果 Shield 设置的缓解措施限制为每秒 100,000 个数据包 (pps)，则它最初将允许在每个位置使用 100,000 pps。然后，Shield 会持续汇总缓解指标以确定实际流量比例，并使用该比率调整每个地点的速率限制。这样可以防止误报，并确保缓解措施不会过于宽松。

Amazon ShieldAmazon Global Accelerator 标准加速器的缓解逻辑

Shield 缓解措施仅允许有效流量到达全球加速器标准加速器的侦听器端点。标准加速器在全球部署，它们为您提供 IP 地址，您可以使用这些地址将流量路由到任何 Amazon 地区 Amazon 的资源。Shield 为缓解全球加速器而实施的速率限制基于标准加速器将流量路由到的资源的容量。当总流量超过确定的速率时，以及已知的 DDoS 向量超过该速率的一小部分时，Shield 会采取缓解措施。

配置标准加速器时，您需要为每个 Amazon 区域定义终端节点组，您将在其中为应用程序路由流量。当 Shield 发布缓解措施时，它会计算每个端点组的容量，并相应地更新每个 Shield DDoS 缓解系统的速率限

制。每个地点的费率各不相同，具体取决于 Shield 对流量将如何从互联网传输到您的 Amazon 资源所做的假设。端点组容量的计算方法是该组中的资源数量乘以该组中任何资源的最低容量。Shield 会定期重新计算应用程序的容量并根据需要更新速率限制。

Note

使用流量拨号更改流向终端节点组的流量的百分比不会改变 Shield 计算或向其 DDoS 缓解系统分配速率限制的方式。如果您使用流量拨号，请将您的终端节点组配置为在资源类型和数量方面相互镜像。这有助于确保 Shield 计算的容量代表为您的应用程序提供流量的资源。

有关 Global Accelerator 中的端点组和流量拨号的更多信息，请参阅[Amazon Global Accelerator 标准加速器中的端点组](#)。

Amazon Shield Advanced 弹性 IP 的缓解逻辑

当您使用 Amazon Shield Advanced 保护弹性 IP (EIP) 时，Shield Advanced 会增强 Shield 在 DDoS 事件期间采取的缓解措施。Shield Advanced DDoS 缓解系统会复制 EIP 关联的公有子网的网络 ACL (NACL) 配置。例如，如果您的 NACL 配置为屏蔽所有 UDP 流量，则 Shield Advanced 会将该规则合并到 Shield 提供的缓解措施中。

此附加功能可以帮助您避免由于流量对您的应用程序无效而导致的可用性风险。您也可以使用 NACL 来屏蔽单个源 IP 地址或源 IP 地址 CIDR 范围。对于非分布式的 DDoS 攻击，这可能是一种有用的缓解工具。它还允许您轻松管理自己的允许列表或屏蔽不应与您的应用程序通信的 IP 地址，而无需依赖 Amazon 工程师的干预。

Amazon Shield Advanced Web 应用程序的缓解逻辑

Amazon Shield Advanced Amazon WAF 用于缓解 Web 应用程序层攻击。Amazon WAF 包含在 Shield Advanced 中，不产生额外的成本。当您使用 Shield Advanced 保护亚马逊 CloudFront 分配或 Application Load Balancer 时，如果您还没有关联 Amazon WAF Web ACL，则可以使用 Shield Advanced 将 Web ACL 与您的受保护资源关联。如果您尚未配置 Web ACL，则可以使用 Shield Advanced 控制台向导创建一个 Web ACL，然后向其添加基于速率的规则。基于速率的规则限制每个 IP 地址每五分钟时间窗口的请求数，从而提供基本保护，以防止 Web 应用程序层请求泛洪。您可以配置速率，起始值低至 100。有关更多信息，请参阅[Shield 高级应用层 Amazon WAF Web ACL 和基于速率的规则 \(p. 353\)](#)。

要增强保护，请启用 Shield Advanced 自动应用层缓解。使用此选项，当 Shield Advanced 检测到对受保护资源的攻击时，它会尝试识别一种攻击特征，将攻击流量与应用程序的正常流量隔离开来。Shield Advanced 会根据受攻击资源的历史流量模式以及同一 Web ACL 关联的任何其他资源的历史流量模式评估已识别的攻击特征。

如果 Shield Advanced 确定攻击签名仅隔离涉及 DDoS 攻击的流量，则它会在关联的 Web ACL 内的 Amazon WAF 规则中实现该签名。你可以指示 Shield Advanced 设置缓解措施，只计算他们匹配的流量，也可以屏蔽这些缓解措施，并且可以随时更改设置。当 Shield Advanced 确定不再需要其缓解规则时，它会将其从 Web ACL 中删除。

有关更多信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

基本 DDoS 弹性架构示例

DDoS 弹性是指应用程序架构能够抵御分布式拒绝服务 (DDoS) 攻击，同时继续为合法的最终用户提供服务。具有高度弹性的应用程序可以在攻击期间保持可用，而对性能指标（例如错误或延迟）的影响最小。本节介绍一些常见的示例架构，并介绍如何使用由提供的 DDoS 检测和缓解功能 Amazon 和 Shield Advanced 来提高他们的 DDoS 弹性。

本节中的示例架构重点介绍了 Amazon 为您部署的应用程序提供最大的 DDoS 弹性优势的服务。突出显示的服务的优点包括：

- 访问全球分布式网络容量— 亚马逊的服务 CloudFront、Amazon Global Accelerator，Amazon Route 53 可让您访问互联网和 DDoS 缓解能力 Amazon 全球边缘网络。这对于缓解更大规模的体积攻击非常有用，

这种攻击的规模可能达到太比特。您可以在任何Amazon区域并使用这些服务来保护合法用户的可用性并优化性能。

- 防范 Web 应用层 DDoS 攻击媒介— Web 应用程序层 DDoS 攻击最好结合使用应用程序规模和 Web 应用程序防火墙 (WAF) 来缓解。Shield Advanced 使用来自Amazon WAF检测可以自动缓解的异常情况，也可以通过与AmazonShield 响应小组 (SRT)。通过部署可实现自动缓解Amazon WAF基于速率的规则，也可以通过 Shield Advanced 自动应用层 DDoS 缓解。

除了查看这些示例外，请查看并遵循适用的最佳实践[Amazon实现 DDoS 弹性的 最佳实践](#)。

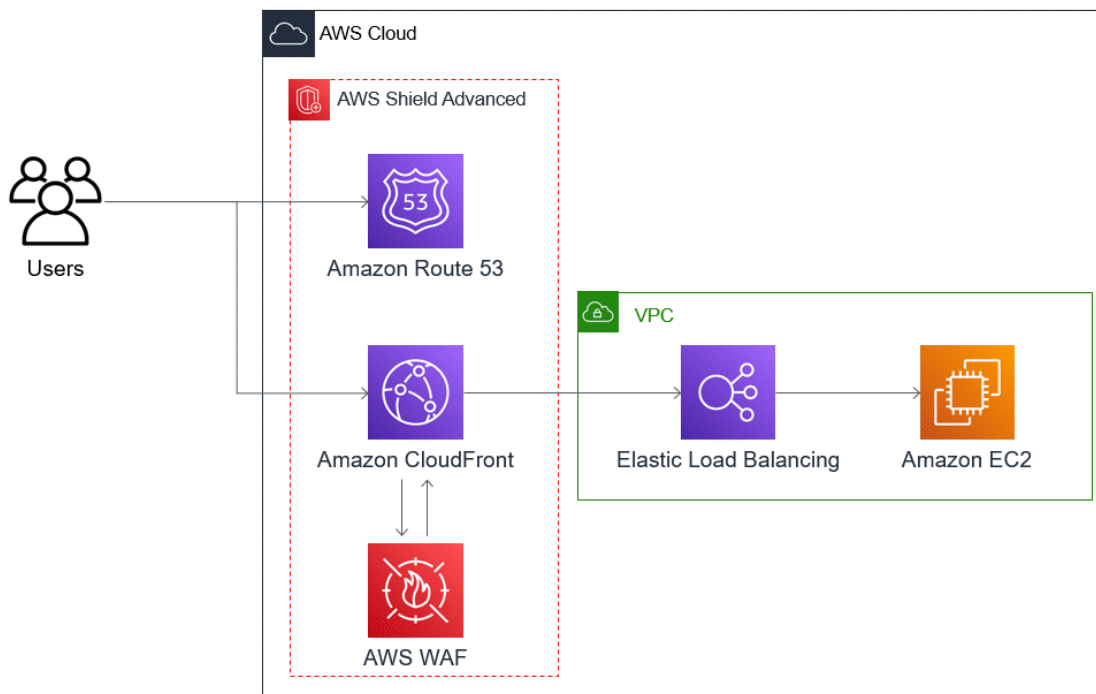
常见 Web 应用程序的 DDoS 弹性示例

您可以在任何版本中构建 Web 应用程序Amazon通过检测和缓解功能划分区域并获得自动 DDoS 保护 Amazon在该地区提供。

此示例适用于使用经典负载均衡器、应用程序负载均衡器、网络负载均衡器、网络负载均衡器、网络负载均衡器、网络负载均衡器、网络负载均衡器AmazonMarketplace 解决方案，或者你自己的代理层。您可以通过插入 Amazon Route 53 托管区域来提高 DDoS 弹性 CloudFront 分配和Amazon WAF这些 Web 应用程序资源与您的用户之间的 Web ACL。这些插入可以混淆应用程序源，为更接近最终用户的请求提供服务，并检测和缓解应用程序层请求泛洪。向用户提供静态或动态内容的应用程序 CloudFront 和 Route 53 受到集成的完全内联 DDoS 缓解系统的保护，该系统可实时缓解基础设施层攻击。

有了这些架构改进，您就可以保护您的 Route 53 托管区域和您的 CloudFront 使用Shield 高级分发。当你保护 CloudFront 分配，Shield 高级会提示你关联Amazon WAFWeb ACL，并为其创建基于速率的规则，并允许您选择启用自动应用层 DDoS 缓解或主动参与。主动参与和自动应用层 DDoS 缓解使用与资源关联的 Route 53 运行状况检查。要了解有关这些选项的更多信息，请参阅 [中的资源保护Amazon Shield Advanced \(p. 351\)](#)。

以下参考图描述了适用于 Web 应用程序的 DDoS 弹性架构。



此方法为您的 Web 应用程序带来的好处包括：

- 防范常用的基础设施层 (第 3 层和第 4 层) DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD 此外，如果资源经常成为攻击目标，Shield Advanced 会将缓解措施放置更长的时间。Shield Advanced 还使用从网络 ACL (NACL) 推断出的应用程序上下文来阻止更远的上游不需要的流量。这样可以将故障隔离到更接近其源头的位置，从而最大限度地减少对合法用户的影响。
- 防止 TCP SYN 泛洪攻击。与集成的 DDoS 缓解系统 CloudFront、53 号公路和 Amazon Global Accelerator 提供 TCP SYN 代理功能，该功能可以挑战新的连接尝试，并且仅为合法用户提供服务。
- 防止 DNS 应用层攻击，因为 Route 53 负责提供权威 DNS 响应。
- 防止 Web 应用程序层请求泛滥。您在中配置的基于速率的规则 Amazon WAF 当源 IP 发送的请求超出规则允许范围时，Web ACL 会阻止源 IP。
- 自动缓解应用层 DDoS CloudFront 分配中，如果您选择启用此选项。当 Shield Advanced 检测到影响应用程序运行状况的事件时，它会自动创建、测试和管理分发的关联缓解规则 Amazon WAF Web ACL ACB AC
- 如果您选择启用此选项，请主动与 Shield 响应团队 (SRT) 接触。当 Shield Advanced 检测到影响应用程序运行状况的事件时，SRT 会使用您提供的联系信息做出响应，并主动与您的安全或运营团队互动。SRT 会分析您的流量模式，并可以更新您的 Amazon WAF 规则来阻止攻击。

TCP 和 UDP 应用程序的 DDoS 弹性示例

此示例显示了适用于 TCP 和 UDP 应用程序的 DDoS 弹性架构 Amazon 使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 EIP (Amazon EC2) 实例的区域。

您可以按照此一般示例来提高以下应用程序类型的 DDoS 弹性：

- TCP 或 UDP 应用程序。例如，用于游戏、IoT 和 IP 语音的应用程序。
- 需要静态 IP 地址或使用亚马逊协议的 Web 应用程序 CloudFront 不支持。例如，您的应用程序可能需要 IP 地址，您的用户可以将其添加到防火墙允许列表中，而其他任何用户都不会使用这些地址 Amazon 顾客们。

您可以通过引入 Amazon Route 53 和 Amazon Global Accelerator。这些服务可以将用户路由到您的应用程序，并且可以为您的应用程序提供静态 IP 地址，这些静态 IP 地址可通过 Amazon 全球边缘网络。全球加速器标准加速器可将用户延迟缩短多达 60%。如果您有 Web 应用程序，则可以通过在 Application Load Balancer 上运行应用程序，然后使用保护 Application Load Balancer 来检测和缓解 Web 应用程序层请求泛滥 Amazon WAF Web ACL ACB AC

构建应用程序后，使用 Shield Advanced 保护您的 Route 53 托管区域、全球加速器标准加速器和任何应用程序负载均衡器。当您保护应用程序负载均衡器时，您可以关联 Amazon WAF Web ACL 为其创建基于速率的规则。您可以通过关联新的或现有的 Route 53 运行状况检查，为全球加速器标准加速器和应用程序负载均衡器配置与 SRT 的主动交互。要了解有关选项的更多信息，请参阅 [中的资源保护 Amazon Shield Advanced \(p. 351\)](#)。

以下参考图描述了适用于 TCP 和 UDP 应用程序的 DDoS 弹性架构示例。

附录二 附录三 附录四 附录五 附录六 附录七 附录八 附录九 附录十 附录十一 附录十二 附录十三 附录十四 附录十五 附录十六 附录十七 附录十八 附录十九 附录二十 附录二十一 附录二十二 附录二十三 附录二十四 附录二十五 附录二十六 附录二十七 附录二十八 附录二十九 附录三十 附录三十一 附录三十二 附录三十三 附录三十四 附录三十五 附录三十六 附录三十七 附录三十八 附录三十九 附录四十 附录四十一 附录四十二 附录四十三 附录四十四 附录四十五 附录四十六 附录四十七 附录四十八 附录四十九 附录五十 附录五十一 附录五十二 附录五十三 附录五十四 附录五十五 附录五十六 附录五十七 附录五十八 附录五十九 附录六十 附录六十一 附录六十二 附录六十三 附录六十四 附录六十五 附录六十六 附录六十七 附录六十八 附录六十九 附录七十 附录七十一 附录七十二 附录七十三 附录七十四 附录七十五 附录七十六 附录七十七 附录七十八 附录七十九 附录八十 附录八十一 附录八十二 附录八十三 附录八十四 附录八十五 附录八十六 附录八十七 附录八十八 附录八十九 附录九十 附录九十一 附录九十二 附录九十三 附录九十四 附录九十五 附录九十六 附录九十七 附录九十八 附录九十九 附录一百

目标	推荐的服务	相关服务文档
保护基于 UDP 的游戏服务器免受 DDoS 攻击	Shield Advanced 可保护附加到弹性 IP 地址的 Amazon EC2 实例	Amazon Elastic Compute Cloud 文档

例如，如果您使用 Shield Advanced 保护弹性 IP 地址，Shield Advanced 将保护与此地址相关联的任何资源。在攻击期间，Shield Advanced 会自动将网络 ACL 部署到 Amazon 网络。当您的网络 ACL 位于网络边界时，Shield Advanced 可以提供保护以防范更大的 DDoS 事件。通常情况下，网络 ACL 会应用到您的 Amazon VPC 中的 Amazon EC2 实例附近。网络 ACL 只能缓解您的 Amazon VPC 和实例可以处理的攻击。如果连接到您的 Amazon EC2 实例的网络接口可以处理高达 10 Gbps，那么超过 10 Gbps 的流量将会减速并可能阻止通往此实例的流量。在攻击期间，Shield Advanced 将您的网络 ACL 提升至 Amazon 边界，它可以处理多个 TB 的流量。您的网络 ACL 能够为您的资源提供超出您的网络典型容量的保护。有关网络 ACL 的更多信息，请参阅[网络 ACL](#)。

Amazon Shield Advanced 入门

本教程将指导您完成入门 Amazon Shield Advanced。Shield Advanced 为网络层（第 3 层）、传输层（第 4 层）和应用层（第 7 层）攻击提供高级 DDoS 检测和缓解保护。

Shield [Amazon Shield Advanced 概览 \(p. 331\)](#)。

Note

在分布式拒绝服务 (DDoS) 事件发生之前，必须完全配置 Shield Advanced。完成以下步骤，以帮助确保您的应用程序受到保护，并在应用程序受到 DDoS 攻击时做好响应准备。

请按顺序执行以下步骤。

目录

- [订阅 Amazon Shield Advanced \(p. 343\)](#)
- [添加资源以保护和配置保护 \(p. 344\)](#)
 - [使用以下配置应用层（第 7 层）DDoS 保护 Amazon WAF \(p. 345\)](#)
 - [配置基于健康的检测以保护您的安全 \(p. 346\)](#)
 - [配置警报和通知 \(p. 346\)](#)
 - [查看并完成您的保护配置 \(p. 346\)](#)
- [配置 Amazon SRT 支持 \(p. 346\)](#)
- [在中创建 DDoS 仪表板 CloudWatch 并设置 CloudWatch 警报 \(p. 348\)](#)

订阅 Amazon Shield Advanced

要保护的每种 Amazon Web Services 账户，都必须订阅。

对于属于 Amazon Organizations 组织成员的账户，无论付款人账户本身是否已订阅，Shield Advanced 订阅都将计入该组织的付款人账户。Amazon

订阅多个账户

当您订阅同一个 [Amazon Organizations 整合账单账户系列中的多个账户](#) 时，一个订阅价格涵盖该系列中的所有订阅账户。该组织必须拥有所有 Amazon Web Services 账户及其资源。例外情况适用于 Amazon 渠道经销商。有关详细的定价信息和示例，请参阅 [Amazon Shield Advanced 定价](#)。

如果您的账户是组织的一部分，我们建议您尽可能使用 Amazon Firewall Manager 该组织自动订阅和保护。Firewall Manager 支持除了 Amazon Route 53 和之外的所有受保护资源类型 Amazon Global

Accelerator。要使用 Firewall Manager，请参阅[Amazon Firewall Manager \(p. 403\)](#)和[开始使用 Amazon Firewall Manager Amazon Shield Advanced 策略 \(p. 410\)](#)。

如果您不使用 Firewall Manager，请使用以下步骤为每个拥有保护资源的账户订阅和添加保护。

订阅账户 Amazon Shield Advanced

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在 Amazon Shield 导航栏中，选择“入门”。选择“订阅 Shield 高级版”。
3. 在“订阅 Shield Advanced”页面中，阅读协议的每个条款，然后选中所有复选框以表明您接受这些条款。对于整合账单系列中的账户，您必须同意每个账户的条款。

Important

订阅后，您必须联系才能取消订阅 [Amazon Web Services Support](#)。
要禁用订阅的自动续订，必须使用 Shield API 操作 [UpdateSubscription](#) 或 CLI 命令 [更新订阅](#)。

选择“订阅 Shield 高级版”。这将使您的账户订阅 Shield Advanced 并激活该服务。

您的账户已订阅。继续执行以下步骤，使用 Shield Advanced 保护您的账户资源。

Note

订阅后，Shield Advanced 不会自动保护您的资源。您必须指定您希望 Shield Advanced 保护的资源配置保护。

添加资源以保护和配置保护

Shield Advanced 仅保护您通过 Shield Advanced 或 Firewall Manager Shield Advanced 策略中指定的资源。它不会自动保护订阅账户的资源。

如果您使用 Amazon Firewall Manager，您可以使用要保护的资源类型配置策略，Firewall Manager 会自动为策略范围内的资源添加保护。

如果您不使用 Firewall Manager，请为每个有资源需要保护的账户执行以下步骤。

使用 Shield Advanced 选择要保护的资源

1. 从先前过程的订阅确认页面或受保护的资源或概述页面中选择“添加要保护的资源”。
2. 在“使用 Shield Advanced 选择要保护的资源”页面的“指定区域和资源类型”中，提供要保护的资源的区域和资源类型规范。您可以通过选择“所有区域”来保护多个区域中的资源，也可以通过选择“全球”将选择范围缩小到全局资源。您可以取消选择任何不想保护的资源类型。有关保护您的资源类型的信息，请参阅[Amazon Shield Advanced 按资源类型划分的保护 \(p. 352\)](#)。
3. 选择加载资源。Shield Advanced 会使用符合您的标准的 Amazon 资源填充选择资源部分。
4. 在选择资源部分中，您可以通过在资源列表中输入要搜索的字符串来筛选资源列表。

选择要保护的资源。

5. 在“标签”部分中，如果您想向正在创建的 Shield Advanced 保护添加标签，请指定这些标签。有关为 Amazon 资源添加标签的信息，请参阅[使用标签编辑器](#)。
6. 选择“使用 Shield 高级保护”。这为资源增加了 Shield 高级保护。

继续浏览控制台向导屏幕以完成资源保护的配置。

主题

- [使用以下配置应用层 \(第 7 层\) DDoS 保护 Amazon WAF \(p. 345\)](#)
- [配置基于健康的检测以保护您的安全 \(p. 346\)](#)
- [配置警报和通知 \(p. 346\)](#)
- [查看并完成您的保护配置 \(p. 346\)](#)

使用以下配置应用层 (第 7 层) DDoS 保护 Amazon WAF

为了保护应用层资源，Shield Advanced Amazon WAF 使用基于速率的规则 Web ACL 作为起点。Amazon WAF 是一种 Web 应用程序防火墙，可让您监视转发到应用程序层资源的 HTTP 和 HTTPS 请求，并控制对您的内容的访问。基于速率的规则限制来自任何单个 IP 地址的流量，为您的应用程序提供基本的 DDoS 保护。有关更多信息，请参阅 [Amazon WAF 的工作原理 \(p. 6\)](#) 和 [基于速率的规则语句 \(p. 95\)](#)。

在 Shield Advanced 中使用 Amazon WAF 网络 ACL 的基本费用由您的 Shield Advanced 订阅支付。有关定价信息和示例，请参阅 [Amazon Shield Advanced 定价](#)。

您还可以选择启用 Shield Advanced 自动应用层 DDoS 缓解功能，让 Shield Advanced 自动为您提供针对特定事件的保护。

Important

如果您通过 Amazon Firewall Manager 使用 Shield Advanced 策略来管理您的 Shield Advanced 保护，则无法在此处管理应用程序层保护。您必须在 Firewall Manager 中管理。

为区域配置第 7 层 DDoS 保护

Shield Advanced 允许您选择为所选资源所在的每个区域配置第 7 层 DDoS 缓解措施。如果您要在多个区域添加保护，则向导会引导您完成每个区域的以下步骤。

1. 配置第 7 层 DDoS 保护页面列出了尚未与 Web ACL 关联的每种资源。对于每个，要么选择现有的 Web ACL，要么创建一个新的 Web ACL。对于任何已经有关联 Web ACL 的资源，您可以先通过取消当前 ACL 的关联来更改 Web ACL Amazon WAF。有关更多信息，请参阅 [将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)：

对于还没有基于速率的规则 Web ACL，配置向导会提示您添加一个。基于速率的规则限制了来自 IP 地址发送大量请求的流量。基于速率的规则有助于保护您的应用程序免受 Web 请求泛滥的影响，并可以提供有关流量突然激增的警报，这可能表明存在潜在的 DDoS 攻击。选择添加速率限制规则，然后提供速率限制和规则操作，将基于速率的规则添加到 Web ACL。您可以通过在 Web ACL 中配置其他保护 Amazon WAF。

有关在 Shield Advanced 保护中使用 Web ACL 和基于速率的规则（包括基于速率的规则的其他配置选项）的信息，请参阅 [Shield 高级应用层 Amazon WAF Web ACL 和基于速率的规则 \(p. 353\)](#)。

2. 对于自动应用层 DDoS 缓解，如果您想让 Shield Advanced 自动缓解针对您的应用层资源的 DDoS 攻击，请选择“启用”，然后选择您希望 Shield Advanced 在其自定义规则中使用的规则操作。Amazon WAF 此设置适用于您在此向导会话中管理的资源的所有 Web ACL。

借助应用层 DDoS 自动缓解功能，Shield Advanced 将当前流量模式与历史流量基准进行比较，以检测可能预示 DDoS 攻击的偏差。如果为资源启用了自动缓解功能，则当 Shield Advanced 检测到 DDoS 攻击时，它会通过创建、评估和部署自定义 Amazon WAF 规则进行响应。您可以指定自定义规则是计算还是代表您阻止攻击。

Note

自动应用层 DDoS 缓解仅适用于使用最新版本 Amazon WAF (v2) 创建的 Web ACL。

有关 Shield Advanced 自动应用层 DDoS 缓解的更多信息，请参阅 [Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

3. 选择 Next (下一步)。控制台向导进入基于健康状况的检测页面。

配置基于健康的检测以保护您的安全

您可以选择将 Shield Advanced 配置为使用基于健康的检测，这可以提高攻击检测和缓解的响应能力和准确性。您可以将此选项用于除了 Route 53 托管区域之外的任何资源类型。

要使用基于生命值的检测，您首先需要在 Route 53 中为您的资源定义运行状况检查，然后将运行状况检查与 Shield Advanced 保护关联起来。您配置的运行状况检查必须准确反映资源的运行状况，这一点很重要。有关配置运行状况检查以与 Shield Advanced 一起使用的信息和示例，请参阅[使用运行状况检查配置基于健康的检测 \(p. 358\)](#)。

Shield 响应小组 (SRT) 主动参与支持需要进行 Health 检查。有关主动参与的信息，请参阅[配置主动参与操作 \(p. 350\)](#)。

Note

将 Health 检查与 Shield Advanced 保护关联时，必须报告健康状况良好。

配置基于健康的检测

1. 在 Associated Health Check (关联运行状况检查) 下，选择要与保护关联的运行状况检查的 ID。

Note

如果您没有看到所需的运行状况检查，请前往 Route 53 控制台验证运行状况检查及其 ID。有关信息，请参阅[创建和更新运行状况检查](#)。

2. 选择 Next (下一步)。控制台向导进入警报和通知页面。

配置警报和通知

您可以选择为检测到的 Amazon CloudWatch 警报和基于费率的规则活动配置亚马逊简单通知服务通知。当 Shield 检测到受保护资源上的事件或超过基于速率的规则中配置的速率限制时，您可以使用它们接收通知。

有关 Shield Advanced CloudWatch 指标的信息，请参阅[the section called “指标” \(p. 377\)](#)。有关 Amazon SNS 的信息，请参阅 A [amazon Simple Notifce 开发人员指南](#)。

配置警报和通知

1. 选择要通知的 Amazon SNS 主题。您可以对所有受保护的资源和基于费率的规则使用单个 Amazon SNS 主题，也可以选择针对您的组织自定义的不同主题。例如，您可以为负责一组特定资源的事件响应的每个团队创建一个 SNS 主题。
2. 选择 Next (下一步)。控制台向导前进到资源保护审查页面。

查看并完成您的保护配置

查看和配置您的设置

1. 在查看和配置 DDoS 缓解和可见性页面中，查看您的设置。要进行修改，请在要修改的区域中选择 Ed ianager。系统会带您返回控制台向导中的关联页面。进行更改，然后在后续页面中选择“下一步”，直到返回“查看并配置 DDoS 缓解和可见性”页面。
2. 选择“完成配置”。受保护的资源页面列出了您的新保护资源。

配置Amazon SRT 支持

Shield Response Team (SRT) 是专门研究 DDoS 事件响应的安全工程师。您可以选择添加权限，允许 SRT 在 DDoS 事件期间代表您管理资源。此外，您可以配置 SRT，使其在检测到的事件期间与您的受保护资源相

关的 Route 53 运行状况检查运行状况不佳时主动与您联系。这两项保护措施都使您能够更快地响应 DDoS 事件。

Note

要使用 Shield Response Team (SRT) 的服务，您必须订阅[业务Support 计划](#)或[企业Support 计划](#)。

SRT 可以在应用层事件期间监控Amazon WAF请求数据和日志，以识别异常流量。他们可以帮助制定自定义Amazon WAF规则，以减少违规流量来源。根据需要，SRT 可能会提出架构建议，以帮助您更好地根据Amazon建议调整资源。

有关 SRT 的更多信息，请参阅[Shield 响应小组 \(SRT\) 支持 \(p. 348\)](#)。

向 SRT 授予权限

1. 在Amazon Shield控制台概述页面的配置Amazon SRT 支持下，选择编辑 SRT 访问权限。编辑Amazon Shield 响应小组 (SRT) 访问页面打开。
2. 对于 SRT 访问设置，请选择以下选项之一：
 - 不要授予 SRT 访问我的账户的权限 — Shield 会删除您之前授予 SRT 访问您的账户和资源的任何权限。
 - 为 SRT 创建一个新角色来访问我的账户 — Shield 创建了一个信任代表 SRT 的服务委托 `drt.shield.amazonaws.com` 托人的角色，并将托管策略附加 `AWSShieldDRTAccessPolicy` 到该角色。托管策略允许 SRT 代表您Amazon WAF进行 API 调用并访问您的Amazon WAF日志。Amazon Shield Advanced有关托管策略的更多信息，请参阅[Amazon 托管策略：AWSShieldDRTAccessPolicy \(p. 396\)](#)。
 - 为 SRT 选择一个现有角色来访问我的账户 — 对于此选项，您必须按如下方式修改Amazon Identity and Access Management (IAM) 中的角色配置：
 - 将托管策略 `AWSShieldDRTAccessPolicy` 附加到角色。此托管策略允许 SRT 代表您Amazon WAF进行 API 调用并访问您的Amazon WAF日志。Amazon Shield Advanced有关托管策略的更多信息，请参阅[Amazon托管策略：AWSShieldDRTAccessPolicy \(p. 396\)](#)。有关将托管策略附加到您的角色的信息，请参阅[附加和分离 IAM 策略](#)。
 - 修改角色以信任 `drt.shield.amazonaws.com` 服务主体。这是代表 SRT 的服务主体。有关更多信息，请参阅[IAM JSON 策略元素：主体](#)。
3. 选择 Save (保存) 以保存您的更改。

有关授予 SRT 访问您的保护和数据的更多信息，请参阅[为Shield 响应小组 \(SRT\) 配置访问权限 \(p. 349\)](#)。

启用 SRT 主动参与

1. 在Amazon Shield控制台概述页面的主动互动和联系人下，在联系人区域中选择编辑。

在编辑联系人页面中，提供您希望 SRT 联系以主动参与的人员的联系信息。

如果您提供多个联系人，请在注释中注明应在何种情况下使用每个联系人。包括主要和次要联系人的名称，并提供每个联系人的可用时间和时区。

联系人备注示例：

- 这是一条全天候有人值守的热线。请与回应的分析师合作，他们将安排相应的人接听电话。
- 如果热线在 5 分钟内没有回复，请与我联系。

2. 选择 Save (保存)。

概览页面反映了更新的联系信息。

3. 选择“编辑主动参与功能”，选择“启用”，然后选择“保存”以启用主动互动。

您可以使用亚马逊监视潜在的 DoS 活动 CloudWatch，Amazon 收集来自 Amazon 的原始数据，并将其处理为易读且近乎实时的指标。您可以使用中的统计数据 CloudWatch 来了解您的 Web 应用程序或服务的执行情况。有关使用的更多信息 CloudWatch，请参阅亚马逊 CloudWatch 用户指南 CloudWatch 中的[内容](#)。

- Shield Advanced 在 DDoS 事件期间报告资源指标的频率比没有事件发生时 CloudWatch 更频繁。Shield Advanced 在活动期间每分钟报告一次指标，然后在活动结束后立即报告一次。虽然没有事件在进行中，但 Shield Advanced 会在分配给资源的时间每天报告一次指标。此定期报告使指标保持活动状态并可用于您的自定义 CloudWatch 警报。

Shield 响应小组 (SRT) 为 Shield Advanced 客户提供额外支持。SRT 是专门研究 DDoS 事件响应的安全工程师。作为对您的 Amazon Web Services Support 计划的额外支持，您可以直接与 SRT 合作，利用他们的专业知识作为事件响应工作流程的一部分。有关选项的信息和配置指南，请参阅以下主题。

与 SRT 合作的主要目标是保护应用程序的可用性和性能。根据 DDoS 事件的类型和应用程序的架构，SRT 可能会采取以下一项或多项操作：

- 为Shield 响应小组 (SRT) 配置访问权限 (p. 349)

- [配置主动参与操作 \(p. 350\)](#)
- [联系Shield 响应小组 \(SRT\) \(p. 351\)](#)
- [使用Shield 响应小组 \(SRT\) 配置自定义缓解措施 \(p. 351\)](#)

为Shield 响应小组 (SRT) 配置访问权限

您可以向 Shield Response Team (SRT) 授予代表您采取行动的权限，访问您的Amazon WAF日志并调用 Amazon Shield Advanced和Amazon WAF API 来管理保护。在应用层 DDoS 事件期间，SRT 可以监控 Amazon WAF请求以识别异常流量，并帮助制定自定义Amazon WAF规则以缓解违规流量来源。

此外，您可以授予 SRT 访问您存储在 Amazon S3 存储桶中的其他数据的权限，例如来自Application Load Balancer CloudFront、Amazon 或第三方来源的数据包捕获或日志。

Note

要使用 Shield Response Team (SRT) 的服务，您必须订阅[业务Support 计划](#)或[企业Support 计划](#)。

管理 SRT 的权限

1. 在Amazon Shield控制台概述页面的配置Amazon SRT 支持下，选择编辑 SRT 访问权限。编辑Amazon Shield 响应小组 (SRT) 访问页面打开。
2. 对于 SRT 访问设置，请选择以下选项之一：
 - 不要授予 SRT 访问我的账户的权限 — Shield 会删除您之前授予 SRT 访问您的账户和资源的任何权限。
 - 为 SRT 创建一个新角色来访问我的账户 — Shield 创建了一个信任代表 SRT 的服务委托 `drt.shield.amazonaws.com` 托人的角色，并将托管策略附加 `AWSShieldDRTAccessPolicy` 到该角色。托管策略允许 SRT 代表您Amazon WAF进行 API 调用并访问您的Amazon WAF日志。Amazon Shield Advanced有关托管策略的更多信息，请参阅[Amazon 托管策略：AWSShieldDRTAccessPolicy \(p. 396\)](#)。
 - 为 SRT 选择一个现有角色来访问我的账户 — 对于此选项，您必须按如下方式修改Amazon Identity and Access Management (IAM) 中的角色配置：
 - 将托管策略 `AWSShieldDRTAccessPolicy` 附加到角色。此托管策略允许 SRT 代表您Amazon WAF进行 API 调用并访问您的Amazon WAF日志。Amazon Shield Advanced有关托管策略的更多信息，请参阅[Amazon托管策略：AWSShieldDRTAccessPolicy \(p. 396\)](#)。有关将托管策略附加到您的角色的信息，请参阅[附加和分离 IAM 策略](#)。
 - 修改角色以信任 `drt.shield.amazonaws.com` 服务主体。这是代表 SRT 的服务主体。有关更多信息，请参阅[IAM JSON 策略元素：主体](#)。
3. 用于（可选）：授予 Amazon S3 存储桶的 SRT 访问权限，如果您需要共享不在Amazon WAF Web ACL 日志中的数据，请配置此项。例如，Application Load Balancer 访问 CloudFront 日志、Amazon 日志或来自第三方来源的日志。

Note

您无需为Amazon WAF Web ACL 日志执行此操作。当您向您的账户授予访问权限时，SRT 将获得访问这些权限。

a. 根据以下准则配置 Amazon S3 存储段：

- 存储桶位置必须与您在之前Amazon Web Services 账户的步骤Amazon中授予 SRT 常规访问权限的存储桶位置相同。
- 存储桶可以是纯文本的，也可以是 SSE-S3 加密的。有关 Amazon S3 SSE-S3 加密的更多信息，请参阅[Amazon S3 托管加密密钥 \(SSE-S3\) 保护数据](#)。

SRT 无法查看或处理存储在使用存储在Amazon Key Management Service (Amazon KMS) 中的密钥加密的存储桶中的日志。

- b. 在 Shield Advanced (可选) : 授予 SRT 对 Amazon S3 存储桶的访问权限部分, 对于存储您的数据或日志的每个 Amazon S3 存储桶, 输入存储桶的名称并选择添加存储桶。您最多可以添加 10 个存储桶。

这会授予 SRT 对每个存储段的以下权限: s3:GetBucketLocations3:GetObject、和s3:ListBucket。

如果您想授予 SRT 访问超过 10 个存储段的权限, 则可以通过编辑其他存储段策略并手动授予此处列出的 SRT 权限来实现此目的。

4. 选择 Save (保存) 以保存您的更改。

您还可以通过 API 授权 SRT, 方法是创建 IAM 角色, 将策略附加 AWSShieldDRTAccessPolicy 到该角色, 然后将该角色传递给 Assoc [iatedRTrole](#) 操作。

配置主动参与操作

通过主动接触, 当您的应用程序的可用性或性能因可能的攻击而受到影响时, Shield Response Team (SRT) 会直接与您联系。我们之所以推荐这种互动模式, 是因为它提供了最快的 SRT 响应, 而且它允许 SRT 在与您建立联系之前就开始进行故障排除。

主动参与可用于弹性 IP 地址和Amazon Global Accelerator标准加速器上的网络层和传输层事件, 以及 Amazon CloudFront 发行版和应用程序负载均衡器上的 Web 请求泛滥。主动参与仅适用于具有相关亚马逊 Route 53 运行状况检查的 Shield Advanced 资源保护。有关管理和使用运行状况检查的信息, 请参阅[使用运行状况检查配置基于健康的检测 \(p. 358\)](#)。

在 Shield Advanced 检测到的活动中, SRT 会使用您的健康检查状态来确定该活动是否符合主动参与的条件。如果是, SRT 将根据您在主动参与配置中提供的联系指南与您联系。

您最多可以配置十个联系人以进行主动接触, 并且可以提供备注来指导 SRT 与您联系。在活动期间, 您的主动参与联系人应能与 SRT 互动。如果您没有全天候运营中心, 则可以提供寻呼机联系人, 并在联系人备注中注明此联系人偏好。

主动参与要求您执行以下操作:

- 您必须订阅[业务Support 计划](#)或[企业Support 计划](#)。
- 您必须将 Amazon Route 53 运行状况检查与您想要通过主动参与保护的任何资源相关联。SRT 使用您的运行状况检查状态来帮助确定某一事件是否需要主动参与, 因此, 您的运行状况检查必须准确反映受保护资源的状态。有关更多信息和指导, 请参阅[使用运行状况检查配置基于健康的检测 \(p. 358\)](#)。
- 对于关联了Amazon WAF Web ACL 的资源, 必须使用Amazon WAF (v2) 创建 Web ACL, 这是的最新版 Amazon WAF。
- 您必须提供至少一名联系人, SRT 才能在活动期间主动参与。保持您的联系信息完整且最新。

启用 SRT 主动参与

1. 在Amazon Shield控制台概述页面的主动互动和联系人下, 在联系人区域中选择编辑。

在编辑联系人页面中, 提供您希望 SRT 联系以主动参与的人员的联系信息。

如果您提供多个联系人, 请在注释中注明应在何种情况下使用每个联系人。包括主要和次要联系人的名称, 并提供每个联系人的可用时间和时区。

联系人备注示例:

- 这是一条全天候有人值守的热线。请与回应的分析师合作, 他们将安排相应的人接听电话。
- 如果热线在 5 分钟内没有回复, 请与我联系。

2. 选择保存。

概览页面反映了更新的联系信息。

3. 选择“编辑主动参与功能”，选择“启用”，然后选择“保存”以启用主动互动。

联系Shield 响应小组 (SRT)

您可以通过以下方式联系Shield 响应小组 (SRT)：

- Su@@pport 案例 — 您可以在[Amazon Web Services Support中心](#)下Amazon Shield方打开案例。选择适合您的情况的严重程度，并提供您的联系方式。在描述中，提供尽可能多的细节。提供有关您认为可能受到影响的任何受保护资源的信息，以及您的最终用户体验的当前状态。例如，如果用户体验变差或应用程序的某些部分当前无法可用，请提供该信息。

如果您的应用程序的可用性或性能目前受到可能的 DDoS 攻击的影响，请选择以下严重程度和联系选项：

- 对于严重性，请选择您的支持计划可用的最高严重性：
 - 对于业务支持，这是生产系统停机：< 1 小时。
 - 对于企业支持，这是关键业务系统停机：< 15 分钟。
- 对于联系选项，请选择“电话”或“聊天”并提供您的详细信息。使用实时联系方法可提供最快的响应。
- 主动参与 — 通过Amazon Shield Advanced主动参与，如果您的受保护资源相关的 Amazon Route 53 运行状况检查在检测到的事件期间变得不正常，SRT 会直接与您联系。有关此选项的更多信息，请参阅[配置主动参与操作 \(p. 350\)](#)。

使用Shield 响应小组 (SRT) 配置自定义缓解措施

对于您的弹性 IP (EIP) 和Amazon Global Accelerator标准加速器，您可以与Shield 响应团队 (SRT) 合作配置自定义缓解措施。如果您知道在实施缓解措施时应强制执行的特定逻辑，这将很有用。例如，您可能希望仅允许来自某些国家/地区的流量、强制执行特定的速率限制、配置可选验证、禁止分段或仅允许与数据包有效载荷中特定模式相匹配的流量。

常见的自定义缓解措施包括：

- 模式匹配-如果您运行与客户端应用程序交互的服务，则可以选择根据这些应用程序特有的已知模式进行匹配。例如，您可能运营一项游戏或通信服务，要求最终用户安装您分发的特定软件。您可以在应用程序发送到您的服务的每个数据包中加入“魔法数字”。您最多可以匹配 128 字节（单独或连续）的非分段 TCP 或 UDP 数据包负载和标头。匹配可以用十六进制表示法表示为距离数据包有效载荷开头的特定偏移量或已知值之后的动态偏移量。例如，缓解措施可以查找该字节，0x01然后预期0x12345678为接下来的四个字节。
- DNS 专用 — 如果您使用全球加速器或 Amazon Elastic Compute Cloud (Amazon EC2) 等服务运营自己的权威 DNS 服务，则可以请求自定义缓解措施来验证数据包以确保它们是有用的 DNS 查询，并应用可疑评分来评估特定于 DNS 流量的属性。

要询问有关与 SRT 合作构建自定义缓解措施的问题，请在下方创建支持案例Amazon Shield。要了解有关创建Amazon Web Services Support案例的更多信息，请参阅[入门Amazon Web Services Support](#)。

中的资源保护Amazon Shield Advanced

您可以添加和配置Amazon Shield Advanced保护你的资源。您可以管理单个资源的保护，也可以将受保护的资源分组到逻辑集合中，以便更好地管理事件。您还可以使用以下方式跟踪您的 Shield Advanced 防护 Amazon Config。

主题

- [Amazon Shield Advanced按资源类型划分的保护 \(p. 352\)](#)
- [Amazon Shield Advanced应用层 \(第 7 层\) 保护 \(p. 353\)](#)
- [使用运行状况检查配置基于健康的检测 \(p. 358\)](#)
- [管理中的资源保护Amazon Shield Advanced \(p. 364\)](#)
- [Amazon Shield Advanced保护 \(p. 368\)](#)
- [跟踪中的资源保护变化Amazon Config \(p. 369\)](#)

Amazon Shield Advanced按资源类型划分的保护

Shield Advanced 保护网络和传输层 (第 3 层和第 4 层) 以及应用层 (第 7 层) 中的 Amazon 资源。您可以直接保护某些资源, 而通过关联受保护的资源来保护其他资源。此部分提供有关针对每种资源类型的 Shield Application

Note

Shield Advanced 仅保护您在 Shield Advanced 中或通过 Amazon Firewall Manager Shield 高级策略指定的资源。它不会自动保护您的资源。

您可以使用 Shield Advanced 对以下资源类型进行高级监控和保护：

- 亚马逊 CloudFront 分发。对于 CloudFront 持续部署, Shield Advanced 可保护与受保护的主发行版相关的任何暂存发行版。
- 亚马逊 Route 53 托管区域。
- Amazon Global Accelerator 标准加速器。
- Amazon EC2 弹性 IP 地址。Shield Advanced 保护与受保护的弹性 IP 地址相关的资源。
- Amazon EC2 实例, 通过关联 Amazon EC2 弹性 IP 地址。
- 以下 Elastic Load Balancing 器 (ELB) :
 - 应用程序负载均衡器。
 - 经典负载均衡器。
 - 网络负载均衡器, 通过关联到 Amazon EC2 弹性 IP 地址。

你不能使用 Shield Advanced 来保护任何其他资源类型。例如, 您无法保护 Amazon Global Accelerator 自定义路由加速器或网关负载均衡器。

您可以监控和保护每种资源类型的最多 1,000 个资源 Amazon Web Services 账户。例如, 在单个账户中, 您可以保护 1,000 个 Amazon EC2 弹性 IP 地址、1,000 个 CloudFront 分配和 1,000 个应用程序负载均衡器。你可以通过 Service 配额控制台 <https://console.aws.amazon.com/servicequotas/> 申请增加可以使用 Shield Advanced 保护的资源数量。

使用 Shield Advanced 保护 Amazon EC2 实例和网络负载均衡器

您可以先将这些资源连接到弹性 IP 地址, 然后在 Shield Advanced 中保护弹性 IP 地址, 从而保护 Amazon EC2 实例和网络负载均衡器。

当您保护弹性 IP 地址时, Shield Advanced 会识别并保护它们所连接的资源。Shield Advanced 会自动识别连接到弹性 IP 地址的资源类型, 并对该资源应用适当的检测和缓解措施。这包括配置特定于弹性 IP 地址的网络 ACL。有关在 Amazon 资源中使用弹性 IP 地址的更多信息, 请参阅以下指南: [Amazon Elastic Compute Cloud 文档](#) 或 [Elastic Load Balancing 文档](#)。

在攻击期间, Shield Advanced 会自动将您的网络 ACL 部署到 Amazon 网络边界。当您的网络 ACL 位于网络边界时, Shield Advanced 可以针对更大的 DDoS 事件提供保护。通常, 网络 ACL 应用于亚马逊 VPC 内的 Amazon EC2 实例附近。网络 ACL 只能缓解您的 Amazon VPC 和实例能够处理的大型攻击。例如, 如果连

接到您的 Amazon EC2 实例的网络接口最多可以处理 10 Gbps，则超过 10 Gbps 的容量将减慢并可能阻塞流向该实例的流量。在攻击期间，Shield Advanced 会将您的网络 ACL 提升到 Amazon 边界，这可以处理数 TB 的流量。您的网络 ACL 能够为您的资源提供超出您的网络典型容量的保护。有关网络 ACL 的更多信息，请参阅[网络 ACL](#)。

一些扩展工具，例如 Amazon Elastic Beanstalk，不允许您将弹性 IP 地址自动连接到 Network Load Balancer。对于这些情况，您需要手动连接弹性 IP 地址。

Amazon Shield Advanced 应用层（第 7 层）保护

要使用 Shield Advanced 保护您的应用层资源，首先要将 Amazon WAF Web ACL 与该资源相关联，然后向其添加一个或多个基于速率的规则。此外，您还可以启用自动应用层 DDoS 缓解，这会让 Shield Advanced 自动代表您创建和管理 Web ACL 规则，以响应 DDoS 攻击。

当您使用 Shield Advanced 保护应用程序层资源时，Shield Advanced 会分析一段时间内的流量，以建立和维护基准。Shield Advanced 使用这些基准来检测流量模式中可能表明 DDoS 攻击的异常情况。Shield Advanced 检测到攻击的时间点取决于 Shield Advanced 在攻击之前能够观察到的流量以及您用于 Web 应用程序的架构。可能影响 Shield Advanced 行为的架构变体包括您使用的实例类型、您的实例大小以及该实例类型是否支持增强联网。您还可以将 Shield Advanced 配置为自动缓解应用层攻击。

主题

- [Shield 高级应用层 Amazon WAF Web ACL 和基于速率的规则 \(p. 353\)](#)
- [Shield Advanced 自动应用层 DDoS \(p. 354\)](#)

Shield 高级应用层 Amazon WAF Web ACL 和基于速率的规则

要使用 Shield Advanced 保护应用层资源，首先要将 Amazon WAF Web ACL 与该资源关联。Amazon WAF 是一种 Web 应用程序防火墙，可让您监视转发到应用程序层资源的 HTTPS 和 HTTP 请求，并根据请求的特征控制对您的内容的访问。您可以配置 Web ACL 以根据请求的来源、查询字符串和 cookie 的内容以及来自单个 IP 地址的请求速率等因素来监控和管理请求。您的 Shield Advanced 保护至少要求您将 Web ACL 与基于速率的规则关联，该规则限制了每个 IP 地址的请求速率。

如果关联的 Web ACL 没有定义基于速率的规则，Shield Advanced 会提示您至少定义一个规则。当来自源 IP 的流量超过您定义的阈值时，基于速率的规则会自动阻止这些流量。它们有助于保护您的应用程序免受网络请求泛洪的影响，并可以提供有关流量突然激增的警报，这可能表明存在潜在的 DDoS 攻击。

在您的 Web ACL 到位后，如果发生 DDoS 攻击，您可以通过在 Web ACL 中添加和管理规则来采取缓解措施。您可以在 Shield 响应小组 (SRT) 的协助下直接执行此操作，也可以通过自动应用层 DDoS 缓解来执行此操作。

基于速率的规则是如何运作的

当您使用基于速率的规则时，每 30 秒 Amazon WAF 评估前五分钟的流量。Amazon WAF 阻止来自任何超过阈值的源 IP 地址的请求，直到请求速率降至可接受的水平。配置基于速率的规则时，将其速率阈值配置为一个大于您在任何五分钟时间段内来自任何一个源 IP 的正常流量速率的值。

您可能需要在 Web ACL 中使用多个基于速率的规则。例如，您可以为所有具有较高阈值的流量设置一条基于速率的规则，外加一条或多条配置为匹配 Web 应用程序的选定部分且阈值较低的附加规则。例如，您可以在 URI 上匹配 /login.html 具有较低阈值的 URI，以减少对登录页面的滥用。

有关其他信息和指导，请参阅安全博客文章“[三个最重要的 Amazon WAF 基于速率的规则](#)”。

通过扩展配置选项 Amazon WAF

Shield Advanced 控制台允许您添加基于速率的规则并使用基本设置对其进行配置。您可以通过管理基于速率的规则来定义其他配置选项 Amazon WAF。例如，您可以将规则配置为聚合转发的 IP 地址，也可以添加

范围缩小语句以过滤掉评估中的某些请求。有关所有配置选项，请参阅[基于速率的规则语句 \(p. 95\)](#)。有关使用 Amazon WAF 管理 Web 请求监控和管理规则的信息，请参阅[创建 Web ACL \(p. 17\)](#)。

Shield Advanced 自动应用层 DDoS

您可以将 Shield Advanced 配置为自动响应，通过计算或阻止作为攻击一部分的 Web 请求，来缓解针对受保护应用程序层资源的应用程序层（第 7 层）攻击。此选项是您通过 Shield Advanced 通过 Amazon WAF Web ACL 和基于速率的规则添加的应用层保护的补充。有关控制台步骤的信息，请参阅[配置应用层 DDoS 保护 \(p. 365\)](#)。

Shield Advanced 将当前的流量模式与历史流量基准进行比较，以检测可能表明 DDoS 攻击的偏差。当您为资源启用自动应用层 DDoS 缓解时，Shield Advanced 会通过创建、评估和部署自定义 Amazon WAF 规则来响应检测到的 DDoS 攻击。

Shield Advanced 自动应用层 DDoS 缓解注意事项

以下列表描述了 Shield Advanced 自动应用层 DDoS 缓解的注意事项，并描述了您可能需要采取的应对措施。

- 自动应用层 DDoS 缓解仅适用于使用最新版本的 Amazon WAF (v2) 创建的 Web ACL。
- 为了检测和自动缓解应用层攻击，Shield Advanced 利用了您的受保护资源的历史流量。了解应用程序的正常流量模式使 Shield Advanced 能够将攻击流量与应用程序的正常流量隔离开来。如果您的受保护资源还没有正常应用程序流量的历史记录（例如在应用程序启动之前），或者如果它长时间没有生产流量，我们建议在正常应用程序流量的历史记录出现之前，在 COUNT 模式下启用自动缓解功能为资源建立。
- Shield Advanced 需要 24 小时到 30 天才能建立应用程序流量的基准。
- 应用层 DDoS 自动缓解只有在根据历史流量进行测试后才会放置缓解 DDoS 攻击的规则，以验证它们是否缓解了攻击流量并且不会影响应用程序的正常流量。
- 从 DDoS 攻击开始到 Shield Advanced 设置自动缓解规则的时间因每个事件而异。某些 DDoS 攻击可能会在部署缓解规则之前结束。其他攻击可能在缓解措施已经到位时发生，因此可能从事件一开始就得到缓解。
- 对于通过内容分发网络 (CDN) 接收任何流量的 Amazon CloudFront 应用负载均衡器，Shield Advanced 针对这些应用程序负载均衡器资源的应用层自动缓解功能将降低。Shield Advanced 使用客户端流量属性来识别攻击流量并将其与正常流量隔离到您的应用程序，CDN 可能不会保留或转发原始客户端流量属性。如果您使用 CloudFront，我们建议在 CloudFront 发行版上启用自动缓解功能。
- 自动应用层 DDoS 缓解不与保护组交互。您可以为保护组中的资源启用自动缓解功能，但是 Shield Advanced 不会根据保护组的发现自动应用攻击缓解措施。Shield Advanced 对单个资源应用自动攻击缓解措施。

目录

- [使用自动缓解的最佳实践 \(p. 355\)](#)
- [在启用自动缓解所需的配置 \(p. 355\)](#)
- [Shield Advanced 如何管理自动 \(p. 355\)](#)
 - [在启用自动缓解时在启用自动缓解时在启用自动 \(p. 355\)](#)
 - [Shield Advanced 如何通过自动缓解来响应 DDoS 攻击 \(p. 356\)](#)
 - [在对规则和操作设置时在更改规则时在更改规则时在更改规则时 \(p. 356\)](#)
 - [攻击平息后，Shield Advanced 如何管理缓解措施 \(p. 356\)](#)
 - [在禁用自动缓解时在禁用自动缓解时 \(p. 357\)](#)
- [Shield Advanced 规则组参考声明 \(p. 357\)](#)
- [管理自动应用层 DDoS 缓解 \(p. 357\)](#)
 - [查看资源的自动应用层 DDoS 缓解配置 \(p. 357\)](#)
 - [启用和禁用自动应用层 DDoS 缓解 \(p. 357\)](#)
 - [更改用于自动应用层 DDoS 缓解的操作 \(p. 358\)](#)

使用自动缓解的最佳实践

使用自动缓解时，请遵循此处提供的指南。

- 通过 Shield Advanced 管理所有自动缓解保护，或者如果您使用 Amazon Firewall Manager 管理 Shield Advanced 自动缓解设置，则通过 Firewall Manager 管理所有自动缓解保护。不要混用 Shield Advanced 和 Firewall Manager 来管理这些保护。
- 使用相同的 Web ACL 和保护设置管理相似的资源，使用不同的 Web ACL 管理不同的资源。当 Shield Advanced 缓解对受保护资源的 DDoS 攻击时，它会为与该资源关联的 Web ACL 定义规则，然后针对与 Web ACL 关联的所有资源的流量测试规则。只有在规则不会对任何相关资源产生负面影响的情况下，Shield Advanced 才会应用这些规则。有关更多信息，请参阅 [Shield Advanced 如何管理自动 \(p. 355\)](#)。
- 不要从您的 Web ACL 中删除名称以开头的任何规则组 ShieldMitigationRuleGroup。如果这样做，则会禁用 Shield Advanced 自动缓解为与 Web ACL 关联的所有资源提供的保护。此外，Shield Advanced 可能需要一些时间才能收到更改通知并更新其设置。在此期间，Shield Advanced 控制台页面将提供错误的信息。有关更多信息，请参阅 [Shield Advanced 规则组参考声明 \(p. 357\)](#)。
- 对于所有互联网流量都通过 Amazon CloudFront 分配进行代理的应用程序负载均衡器，只能对 CloudFront 分配启用自动缓解。该 CloudFront 分配将始终拥有最多的原始流量属性，Shield Advanced 利用这些属性来缓解攻击。

在启用自动缓解所需的配置

您可以启用 Shield Advanced 自动缓解作为资源应用层 DDoS 保护的一部分。有关通过控制台执行此操作的更多信息，请参阅 [配置应用层 DDoS 保护 \(p. 365\)](#)。

自动缓解功能要求您执行以下操作：

- 将 Web ACL 与资源关联 — 这是任何 Shield Advanced 应用层保护所必需的。您可以对多个资源使用相同的 Web ACL。我们建议仅对流量相似的资源执行此操作。有关 Web ACL 的信息，包括将其用于多个资源的要求，请参阅 [Amazon WAF 的工作原理 \(p. 6\)](#)。
- 启用和配置 Shield Advanced 自动应用层 DDoS 缓解 — 启用此功能后，您需要指定是希望 Shield Advanced 自动屏蔽还是计算其确定为 DDoS 攻击一部分的 Web 请求。Shield Advanced 向关联的 Web ACL 添加了一个规则组，并使用它来动态管理其对资源上的 DDoS 攻击的响应。有关规则操作设置的更多信息，请参阅 [Amazon WAF 规则操作 \(p. 81\)](#)。
- (可选，但推荐) 在 Web ACL 中添加基于速率的规则 — 基于速率的规则通过防止任何单个 IP 地址在短时间内发送过多请求，为您的资源提供抵御 DDoS 攻击的基本保护。有关基于速率的规则的信息，请参阅 [基于速率的规则语句 \(p. 95\)](#)。

Shield Advanced 如何管理自动

本节中的主题介绍了 Shield Advanced 如何处理您的自动应用层 DDoS 缓解配置更改，以及启用自动缓解后如何处理 DDoS 攻击。

主题

- [在启用自动缓解时在启用自动缓解时在启用自动 \(p. 355\)](#)
- [Shield Advanced 如何通过自动缓解来响应 DDoS 攻击 \(p. 356\)](#)
- [在对规则和操作设置时在更改规则时在更改规则时在更改规则时 \(p. 356\)](#)
- [攻击平息后，Shield Advanced 如何管理缓解措施 \(p. 356\)](#)
- [在禁用自动缓解时在禁用自动缓解时 \(p. 357\)](#)

在启用自动缓解时在启用自动缓解时在启用自动

当您启用自动缓解时，Shield Advanced 会执行以下操作：

- 根据需要添加一个规则组供 Shield Advanced 使用 — 如果您与该资源关联的 Amazon WAF Web ACL 还没有专门用于自动应用层 DDoS 缓解的 Amazon WAF 规则组参考声明，Shield Advanced 会添加一个规则组参考语句。规则组引用语句的名称以开头 ShieldMitigationRuleGroup。有关此规则组的更多详细信息，请参阅[Shield Advanced 规则组参考声明 \(p. 357\)](#)。
- 开始响应针对资源的 DDoS 攻击 — Shield Advanced 会自动响应受保护资源的 DDoS 攻击。Shield Advanced 使用 Amazon WAF 规则组部署用于缓解 DDoS 攻击的规则。Shield Advanced 会根据您的应用程序和应用程序遇到的攻击量身定制这些规则，并在部署之前根据资源的历史流量对其进行测试。以下各节提供了有关 Shield Advanced 如何做到这一点的更多信息。

Shield Advanced 在您用于自动缓解的任何 Web ACL 中使用单个规则组引用语句。如果你已经在使用 Web ACL 进行自动缓解，Shield Advanced 不会向其添加其他规则组。应用层 DDoS 的自动缓解取决于规则组的存在来缓解攻击。如果出于任何原因将规则组从 Amazon WAF Web ACL 中删除，则删除会禁用与该 Web ACL 关联的所有资源的自动缓解。

Shield Advanced 如何通过自动缓解来响应 DDoS 攻击

当 Shield Advanced 检测到对启用了自动缓解的受保护资源的攻击时，它会执行以下操作：

1. 尝试识别一种攻击特征，该特征将攻击流量与应用程序的正常流量隔离开来。目标是生成高质量的 DDoS 缓解规则，这些规则放置后仅影响攻击流量，不会影响应用程序的正常流量。
2. 根据受到攻击的资源以及与同一 Web ACL 关联的任何其他资源的历史流量模式评估已识别的攻击特征。Shield Advanced 会在部署任何规则来应对事件之前执行此操作。

根据评估结果，Shield Advanced 执行以下操作之一：

- 如果 Shield Advanced 确定攻击签名仅隔离涉及 DDoS 攻击的流量，则它将在 Amazon WAF Web ACL 的 Shield Advanced 缓解规则组下的规则中实现签名。Shield Advanced 为这些规则提供了你为资源自动缓解配置的操作设置，要 COUNT 还是 BLOCK。
- 否则，Shield Advanced 不会提供缓解措施。

在整个攻击过程中，Shield Advanced 会发送与基本 Shield Advanced 应用层保护相同的通知并提供相同的事件信息。您可以在 Shield Advanced 事件控制台中查看有关事件和 DDoS 攻击以及任何 Shield Advanced 攻击缓解措施的信息。有关信息，请参阅[对 DDoS 事件的可见性 \(p. 369\)](#)。

如果您已将自动缓解配置为使用 BLOCK 规则操作，并且遇到 Shield Advanced 部署的缓解规则出现误报，则可以将规则操作更改为 COUNT。有关如何执行此操作的信息，请参阅[更改用于自动应用层 DDoS 缓解的操作 \(p. 358\)](#)。

在对规则和操作设置时在更改规则时在更改规则时在更改规则时

当您更改受保护资源的自动缓解规则操作设置时，Shield Advanced 会更新该资源的所有规则设置。它更新托管规则组中当前存在的所有资源规则，并在创建新规则时使用新的操作设置。

在更改操作设置可能需要几秒钟进行传播。在此期间，您可能在使用规则组的某些地方看到旧设置，而在其他地方看到新设置。

您可以在控制台的事件页面中以及通过应用层配置页面更改自动缓解配置的规则操作设置。有关活动页面的信息，请参阅[响应 DDoS 事件 \(p. 380\)](#)。有关配置页面的更多信息，请参阅[配置应用层 DDoS 保护 \(p. 365\)](#)。

攻击平息后，Shield Advanced 如何管理缓解措施

当 Shield Advanced 确定不再需要为特定攻击部署的缓解规则时，它会将其从 Shield Advanced 缓解规则组中删除。

删除缓解规则不一定与攻击的结束相吻合。Shield Advanced 监控它在您的受保护资源上检测到的攻击模式。它可以通过保留其针对最初发生的攻击而部署的规则，主动防御具有特定签名的攻击再次发生。根据需

要，Shield Advanced 会延长其维持规则的时间窗口。这样，Shield Advanced 就可以在反复攻击影响您的受保护资源之前，使用特定的签名来缓解这些攻击。

在禁用自动缓解时在禁用自动缓解时

当您禁用资源的自动缓解时，Shield Advanced 会执行以下操作：

- 停止自动响应 DDoS 攻击 — Shield Advanced 停止对该资源的自动响应活动。
- 从 Shield Advanced 规则组中移除不需要的规则 — 如果 Shield Advanced 代表受保护资源维护其托管规则组中的任何规则，则会将其删除。
- 如果不再使用 Shield Advanced 规则组，则将其删除 — 如果您与该资源关联的 Web ACL 未与任何其他启用自动缓解的资源相关联，则 Shield Advanced 会将其规则组参考语句从 Web ACL 中删除。

Shield Advanced 规则组参考声明

Shield Advanced 使用您与资源关联的 Web ACL 中的规则组管理应用层 DDoS 自动缓解活动。

您的 Web ACL 中的 Shield Advanced 规则组参考语句具有以下属性：

- 名称 – `ShieldMitigationRuleGroup_account-id_web-acl-id_unique-identifier`
- Web ACL 容量单位 (WCU) — 150。这些 WCU 计入您的 Web ACL 中的 WCU 使用量。
- 优先级 — 1000000000000000,000 此高优先级设置让您有空间在 Web ACL 中运行其他规则和规则组，然后再运行 Shield Advanced 规则组。Amazon WAF 从最低数值优先级设置向上运行 Web ACL 中的规则，按优先级顺序运行 Web ACL 中的规则。

自动缓解功能不会消耗您账户中除 Web ACL 中的规则组 WCU 之外的任何额外 Amazon WAF 资源。例如，Shield Advanced 规则组不算作您账户的规则组之一。有关中的账户限制的信息 Amazon WAF，请参阅 [Amazon WAF 配额 \(p. 230\)](#)。

管理自动应用层 DDoS 缓解

使用本节中的指南来管理您的自动应用层 DDoS 缓解配置。有关自动缓解工作原理的信息，请参阅前面的主题。

主题

- [查看资源的自动应用层 DDoS 缓解配置 \(p. 357\)](#)
- [启用和禁用自动应用层 DDoS 缓解 \(p. 357\)](#)
- [更改用于自动应用层 DDoS 缓解的操作 \(p. 358\)](#)

查看资源的自动应用层 DDoS 缓解配置

您可以在受保护资源页面和各个保护页面中查看资源的自动应用层 DDoS 缓解配置。

查看应用层 DDoS 自动缓解配置

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF & Shield 控制台，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在 Amazon Shield 导航窗格中，选择受保护的资源。在受保护资源列表中，自动应用层 DDoS 缓解列表是否启用了自动缓解，以及 Shield Advanced 将在其缓解措施中使用的操作（如果启用）。

您也可以选择任何应用层资源，以查看资源保护页面上列出的相同信息。

启用和禁用自动应用层 DDoS 缓解

以下过程介绍如何启用或禁用受保护资源的自动响应。

为单个资源启用或禁用自动应用层 DDoS 缓解

1. 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 控制台，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在Amazon Shield导航窗格中，选择受保护的资源。
3. 在“保护”选项卡中，选择要为其启用自动缓解的应用层资源。资源的保护页面打开。
4. 在资源的保护页面中，选择编辑。
5. 在“为全球资源配置第 7 层 DDoS 缓解-可选”页面中，对于应用层 DDoS 自动缓解，选择要用于自动缓解的选项。控制台中的选项如下所示：
 - 保留当前设置-不更改受保护资源的自动缓解设置。
 - 启用-为受保护资源启用自动缓解。选择此选项时，还要选择要在 Web ACL 规则中使用自动缓解措施的规则操作。有关规则操作设置的更多信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。
 - 禁用-禁用受保护资源的自动缓解。
6. 浏览其余页面，直到完成并保存配置。

在“保护”页面中，资源的自动缓解设置已更新。

更改用于自动应用层 DDoS 缓解的操作

您可以在控制台的多个位置更改 Shield Advanced 用于其应用层自动响应的操作：

- 自动缓解配置-在为资源配置自动缓解时更改操作。有关程序，请参阅上部分中的[启用和禁用自动应用层 DDoS 缓解 \(p. 357\)](#)。
- 事件详细信息页面-在控制台中查看事件信息时，更改事件详细信息页面中的操作。有关信息，请参阅[Amazon Shield Advanced事件详细信息 \(p. 375\)](#)。

使用运行状况检查配置基于健康的检测

您可以将 Shield Advanced 配置为使用基于健康的检测来提高攻击检测和缓解的响应能力和准确性。您可以将此选项用于除了 Route 53 托管区域之外的任何资源类型。

要配置基于运行状况的检测，您需要在 Route 53 中为资源定义运行状况检查，验证其报告是否正常，然后将其与 Shield Advanced 保护相关联。有关 Route 53 运行状况检查的信息，请参阅[Amazon Route 53 开发者指南中的 Amazon Route 53 如何检查您的资源的运行状况以及创建、更新和删除运行状况检查](#)。

Note

Shield 响应小组 (SRT) 主动参与支持需要进行Health 检查。有关主动参与的信息，请参阅[配置主动参与操作 \(p. 350\)](#)。

运行Health 检查将根据您定义的要求来衡量资源的运行状况。运行状况检查状态为 Shield Advanced 检测机制提供输入，这使它们对特定应用程序的当前状态具有更高的敏感度。

您可以为除 Route 53 托管区域之外的任何资源类型启用基于健康状况的检测。

- 网络和传输层（第 3 层/第 4 层）资源 — 基于Health 的检测提高了网络负载均衡器、弹性 IP 地址和全球加速器的网络层和传送层事件检测和缓解的准确性。当您使用 Shield Advanced 保护这些资源类型时，Shield Advanced 可以为较小的攻击提供缓解措施，并更快地缓解攻击，即使流量在应用程序的容量范围内。

当您添加基于健康状况的检测时，在相关的健康检查不健康期间，Shield Advanced 可以更快地在更低的阈值下采取缓解措施。

- 应用层（第 7 层）资源 — 基于 Health 的检测提高了 CloudFront 分布层和应用程序负载均衡器的 Web 请求洪水检测的准确性。当您使用 Shield Advanced 保护这些资源类型时，根据请求特征，当流量出现统计学上的显著偏差以及流量模式的显著变化时，您会收到 Web 请求洪水检测警报。

通过基于健康的检测，当相关的 Route 53 运行状况检查不健康时，Shield Advanced 需要较小的偏差才能发出警报，并且可以更快地报告事件。相反，当相关的 Route 53 健康检查处于健康状态时，Shield Advanced 需要更大的偏差才能发出警报。

目录

- [在 Shield Advanced 中使用 \(p. 359\)](#)
- [常用于检查的指标 \(p. 360\)](#)
 - [用于监控应用程序运行状况 \(p. 360\)](#)
 - [每种资源类型的亚马逊 CloudWatch 指标 \(p. 361\)](#)
- [管理管理可选 \(p. 361\)](#)
 - [将运行状况检查与您的资源相关联 \(p. 362\)](#)
 - [取消运行状况检查与您的资源的关联 \(p. 362\)](#)
 - [运行状况检查关联状态 \(p. 363\)](#)
- [Health 检查示例 \(p. 363\)](#)
 - [亚马逊 CloudFront 分发 \(p. 364\)](#)
 - [负载均衡器 \(p. 364\)](#)
 - [Amazon EC2 弹性 IP 地址 \(EIP\) \(p. 364\)](#)

在 Shield Advanced 中使用

使用 Shield Advanced 创建和使用健康检查时，请遵循本节中的最佳做法。

- 通过确定要监控的基础架构组件来规划运行状况检查。考虑使用以下资源类型进行运行状况检查：
 - 关键资源。
 - 任何你想在 Shield Advanced 检测和缓解中获得更高灵敏度的资源。
 - 你希望 Shield Advanced 主动联系你的资源。主动参与取决于您的运行状况检查状态。

您可能需要监控的资源示例包括 Amazon CloudFront 分配、面向互联网的负载均衡器和 Amazon EC2 实例。

- 定义运行状况检查，以尽可能少的通知准确反映应用程序来源的运行状况。
 - 编写运行状况检查，这样只有当您的应用程序不可用或运行不在可接受的参数范围内时，这些检查才不正常。您负责根据应用程序的特定要求定义和维护运行状况检查。
 - 尽可能少地进行运行状况检查，同时仍能准确报告应用程序的运行状况。例如，来自应用程序多个区域的多个警报都报告了相同的问题，这可能会在不增加信息价值的情况下增加响应活动的开销。
 - 使用计算得出的运行状况检查，使用亚马逊 CloudWatch 指标的组合来监控应用程序的运行状况。例如，您可以根据应用程序服务器的延迟和其 5xx 错误率计算综合运行状况，这表明源服务器没有满足请求。
 - 根据需要创建自己的应用程序运行状况指标并将其发布到 CloudWatch 自定义指标，并在计算出的运行状况检查中使用它们。
- 实施和管理您的健康检查，以改善检测并减少不必要的维护活动。
 - 在将健康检查与 Shield Advanced 保护关联之前，请确保其处于健康状态。关联报告不健康状况的运行状况检查可能会使受保护资源的 Shield Advanced 检测机制出现偏差。
 - 保持你的健康检查可供 Shield Advanced 使用。不要删除 Route 53 中用于 Shield 高级保护的生命值检查。
 - 仅使用暂存和测试环境来测试您的运行状况检查。仅维护需要生产级性能和可用性的环境的运行状况检查关联。不要在 Shield Advanced 中保持暂存和测试环境的运行状况检查关联。

常用于检查的指标

本部分列出了在运行状况检查中常用的 Amazon CloudWatch 指标，用于在分布式拒绝服务 (DDoS) 事件期间衡量应用程序运行状况。有关每种资源类型 CloudWatch 指标的完整信息，请参阅表后的列表。

主题

- [用于监控应用程序运行状况 \(p. 360\)](#)
- [每种资源类型的亚马逊 CloudWatch 指标 \(p. 361\)](#)

用于监控应用程序运行状况

资源	指标	描述
Route 53	HealthCheckStatus	运行状况检查终端节点的状态。
CloudFront	5xxErrorRate	HTTP 状态代码为 5xx 的所有请求所占的百分比。这表示攻击正在影响应用程序。
Application Load Balancer	ActiveConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标的并发活动 TCP 连接的并发活动 TCP 连接数量。
Application Load Balancer	ConsumedLCUs	负载均衡器使用的负载均衡器容量单位 (LCU) 数量。
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	负载均衡器生成的 HTTP 4xx 或 5xx 客户端错误代码的 HTTP 4xx 或 5xx 客户端错误代码的数量。
Application Load Balancer	NewConnectionCount	从客户端到负载均衡器以及从负载均衡器到目标到目标建立的新 TCP 连接的新 TCP 连接数量。
Application Load Balancer	ProcessedBytes	负载均衡器处理的字节数。
Application Load Balancer	RejectedConnectionCount	由于负载均衡器达到连接数上限被拒绝的连接数。
Application Load Balancer	TargetConnectionErrorCount	负载均衡器和目标之间连接连接建立不成功的次数。
Application Load Balancer	TargetResponseTime	请求离开负载均衡器到来自目标的响应所用的时间（以秒为单位）。
Application Load Balancer	UnHealthyHostCount	被视为未正常运行的目标数量。
Network Load Balancer	ActiveFlowCount	从客户端到目标的并发 TCP 连接数量。
Network Load Balancer	ConsumedLCUs	负载均衡器使用的负载均衡器容量单位 (LCU) 数量。
Network Load Balancer	NewFlowCount	从客户端到目标建立的新 TCP 连接数量。

资源	指标	描述
Network Load Balancer	PeakPacketsPerSecond	最高平均数据包速率（每秒处理的数据包数），在采样窗口期间每 10 秒计算一次。此指标包含运行状况检查流量。
Network Load Balancer	ProcessedBytes	负载均衡器处理的字节数，包括 TCP/IP 标头。
Global Accelerator	NewFlowCount	从客户端到目标建立的新 TCP 连接数量。
Global Accelerator	ProcessedBytesIn	加速器处理的传入字节数，包括 TCP/IP 标头。
Amazon EC2	CPUUtilization	当前正在使用的已分配 EC2 计算单位的百分率。
Amazon EC2	NetworkIn	实例在所有网络接口上收到的字节数。
Amazon EC2 Auto Scaling	GroupMaxSize	自动扩缩组的最大大小。

每种资源类型的亚马逊 CloudWatch 指标

有关适用于您的受保护资源的指标的更多信息，请参阅资源指南中的以下部分：

- Amazon Route 53 — [通过Amazon Route 53 状况检查和Amazon Route 53 开发人员指南 CloudWatch中的Amazon Route](#)
- 亚马逊 CloudFront — 《[亚马逊 CloudFront 开发者指南](#)》CloudWatch中的“[CloudFront 使用亚马逊进行监控](#)”。
- Application Load Balancer — [适用于 Application Load Balancer 的用户指南中的应用程序负载均衡器 CloudWatch 指标](#)。
- Network Load Balancer — [Network Load Balancer 用户指南中的网络负载均衡器 CloudWatch 指标](#)。
- Amazon Global Accelerator — Amazon Global Accelerator 在《Amazon Global Accelerator 开发者指南》中[使用亚马逊 CloudWatch](#)。
- 亚马逊 Elastic Compute Cloud — 在 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/> 中[列出您的实例的可用 CloudWatch 指标](#)。
- Amazon EC2 Auto Scaling — [Auto Scaling 用户指南中的监控 Auto Scaling 组和实例的 CloudWatch 指标](#)。

管理管理可选

如果运行状况检查仅在应用程序在可接受的参数内运行时报告运行状况良好，而只有在不在可接受的参数内运行时才报告不正常，那么使用Shield Advanced的运行状况检查将使你受益最大。使用本节中的指南在Shield Advanced 中管理您的健康检查关联。

Note

Shield Advanced 无法自动管理你的健康检查。

使用 Shield Advanced 进行健康检查需要满足以下条件：

- 当你将健康检查与 Shield Advanced 防护关联时，它必须报告健康状况良好。

- 运行状况检查必须与您的受保护资源的运行状况相关。您负责定义和维护运行状况检查，根据应用程序的特定要求准确报告应用程序的运行状况。
- 生命值检查必须保持可供Shield 高级保护使用。不要删除 Route 53 中用于Shield 高级保护的生命值检查。

主题

- [将运行状况检查与您的资源相关联 \(p. 362\)](#)
- [取消运行状况检查与您的资源的关联 \(p. 362\)](#)
- [运行状况检查关联状态 \(p. 363\)](#)

将运行状况检查与您的资源相关联

以下过程显示如何将 Amazon Route 53 运行状况检查与受保护的资源相关联。

Note

在将健康检查与 Shield Advanced 保护关联之前，请确保其处于健康状态。有关信息，请参阅 Amazon Route 53 开发人员指南中的[监控运行状况检查状态和获取通知](#)。

关联可选

1. 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在Amazon Shield导航窗格中，选择受保护的资源。
3. 在“保护”选项卡上，选择要与运行状况检查关联的资源。
4. 选择“配置保护”。
5. 选择“下一步”，直到进入“配置基于运行状况检查的 DDoS 检测-可选”页面。
6. 在 Associated Health Check (关联运行状况检查) 下，选择要与保护关联的运行状况检查的 ID。

Note

如果您没有看到所需的运行状况检查，请前往 Route 53 控制台验证运行状况检查及其 ID。有关信息，请参阅[创建和更新运行状况检查](#)。

7. 浏览其余页面，直到完成配置。在“保护”页面上，列出了您更新的资源运行状况检查关联。
8. 在“保护”页面上，检查您新关联的运行状况检查报告是否正常。

当健康检查报告不健康时，你无法在 Shield Advanced 中成功开始使用健康检查。这样做会导致 Shield Advanced 在非常低的阈值下检测到误报，还可能对Shield 响应小组 (SRT) 主动参与资源的能力产生负面影响。

如果新关联的运行状况检查报告不正常，请执行以下操作：

- a. 在 Shield Advanced 中，解除生命值检查与保护的关联。
- b. 在 Amazon Route 53 中重新查看您的运行状况检查规范，验证您的整体应用程序性能和可用性。
- c. 当您的应用程序在正常运行的参数范围内运行，并且运行状况检查报告运行状况正常时，请再次尝试在 Shield Advanced 中关联运行状况检查。

当你建立了新的健康检查关联并且它在 Shield Advanced 中报告运行状况正常时，健康检查关联程序即告完成。

取消运行状况检查与您的资源的关联

以下过程显示如何解除 Amazon Route 53 运行状况检查与受保护资源的关联。

取消关联可选

1. 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在Amazon Shield导航窗格中，选择受保护的资源。
3. 在“保护”选项卡上，选择要与运行状况检查取消关联的资源。
4. 选择“配置保护”。
5. 选择“下一步”，直到进入“配置基于运行状况检查的 DDoS 检测-可选”页面。
6. 在“关联Health 检查”下，选择空白选项，列为 -。
7. 浏览其余页面，直到完成配置。

在“保护”页面上，您的资源的运行状况检查字段设置为 -，表示没有运行状况检查关联。

运行状况检查关联状态

您可以在Amazon WAF & Shield 控制台的受保护资源页面和每个资源的详细信息页面上查看与保护相关的运行状况检查的状态。

- 正@@ 常 — 运行状况检查可用，并且报告运行状况良好。
- 不正@@ 常-运行状况检查可用且报告不正常。
- 不可用 — Shield Advanced 无法使用健康检查。

解决不可用运行状况检查

创建和使用新的健康检查。当健康检查在 Shield Advanced 中处于不可用状态后，不要再次尝试关联该检查。

有关按照执行这些步骤的详细指导，请参阅前面的主题。

1. 在 Shield Advanced 中，取消生命值检查与资源的关联。
2. 在 Route 53 中，为资源创建新的运行状况检查并记下其 ID。有关信息，请参阅 Amazon Route 53 [开发人员指南中的创建和更新](#)可选。
3. 在 Shield Advanced 中，将新的可选、与资源关联。

Health 检查示例

本部分显示了可以在计算后的运行状况检查中使用的运行状况检查的示例。计算出的运行状况检查使用多项单独的运行状况检查来确定综合状态。每项运行状况检查的状态都基于终端节点的运行状况或亚马逊 CloudWatch 指标的状态。您可以将运行状况检查合并为计算出的运行状况检查，然后将计算出的运行状况检查配置为根据单个运行状况检查的综合健康状态报告运行状况。根据您的应用程序性能和可用性的要求调整计算出的运行状况检查的灵敏度。

有关计算运行状况检查的信息，请参阅 Amazon Route 53 开发者指南中的[监控其他运行状况检查（计算出的运行状况检查）](#)。有关更多信息，请参阅博客文章 [Route 53 的改进 — 计算后的运行Health 检查和延迟检查](#)。

主题

- [亚马逊 CloudFront 分发 \(p. 364\)](#)
- [负载均衡器 \(p. 364\)](#)
- [Amazon EC2 弹性 IP 地址 \(EIP\) \(p. 364\)](#)

亚马逊 CloudFront 分发

以下示例描述了运行状况检查，这些检查可以合并为 CloudFront 分配的计算运行状况检查：

- 通过为发行版中提供动态内容的路径指定域名来监控端点。健康的响应将包括 HTTP 响应代码 2xx 和 3xx。
- 监控用于测量 CloudFront 来源健康状况的 CloudWatch 警报的状态。例如，您可以维护 Application Load Balancer 指标 TargetResponseTime 的 CloudWatch 警报，并创建反映警报状态的运行状况检查。当请求离开负载均衡器与负载均衡器收到来自目标的响应之间的响应时间超过警报中配置的阈值时，运行状况检查可能不正常。
- 监控警报的状态，该 CloudWatch 警报用于衡量响应的 HTTP 状态代码为 5xx 的请求所占的百分比。如果 CloudFront 分配的 5xx 错误率高于 CloudWatch 警报中定义的阈值，则此运行状况检查的状态将切换为不正常。

负载均衡器

以下示例描述了运行状况检查，这些检查可用于 Application Load Balancer、Network Load Balancer 或全球加速器标准加速器的计算运行状况检查。

- 监控警报的状态，该 CloudWatch 警报用于衡量客户端与负载均衡器建立的新连接的数量。您可以将平均新连接数的警报阈值设置为比每天的平均值高出一定程度。每种资源类型的指标如下：
 - Application Load Balancer : NewConnectionCount
 - Network Load Balancer : ActiveFlowCount
 - 全球加速器 : NewFlowCount
- 对于 Application Load Balancer Network Load Balancer，监控 CloudWatch 警报的状态，该警报用于衡量被视为正常的负载均衡器的数量。您可以在可用区或负载均衡器所需的最小正常主机数量上设置警报阈值。负载均衡器资源的可用指标如下：
 - Application Load Balancer : HealthyHostCount
 - Network Load Balancer : HealthyHostCount
- 对于 Application Load Balancer，监控 CloudWatch 警报的状态，该警报用于测量负载均衡器目标生成的 HTTP 5xx 响应代码的数量。对于 Application Load Balancer，您可以使用该指标，HTTPCode_Target_5XX_Count 并根据负载均衡器的所有 5xx 错误之和来确定警报阈值。

Amazon EC2 弹性 IP 地址 (EIP)

以下示例运行状况检查可以合并为 Amazon EC2 弹性 IP 地址的计算运行状况检查：

- 通过为弹性 IP 地址指定 IP 地址，监控端点。只要可以与 IP 地址后面的资源建立 TCP 连接，运行状况检查就会保持正常。
- 监控可选 Amazon CloudWatch EC2 计算单位中当前正在实例上使用的已分配 Amazon EC2 计算单位的百分率。您可以使用 Amazon EC2 指标，CPUUtilization 并根据您认为应用程序的高 CPU 利用率（例如 90%）来设定警报阈值。

管理中的资源保护 Amazon Shield Advanced

使用本节中的指南来管理对您的资源的 Shield Advanced 保护。

Note

Shield Advanced 仅保护您在 Shield Advanced 中或通过 Amazon Firewall Manager Shield 高级策略指定的资源。它不会自动保护您的资源。

如果您使用的是Amazon Firewall Manager Shield Advanced 策略，则无需管理该策略范围内资源的保护。Firewall Manager 根据策略配置自动管理策略范围内的帐户和资源的保护。有关更多信息，请参阅[Amazon Shield Advanced 策略 \(p. 449\)](#)：

主题

- [向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)
- [配置Amazon Shield Advanced保护 \(p. 365\)](#)
- [从 Amazon 资源中删除 Amazon Shield Advanced 保护 \(p. 367\)](#)

向 Amazon 资源添加 Amazon Shield Advanced 保护

按照本节中的指导为一个或多个资源添加 Shield Advanced 保护。

为 Amazon 资源添加防护

1. 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在导航窗格中，在导航窗格中Amazon Shield选择 Sches。
3. 选择“添加要保护的资源”。
4. 在“使用 Shield Advanced 选择要保护的资源”页面的“指定区域和资源类型”中，提供要保护的资源的区域和资源类型规范。您可以通过选择“所有区域”来保护多个区域中的资源，也可以通过选择“全球”将选择范围缩小到全局资源。您可以取消选择任何不想保护的资源类型。有关保护您的资源类型的信息，请参阅[Amazon Shield Advanced按资源类型划分的保护 \(p. 352\)](#)。
5. 选择加载资源。Shield Advanced 会使用符合您的标准的Amazon资源填充选择资源部分。
6. 在选择资源部分中，您可以通过在资源列表中输入要搜索的字符串来筛选资源列表。

选择要保护资源。

7. 在“标签”部分中，如果您想向正在创建的 Shield Advanced 保护添加标签，请指定这些标签。有关为 Amazon资源添加标签的信息，请参阅[使用标签编辑器](#)。
8. 选择“使用Shield 高级保护”。这为资源增加了Shield 高级保护。

配置Amazon Shield Advanced保护

您可以随时更改 Amazon Shield Advanced 保护的设置。为此，请浏览所选保护的选项并修改需要更改的设置。

管理受保护资源

1. 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在Amazon Shield导航窗格中，选择受保护的资源。
3. 在 Security”，选择要保护的资源。
4. 选择所需的配置保护和资源规格选项。
5. 浏览每个资源保护选项，根据需要进行更改。

配置应用层 DDoS 保护

为了防止 Amazon CloudFront 和Application Load Balancer 资源受到攻击，您可以添加Amazon WAF Web ACL 并添加基于速率的规则。有关此问题的信息，请参阅[Shield 高级应用层Amazon WAF Web ACL 和基于速率的规则 \(p. 353\)](#)。

您还可以启用 Shield Advanced 自动应用层 DDoS 缓解功能。有关 Amazon WAF 工作方式的信息，请参阅[Amazon WAF \(p. 5\)](#)。有关自动缓解功能的信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

Important

如果您通过 Amazon Firewall Manager 使用 Shield Advanced 策略来管理您的 Shield Advanced 保护，则无法在此处管理应用层保护。对于所有其他资源，我们建议您至少为每个资源附加 Web ACL，即使 Web ACL 不包含任何规则。

Note

当您为资源启用自动应用层 DDoS 缓解时，如果需要，该操作会自动向您的账户添加服务相关角色，以授予 Shield Advanced 管理您的 Web ACL 保护所需的权限。有关信息，请参阅[使用 Shield Advanced 的服务 \(p. 398\)](#) the section called “使用服务相关角色” (p. 398)。

配置应用层 DDoS 保护

1. 在配置第 7 层 DDoS 保护页面中，如果资源尚未与 Web ACL 关联，则可以选择现有的 Web ACL 或创建自己的 Web ACL。

要创建 Web ACL，请执行以下操作：

- a. 选择 Create web ACL (创建 Web ACL)。
- b. 输入名称。Web ACL 在创建之后无法更改名称。
- c. 选择 Create (创建)。

Note

如果资源已与一个 Web ACL 关联，则不能更改为其他 Web ACL。如果要更改 Web ACL，您必须先删除资源中删除关联的 Web ACL。有关更多信息，请参阅[将 Web ACL 与 Amazon 资源关联或取消关联 \(p. 22\)](#)：

2. 如果 Web ACL 未定义基于速率的规则，则可以通过选择添加速率限制规则然后执行以下步骤来添加一个规则：
 - a. 输入名称。
 - b. 输入速率限制。这是在将基于速率的规则操作应用于 IP 地址之前，任何五分钟内允许来自任何单个 IP 地址的最大请求数。当来自 IP 地址的请求低于限制时，操作将停止。
 - c. 将规则操作设置为在请求数超过限制时对来自 IP 地址的请求进行计数或屏蔽。应用和删除规则操作可能会在 IP 地址请求速率更改一两分钟后生效。
 - d. 选择 Add rule。
3. 要自动缓解应用层 DDoS 攻击，请选择是否希望 Shield Advanced 代表您自动缓解 DDoS 攻击，如下所示：
 - 要启用自动缓解，请选择“启用”，然后选择您希望 Shield Advanced 在其自定义规则中使用的规则操作。Amazon WAF 您的选择是 Count 和 Block。有关这些操作的信息，请参阅[Amazon WAF 规则操作 \(p. 81\)](#)。
 - 要禁用自动缓解，请选择“禁用”。
 - 要保持您正在管理的资源的自动缓解设置不变，请保留默认选择“保留当前设置”。

有关 Shield Advanced 自动应用层 DDoS 缓解的信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

4. 选择 Next (下一步)。

创建警报和通知

以下过程展示如何管理受保护资源的 CloudWatch 警报。

Note

CloudWatch 会产生额外费用。有关 CloudWatch 定价，请参阅[亚马逊 CloudWatch 定价](#)。

创建警报和通知

1. 在保护页面创建警报和通知（可选）中，为要接收的警报和通知配置 SNS 主题。对于不想接收通知的资源，请选择 No topic（无主题）。您可以添加 Amazon SNS 主题或创建新主题。
2. 要创建 Amazon SNS 主题，请执行下列步骤：
 - a. 在下拉列表中，选择创建 SNS 主题。
 - b. 输入主题名称。
 - c. （可选）输入 Amazon SNS 消息要发送到的电子邮件地址，然后选择添加电子邮件。您可以输入多个。
 - d. 选择 Create（创建）。
3. 选择 Next（下一步）。

从 Amazon 资源中删除 Amazon Shield Advanced 保护

您可以随时从您的任何 Amazon 资源中删除 Amazon Shield Advanced 保护。

Important

删除 Amazon 资源不会从 Amazon Shield Advanced 中删除资源。您还必须从 Amazon Shield Advanced 中删除对资源的保护，如该过程所述。

从 Amazon 资源中删除 Amazon Shield Advanced 保护

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF & Shield 主机，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在 Amazon Shield 导航窗格中，选择受保护的资源。
3. 在“保护”选项卡中，选择要删除其保护的资源。
4. 选择“删除保护”。
 - 如果您将 Amazon CloudWatch 警报配置为保护，则可以选择删除警报和保护。如果您选择此时不删除警报，则可以稍后使用 CloudWatch 控制台将其删除。

Note

对于配置了 Amazon Route 53 运行状况检查的保护，如果您稍后再次添加保护，则保护仍包括运行状况检查。

前面的步骤取消了对特定 Amazon 资源的 Amazon Shield Advanced 保护。但不会取消您的 Amazon Shield Advanced 订阅。您将继续为该服务付费。有关您的 Amazon Shield Advanced 订阅的信息，请联系[Amazon Web Services Support 中心](#)。

从 Shield 高级保护中移除 CloudWatch 警报

要从 Sched CloudWatch uleShield ecurity”，请执行下列操作之一：

- 删除保护，如[从 Amazon 资源中删除 Amazon Shield Advanced 保护 \(p. 367\)](#)中所述。确保选中 Also delete related DDoSDetection alarm（同时删除相关的 DDoSDetection 警报）旁边的复选框。

- 使用 CloudWatch 控制台删除警报。要删除的警报名称以 DDoS 开头 DetectedAlarmForProtection。

Amazon Shield Advanced 保护

使用保护组创建受保护资源的逻辑集合，并将其保护作为一个组进行管理。有关管理资源保护，请参阅[配置 Amazon Shield Advanced 保护 \(p. 365\)](#)。

Note

自动应用层 DDoS 缓解功能不会与保护组交互。您可以为保护组中的资源启用自动缓解功能，但是 Shield Advanced 不会根据保护组的发现自动应用攻击缓解措施。Shield Advanced 会对单个资源应用自动攻击缓解措施。

Amazon Shield Advanced 保护组为您提供了一种自助服务方式，通过将多个受保护资源视为一个单元，自定义检测和缓解范围。资源分组可以带来许多好处。

- 提高检测精度。
- 减少不可操作的事件通知。
- 扩大缓解措施的覆盖范围，将事件期间也可能受到影响的受保护资源包括在内。
- 加快缓解具有多个相似目标的攻击的时间。
- 促进对新创建的受保护资源的自动保护。

在蓝/绿交换等情况下，保护组可以帮助减少误报，在这种情况下，资源在接近零负载和满载之间交替出现。另一个例子是，您经常创建和删除资源，同时保持群组成员共享的负载级别。对于此类情况，监控单个资源可能会导致误报，而监控资源组的运行状况则不会。

您可以将保护组配置为包括所有受保护资源、特定资源类型的所有资源或单独指定的资源。满足保护组条件的新受保护资源将自动包含在您的保护组中。受保护 RESS 可归属于多个保护。

管理 Amazon Shield Advanced 保护

使用本部分中的指导管理保护 Groupments (保护) 配置。

创建 Shield 高级保护组

创建保护组

1. 登录 Amazon Web Services Management Console 然后打开 Amazon WAF & Shield 控制台位于 <https://console.aws.amazon.com/wafv2/>。
2. 在里面 Amazon Shield 导航窗格中，选择保护。
3. 选择保护选项卡，然后选择创建保护。
4. 在里面创建保护页面上，为群组提供名称。您将使用此名称来标识受保护资源列表中的群组。在创建保护组后，您无法更改其名称。
5. 对于保护 SUP 标准，选择您希望 Shield Advanced 用来识别要包含在群组中的受保护资源的标准。根据您的选择的标准进行其他选择。
6. 对于聚合，选择您希望 Shield Advanced 如何合并群组的资源数据以检测、缓解和报告事件。
 - 总计— 使用整个群组的总流量。对于大多数情况，这是一个很好的选择。示例包括手动或自动扩展的 Amazon EC2 实例的弹性 IP 地址。
 - Mean— 使用整个群组的平均流量。对于统一共享流量的资源来说，这是一个很好的选择。示例包括加速器和负载均衡器。
 - 马克斯— 使用每种资源的最大流量。这对于不共享流量的资源以及以非统一方式共享流量的资源，非常有用。示例包括亚马逊 CloudFront 的分布和原始资源 CloudFront 分配。
7. 选择 Save (保存) 保存您的保护组并返回保护页面。

在里面Shield 事件页面上，您可以查看保护组的事件并深入查看该组中受保护资源的其他信息。

更新Shield 高级保护组

更新保护

1. 登录Amazon Web Services Management Console然后打开Amazon WAF& Shield 控制台位于<https://console.aws.amazon.com/wafv2/>.
2. 在里面Amazon Shield导航窗格中，选择保护.
3. 在里面保护选项卡上，选中您要修改的保护 Groups 旁边的复选框。
4. 在保护组的页面中，选择编辑. 对保护组设置进行更改。
5. 选择 Save (保存) 以保存您的更改。

删除 Shield 高级保护组

删除保护组

1. 登录Amazon Web Services Management Console然后打开Amazon WAF& Shield 控制台位于<https://console.aws.amazon.com/wafv2/>.
2. 在里面Amazon Shield导航窗格中，选择保护.
3. 在里面保护选项卡上，选中您要删除的保护 Groups 旁边的复选框。
4. 在保护组的页面中，选择Delete然后确认操作。

跟踪中的资源保护变化Amazon Config

您可以使用 Amazon Config 记录资源的 Amazon Shield Advanced 保护更改。然后，您可以使用此信息来维护配置更改历史记录以进行审核和故障排除。

要记录保护更改，请为要跟踪的每个资源启用 Amazon Config。有关更多信息，请参阅 Amazon Config 开发人员指南中的 [Amazon Config 入门](#)

您必须启用Amazon Config每个Amazon Web Services 区域其中包含跟踪的资源。你可以启用 Amazon Config手动，或者你可以使用Amazon CloudFormation模板“启用Amazon Config”在[Amazon CloudFormation StackSets 示例模板](#)中的Amazon CloudFormation用户指南。

如果您启用 Amazon Config，则需付费，如 [Amazon Config 定价](#)页面上详述。

Note

如果您已为必要的区域和资源启用 Amazon Config，则无需执行任何操作。有关对资源所做的保护更改的 Amazon Config 日志会自动填充。

启用后Amazon Config中使用美国东部（弗吉尼亚北部）区域Amazon Config控制台查看的配置更改历史记录Amazon Shield Advanced全球资源。

查看更改历史记录Amazon Shield Advanced区域资源通过Amazon Config控制台位于美国东部（弗吉尼亚北部）、美国东部（俄亥俄）、美国西部（俄勒冈）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、欧洲（爱尔兰）、欧洲（法兰克福）、亚太区域（东京）和亚太区域（悉尼）。

对 DDoS 事件的可见性

Amazon Shield提供对以下类别的事件和事件活动的可见性：

- 全球 — 所有客户都可以访问过去两周全球威胁活动的汇总视图。您可以在Amazon Shield控制台的“入门”和“全球威胁”仪表板页面下看到此信息。有关更多信息，请参阅[Amazon Shield全球和账户活动 \(p. 370\)](#)。
- 账户 — 所有客户都可以访问其账户上一年的活动摘要。您可以在Amazon Shield控制台的“入门”页面下看到此信息。有关更多信息，请参阅[Amazon Shield全球和账户活动 \(p. 370\)](#)。

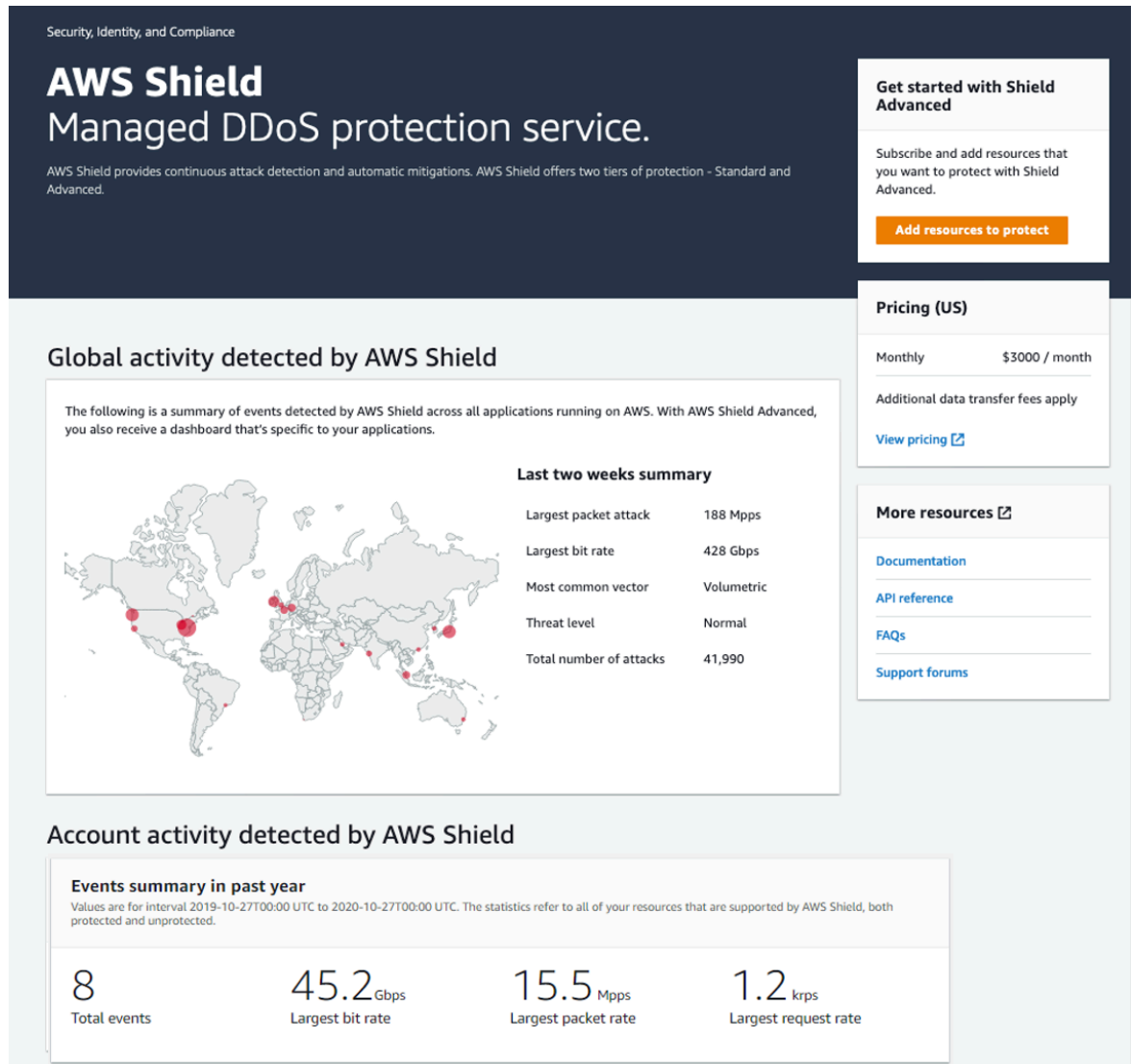
订阅 Shield Advanced 并为资源添加保护后，您可以访问有关受保护资源的事件和 DDoS 攻击的更多信息：

- 受保护资源上的事件 — Shield Advanced 通过Amazon Shield控制台的事件页面提供每个事件的详细信息。有关更多信息，请参阅[Amazon Shield Advanced 事件 \(p. 373\)](#)。
- 受保护资源的事件指标 — Shield Advanced 发布了其保护的所有资源的亚马逊 CloudWatch 指标，您可以使用这些指标来配置 CloudWatch 仪表板和警报。有关更多信息，请参阅[Amazon Shield Advanced亚马逊 CloudWatch 指标 \(p. 377\)](#)。
- 受保护资源的跨账户事件可见性 — 如果您使用Amazon Firewall Manager来管理 Shield Advanced 保护，则可以将 Firewall Manager 与之结合使用，从而实现对多个账户的保护的可见性Amazon Security Hub。有关更多信息，请参阅[事件跨账户可见性 \(p. 378\)](#)。

Amazon Shield全球和账户活动

您可以在控制台“入门”和“全球威胁Amazon Shield控制面板”页面中访问全球威胁活动的汇总视图和每个账户的事件摘要。

以下屏幕截图显示了示例入门页面的。



访问控制Amazon Shield台

- 登录Amazon Web Services Management Console并打开Amazon WAF & Shield 控制台，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。

您无需订阅 Shield Advanced 即可访问全球活动和账户事件摘要信息。

全局活动

此信息可通过Amazon Shield控制台“全球威胁”仪表板和“入门”页面获得。以下屏幕截图显示全局活动窗格的。

Global activity detected by AWS Shield

The following is a summary of events detected by AWS Shield across all applications running on AWS. With AWS Shield Advanced, you also receive a dashboard that's specific to your applications.



全球活动描述了在所有Amazon客户中观察到的 DDoS 事件。每小时Amazon更新一次，更新前两周的信息。在控制台窗格中，您可以看到按Amazon地区分区并显示在世界热图上的结果。在地图旁边，Shield 显示摘要信息，例如最大的数据包攻击、最大比特率、最常见的向量、攻击总数和威胁级别。威胁级别是对当前全球活动与Amazon通常观察到的活动进行比较的评估。默认威胁等级值为“正常”。Amazon当 DDoS 活动增加时，会自动将该值更新为“高”。

全球威胁仪表板还提供时间序列指标，使您能够在持续时间之间进行更改。要查看重大 DDoS 攻击的历史记录，您可以自定义控制面板以查看从最后一天到最近两周的视图。时间序列指标提供了在您选择的时间窗口内运行的应用程序检测到的所有事件的最大比特率、数据包速率或请求速率的视图。Amazon ShieldAmazon

账户活动

此信息可在Amazon Shield控制台的“入门”页面中找到。

以下屏幕截图显示了示例账户活动窗格。

Account activity detected by AWS Shield

Events summary in past year

Values are for interval 2019-10-27T00:00 UTC to 2020-10-27T00:00 UTC. The statistics refer to all of your resources that are supported by AWS Shield, both protected and unprotected.

8	45.2 Gbps	15.5 Mpps	1.2 krps
Total events	Largest bit rate	Largest packet rate	Largest request rate

账户活动描述了 Shield 在您的资源中检测到的 DDoS 事件，这些资源符合 Shield Advanced 的保护条件。每天，Shield 都会为截至前一天 00:00 UTC 的年度创建汇总指标，然后显示事件总数、最大比特率、最大数据包速率和最大请求速率。

- 每次Shield在发往您的应用程序的流量中观察到可疑属性时，事件总数指标都会反映出来。可疑属性可能包括流量高于正常流量、与应用程序历史配置文件不匹配的流量，或者与 Shield 为有效应用程序流量定义的启发式方法不匹配的流量。

- 每种资源都有最大的比特率和最大的数据包速率统计信息。
- 最大的请求速率统计数据仅适用于具有关联 Amazon WAF Web ACL 的 Amazon CloudFront 分配和应用程序负载均衡器。

Note

您也可以通过 Amazon Shield API 操作访问账户级别的事件摘要 [DescribeAttackStatistics](#)。

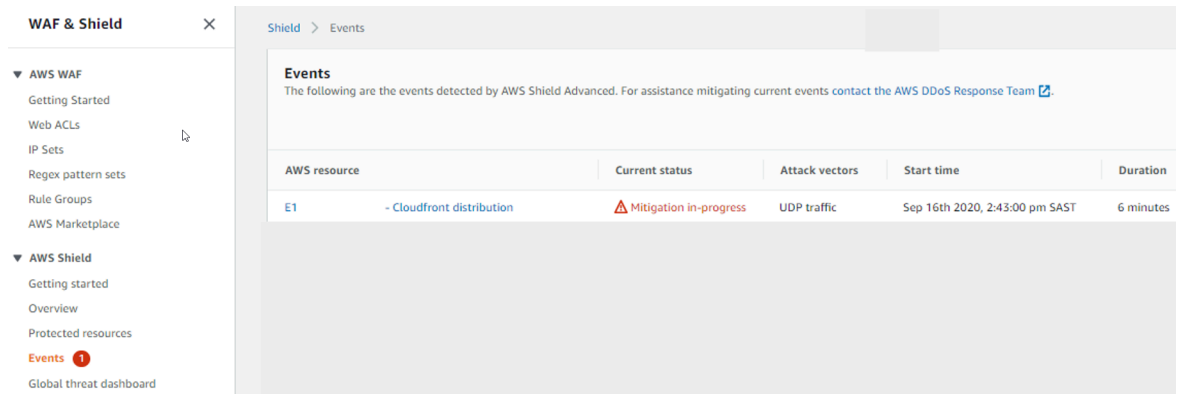
Amazon Shield Advanced 事件

当您订阅 Shield Advanced 并保护您的资源时，您可以访问资源的其他可见性功能。其中包括近乎实时地通知 Shield Advanced 检测到的事件以及有关检测到的事件和缓解措施的其他信息。

Amazon Shield 从多个维度评估您的受保护资源的流量。当检测到异常时，Shield Advanced 会为每种受影响的资源创建一个单独的事件。

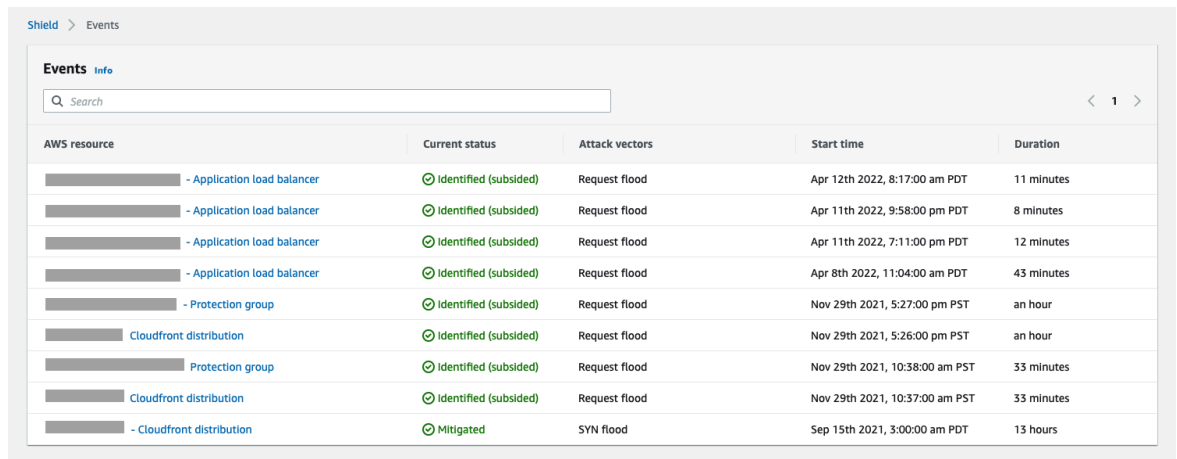
您可以通过 Shield 控制台的事件页面访问事件摘要和详细信息。顶级活动页面概述了当前和过去的事件。

以下屏幕截图显示了包含单个正在进行的事件的示例活动页面。左侧的导航窗格中，还会标记该活动事件的左侧导航窗格中。



Shield Advanced 还可能会根据流量类型和您配置的保护措施自动对攻击进行缓解。这些缓解措施可以保护您的资源免受与已知 DDoS 攻击签名匹配的过量流量或流量。

以下屏幕截图显示了一个示例事件列表，其中所有事件都已被 Shield Advanced 缓解或自行消退。



在活动开始前保护您的资源

在资源接收正常预期流量时，使用 Shield Advanced 保护资源，避免受到 DDoS 攻击，从而提高事件检测的准确性。

为了准确报告受保护资源的事件，Shield Advanced 必须首先为其建立预期流量模式的基准。

- Shield Advanced 会在资源受到保护至少 15 分钟后报告资源的基础设施层事件。
- Shield Advanced 会在资源受到保护至少 24 小时后报告资源的 Web 应用程序层事件。在 Shield Advanced 观测了 30 天的预期流量之后，应用层事件的检测准确性最佳。

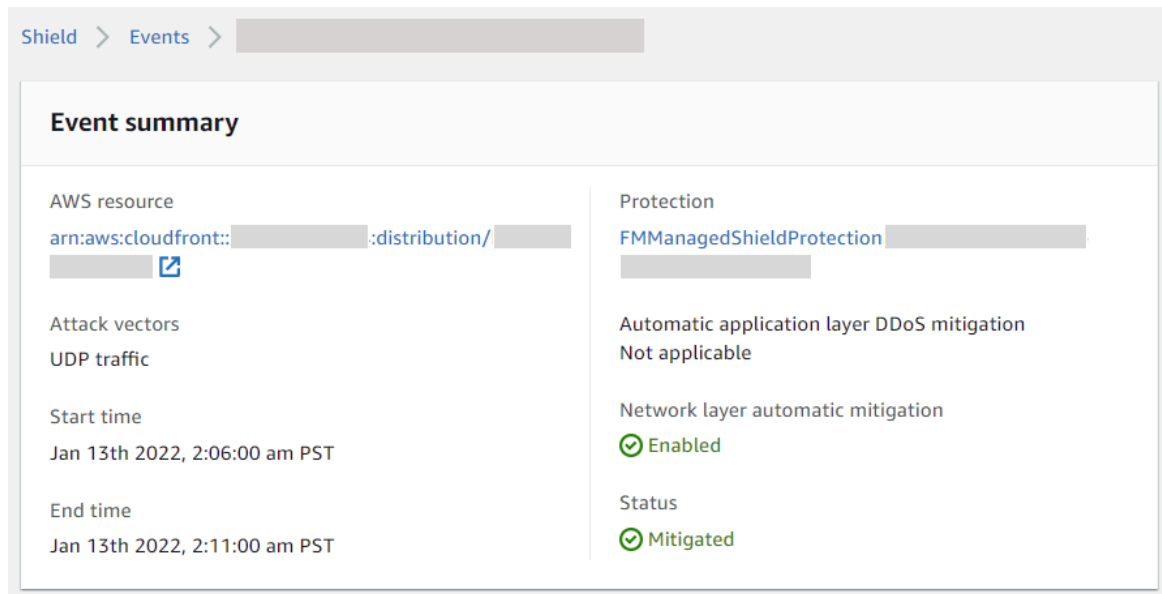
在 Amazon Shield 控制台中访问事件信息

1. 登录 Amazon Web Services Management Console 并打开 Amazon WAF & Shield 控制台，[网址为 https://console.aws.amazon.com/wafv2/](https://console.aws.amazon.com/wafv2/)。
2. 在 Amazon Shield 导航窗格中，选择 Events。控制台显示“事件”页面。
3. 在“事件”页面上，您可以选择列表中的任何事件，以查看该事件的其他摘要信息和详细信息。

Amazon Shield Advanced 活动摘要

您可以在事件的控制台页面中查看该事件的摘要和详细信息。要打开某个活动的页面，请从“活动”页面列表中选择其 Amazon 资源名称。

以下屏幕截图显示了网络层事件的事件摘要示例。



事件页面摘要信息包括以下内容。

- 当前状态 — 表示事件状态以及 Shield Advanced 对事件采取的操作的值。状态值适用于基础架构层（第 3 层或第 4 层）和应用层（第 7 层）事件。
- 已识别（正在进行）和已识别（已消退） — 这表明 Shield Advanced 检测到了事件，但到目前为止尚未采取任何行动。已识别（消退）表明 Shield 检测到的可疑流量已在没有干预的情况下停止。
- 缓解正在进行中且已缓解 — 这表明 Shield Advanced 检测到事件并已采取措施。当目标资源是 Amazon CloudFront 分发或 Amazon Route 53 托管区域时，也可使用 @@ 缓解，这些托管区域有自己的自动内联缓解措施。
- 攻击向量 — DDoS 攻击向量，例如 TCP SYN 泛洪和请求泛洪等 Shield 高级检测启发式方法。这些可能是 DDoS 攻击的指标。

- 开始时间-检测到第一个异常交通数据点的日期和时间。
- 持续时间或结束时间 — 表示从事件开始时间到 Shield Advanced 上次观测到的异常数据点之间经过的时间。在活动进行期间，这些值将继续增加。
- 保护 — 命名与资源关联的 Shield Advanced 保护，并提供指向其保护页面的链接。这可以在单个活动的页面上找到。
- 自动应用层 DDoS 缓解 — 用于应用程序层保护，用于指示是否为资源启用 Shield Advanced 自动应用层 DDoS 缓解。如果已启用，则会提供访问和管理配置的链接。这可以在单个活动的页面上找到。
- 网络层自动缓解-表示资源在网络层是否具有自动缓解功能。如果资源有网络层组件，它将启用该组件。此信息可在单个活动的页面上找到。

对于经常成为攻击目标的资源，Shield 可能会在过度流量消退后保留缓解措施，以防止事件再次发生。

Note

您还可以通过Amazon Shield API 操作访问受保护资源的事件摘要[ListAttacks](#)。

Amazon Shield Advanced事件详细信息

您可以在事件控制台页面的底部查看有关事件检测、缓解和主要贡献者的详细信息。此部分可能包括合法流量和潜在有害流量，可能既代表传递到您的受保护资源的流量，也可能代表被 Shield 缓解措施阻止的流量。

- 检测和缓解-提供有关观察到的事件以及针对该事件应用的任何缓解措施的信息。有关事件缓解的信息，请参阅[响应 DDoS 事件 \(p. 380\)](#)。
- 主要贡献者 — 对事件涉及的流量进行分类，并列出了每个类别的主要流量来源。

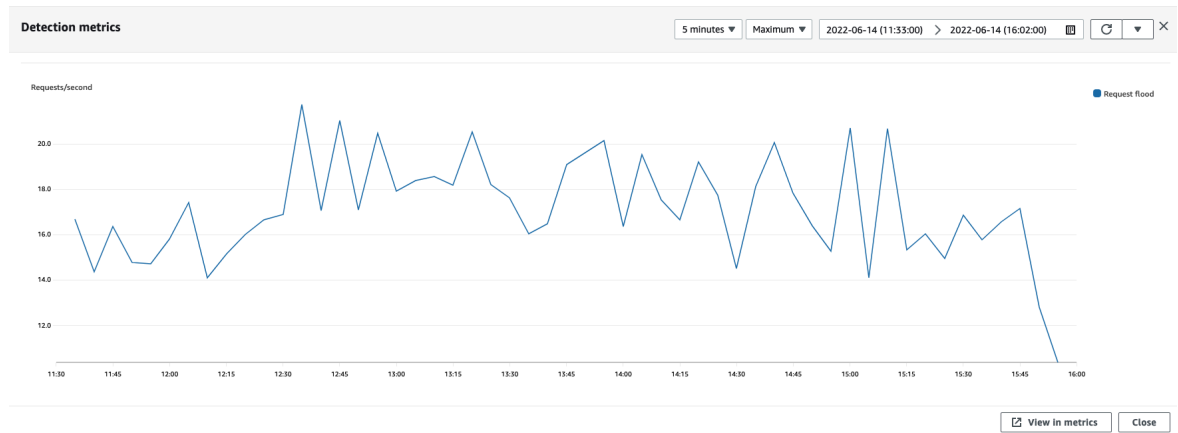
Amazon CloudFront 或 Amazon Route 53 资源的缓解指标不包括在内，因为这些服务受缓解系统的保护，该系统始终处于启用状态，不需要对单个资源进行缓解。

详细信息部分因信息是针对基础架构层还是应用层事件而有所不同。

应用程序层事件详细信息

对于应用层（第 7 层）事件，“检测和缓解”选项卡显示基于从Amazon WAF日志中获得的信息的检测指标。缓解指标基于相关的 Web ACL 中的Amazon WAF规则，这些规则配置为阻止有害流量。

以下屏幕截图显示了应用层事件的检测指标示例，该事件在数小时后消退。

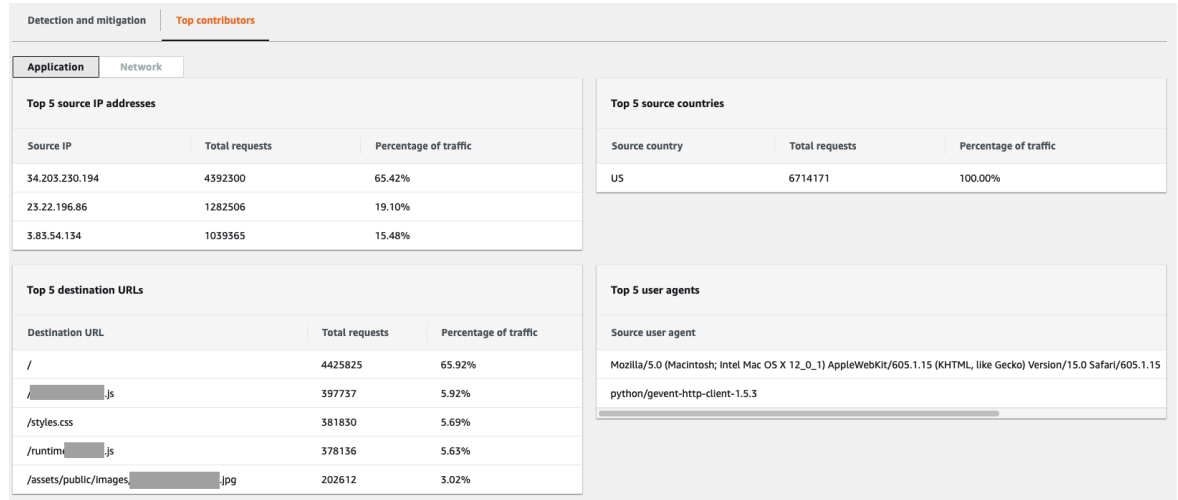


缓解规则生效之前消退的事件流量不会显示在缓解指标中。这可能会导致检测图中显示的 Web 请求流量与缓解图表中显示的允许和屏蔽指标之间出现差异。

对于亚马逊 CloudFront 发行版，您可以配置 Shield Advanced 以为您应用自动缓解措施。对于任何应用层资源，您可以选择在 Web ACL 中定义自己的缓解规则，也可以向 Shield 响应小组 (SRT) 寻求帮助。有关这些选项的信息，请参阅 [响应 DDoS 事件 \(p. 380\)](#)。

应用层事件的“主要贡献者”选项卡显示事件的前 5 位贡献者，按来源 IP、来源国家/地区和目标 URL 等维度进行分类。

以下屏幕截图显示了示例应用程序层事件的 Osh（主要贡献者）。

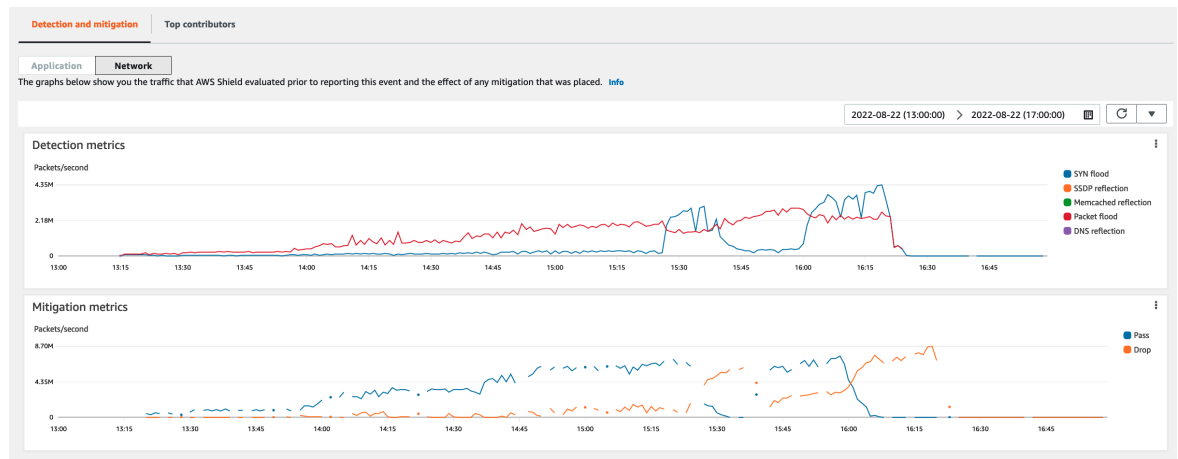


贡献者信息基于对合法和潜在有害流量的请求。数量较大的事件和请求源分布不高度的事件更有可能有可识别的顶级贡献者。大规模分布式攻击可能有任意数量的来源，因此很难确定攻击的主要贡献者。如果 Shield Advanced 未确定特定类别的重要贡献者，则会将数据显示为不可用。

基础设施层事件详细信息

对于基础设施层（第 3 层或第 4 层）事件，“检测和缓解”选项卡显示基于抽样网络流量的检测指标和基于缓解系统观测到的流量的缓解指标。缓解指标可以更精确地衡量您的资源流量。

以下屏幕截图显示了基础设施层事件的“检测和缓解”选项卡示例。



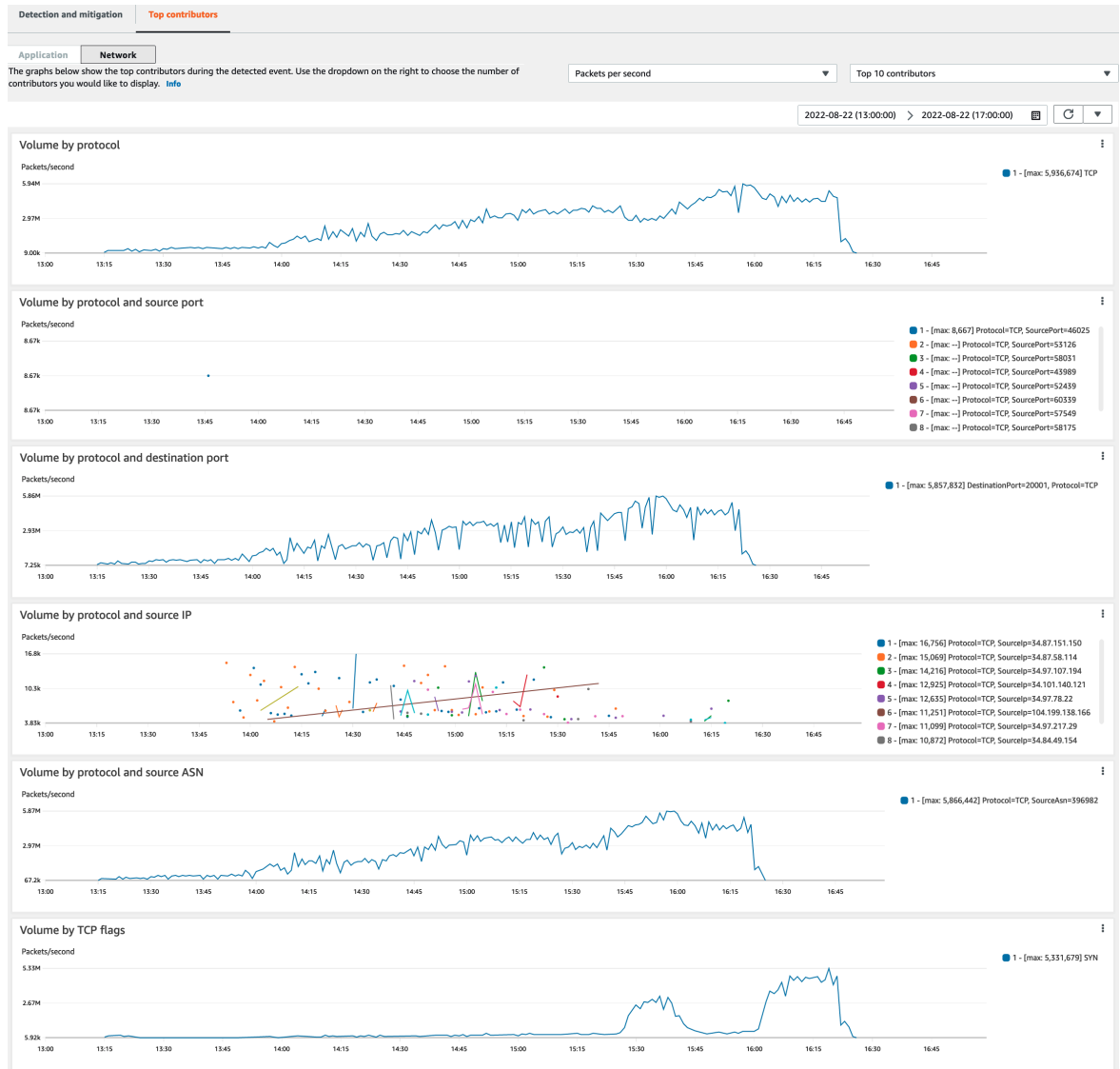
在 Shield 实施缓解措施之前消退的事件流量不会反映在缓解指标中。这可能会导致检测图中显示的流量与缓解图表中显示的通过和丢弃指标之间出现差异。

Shield 会自动为受保护资源类型弹性 IP (EIP)、Classic Load Balancer (CLB)、Application Load Balancer (ALB) 和 Amazon Global Accelerator 标准加速器创建缓解措施。EIP 地址和 Amazon Global Accelerator 标准加速器的缓解指标表明了通过和丢弃的数据包的数量。

Amazon WAF、Amazon Firewall Manager 和 Amazon Shield Advanced 开发人员指南 指标

基础设施层事件的主要贡献者选项卡列出了多个流量维度上最多 100 个主要贡献者的指标。详细信息包括可以识别至少五个重要流量来源的任何维度的网络层属性。流量来源的示例包括源 IP 和源 ASN。

以下屏幕截图展示了基础设施层事件的 Tod Sights (主要贡献者)。



贡献者指标基于合法和可能有害流量的抽样网络流量。数量较大的事件和流量来源不高度分布的事件更有可能出现可识别的主要贡献者。大规模分布式攻击可能有任意数量的来源，因此很难确定攻击的主要贡献者。如果 Shield 未确定特定指标或类别的任何重要贡献者，则会将数据显示为不可用。

在基础设施层 DDoS 攻击中，流量源可能会被欺骗或反射。欺骗来源是攻击者故意伪造的。反射源是检测到的流量的真实来源，但它不是攻击的自愿参与者。例如，攻击者可能通过反射来自互联网上通常合法的服务的攻击，向目标产生大量扩大的流量。在这种情况下，源信息可能是有效的，但它不是攻击的实际来源。这些因素可能会限制基于数据包标头屏蔽源的缓解技术的可行性。

Amazon Shield Advanced 亚马逊 CloudWatch 指标

Shield Advanced 发布了其保护的所有资源的亚马逊 CloudWatch 事件指标。这些指标使您可以为资源创建和配置 CloudWatch 仪表板和警报，从而提高您监控资源的能力。

Shield 亚马逊高级 CloudWatch 指标

指标	描述
DDoSDetected	表示特定亚马逊资源名称 (ARN) 的 DDoS 事件的 DDoS 事件。该指标在事件期间的值为 1，否则值为 0。
DDoSAttackBitsPerSecond	在特定 ARN 的 DDoS 事件期间观察到的字节数。此指标仅适用于网络和传输层（第 3 层或第 4 层）DDoS 事件。该指标的单位是比特。
DDoSAttackPacketsPerSecond	在特定 ARN 的 DDoS 事件期间观察到的数据包数量。此指标仅适用于网络和传输层（第 3 层或第 4 层）DDoS 事件。该指标的单位是数据包。
DDoSAttackRequestsPerSecond	在 DDoS 事件期间观察到的针对特定 ARN 的请求数。此指标仅适用于应用层（第 7 层）DDoS 事件。该指标的单位是请求。

如果没有事件可记录到某个 CloudWatch 指标，则 Shield Advanced 每天发布一次零值指标。这会使指标保持活动状态，并可用于自定义 CloudWatch 警报和仪表板。

我们建议您创建警报以在需要注意的情况下通知您。首先，您可以为每个受保护资源创建警报，报告 DDoSDetected 指标何时为非零。此指标中的非零值并不意味着正在进行 DDoS 攻击，但我们建议在指标处于该状态时仔细查看资源状态。

对于请求泛滥，我们建议您为复合检查创建警报，这些警报还要考虑应用程序运行状况和 Web 请求量等因素。您可以选择对报告不同攻击向量维度的流量的其他三个指标发出警报。通过考虑应用程序的容量并在流量接近应用程序限制时发出警报，您可以创建一组规则，在需要时通知您，而不会产生太多不必要的噪音。

有关 Shield Advanced 指标的更多信息，包括缓解和主要贡献者指标、指标维度以及有关创建警报的信息，请参阅 [Amazon Shield Advanced 指标和警报 \(p. 506\)](#)。

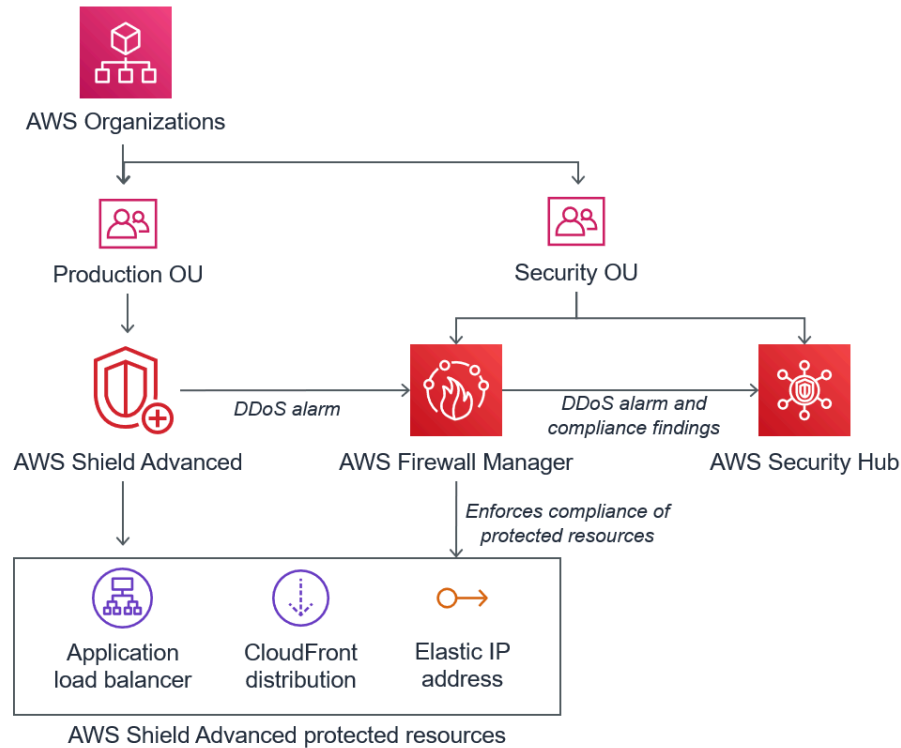
事件跨账户可见性

您可以使用 Amazon Firewall Manager 和 Amazon Security Hub 来管理和监控多个账户中的 Amazon Shield Advanced 受保护资源。

使用 Firewall Manager，您可以创建 Shield Advanced 安全策略，报告并强制执行所有账户的 DDoS 保护合规性。Firewall Manager 监控您的受保护资源，包括为 Shield Advanced 策略范围内的新资源添加保护。

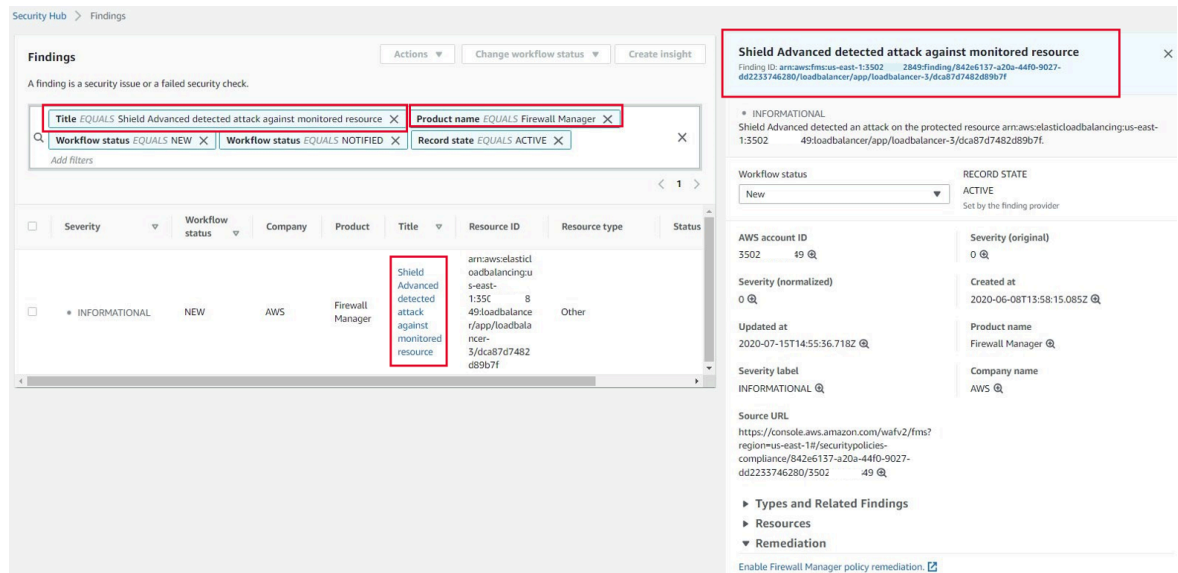
您可以将 Firewall Manager 与集成，Amazon Security Hub 以获得一个仪表板，当 Firewall Manager 发现资源不符合您的 Shield Advanced 安全策略时，Shield Advanced 和 Firewall Manager 合规性调查结果检测到的 DDoS 事件。

下图描述了使用 Firewall Manager Security Hub 监控 Shield Advanced 保护资源的典型架构。



将 Firewall Manager 与 Security Hub 集成后，可以在一个地方查看安全调查结果，以及您运行的应用程序的其他警报和合规性状态信息Amazon。

以下屏幕截图重点显示了当您进行此类集成时，您可以在 Security Hub 控制台看到的有关 Shield Advanced 事件的信息。



要了解如何将 Firewall Manager 和 Security Hub 与 Shield Advanced 集成，以集中监控受保护账户的事件和合规性，请参阅Amazon安全博客为 [DDoS 事件设置集中监控并自动修复不合规的资源](#)。

响应 DDoS 事件

Amazon 自动缓解网络和传输层 (第 3 层和第 4 层) 分布式拒绝服务 (DDoS) 攻击。如果您使用 Shield Advanced 保护您的 Amazon EC2 实例，在攻击期间，Shield Advanced 会自动将您的 Amazon VPC 网络 ACL 部署到 Amazon 网络。这使得 Shield Advanced 能够针对较大的 DDoS 事件提供保护。有关网络 ACL 的更多信息，请参阅[网络 ACL](#)。

对于应用程序层 (第 7 层) DDoS 攻击，Amazon 尝试检测和通知 Amazon Shield Advanced 客户通过 CloudWatch 警报。默认情况下，它不会自动应用缓解措施，以避免无意中阻止有效的用户流量。

对于应用层 (第 7 层) 资源，您可以使用以下选项来响应攻击。

- 提供您自己的缓解措施— 您可以自己调查和缓解攻击。有关信息，请参阅[手动缓解应用层 DDoS 攻击 \(p. 381\)](#)。
- 联系支持部— 如果您是 Shield Advanced 客户，您可以联系[Amazon Web Services Support Center](#)以获取缓解措施的帮助。重大和紧急案例将直接转给 DDoS 专家。有关信息，请参阅[在应用层 DDoS 攻击期间联系支持中心 \(p. 380\)](#)。

此外，在攻击发生之前，您可以主动启用以下缓解选项：

- 亚马逊上的自动缓解措施 CloudFront 分布— 使用此选项，Shield Advanced 在 Web ACL 中为您定义和管理缓解规则。有关自动缓解应用程序层的信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。
- 主动联系— 当 Amazon Shield Advanced 检测到针对您的应用程序发起的大型应用程序层攻击，SRT 可以主动与您联系。SRT 会分 DDoS 事件并创建 Amazon WAF 缓解措施。SRT 与您联系，并在征得您同意的情况下，可以应用 Amazon WAF 规则。有关此选项的更多信息，请参阅[配置主动参与操作 \(p. 350\)](#)。

在应用层 DDoS 攻击期间联系支持中心

如果您是 Amazon Shield Advanced 客户，您可以联系[Amazon Web Services Support Center](#)以获取缓解措施的帮助。重大和紧急案例将直接转给 DDoS 专家。与 Amazon Shield Advanced，复杂的案例可以上报到 Amazon Shield 响应团队 (SRT)，在保护方面有丰富的经验 Amazon、Amazon.com 及其子公司。有关 SRT 的更多信息，请参阅[Shield 响应小组 \(SRT\) 支持 \(p. 348\)](#)。

要获得 Shield 牌响应团队 (SRT) 支持，请联系[Amazon Web Services Support Center](#)。对您的案例的响应时间取决于您选择的严重性以及响应时间，在[Amazon Web Services Support 计划](#)页。

选择以下选项：

- 案例类型：技术支持
- Service (服务)：分布式拒绝服务 (DDoS)
- 类别：入站至 Amazon
- 严重性：选择适当的选项

当与我们的代表讨论时，请说明您是 Amazon Shield Advanced 客户遇到可能的 DDoS 攻击。我们的代表会将您的电话转给适当的 DDoS 专家。如果您使用[Amazon Web Services Support Center](#)使用分布式拒绝服务 (DDoS) 服务类型，您可以通过聊天或电话直接与 DDoS 专家交流。DDoS 支持工程师可以帮助您识别攻击、建议对 Amazon 架构的改进，并提供关于使用 Amazon 服务缓解 DDoS 攻击的指导。

对于应用程序层攻击，SRT 可帮助您分析可疑活动。如果您为资源启用了自动缓解功能，则 SRT 可以查看 Shield Advanced 自动对攻击实施的缓解措施。无论如何，SRT 可以帮助您审查和缓解问题。SRT 建议的缓解措施通常需要 SRT 创建或更新 Amazon WAF 您账户中的 Web 访问控制列表 (Web ACL)。SRT 将需要您的授权才能完成此项工作。

Important

我们建议作为启用的一部分 Amazon Shield Advanced，请按中的步骤操作。[为 Shield 响应小组 \(SRT\) 配置访问权限 \(p. 349\)](#) 主动向 SRT 提供在攻击期间为您提供帮助所需的权限。提前提供授权有助于防止在实际发生攻击时耽误问题的解决。

SRT 可帮助您筛选 DDoS 攻击，以识别攻击签名和模式。经您同意后，SRT 将创建和部署 Amazon WAF 减轻攻击的规则。

您也可以在可能发起攻击前或期间联系 SRT，以查看缓解措施以及开发和部署自定义缓解措施。例如，如果您正在运行一个 Web 应用程序且只需打开端口 80 和 443，您可以与 SRT 一起预先配置一个 Web ACL，只“允许”打开端口 80 和 443。

您在账户级别授权和联系 SRT。也就是说，如果您在 Firewall Manager Shield 牌高级策略中使用 Shield Advanced，帐户所有者，而不是防火墙管理员必须联系 SRT 以获得支持。防火墙管理员只能为他们拥有的帐户联系 SRT。

手动缓解应用层 DDoS 攻击

如果您确定您的资源事件页面中的活动属于 DDoS 攻击，您可以创建自己的活动。Amazon WAF Web ACL 中的规则以缓解攻击。如果您不是 Shield Advanced 客户，这是唯一可用的选择。Amazon WAF 随提供 Amazon Shield Advanced 没有任何额外费用。有关在 Web ACL 中创建规则的信息，请参阅 [Web ACL \(Web ACL \) \(p. 11\)](#)。

如果您使用 Amazon Firewall Manager，您可以添加您的 Amazon WAF Firewall Manager 器的规则 Amazon WAF 政策。

手动缓解潜在的应用层 DDoS 攻击

1. 使用符合异常行为的条件在 Web ACL 中创建规则语句。首先，请将其配置为对匹配请求计数。有关配置 Web ACL 和规则语句的信息，请参阅 [Web ACL 规则和规则组评估 \(p. 12\)](#) 和 [测试和调整您的 Amazon WAF 保护措施 \(p. 200\)](#)。

Note

始终首先使用规则操作来测试规则。Count 而不是 Block。当您认为您的新规则能确定正确的请求后，可以修改它们以阻止请求。

2. 监控请求计数以确定是否要阻止匹配的请求。如果请求量仍然异常高，并且您确信自己的规则正在捕获导致大容量的请求，请更改 Web ACL 中的规则以阻止请求。
3. 继续监控活动页面，以确保您的流量能够按照自己的要求进行处理。

Amazon 提供了预配置的模板，旨在帮助您快速入门。这些模板包含一组 Amazon WAF 规则，可供您进行自定义或用于阻止基于 Web 的常见攻击。有关更多信息，请参阅 [Amazon WAF 安全自动化](#)。

在申请服务抵扣金额 Amazon Shield Advanced

如果你已经订阅 Amazon Shield Advanced 而且您遇到的 DDoS 攻击会提高 Shield Advanced 受保护资源的利用率，您可以请求扣除与提高利用率相关的费用，但以 Shield Advanced 无法缓解的范围为限。积分仅适用于以下类型的费用：亚马逊 CloudFront HTTP/HTTPS 请求，CloudFront 数据传出、亚马逊路线 53 查询，Amazon Global Accelerator 标准加速器数据传输、应用程序负载均衡器的负载均衡器容量单位，以及受保护的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的使用峰值。

申请信贷的先决条件

要有资格获得信贷，在攻击开始之前，您必须执行以下操作：

- 您必须向要申请信贷的资源添加了 Shield Advanced 保护。攻击期间添加的受保护资源不符合成本保护条件。

Note

在你的上启用 Shield 牌高级 Amazon Web Services 账户不会自动为单个资源启用 Shield 牌高级保护。

有关如何保护的更多信息 Amazon 使用 Shield 高级的资源，请参阅[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)。

- 对于适用 CloudFront 和 Application Load Balancer 受保护的资源，您必须将 Amazon WAF Web ACL 并在 Web ACL 中实施了基于速率的规则。有关如何创建的信息 Amazon WAF 基于速率的规则，请参阅[基于速率的规则语句 \(p. 95\)](#)。有关如何将 Web ACL 与之关联的信息 Amazon 请参阅。[Web ACL \(Web ACL \) \(p. 11\)](#)。
- 你必须实施了适当的最佳实践[Amazon 实现 DDoS 弹性的 最佳实践](#) 以便以最大限度地降低 DDoS 攻击期间成本的方式配置应用程序。

如何申请信贷

要获取服务抵扣金额，您必须在攻击发生的账单月份结束之后的 15 天内提交服务抵扣金额申请。

要申请信用，请通过[Amazon Web Services Support Center](#)。在请求中包括以下内容：

- 主题行中的词语“DDoS Concession”
- 您要申请服务抵扣金额的每个活动或服务情况中断的日期和时间
- 这些区域有：Amazon 受影响的服务和具体资源

提交请求后，Amazon Shield 响应团队 (SRT) 将验证是否发生了 DDoS 攻击，如果是的话，是否有任何受保护的资源扩展以吸收 DDoS 攻击。如果 Amazon 确定受保护的资源扩展以吸收 DDoS 攻击，Amazon 将为那部分流量发放信用 Amazon 确定是由 DDoS 攻击造成的。服务抵扣金额有效期为 12 个月。

您使用 Amazon Shield 服务的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

Note

本节为您提供使用 Amazon Shield 服务及其 Amazon 资源（例如 Shield Advanced 保护）提供标准 Amazon 安全指导。

有关使用 Shield 和 Shield Advanced 保护 Amazon 资源的信息，请参阅 Amazon Shield 指南的其余部分。

安全性是 Amazon 和您的共同责任。[责任共担模型](#) 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 Web Services 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，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Shield 的合规性计划，请参阅[合规性计划范围内的 Amazon 服务](#)。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Shield 时应用责任共担模型。以下主题说明如何配置 Shield 以实现您的安全性和合规性目标。您还将了解如何使用其他 Amazon 服务来帮助您监控和保护您的 Shield 资源。

主题

- [保护 \(p. 383\)](#)
- [适用于 Amazon Shield 的 Identity and Access Management \(p. 383\)](#)
- [中的日志记录和监控 \(p. 400\)](#)
- [的合规性验证 \(p. 401\)](#)
- [Shield 中的弹性 \(p. 401\)](#)
- [Amazon Shield 中的基础设施安全性 \(p. 401\)](#)

保护

Amazon [责任共担模式](#) 适用于 Amazon Shield 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（例如您客户的电子邮件地址）放入标签或自由格式文本字段（例如名称字段）。这包括 Amazon Web Services 使用控制台、API 或 Amazon 开发工具包处理 Shield 或其他情况。Amazon CLI 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保护。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。

Shield 实体（例如保护）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

适用于 Amazon Shield 的 Identity and Access Management

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用 Shield 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- [受众 \(p. 210\)](#)
- [使用身份进行身份验证 \(p. 211\)](#)
- [使用策略管理访问 \(p. 212\)](#)
- [Amazon Shield 如何与 IAM 协同工作 \(p. 387\)](#)
- [适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)

- [Amazon 适用于 Amazon Shield 的托管策略 \(p. 395\)](#)
- [对 Amazon Shield 身份和访问进行故障排除 \(p. 396\)](#)
- [使用 ShieldAdvidently 的服务 \(p. 398\)](#)

受众

使用 Amazon Identity and Access Management (IAM) 的方式因您可以在 Shield 中执行的操作而异。

服务用户 - 如果您使用 Shield 服务来完成作业，则管理员会为您提供所需的凭证和权限。当您使用更多 Shield 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Shield 中的一项功能，请参阅[对 Amazon Shield 身份和访问进行故障排除 \(p. 396\)](#)。

服务管理员 — 如果您在公司负责管理 Shield 的资源，您可能对 Shield 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Shield 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Shield 搭配使用的更多信息，请参阅[Amazon Shield 如何与 IAM 协同工作 \(p. 387\)](#)。

IAM 管理员 — 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Shield 的访问的详细信息。要查看您可在 IAM 中使用的 Shield 基于身份的策略的示例，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅 Amazon 一般参考中的[签名版本 4 签名流程](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 Amazon Account Management 参考指南 中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

IAM 用户和组

IAM 用户 是 Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有

一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 [对于需要长期凭证的使用场景定期轮换访问密钥](#)。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

IAM 角色是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以担任角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- **Federated user access (联合用户访问)** – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。
- **临时 IAM 用户权限** – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- **跨账户访问** – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。
- **跨服务访问** – 某些 Amazon Web Services 使用其它 Amazon Web Services 中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
 - **主体权限** – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的[Amazon Shield 的操作、资源和条件键](#)。
 - **服务角色** – 服务角色是服务代表您在您的账户中执行操作而担任的 **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](#)。
 - **服务相关角色** – 服务相关角色是与 Amazon Web Service 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- **在 Amazon EC2 上运行的应用程序** – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的[何时创建 IAM 角色（而不是用户）](#)。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的[JSON 策略概览](#)。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 [创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的 [在托管式策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中 [指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 Amazon 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Simple Storage Service (Amazon S3)、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的 [访问控制列表 \(ACL\) 概览](#)。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 [IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 Amazon Web Services 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 [SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的 [会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

Amazon Shield 如何与 IAM 协同工作

在使用 IAM 管理对 Shield 的访问权限之前，您应该了解哪些 IAM 功能可用于 Shield。

您可以与 Amazon Shield 搭配使用的 IAM 功能

IAM 功能	Shield
基于身份的策略 (p. 387)	是
基于资源的策略 (p. 387)	否
策略操作 (p. 388)	是
策略资源 (p. 388)	是
策略条件键 (特定于服务) (p. 390)	是
ACL (p. 390)	否
ABAC (策略中的标签) (p. 390)	部分
临时凭证 (p. 391)	是
委托人权限 (p. 391)	是
服务角色 (p. 391)	是
服务相关角色 (p. 391)	是

要大致了解 Shield 和其他 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅 [IAM 用户指南中的与 IAM 一起使用的 Amazon 服务](#)。

适用于的基于身份的 Shield

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

要查看 Shield 基于身份的策略的示例，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

Shield 内基于资源策略

支持基于资源的策略。	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。

Shield 的政策行动

支持策略操作	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

要查看 Shield 操作的列表，请参阅服务授权参考 Amazon Shield 中的[由定义的操作](#)。

Shield 中的策略操作在操作前使用以下前缀：

```
shield
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
    "shield:action1",
    "shield:action2"
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定 Shield 中以开头的所有操作 List，请包括以下操作：

```
"Action": "shield:List*"
```

要查看 Shield 基于身份的策略的示例，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

Shield 的策略资源

支持策略资源	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Shield 资源类型及其 ARN 的列表，请参阅服务授权参考 Amazon Shield 中的 [定义的资源](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Amazon Shield 定义的操作](#)。要允许或拒绝访问 Shield 资源的子集，请在策略的 resource 元素中包含该资源的 ARN。

其中 Amazon Shield，资源是保护和攻击。这些资源具有关联的唯一 Amazon 资源名称 (ARN)，如下表所示。

Amazon Shield 控制台中的名称	Amazon Shield SDK/CLI 中的名称	ARN 格式	
事件或攻击	AttackDetail	arn:aws:shield:: <i>account</i> :attack/ <i>ID</i>	
保护	Protection	arn:aws:shield:: <i>account</i> :protection/ <i>ID</i>	

要允许或拒绝访问 Shield 资源的子集，请在策略的 resource 元素中包含该资源的 ARN。适用于 Shield 的 ARN 采用以下格式：

```
arn:partition:shield::account:resource/ID
```

将 *account*、*resource* 和 *ID* 变量替换为有效值。有效值如下：

- *##*：您的 IDAmazon Web Services 账户。您必须指定值。
- *##*：Shield 资源的类型，attack 或者 protection。
- *ID*：Shield 资源的 ID，或通配符（*），用于表示与指定资源关联的所有指定类型的资源 Amazon Web Services 账户。

例如，以下 ARN 为账户指定了所有保护 111122223333：

```
arn:aws:shield::111122223333:protection/*
```

ARN of

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

有关 ARN 规格的一般信息，请参阅 [Amazon Web Services 一般参考中的 Amazon 资源名称 \(ARN\)](#)。

以下列出了特定于 wafv2 资源 ARN 的要求：

- *##*：对于您用于保护亚马逊 CloudFront 发行版的 Shield 资源，请将其设置为 us-east-1。否则，请将其设置为与受保护的区域资源一起使用的区域。
- *##*：将范围设置 global 为与亚马逊 CloudFront 发行版一起使用或 regional 与 Amazon WAF 支持的任何区域资源一起使用。区域资源是 Amazon API Gateway REST API、Amazon AppSync GraphQL T API、Gateway 用户群 Amazon App Runner 体。
- *####*：指定以下值之一：attack 用于事件或攻击，protection 用于保护。

- **####**：指定您为 Shield 资源提供的名称，或指定通配符 (*) 以表示满足 ARN 中其他规范的所有资源。您必须指定资源名称和资源 ID，或者为两者都指定通配符。
- **##ID**：指定 Shield 资源的 ID，或指定通配符 (*) 以表示满足 ARN 中其他规范的所有资源。您必须指定资源名称和资源 ID，或者为两者都指定通配符。

例如，以下 ARN 指定区域 us-west-1 中具有账户 111122223333 的区域作用域的所有 Web ACL：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

以下 ARN 为区域 111122223333 中的账户指定了 MyIPManagementRuleGroup 以全局作用域命名的规则组 us-east-1：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

要查看 Shield 基于身份的策略的示例，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

Shield 的策略条件键

支持特定于服务的策略条件键	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。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](#)。

Amazon 支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的[Amazon 全局条件上下文键](#)。

要查看 Shield 条件键的列表，请参阅服务授权参考 Amazon Shield[中的条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅[Amazon Shield 定义的操作](#)。

要查看 Shield 基于身份的策略的示例，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

Shield 中的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带 Shield

支持 ABAC（策略中的标签）	部分

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的 [什么是 ABAC？](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的 [使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证用 Shield

支持临时凭证	是

某些 Amazon Web Services 在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon Web Services 与临时凭证配合使用，请参阅 IAM 用户指南中的 [使用 IAM 的 Amazon Web Services](#)。

如果您不使用用户名和密码而用其它方法登录到 Amazon Web Services Management Console，则使用临时凭证。例如，当您使用贵公司的单点登录 (SSO) 链接访问 Amazon 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 [切换到角色 \(控制台\)](#)。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 [IAM 中的临时安全凭证](#)。

Shield 的跨服务主体权限

支持委托人权限	是

当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为委托人。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的 [Amazon Shield 的操作、资源和条件键](#)。

Shield 的服务角色

支持服务角色	是

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](#)。

Warning

更改服务角色的权限可能会破坏 Shield 的功能。仅当 Shield 提供相关指导时才编辑服务角色。

Shield 的服务相关角色

支持服务相关角色	是

服务相关角色是一种与 Amazon Web Service 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Shield 服务相关角色的详细信息，请参阅[使用 ShieldAdvidently 的服务 \(p. 398\)](#)。

适用于 Amazon Shield 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Shield 资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要用户用户在其需要的资源上执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

有关 Shield 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考 Amazon Shield 中的[的操作、资源和条件键](#)。

主题

- [策略最佳实践 \(p. 392\)](#)
- [使用Shield 控制台 \(p. 393\)](#)
- [允许用户查看他们自己的权限 \(p. 393\)](#)
- [授予您的 Shield 高级保护的读取权限 \(p. 393\)](#)
- [授予 Shield CloudFront、和的只读访问权限 CloudWatch \(p. 394\)](#)
- [授予对Shield 的完全访问权限 CloudFront，和 CloudWatch \(p. 394\)](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Shield 资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的[Amazon 托管策略](#)或[工作职能的 Amazon 托管策略](#)。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的[IAM 中的策略和权限](#)。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy 语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的[IAM Access Analyzer 策略验证](#)。
- Require multi-factor authentication (MFA) [需要多重身份验证 (MFA)] – 如果您所处的场景要求您的 Amazon Web Services 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的[配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的[IAM 中的安全最佳实践](#)。

使用Shield 控制台

要访问 Amazon Shield 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您中的 Shield 资源的详细信息Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

可以访问和使用Amazon控制台的用户也可以访问Amazon Shield控制台。无需额外权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

授予您的 Shield 高级保护的读取权限

Amazon Shield允许跨账户资源访问，但不允许您创建跨账户资源保护。您只能在拥有这些资源的账户内为资源创建保护。

以下示例策略授予对所有资源执行 `shield:ListProtections` 操作的权限。Shield 不支持对某些 API 操作使用资源 ARN（也称为资源级权限）来标识特定资源，因此您可以指定通配符（*）。这仅允许访问您可以通过操作检索的资源`ListProtections`。

```
{
  "Version": "2016-06-02",
  "Statement": [
```

```
{
  "Sid": "ListProtections",
  "Effect": "Allow",
  "Action": [
    "shield:ListProtections"
  ],
  "Resource": "*"
}
```

授予 Shield CloudFront、和的只读访问权限 CloudWatch

以下政策授予用户对 Shield 和相关资源（包括亚马逊 CloudFront 资源和亚马逊 CloudWatch 指标）的只读访问权限。这对于需要权限才能查看 Shield 保护和攻击中的设置以及监控其中的指标的用户非常有用 CloudWatch。这些用户无法创建、更新或删除 Shield 资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ProtectedResourcesReadAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:List*",
        "elasticloadbalancing:List*",
        "route53:List*",
        "cloudfront:Describe*",
        "elasticloadbalancing:Describe*",
        "route53:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:*:*:*",
        "arn:aws:cloudfront:*:*:*:*",
        "arn:aws:route53:::hostedzone/*",
        "arn:aws:cloudwatch:*:*:*:*",
        "arn:aws:globalaccelerator:*:*:*"
      ]
    },
    {
      "Sid": "ShieldReadOnly",
      "Effect": "Allow",
      "Action": [
        "shield:List*",
        "shield:Describe*",
        "shield:Get*"
      ],
      "Resource": "*"
    }
  ]
}
```

授予对Shield 的完全访问权限 CloudFront , 和 CloudWatch

以下策略允许用户执行任何 Shield 操作，在 CloudFront Web 发行版上执行任何操作，并监控中的指标和请求示例 CloudWatch。它对作为 Shield 管理员的用户很有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ProtectedResourcesReadAccess",
      "Effect": "Allow",
      "Action": [
        "cloudfront:List*",
        "elasticloadbalancing:List*",
        "route53:List*",
        "cloudfront:Describe*",
        "elasticloadbalancing:Describe*",
        "route53:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "cloudfront:GetDistribution*",
        "globalaccelerator:ListAccelerators",
        "globalaccelerator:DescribeAccelerator"
      ],
      "Resource": [
        "arn:aws:elasticloadbalancing:*:*:*:*",
        "arn:aws:cloudfront:*:*:*:*",
        "arn:aws:route53:::hostedzone/*",
        "arn:aws:cloudwatch:*:*:*:*",
        "arn:aws:globalaccelerator:*:*:*"
      ]
    },
    {
      "Sid": "ShieldFullAccess",
      "Effect": "Allow",
      "Action": [
        "shield:*"
      ],
      "Resource": "*"
    }
  ]
}
```

强烈建议您为拥有管理权限的用户配置 Multi-Factor Authentication (MFA)。有关更多信息，请参阅《IAM 用户指南》中的[Amazon 在中使用 Multi-Factor Authentication \(MFA\) 设备](#)。

Amazon 适用于 Amazon Shield 的托管策略

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 Web Services 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 Web Services 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，服务最有可能更新 Amazon 托管策略。服务不会从 Amazon 托管策略中删除权限，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，ViewOnlyAccess Amazon 托管策略提供对许多 Amazon Web Services 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：AWSShieldDRTAccessPolicy

Amazon Shield当您授予Shield 响应小组 (SRT) 代表您行事的权限时，会使用此托管策略。此策略授予 SRT 对您的Amazon账户的有限访问权限，以帮助在高严重事件期间缓解 DDoS 攻击。此策略允许 SRT 管理您的 Amazon WAF规则和 Shield Advanced 保护，并访问您的Amazon WAF日志。

有关向 SRT 授予代表您运营的权限的信息，请参阅[为Shield 响应小组 \(SRT\) 配置访问权限 \(p. 349\)](#)。

有关此策略的详细信息，请参阅 IAM 控制台[AWSShieldDRTAccessPolicy](#)中的。

Amazon托管策略：AWSShieldServiceRolePolicy

当您启用应用层 DDoS 自动缓解时，Shield Advanced 会使用此托管策略来设置您的账户管理资源所需的权限。此策略允许 Shield Advanced 在您与受保护资源关联的 Web ACL 中创建和应用Amazon WAF规则和规则组，以自动响应 DDoS 攻击。

您无法附加 AWSShieldServiceRolePolicy 至您的 IAM 实体。Shield 附加到服务相关角色AWSServiceRoleForAWSShield的策略允许 Shield 代表您执行操作。

当您启用自动应用层 DDoS 缓解时，Shield Advanced 允许使用此策略。有关此策略使用的更多信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

有关使用此策略的服务相关角色 AWSServiceRoleForAWSShield 的信息，请参阅[使用 ShieldAdvidently 的服务 \(p. 398\)](#)

有关此策略的详细信息，请参阅 IAM 控制台[AWSShieldServiceRolePolicy](#)中的。

Shield 托管策略的更新

查看有关 Shield ed 的Amazon托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 Shield 文档历史记录页面上的 RSS 源[文档历史记录 \(p. 525\)](#)。

策略	变更描述	日期
AWSShieldServiceRolePolicy 此政策允许 Shield 访问和管理 Amazon资源，以便代表您自动响应应用层 DDoS 攻击。 IAM 控制台中的详细信息： AWSShieldServiceRolePolicy 服务相关角色AWSServiceRoleForAWSShield使用此策略。有关信息，请参阅 使用 ShieldAdvidently 的服务 (p. 398) 。	添加了此政策，以便为 Shield Advanced 提供自动应用层 DDoS 缓解功能所需的权限。有关此功能的信息，请参阅 Shield Advanced 自动应用层 DDoS (p. 354) 。	2021 年 12 月 1 日
Shield 已开启跟踪更改	Shield 已开始为其Amazon托管策略跟踪更改。	2021 年 3 月 3 日

对 Amazon Shield 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Shield 和 IAM 时可能遇到的常见问题。

主题

- [我无权在 Shield 中执行操作 \(p. 397\)](#)
- [我无权执行 iam : PassRole \(p. 397\)](#)
- [我希望允许我的之外的用户Amazon Web Services 账户访问Shield 的 \(p. 397\)](#)

我无权在 Shield 中执行操作

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 shield:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
shield:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 shield:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Shield。

有些 Amazon Web Services 允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户 marymajor 尝试使用控制台在 Shield 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我希望允许我的之外的用户Amazon Web Services 账户访问Shield 的

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Shield 是否支持这些功能，请参阅[Amazon Shield 如何与 IAM 协同工作 \(p. 387\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的[为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方 Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的 Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的[为经过外部身份验证的用户（联合身份验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的[IAM 角色与基于资源的策略有何不同](#)。

使用 ShieldAdvidently 的服务

Amazon Shield Advanced 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 ShieldAdvidently 直接相关。服务相关角色由 ShieldAdvidently 预定义，并具有该服务代表您调用其他 Amazon 服务所需的所有权限。

服务相关角色可让您更轻松地了解 ShieldAdvidently，因为您不必手动添加必要的权限。ShieldAdvidently 定义其服务相关角色的权限，除非另外定义，否则只有 ShieldAdvidently 可以代入该角色。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 Shield Advidently 资源，因为无法意外删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅[使用 IAM 的 Amazon 服务](#)并查找 Service-Linked Role (服务相关角色) 列中显示为 Yes (是) 的服务。请选择 Yes 与[查看该服务的服务相关角色文档](#)的链接。

ShieldAdently 的服务相关角色权限

ShieldAdvidently 使用名为的服务相关角色 AWSServiceRoleForAWSShield。此角色允许 Shield Advanced 访问和管理 Amazon 资源，以便代表您自动响应应用层 DDoS 攻击。有关此功能的更多信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

AWSServiceRoleForAWSShield 服务相关角色信任以下服务代入该角色：

- shield.amazonaws.com

名为的角色权限策略 AWSShieldServiceRolePolicy 允许 ShieldAdvidently 对所有 Amazon 资源完成以下操作：

- wafv2:GetWebACL
- wafv2:UpdateWebACL
- wafv2:GetWebACLForResource
- wafv2:ListResourcesForWebACL
- cloudfront:ListDistributions
- cloudfront:GetDistribution

如果允许对所有 Amazon 资源执行操作，则在策略中将其指示为 "Resource": "*"。这仅意味着服务相关角色可以对该操作支持的所有 Amazon 资源执行每项指示的操作。例如，该操作 wafv2:GetWebACL 仅支持 wafv2 Web ACL 资源。

Shield Advanced 仅对您已启用应用层保护功能的受保护资源以及与这些受保护资源关联的 Web ACL 进行资源级 API 调用。

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](#)。

为 ShieldAdvidently 创建服务相关角色

无需手动创建服务相关角色。当您为 Amazon Web Services Management Console、或 Amazon API 中的资源启用自动应用层 DDoS 缓解时 Amazon CLI，Shield Advanced 会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。启用 Dor 资源的应用层 Dor Dor Dor DoDor 后，ShieldAdvidently 将再次为您创建与服务相关的角色。

编辑 ShieldAdvidently 的服务相关角色

ShieldAdvidently 不允许您编辑 AWSServiceRoleForAWSShield 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 Shield Advidently 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，您必须先清除服务相关角色的资源，然后才能手动删除它。

Note

在您尝试删除资源时，如果 ShieldAdvidently 正在使用该角色，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。

删除 Shield Advanced 使用的盾牌高级资源AWSServiceRoleForAWSShield

对于配置了应用层 DDoS 保护的所有资源，禁用自动应用层 DDoS 缓解。有关控制台的说明，请参见[配置应用层 DDoS 保护 \(p. 365\)](#)。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台，即 Amazon CLI 或 Amazon API 来删除 AWSServiceRoleForAWSShield 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](#)。

Shield高级服务相关角色支持的区域

ShieldAdvidently 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，请参见 [Shield高级终端节点和配额](#)。

中的日志记录和监控

监控是维护 Shield 和您的可靠性、可用性和性能的重要环节。Amazon。你应该从你的所有部分收集监控数据。Amazon 使用解决方案，您可以更轻松地调试出现的多点故障。Amazon 提供了多种工具来监控 Shield 资源并对潜在的事件做出响应：

亚马逊 CloudWatch Alarms

使用 CloudWatch 使用警报，您可在指定时间段内监控某个指标。如果指标超出给定阈值，CloudWatch 发送通知到 Amazon SNS 主题或 Amazon Auto Scaling 政策。有关更多信息，请参阅 [使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。

Amazon CloudTrail 日志

CloudTrail 提供了用户、角色或用户所执行操作的记录。AmazonShield 中的服务。通过使用 CloudTrail 收集的信息，您可以确定向 Shield 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。有关更多信息，请参阅 [使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)。

的合规性验证

作为多个计划的一部分，第三方审计员将评估 Shield 的安全Amazon合规性计划，如 SOC、PCI、FedRAMP、HIPAA 及其他计划。

有关特定合规性计划范围内的Amazon服务的列表，请参阅[合规性计划范围内的Amazon服务](#)。有关一般信息，请参阅[Amazon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[下载 Amazon Artifact 中的报告](#)。

您在使用 Shield 时的合规性责任由您数据的敏感性、您组织的合规性目标以及适用的法律法规决定。如果您对 Shield 的使用需遵守 HIPAA、PCI 或 FedRAMP 等标准，Amazon提供了以下实用资源：

- [《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上部署基于安全性和合规性的基准环境的步骤。
- [HIPAA 安全性和合规性架构设计白皮书](#)— 本出版物介绍了公司如何使用Amazon以创建符合 HIPAA 要求的应用程序。
- [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](#) – 此Amazon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架构完善的框架](#)— 该Amazon架构完善的框架可帮助您构建安全的云应用程序。

Shield 中的弹性

Amazon全球基础设施围绕Amazon Web Services 区域和可用区构建。Amazon Web Services 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。

有关Amazon Web Services 区域和可用区的更多信息，请参阅[Amazon全球基础设施](#)。

Amazon Shield 中的基础设施安全性

作为托管服务，Amazon Shield受保护Amazon中介绍的全局网络安全程序[Amazon Web Services : 安全过程概述](#)。

你用Amazon使用发布的 API 调用通过网络访问 Shield。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 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，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用[Amazon Security Token Service](#) (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon Shield Advanced 配额

Amazon Shield Advanced对每个区域、实体数施加了默认配额。您可以[请求提高](#)这些配额。

资源	默认配额
每种资源类型的最大受保护资源数Amazon Shield Advanced对每个账户的保护了。	1000
每个账户的最大保护组数施加了最大数量。	100

资源	默认配额
可以明确包含在保护组中的单个受保护资源的最大数量。在 API 中，这适用于Members您在设置保护组时指定的Pattern到ARBITRARY. 在控制台中，这适用于您为保护分组选择的资源从受保护的资源中选择.	1000

Amazon Firewall Manager

Amazon Firewall Manager 简化您在多个账户和资源上的管理和维护任务，以提供各种保护，包括 Amazon WAF、Amazon VPC 安全组、Amazon Route 53 解析器 DNS 防火墙、Amazon Shield Advanced 和 Amazon Network Firewall。使用 Firewall Manager，您只需设置一次保护，即使您添加新账户和资源，该服务也会自动跨账户和资源应用您的保护。

Firewall Manager 提供了以下优势：

- 有助于跨账户保护资源
- 帮助保护特定类型的所有资源，例如所有亚马逊 CloudFront 发行版
- 有助于保护带特定标签的所有资源
- 自动向已添加到您账户的资源添加防护
- 允许您让 Amazon Organizations 组织中的所有成员账户订阅 Amazon Shield Advanced，并自动让新加入组织的范围内账户进行订阅
- 允许您将安全组规则应用到 Amazon Organizations 组织中的所有成员账户或特定账户子集，并自动将这些规则应用到新加入组织的范围内账户
- 允许您使用自己的规则，或者从 Amazon Web Services Marketplace 购买托管规则

如果要保护整个组织，而不是少量特定账户和资源，或者经常添加要保护的新资源，Firewall Manager 尤其有用。Firewall Manager 还提供对整个组织的 DDoS 攻击的集中监控。

主题

- [Amazon Firewall Manager 定价 \(p. 403\)](#)
- [Amazon Firewall Manager 先决条件 \(p. 403\)](#)
- [管理 Amazon Firewall Manager 策略 \(p. 406\)](#)
- [了解 Amazon Firewall Manager \(p. 408\)](#)
- [使用 Amazon Firewall Manager 策略 \(p. 422\)](#)
- [在 Firewall Manager 中使用资源集 \(p. 466\)](#)
- [查看 Amazon Firewall Manager 策略的合规性信息 \(p. 467\)](#)
- [Amazon Firewall Manager 结果 \(p. 469\)](#)
- [Amazon Firewall Manager 中的安全性 \(p. 472\)](#)
- [Amazon Firewall Manager 配额 \(p. 497\)](#)

Amazon Firewall Manager 定价

Amazon Firewall Manager 产生的费用是针对底层服务（如 Amazon WAF 和 Amazon Config）的。有关更多信息，请参阅 [Amazon Firewall Manager 定价](#)。

Amazon Firewall Manager 先决条件

本主题向您展示如何做好管理准备 Amazon Firewall Manager。您可以使用一个 Firewall Manager 管理员帐户来管理组织中的所有 Firewall Manager 安全策略 Amazon Organizations。除非另有说明，否则请使用您作为 Firewall Manager 管理员使用的帐户执行先决条件。

首次使用 Firewall Manager 之前，请按顺序执行以下步骤。

主题

- [第第：加入和配置Amazon Organizations \(p. 404\)](#)
- [步骤 2：设置 Amazon Firewall Manager 管理员账户 \(p. 404\)](#)
- [步骤 3：启用 Amazon Config \(p. 404\)](#)
- [步骤 4：对于第三方政策，请在Amazon Marketplace 中订阅并配置第三方设置 \(p. 405\)](#)
- [步骤 5：对于Network Firewall 和 DNS 防火墙策略，启用资源共享 \(p. 406\)](#)
- [第第：Amazon Firewall Manager在默认禁用的区域中使用 \(p. 406\)](#)

第第：加入和配置Amazon Organizations

要使用Firewall Manager，您的账户必须是您要使用Firewall Manager 策略的Amazon Organizations服务中的组织的成员。

Note

有关Organizations 信息，请参阅 [《Amazon Organizations用户指南》](#)。

建立所需的成员Amazon Organizations资格和配置

1. 在“Organizations” 中选择一个帐户作为该组织的Firewall Manager 管理员。
2. 如果您选择的账户还不是该组织的成员，请让它加入。按照[邀请和加入您的组织中的指导Amazon Web Services 账户进行操作](#)。
3. Amazon Organizations 有两个可用的功能集：整合账单功能和所有功能。要使用Firewall Manager，您的组织必须启用所有功能。如果您的组织仅配置为整合账单，请按照在[组织中启用所有功能中的指南进行操作](#)。

步骤 2：设置 Amazon Firewall Manager 管理员账户

此过程使用您在前面的步骤中选择和配置的帐户和组织。

设置Firewall Manager 管理员帐户时，Firewall Manager 会自动将其设置为防火墙管理器的Amazon Organizations委派管理员。这允许FiFirewall Manager atzatl dits dits dits dits dits dits 您可以使用 OU 来指定Firewall Manager 策略的范围。有关设置策略范围的更多信息，请参阅下方针对各个策略类型的指南[创建 Amazon Firewall Manager 策略 \(p. 422\)](#)。有关组织和管理帐户的更多信息，请参阅[管理Organizations 中的Amazon帐户](#)。

设置Firewall Manager 管理员帐户

1. Amazon Web Services Management Console使用现有的Amazon Organizations管理账户登录。
2. 通过以下网址打开 Firewall Manager 控制台：<https://console.amazonaws.cn/wafv2/fmsv2>。
3. 选择开始使用。
4. 键入您选择用作Firewall Manager 管理员的帐户的 ID。

Note

此账户被授予在组织内所有账户中创建和管理Firewall Manager 策略的权限。

5. 选择 Set administrator (设置管理员)。

有关管理 FiFirewall Manager 管理员帐户的更多信息，请参阅[管理管理Amazon Firewall Manager 员 \(p. 406\)](#)。

步骤 3：启用 Amazon Config

要使用Firewall Manager，您必须启用Amazon Config。

Note

根据 Amazon Config 定价，您的 Amazon Config 设置会产生费用。有关更多信息，请参见 [Amazon Config 入门](#)。

为Firewall Manager 启用Amazon Config

1. Amazon Config为您的每个Amazon Organizations成员帐户启用，包括Firewall Manager 管理员帐户。有关更多信息，请参见 [Amazon Config 入门](#)。
2. Amazon Config为每个Amazon Web Services 区域包含您要保护的资源的资源启用。您可以Amazon Config手动启用，也可以使用[Amazon CloudFormation StackSets 示例Amazon CloudFormation模板中的“启用Amazon Config”模板](#)。

如果您不想Amazon Config为所有资源启用，则必须根据您使用的Firewall Manager 策略类型启用以下选项：

- WAF 策略 — 为资源类型启用Config：CloudFront 分配、Application Load Balancer（从列表中选择 ElasticLoadBalancingV2）、API Gateway、WAF WebACL、WAF 区域 WebACL 和 WAFv2 WebACL。Amazon Config要启用 CloudFront 发行版，您必须位于美国东部（弗吉尼亚北部）区域。其他地区没有 CloudFront 选项。
- Shield 策略 — 为保护保护、ShieldRegional 保护、Application Load Balancer、EC2 EIP、WAF WebACL、WAF 区域 WebACL 和 WAFv2 WebACL 等资源类型启用Config。
- 安全组策略 — 为 EC2 SecurityGroup、EC2 实例和 EC2 资源类型启用ConfigNetworkInterface。
- Network Firewall 策略 — 为资源类型 NetworkFirewall FirewallPolicy、EC2 VPC NetworkFirewallRuleGroup、EC2 InternetGateway、EC2 和 EC2 RouteTable 子网启用Config。
- DNS 防火墙策略 — 为资源类型 EC2 VPC 启用Config。
- 第三方防火墙策略 — 为 Amazon EC2 VPC、Amazon EC2、Amazon EC2 InternetGateway、Amazon EC2 RouteTable 子网和Amazon EC2 vpcendPoint 资源类型启用Config。

步骤 4：对于第三方政策，请在Amazon Marketplace 中订阅并配置第三方设置

完成以下先决条件即可开始使用 Firewall Manager 第三方防火墙策略。

Fortigate 云原生防火墙 (CNF) 即服务策略先决条件

将 Fortigate CNF 用于Firewall Manager

1. 在Marketplace 上订阅 [Fortigate 云原生防火墙 \(CNF\) 即服务](#) 服务。
2. 首先，在Fortigate CNF产品门户上注册租户。然后在 Fortigate CNF 产品门户上将您的Firewall Manager 管理员帐户添加到您的租户下。有关更多信息，请参阅 [Fortigate CNF文档](#)。

有关使用 Fortigate CNF策略的信息，请参阅[Fortigate 云原生防火墙 \(CNF\) 即服务策略 \(p. 464\)](#)。

帕洛阿尔托网络云下一代防火墙政策先决条件

使用 Palo Alto Networks Cloud NGFW 作为Firewall Manager

1. 在Marketplace 上订阅 [Palo Alto Networks云下一代防火墙即用即付](#) 服务。
2. 使用 Palo Alto Networks 云下一代防火墙部署指南中的Amazon Firewall Manager主题，完成 [Deploy Palo Alto Networks Cloud NGFW](#) 中列出的帕洛阿尔托网络云 NGFWAmazon 部署步骤。Amazon

有关使用 Palo Alto Networks Cloud NGFW 策略的信息，请参阅[帕洛阿尔托网络云 NGFW 政策 \(p. 464\)](#)。

步骤 5：对于 Network Firewall 和 DNS 防火墙策略，启用资源共享

要管理 Firewall Manager Network Firewall 和 DNS 防火墙策略，必须启用与 Amazon Organizations 中的共享 Amazon Resource Access Manager。这样，当您创建这些策略类型时，Firewall Manager 可以在您的账户中部署保护。

启用与 inAmazon Organizations 的共享 Amazon Resource Access Manager

- 按照《Amazon Resource Access Manager 用户指南》中的[“启用与共享”](#) Amazon Organizations 中的指导进行操作。

如果您在资源共享方面遇到问题，请参阅上的指南[Network Firewall 和 DNS 防火墙策略的资源共享 \(p. 465\)](#)。

第第：Amazon Firewall Manager 在默认禁用的区域中使用

要在默认情况下禁用的区域中使用 Firewall Manager，必须同时为 Amazon 组织的管理账户和 Firewall Manager 管理员账户启用该区域。

有关默认情况下禁用的区域以及如何启用它们的信息，请参阅 Amazon 一般参考 Amazon Web Services 区域中的[管理](#)。

启用禁用区域

- 对于 Organizations 管理账户和 Firewall Manager 管理员账户，请按照《Amazon 一般参考》中的[“启用区域”](#) 中的指导进行操作。

完成这些步骤后，您可以配置 Firewall Manager 以开始保护您的资源。有关更多信息，请参阅[Amazon Firewall Manager Amazon WAF 政策入门 \(p. 408\)](#)。

管理管理 Amazon Firewall Manager 员

您可以使用 Firewall Manager 管理员账户来管理您的 Firewall Manager 策略。设置 Firewall Manager 管理员账户时，Firewall Manager 会自动将其设置为防火墙管理器的 Amazon Organizations 委派管理员。这允许 Firewall Manager 访问有关组织单位 (OU) 的信息，这些组织单位 (OU) 用于指定 Firewall Manager 策略的范围。有关组织和管理账户的更多信息，请参阅[管理 Organizations 中的 Amazon 帐户](#)。

要开始使用 Firewall Manager，您需要设置 Firewall Manager 管理员账户并执行其他必需的步骤。为此，请遵循以下指南[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

本主题提供有关管理现有管理员账户的信息和指导。

Firewall Manager 管理员所需的设置

Firewall Manager 管理员账户必须具有以下设置：

- 它必须是您要在 Amazon Organizations 其中应用 Firewall Manager 策略的组织成员。

- 必须由组织的 Organizations 管理帐户将其指定为 Firewall Manager 管理员。

更改Amazon Firewall Manager管理员账户

要使用Amazon Firewall Manager，必须使用 Firewall Manager 管理员帐户登录控制台。您只能指定组织中的一个账户作为 Firewall Manager 管理员账户。

要首次设置管理员账户，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

将一个帐户指定为管理员帐户后，如果以后要将其他帐户指定为管理员帐户，请执行以下步骤。

Important

要指定另一个账户，您首先必须从当前管理员账户中撤销管理员权限。当您撤销权限时，由该账户创建的所有 Firewall Manager 策略都将删除。然后，您必须使用Amazon Organizations管理帐户登录 Firewall Manager 才能指定新的管理员帐户。

指定另一个账户作为 Amazon Firewall Manager 管理员账户（控制台）

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。
2. 在导航窗格中，选择 Settings (设置)。
3. 选择 Revoke administrator account (撤销管理员账户)。

Important

当您从当前管理员账户中撤销管理员权限时，由该账户创建的所有 Firewall Manager 策略都将删除。

4. 注销 Amazon Web Services Management Console。
5. Amazon Web Services Management Console使用您的Amazon Organizations管理账户登录。您可以使用该账户的根用户凭证登录 (不推荐)，也可以使用该账户内具有同等权限的 IAM 用户或 IAM 角色登录。
6. 通过以下网址打开 Firewall Manager 控制台：<https://console.amazonaws.cn/wafv2/fmsv2>。
7. 选择开始使用。
8. 键入要与 Firewall Manager 关联的账户 ID。此账户将是新的 Firewall Manager 管理员账户。

Firewall Manager 为您提供的成员帐户设置相应的权限。

Note

该账户被授予在组织内所有账户中创建和管理Amazon WAF规则、规则组和Amazon WAF经典规则的权限。

9. 选择 Set administrator (设置管理员)。

取消Amazon Firewall Manager管理员帐户更改的资格

对Amazon Firewall Manager管理员帐户的某些更改可能会使其失去保留管理员帐户的资格。

本节介绍可能取消Firewall Manager 管理员帐户资格的更改，以及Firewall Manager 如何Amazon处理这些更改。

账户已从组织中删除Amazon Organizations

如果将Amazon Firewall Manager管理员帐户从组织中删除Amazon Organizations，则该帐户将无法再管理该组织的策略。Firewall Manager 以下操作

- 账户已关闭

- Amazon将撤销该账户对防火墙管理访问权限，并且 Firewall Manager 将撤销该帐户管理的任何策略。这些策略提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的提供的
- Amazon将在管理员账户关闭之日起 90 天内保留该账户的策略数据 90 天内保留该账户的策略数据 90 天内保留该账户的策略数据 90 天内保留该账户的在这90天内，您可以重新打开已关闭的账户。
 - 如果您在 90 天内重新打开关闭的账户，就会将该账户重新Amazon分配为Firewall Manager 火并恢复该账户的Firewall Manager 策略数据。
 - 否则，在 90 天期限结束时，会Amazon永久删除该账户的所有策略数据。

您可以使用Amazon Firewall Manager来启用许多不同类型的安全策略。进行设置的步骤对于每一项略有不同。

- [Amazon Firewall ManagerAmazon WAF政策入门 \(p. 408\)](#)
- [开始使用Amazon Firewall Manager Amazon Shield Advanced策略 \(p. 410\)](#)
- [开始使用Amazon Firewall ManagerAmazon VPC 安全组策略 \(p. 413\)](#)
- [开始使用Amazon Firewall Manager Amazon Network Firewall策略 \(p. 415\)](#)
- [开始使用Amazon Firewall ManagerDNS 防火墙策略 \(p. 416\)](#)
- [开始使用Amazon Firewall Manager帕洛阿尔托网络云下一代防火墙政策 \(p. 418\)](#)
- [Amazon Firewall ManagerFortigate CNF 政策入门 \(p. 420\)](#)

主题

- ## 步骤 1：完成先决条件

408

步骤 2：创建并应用Amazon WAF策略

Firewall ManagerAmazon WAF 策略包含要应用于资源的规则组。Firewall Manager 会在您应用策略的每个帐户中创建Firewall Manager Web ACL。除了您在此处定义的规则组之外，各个客户经理还可以向生成的Web ACL 中添加规则和规则组。有关Firewall ManagerAmazon WAF 策略的信息，请参阅[Amazon WAF 策略 \(p. 444\)](#)。

创建Firewall ManagerAmazon WAF 策略 (控制台)

1. Amazon Web Services Management Console使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Amazon WAF。
5. 对于“区域”，选择Amazon Web Services 区域。要保护亚马逊的 CloudFront分销，请选择“全球”。

要保护多个区域 (CloudFront 分布除外) 中的资源，必须为每个区域创建单独的 Firewall Manager 策略。

6. 选择 Next (下一步)。
7. 对于 Policy (策略名称)，输入一个描述性名称。Firewall Manager 在其管理的 Web ACL 的名称中包含策略名称。Web ACL 名称FMManagedWebACLV2-后面是您在此处输入的策略名称，以及以 UTC 毫秒为单位的 Web ACL 创建时间戳。-例如，FMManagedWebACLV2-MyWAFPolicyName-1621880374078。
8. 在 Policy rules (策略规则) 下的 First rule groups (最先运行的规则组) 中，选择 Add rule groups (添加规则组)。扩展托管Amazon管规则组。对于 Core rule set (核心规则集)，切换 Add to web ACL (添加到 Web ACL)。对于Amazon已知的错误输入，请切换“添加到 Web ACL”。选择 Add rules (添加规则)。

对于 Last rule groups (最后运行的规则组)，请选择 Add rule groups (添加规则组)。展开Amazon托管规则组，对于 Amazon IP 信誉列表，切换到 Web ACL。选择 Add rules (添加规则)。

在“第一个规则组”下，选择“核心规则集”，然后选择“下移”。Amazon WAF先根据Amazon已知的错误输入规则组评估 Web 请求，然后再根据核心规则集进行评估。

Note

如果需要，您还可以使用 Amazon WAF 控制台创建自己的 Amazon WAF 规则组。您创建的任何规则组都会显示在“描述策略：添加规则组”页面的“您的规则组”下。

您通过 Firewall Manager 管理的第一个和最后一个Amazon WAF规则组的名称分别以PREFMManaged-或POSTFMManaged-开头，后跟Firewall Manager 策略名称和规则组创建时间戳 (以 UTC 毫秒为单位)。例如，PREFMManaged-MyWAFPolicyName-1621880555123。

9. 将 Web ACL 的默认操作保留为 Allow (允许)。
10. 将 Policy action (策略操作) 保留为默认状态，以便不会自动修复不合规的资源。您随后可以更改此选项。
11. 选择 Next (下一步)。
12. 对于 Policy scope (策略范围)，您可以提供用于标识要应用策略的资源的账户、资源类型和标签设置。在本教程中，保留Amazon Web Services 账户和资源设置，然后选择一种或多种资源类型。
13. 选择 Next (下一步)。
14. 对于策略标记，您可以为 Firewall ManagerAmazon WAF 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。在本教程中，您可以将此选项保留为默认设置。

15. 选择 Next (下一步)。
16. 查看新策略。您可以通过在要更改的区域中选择 Edit (编辑) 进行更改。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

第 3 步：清除

为了避免产生不必要的费用，请删除任何非必要的策略和资源。

删除策略 (控制台)

1. 在 Policies (Amazon Firewall Manager策略) 页面上，选择策略名称旁边的单选按钮，然后选择 Delete (删除)。
2. 在 Delete (删除) 确认框中，选择 Delete all policy resources (删除所有策略资源)，然后再次选择 Delete (删除)。

Amazon WAF 会删除策略及其在您的账户中创建的任何关联资源 (如 Web ACL)。更改可能需要几分钟才能传播到所有账户。

开始使用Amazon Firewall Manager Amazon Shield Advanced策略

您可以使用Amazon Firewall Manager启用Amazon Shield Advanced整个组织的保护。

Important

Firewall Manager 不支持亚马逊 Route 53 或Amazon Global Accelerator. 如果您需要使用 Shield Advanced 保护这些资源，则不能使用Firewall Manager 策略。而是应按照[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)中的说明操作。

要使用Firewall Manager 启用 Shield 高级保护，请按顺序执行以下步骤。

主题

- [第 1 步：完成先决条件 \(p. 410\)](#)
- [第 2 步：创建并应用 Shield Advanced 策略 \(p. 410\)](#)
- [第 3 步：\(可选 \) 授权Shield 响应小组 \(SRT\) \(p. 412\)](#)
- [第 4 步：配置 Amazon SNS 通知和Amazon CloudWatch 警报 \(p. 412\)](#)

第 1 步：完成先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager先决条件 \(p. 403\)](#)介绍了这些步骤。在继续执行[第 2 步：创建并应用 Shield Advanced 策略 \(p. 410\)](#)之前，请满足所有先决条件后。

第 2 步：创建并应用 Shield Advanced 策略

完成先决条件后，您创建一个Amazon Firewall ManagerShield Shield S Firewall Manager Shield Advanced 策略包含你想要使用 Shield Advanced 保护的账户和资源。

Important

Firewall Manager 不支持 Amazon Route 53 或Amazon Global Accelerator. 如果您需要使用 Shield Advanced 保护这些资源，则不能使用Firewall Manager 策略。而是应按照[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)中的说明操作。

创建 Firewall Manager Shield Shield

1. 登录Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户，然后打开 Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>.

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于策略类型，选择Shield Advanced.

要创建 Shield Advanced 策略，你的Firewall Manager 管理员账户必须订阅 Shield Advanced。如果您尚未订阅，则会提示您订阅。有关订阅成本的信息，请参阅[Amazon Shield Advanced定价](#)。

Note

无需手动为每个成员账户订阅 Shield Shield Shield Shield Firewall Manager 在创建策略时会为您执行此操作。

5. 对于区域，请选择一个Amazon Web Services 区域。为了保护亚马逊 CloudFront 资源，选择服务全球。

保护多个区域（除外）中的资源 CloudFront 资源），则必须为每个区域创建单独的Firewall Manager 策略。

6. 选择 Next (下一步)。
7. 对于名称，输入一个描述性名称。
8. （仅限全球区域）适用于服务全球区域策略，你可以选择是否要管理 Shield Advanced 自动应用层 DDoS 缓解措施。在本教程中，将此选项保留为默认设置Ignore。
9. 对于策略操作，请选择不会自动修复的选项。
10. 选择 Next (下一步)。
11. Amazon Web Services 账户本政策适用于允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 Include all accounts under my organization (包括我的组织下的所有账户)。
12. 选择要保护的资源的类型。

Firewall Manager 不支持亚马逊 Route 53 或Amazon Global Accelerator. 如果您需要使用 Shield Advanced 保护这些资源，则不能使用Firewall Manager 策略。相反，请按照Shield 高级指导进行操作[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)。

13. 如果您只想保护带有特定标签的资源，或者要排除带有特定标签的资源，请选择使用标签来包含/排除资源，输入用逗号分隔的标签，然后选择其中一个Include要么Exclude. 您只能选择一个选项。

如果您输入多个标签，并且资源具有这些标签中的任何一个，则将其视为匹配项。

有关标签的更多信息，请参阅[使用标签编辑器](#)。

14. 选择 Next (下一步)。
15. 对于策略标签，为Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
16. 选择 Next (下一步)。
17. 查看新策略。要进行任何更改，请选择 Previous (上一步)。若您满意所创建的策略，请选择 Create policy (创建策略)。

继续浏览 [第 3 步：（可选）授权Shield 响应小组 \(SRT\) \(p. 412\)](#)。

第 3 步：（可选）授权 Shield 响应小组 (SRT)

的好处之一 Amazon Shield Advanced 是 Shield 反应小组 (SRT) 的支持。当您遇到潜在的 DDoS 攻击时，可以联系 [Amazon Web Services Support 中心](#)。如有必要，Support 中心会将您的问题上报给 SRT。SRT 可帮助您分析可疑活动并帮助您缓解问题。缓解措施通常涉及在您的账户中创建或更新 Amazon WAF 规则和 Web ACL。SRT 可以检查您的 Amazon WAF 配置并创建或更新 Amazon WAF 规则和 Web ACL 可供您使用，但团队需要您的授权才能这样做。我们建议将其作为设置的一部分 Amazon Shield Advanced，您主动向 SRT 提供所需的授权。提前提供授权有助于防止在实际发生攻击时耽误问题的解决。

您已在账户级别授权并联系 SRT。也就是说，必须由账户所有者（而非 Firewall Manager 管理员）执行以下步骤以授权 SRT 来缓解潜在攻击。Firewall Manager 管理员只能为自己拥有的帐户授权 SRT。同样，只有账户所有者可以联系 SRT 寻求支持。

Note

要使用 SRT 的服务，您必须订阅 [业务 Support 计划](#) 或者 [“企业” Support 计划](#)。

要授权 SRT 代表您缓解潜在攻击，请按照中的说明进行操作 [Shield 响应小组 \(SRT\) 支持 \(p. 348\)](#)。您可以使用相同的步骤随时更改 SRT 访问和权限。

继续浏览 [第 4 步：配置 Amazon SNS 通知和 Amazon CloudWatch 警报 \(p. 412\)](#)。

第 4 步：配置 Amazon SNS 通知和 Amazon CloudWatch 警报

您可以使用 Amazon SNS 监控您的受保护资源是否存在潜在的 DDoS 活动。要接收可能的攻击通知，请为每个区域创建一个 Amazon SNS 主题。

在 Firewall Manager（控制台）中创建 Amazon SNS 主题

1. 登录 Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户，然后打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，在导航窗格中 Amazon FMS，选择设置。
3. 选择 Create new topic (创建新主题)。
4. 输入主题名称。
5. 输入要将 Amazon SNS 消息发送到的电子邮件地址，然后选择添加电子邮件地址。
6. 选择 Update SNS configuration (更新 SNS 配置)。

配置 Amazon CloudWatch 警报

Shield Advanced 在 CloudWatch 你可以监控。有关更多信息，请参阅 [Amazon Shield Advanced 指标和警报 \(p. 506\)](#)。CloudWatch 会产生额外费用。对于 CloudWatch 定价，请参阅 [亚马逊 CloudWatch 定价](#)。

创建集群 CloudWatch 告警，请按照中的说明操作 [使用 Amazon CloudWatch 警报](#)。默认情况下，Shield Advanced 配置 CloudWatch 仅在出现一个潜在的 DDoS 事件迹象后提醒您。如果需要，您可以使用 CloudWatch 控制台来更改此设置，以便在检测到多个提示信号时再通知您。

Note

除了警报之外，您还可以使用 CloudWatch 控制面板用于监控潜在的 DDoS 活动。控制面板，可从 Shield Shield Shield Shield Shield Shield 你可以在亚马逊使用统计数据 CloudWatch 了

解您的 Web 应用程序或服务的执行情况。有关更多信息，请参阅 [什么是 CloudWatch](#) 在亚马逊 CloudWatch 用户指南。

有关创建 CloudWatch 控制面板，请参阅 [使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。有关您可以添加到控制面板的特定 Shield Advanced 指标的信息，请参阅 [Amazon Shield Advanced 指标和警报 \(p. 506\)](#)。

您可以继续执行此步骤，而无需配置 Amazon SNS 通知或 CloudWatch 告警。但是，这样做会显著降低对 DDoS 事件的可见性。

完成 Shield Advanced 配置后，请熟悉一下查看事件的选项 [对 DDoS 事件的可见性 \(p. 369\)](#)。

开始使用 Amazon Firewall Manager Amazon VPC 安全组策略

要使用 Amazon Firewall Manager 要在您的组织中启用 Amazon VPC 安全组，请按顺序执行以下步骤。

主题

- [第 1 步：完成先决条件 \(p. 413\)](#)
- [第 2 步：创建要在您的策略中使用的 Amazon VPC 安全组 \(p. 413\)](#)
- [第 3 步：创建、应用通用安全组策略 \(p. 413\)](#)

第 1 步：完成先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager 先决条件 \(p. 403\)](#) 介绍了这些步骤。在继续执行 [第 2 步：创建要在您的策略中使用的 Amazon VPC 安全组 \(p. 413\)](#) 之前，请满足所有先决条件后。

第 2 步：创建要在您的策略中使用的 Amazon VPC 安全组

在此步骤中，您将创建一个可以使用 Firewall Manager 在整个组织中应用的安全组。

Note

在本教程中，您不将安全组策略应用到组织中的资源。您仅仅创建策略，并查看将策略的安全组应用到资源时会发生什么情况。您可以通过在策略上禁用自动修复来执行此操作。

如果您已经定义了通用安全组，请跳过此步骤并转到 [第 3 步：创建、应用通用安全组策略 \(p. 413\)](#)。

要创建 Firewall Manager 通用安全组策略

- 按照下面的指导，创建一个可以应用于组织中所有账户和资源的安全组 [您的 VPC 的安全组](#) 在里面 [Amazon VPC User Guide](#)。

有关安全组规则选项的信息，请参阅 [安全组规则参考](#)。

您现在已准备好转到 [第 3 步：创建、应用通用安全组策略 \(p. 413\)](#)。

第 3 步：创建、应用通用安全组策略

满足先决条件后，您将创建 Amazon Firewall Manager 通用安全组策略。通用安全组策略为您的整个 Amazon 组织提供集中控制的安全组。它还定义了 Amazon Web Services 账户以及安全组所适用的资源。除了常见的安全组策略外，Firewall Manager 还支持内容审计安全组策略（用于管理组织中使用的

安全组规则) 和使用审计安全组策略 (管理未使用和冗余的安全组)。有关更多信息, 请参阅 [安全组策略 \(p. 452\)](#)。

对于本教程, 您将创建通用安全组策略并将其操作设置为不自动修复。这使您可以查看策略将产生的效果而不对 Amazon 组织进行更改。

创建 Firewall Manager 通用安全组策略 (控制台)

1. 登录Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户, 然后打开 Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息, 请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中, 选择 Security policies (安全策略)。
3. 如果您未满足先决条件, 控制台会显示有关如何解决任何问题的说明。按照说明操作, 然后返回此步骤以创建通用安全组策略。
4. 选择 Create policy (创建策略)。
5. 对于 Policy type (策略类型), 选择 Security group (安全组)。
6. 对于 Security group policy type (安全组策略类型), 选择 Common security groups (通用安全组)。
7. 对于区域, 请选择一个Amazon Web Services 区域。
8. 选择 Next (下一步)。
9. 对于策略名称, 输入一个描述性名称。
10. Policy rules (策略规则) 选项允许您选择如何应用和维护此策略中的安全组。在本教程中, 不要选中这些选项。
11. 选择 Add primary security group (添加主安全组), 选择您为本教程创建的安全组, 然后选择 Add security group (添加安全组)。
12. 对于 Policy action (策略操作), 请选择 Identify resources that don't comply with the policy rules, but don't auto remediate (确定不符合策略规则的资源, 但不自动修复)。
13. 选择 Next (下一步)。
14. Amazon Web Services 账户受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程, 选择 Include all accounts under my organization (包括我的组织下的所有账户)。
15. 对于 Resource type (资源类型), 根据为您的 Amazon 组织定义的资源, 选择一个或多个类型。
16. Resources (资源) 允许您通过指定要包含还是排除的资源标签, 缩小策略的范围。要使用标签, 您需要先标记资源。有关标记资源的更多信息, 请参阅[使用标签编辑器](#)。对于本教程, 选择 Include all resources that match the selected resource type (包括与所选资源类型匹配的所有资源)。
17. 选择 Next (下一步)。
18. 查看您的策略设置。进行检查以确保 Policy actions (策略操作) 设置为 Identify resources that don't comply with the policy rules, but don't auto remediate (确定不符合策略规则的资源, 但不自动修复)。这使您可以检查策略所要进行的更改, 但此时不进行更改。
19. 选择 Create policy (创建策略)。

在里面Amazon Firewall Manager策略窗格中, 您的策略已列出。它可能会在账户标题下指示 Pending (待处理), 并支持禁用 Automatic remediation (自动修复)。策略的创建可能需要几分钟的时间。当 Pending (待处理) 状态替换为账户计数时, 您可以选择策略名称来探索账户和资源的合规状态。有关信息, 请参阅 [查看Amazon Firewall Manager策略的合规性信息 \(p. 467\)](#)

20. 在探索完成后, 如果您不希望保留为本教程创建的策略, 请依次选择策略名称、Delete (删除)、Clean up resources created by this policy (清除此策略创建的资源), 最后选择 Delete (删除)。

有关 Firewall Manager 安全组策略的更多信息, 请参阅[安全组策略 \(p. 452\)](#)。

开始使用Amazon Firewall Manager Amazon Network Firewall策略

要使用Amazon Firewall Manager要启用Amazon整个组织的Network Firewall 防火墙，按顺序执行以下步骤。有关Firewall Manager Network Firewall 策略的信息，请参阅[Amazon Network Firewall 策略 \(p. 457\)](#)。

主题

- [第 1 步：完成一般先决条件 \(p. 415\)](#)
- [第 2 步：创建要在策略中使用的Network Firewall 规则组 \(p. 415\)](#)
- [第 3 步：创建和应用Network Firewall 策略 \(p. 415\)](#)

第 1 步：完成一般先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager先决条件 \(p. 403\)](#)介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

第 2 步：创建要在策略中使用的Network Firewall 规则组

要完成本教程，您应熟悉以下内容Amazon Network Firewall并且知道如何配置其规则组和防火墙策略。

Network Firewall 中必须至少有一个规则组用于您的Amazon Firewall Manager策略。如果您尚未在Network Firewall 中创建规则组，请立即创建规则组。有关使用Network Firewall 的信息，请参阅[Amazon Network Firewall开发人员指南](#)。

第 3 步：创建和应用Network Firewall 策略

完成先决条件后，您创建一个Amazon Firewall ManagerNetwork Firewall 策略。Network Firewall 策略提供集中控制Amazon Network Firewall整个防火墙Amazon组织。它还定义了Amazon Web Services 账户以及防火墙适用的资源。

有关 Firewall Manager 如何管理Network Firewall 策略的更多信息，请参阅[Amazon Network Firewall 策略 \(p. 457\)](#)。

创建 Firewall Manager Network Firewall 策略

1. 登录Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户，然后打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 如果您未满足先决条件，控制台将显示有关如何修复任何问题的说明。按照说明进行操作，然后返回到此步骤，创建Network Firewall 策略。
4. 选择创建安全策略。
5. 对于 Policy type (策略类型)，选择 Amazon Network Firewall。
6. 对于区域，请选择一个Amazon Web Services 区域。
7. 选择 Next (下一步)。
8. 对于策略名称，输入一个描述性的名称。

- 策略配置允许您定义防火墙策略。这与您在中使用的过程相同Amazon Network Firewall控制台。您可以添加要在策略中使用的规则组，并提供默认的无状态操作。在本教程中，请像在Network Firewall 中配置防火墙中的防火墙策略一样配置此策略。

Note

自动修复会自动进行Amazon Firewall ManagerNetwork Firewall 策略，因此您不会在此处看到选择不auto 修复的选项。

- 选择 Next (下一步) 。
- 对于防火墙端点，选择多个防火墙端点。此选项为您的防火墙提供高可用性。创建策略时，Firewall Manager 会在每个公有子网需要保护的可用区中创建一个防火墙子网。
- 对于Amazon Network Firewall路由配置，选择显示器让 Firewall Manager 监控您的 VPC 是否存在路由配置违规情况，并提醒您提供补救建议，以帮助您使路由合规。（可选）如果您不想让 Firewall Manager 监控您的路由配置并接收这些警报，请选择Off。

Note

监控可为您提供有关由于路由配置错误而导致的不合规资源的详细信息，并建议Firewall Manager 采取补救措施GetViolationDetailsAPI。例如，如果流量未通过您的策略创建的防火墙端点进行路由，则Network Firewall 会提醒您。

Warning

如果选择显示器，您将无法将其更改为Offfuture 会采用同样的政策。您必须创建新策略。

- 对于流量类型，select添加到防火墙策略通过互联网网关路由流量。
- Amazon Web Services 账户受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 Include all accounts under my organization (包括我的组织下的所有账户)。
- 这些区域有：资源类型对于Network Firewall 策略始终为VPC。
- Resources (资源) 允许您通过指定要包含还是排除的资源标签，缩小策略的范围。要使用标签，您需要先标记资源。有关标记资源的更多信息，请参阅[使用标签编辑器](#)。对于本教程，选择 Include all resources that match the selected resource type (包括与所选资源类型匹配的所有资源)。
- 选择 Next (下一步) 。
- 检查您的策略设置，然后SELECT创建策略。

在Amazon Firewall Manager策略窗格中，您的策略已列出。策略的创建可能需要几分钟的时间。在创建过程完成之前，策略会显示其处于待处理状态。当策略准备就绪时，状态会随着范围内账户的数量而更新。您可以选择策略名称来浏览账户和资源的合规性状态。有关信息，请参阅[查看Amazon Firewall Manager策略的合规性信息 \(p. 467\)](#)

- 浏览完毕后，如果您不想保留为本教程创建的策略，请选择策略名称，选择Delete，选择清理此策略创建的资源。，最后选择Delete。

有关 Firewall Manager Network Firewall 策略的更多信息，请参阅[Amazon Network Firewall 策略 \(p. 457\)](#)。

开始使用Amazon Firewall ManagerDNS 防火墙策略

要使用Amazon Firewall Manager要在您的组织中启用 Amazon Route 53 解析器 DNS 防火墙，请按顺序执行以下步骤。有关Firewall Manager DNS 防火墙策略的信息，请参阅[Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)。

主题

- [第 1 步：完成一般先决条件 \(p. 417\)](#)
- [第 2 步：创建要在策略中使用的 DNS 防火墙规则组 \(p. 417\)](#)
- [第 3 步：创建和应用 DNS 防火墙策略 \(p. 417\)](#)

第 1 步：完成一般先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager 先决条件 \(p. 403\)](#) 介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

第 2 步：创建要在策略中使用的 DNS 防火墙规则组

要学习本教程，您应该熟悉 Amazon Route 53 解析器 DNS 防火墙并知道如何配置其规则组。

您必须在 DNS 防火墙中至少有一个规则组用于您的 Amazon Firewall Manager 策略。如果您尚未在 DNS 防火墙中创建规则组，请立即创建规则组。有关使用 DNS Firewall 的信息，请参阅[Amazon Route 53 Resolver](#)在[Amazon Route 53 开发](#)。

第 3 步：创建和应用 DNS 防火墙策略

完成先决条件后，您创建一个 Amazon Firewall Manager DNS 防火墙策略。DNS 防火墙策略为您的整个用户提供了集中控制的 DNS 防火墙规则组关联 Amazon 组织。它还定义了 Amazon Web Services 账户以及防火墙适用的资源。

有关 Firewall Manager 如何管理您的 DNS 防火墙规则组关联的更多信息，请参阅[Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)。

创建 Firewall Manager DNS Firewall 策略（控制台）

1. 登录 Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户，然后打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。
2. 在导航窗格中，选择 Security policies (安全策略)。
3. 如果您未满足先决条件，控制台将显示有关如何修复任何问题的说明。按照说明进行操作，然后返回到此步骤，创建 DNS 防火墙策略。
4. 选择创建安全策略。
5. 对于策略类型，选择 Amazon Route 53 Resolver。
6. 对于区域，请选择一个 Amazon Web Services 区域。
7. 选择 Next (下一步)。
8. 对于策略名称，输入一个描述性的名称。
9. 策略配置允许您定义要通过 Firewall Manager 管理的 DNS 防火墙规则组关联。您可以添加要在策略中使用的规则组。您可以定义一个关联，先为 VPC 进行评估，最后再定义一个关联。在本教程中，根据需要添加一个或两个规则组关联。
10. 选择 Next (下一步)。
11. Amazon Web Services 账户受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 Include all accounts under my organization (包括我的组织下的所有账户)。
12. 这些区域有：资源类型对于 DNS 防火墙策略始终是 VPC。
13. Resources (资源) 允许您通过指定要包含还是排除的资源标签，缩小策略的范围。要使用标签，您需要先标记资源。有关标记资源的更多信息，请参阅[使用标签编辑器](#)。对于本教程，选择 Include all resources that match the selected resource type (包括与所选资源类型匹配的所有资源)。
14. 选择 Next (下一步)。
15. 检查您的策略设置，然后选择创建策略。

在 Amazon Firewall Manager 策略窗格中，您的策略已列出。策略的创建可能需要几分钟的时间。在创建过程完成之前，策略会显示其处于待处理状态。当策略准备就绪时，状态会随着范围内账户的数量而更新。您可以选择策略名称来浏览账户和资源的合规性状态。有关信息，请参阅[查看 Amazon Firewall Manager 策略的合规性信息 \(p. 467\)](#)。

16. 浏览完毕后，如果您不想保留为本教程创建的策略，请选择策略名称，选择 Delete，选择清理此策略创建的资源，最后选择 Delete。

有关 Firewall Manager DNS Firewall 策略的更多信息，请参阅[Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)。

开始使用Amazon Firewall Manager帕洛阿尔托网络云下一代防火墙政策

要使用Amazon Firewall Manager要启用 Palo Alto Networks Cloud 下一代防火墙 (NGFW) 策略，请按顺序执行以下步骤。有关 Palo Alto Networks Cloud NGFW 政策的信息，请参阅[帕洛阿尔托网络云 NGFW 政策 \(p. 464\)](#)。

主题

- [第 1 步：完成一般先决条件 \(p. 418\)](#)
- [第 2 步：完成帕洛阿尔托网络云 NGFW 政策先决条件 \(p. 418\)](#)
- [第 3 步：创建并应用 Palo Alto Networks Cloud NGFW 政策 \(p. 418\)](#)

第 1 步：完成一般先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager先决条件 \(p. 403\)](#)介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

第 2 步：完成帕洛阿尔托网络云 NGFW 政策先决条件

要使用 Palo Alto Networks Cloud NGFW 政策，您还必须完成几个额外的强制性步骤。[帕洛阿尔托网络云下一代防火墙政策先决条件 \(p. 405\)](#)介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

第 3 步：创建并应用 Palo Alto Networks Cloud NGFW 政策

完成先决条件后，您创建一个Amazon Firewall Manager帕洛阿尔托网络云下一代防火墙政策。

有关 Palo Alto Networks Cloud NGFW 的Firewall Manager 策略的更多信息，请参阅[帕洛阿尔托网络云 NGFW 政策 \(p. 464\)](#)。

为 Palo Alto Networks Cloud NGFW (控制台) 创建Firewall Manager 策略

1. 登录Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户，然后打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于策略类型，选择帕洛阿尔托网络帕洛阿尔托网络云 NGFW. 如果你还没有订阅 Palo Alto Networks Cloud Networks NGFW 服务AmazonMarketplace，您需要先这样做。要订阅AmazonMarketplace查看AmazonMarketplace。
5. 对于部署模型，请选择以下任一项分布式模型要么集中式模型。部署模型决定了Firewall Manager 如何管理策略的端点。在分布式模式下，Firewall Manager 会在策略范围内的每个 VPC 中维护防火墙终端节点。在集中式模式下，Firewall Manager 在检查 VPC 中维护单个终端节点。
6. 对于区域，请选择一个Amazon Web Services 区域。要保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择 Next (下一步)。
8. 对于策略名称，输入一个描述性名称。

9. 在策略配置中，选择要与此策略关联的 Palo Alto Networks Cloud NGFW 防火墙策略。Palo Alto Networks Cloud NGFW 防火墙策略列表包含与您的 Palo Alto Networks Cloud NGFW 租户关联的所有帕洛阿尔托网络 Cloud NGFW 防火墙策略。有关创建和管理 Palo Alto Networks Cloud NGFW 防火墙策略的信息，请参阅[部署 Palo Alto 网络云 NGFWAmazon用Amazon Firewall Manager主题Palo Alto Networks Palo Alto NetworksAmazon部署指南](#)。
10. 对于 Palo Alto Networks Palo Alto Networks Cloud，可以选择为你的策略记录哪种 Palo Alto Networks Cloud NGFW 日志类型。有关 Palo Alto Networks Cloud NGFW 日志类型的信息，请参阅[配置 Palo Alto Networks Cloud NetworksAmazon](#)在里面Palo Alto Networks Palo Alto NetworksAmazon部署指南。

对于日志目标，请指定Firewall Manager 应在何时向其写入日志。

11. 选择 Next (下一步) 。
12. 下面配置第三方防火墙端点根据您是在使用分布式还是集中式部署模式创建防火墙端点，执行以下其中一项操作：
 - 如果您使用的是此策略的分布式部署模型，请在可用区，选择要在哪些可用区中创建防火墙终端节点。您可以通过以下方式选择可用区可用区名称或者通过可用区 ID。
 - 如果您使用此策略的集中部署模型，请在Amazon Firewall Manager终端节点配置下检查 VPC 配置，输入Amazon检查 VPC 的拥有者的账户 ID，以及检查 VPC 的 VPC ID。
 - 下面可用区，选择要在哪些可用区中创建防火墙终端节点。您可以通过以下方式选择可用区可用区名称或者通过可用区 ID。
13. 选择 Next (下一步) 。
14. 对于策略范围，在下Amazon Web Services 账户本政策适用于，请按如下方式选择选项：
 - 如果要将该策略应用于组织中的所有账户，请保留默认选项，包括我下的所有账户Amazon组织。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会自动根据您的设置评估任何新帐户。例如，如果您仅包括特定帐户，Firewall Manager 不会将该策略应用于任何新帐户。再举一个例子，如果您包括一个 OU，则当您向该 OU 或其任何子 OU 添加帐户时，Firewall Manager 会自动将策略应用于新帐户。

15. 这些区域有：资源类型对于Network Firewall 策略，则是VPC。
16. 对于 Resources (资源)，如果要仅保护 (或排除) 具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅[使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。
17. 对于授予跨账户访问权限，选择下载Amazon CloudFormation模板。这下载了Amazon CloudFormation 你可以用它来创建一个模板Amazon CloudFormation堆栈。这个堆栈创建了一个Amazon Identity and Access Management该角色授予Firewall Manager 跨账户权限来管理 Palo Alto Networks Cloud NGFW 资源。有关堆栈的信息，请参阅[使用堆栈](#)在里面Amazon CloudFormation用户指南。
18. 选择 Next (下一步) 。
19. 对于策略标签，为Firewall Manager 策略添加您想要的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
20. 选择 Next (下一步) 。
21. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

有关 Firewall Manager Palo Alto Networks Cloud NGFW 策略的更多信息，请参阅[帕洛阿尔托网络云 NGFW 策略 \(p. 464\)](#)。

Amazon Firewall ManagerFortigate CNF 政策入门

Fortigate 云原生防火墙 (CNF) 即服务是一项第三方防火墙服务，您可以将其用于您的 Amazon Firewall Manager 策略。使用 Fortigate CNF for Firewall Manager，您可以在所有 Amazon 账户中创建和集中部署 Fortigate CNF 资源和策略集。Amazon Firewall Manager 要使用启用 Fortigate CNF 策略，请按顺序执行以下步骤。有关 Fortigate CNF 政策的更多信息，请参阅[Fortigate 云原生防火墙 \(CNF\) 即服务策略 \(p. 464\)](#)。

主题

- [步骤 1：完成一般先决条件 \(p. 420\)](#)
- [第 2 步：完成 Fortigate CNF 策略先决条件 \(p. 420\)](#)
- [步骤 3：创建并应用 Fortigate CNF 策略 \(p. 420\)](#)

步骤 1：完成一般先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager 先决条件 \(p. 403\)](#) 介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

第 2 步：完成 Fortigate CNF 策略先决条件

要使用 Fortigate CNF 政策，还必须完成其他强制性步骤。[Fortigate 云原生防火墙 \(CNF\) 即服务策略先决条件 \(p. 405\)](#) 介绍了这些步骤。在继续下一步之前，请完成所有先决条件。

步骤 3：创建并应用 Fortigate CNF 策略

完成先决条件后，您可以创建 Amazon Firewall Manager Fortigate CNF 策略。

有关 Fortigate CNF 的 Firewall Manager 策略的更多信息，请参阅[Fortigate 云原生防火墙 \(CNF\) 即服务策略 \(p. 464\)](#)。

为 Fortigate CNF (控制台) 创建 Firewall Manager 策略

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于“策略类型”，选择 Fortigate CNF。如果您尚未在 Amazon Marketplace 中订阅 Fortigate CNF 服务，则需要先订阅。要在 Amazon Marketplace 中订阅，请选择查看 Amazon Marketplace 详情。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定了 Firewall Manager 如何管理策略的端点。使用分布式模型，Firewall Manager 在策略范围内的每个 VPC 中维护防火墙终端节点。使用集中式模型，Firewall Manager 在检查 VPC 中维护单个终端节点。
6. 对于“区域”，选择 Amazon Web Services 区域。要保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择 Next (下一步)。

- 8.
 9. 在策略配置中，选择要与此策略关联的 Fortigate CNF 防火墙策略。Fortigate CNF 防火墙策略列表包含与您的 Fortigate CNF 租户关联的所有 Fortigate CNF 防火墙策略。有关创建和管理 Fortigate CNF 防火墙策略的信息，请参阅 [Fortigate CNF 文档](#)。
 10. 选择 Next (下一步)。
 11. 在“配置第三方防火墙端点”下，执行以下操作之一，具体取决于您使用的是分布式部署模型还是集中部署模型来创建防火墙端点：
 - 如果您使用此策略的分布式部署模型，请在可用区下选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
 - 如果您使用此策略的集中部署模型，请在检查 VPC 配置下的 Amazon Firewall Manager 终端节点配置中，输入检查 VPC 所有者的 Amazon 账户 ID 和检查 VPC 的 VPC ID。
 - 在可用区下，选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
 12. 选择 Next (下一步)。
 13. 对于 Amazon Web Services 账户本策略适用的“策略范围”，选择以下选项：
 - 如果您想将该政策应用于组织中的所有帐户，请保留默认选择“包括我的 Amazon 组织下的所有帐户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 您只能选择其中一个选项。
- 应用策略后，Firewall Manager 会自动根据您的设置评估所有新帐户。例如，如果您仅包括特定帐户，则 Firewall Manager 不会将该策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您向该 OU 或其任何子 OU 添加帐户时，Firewall Manager 会自动将策略应用于新帐户。
14. Network Firewall 策略的资源类型为 VPC。
 15. 对于 Resources (资源)，如果要仅保护 (或排除) 具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅 [使用标签编辑器](#)。
- 如果输入多个标签，则资源必须具有要包括或排除的所有标签。
16. 对于授予跨账户访问权限，请选择下载 Amazon CloudFormation 模板。这将下载一个可用于创建 Amazon CloudFormation 堆栈的 Amazon CloudFormation 模板。此堆栈创建了一个 Amazon Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户权限来管理 Fortigate CNF 资源。有关堆栈的信息，请参阅《Amazon CloudFormation 用户指南》中的 [使用堆栈](#)。要创建堆栈，您需要从 Fortigate CNF 门户中获取账户 ID。
 17. 选择 Next (下一步)。
 18. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅 [使用标签编辑器](#)。
 19. 选择 Next (下一步)。
 20. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

有关 Firewall Manager Fortigate CNF 策略的更多信息，请参阅 [Fortigate 云原生防火墙 \(CNF\) 即服务策略 \(p. 464\)](#)。

使用 Amazon Firewall Manager 策略

Amazon Firewall Manager 提供以下类型的策略：

- Amazon WAF 策略 — Firewall Manager 支持 Amazon WAF 和 Amazon WAF 经典策略。对于这两个版本，您都可以定义哪些资源受策略保护。
 - 对于 Amazon WAF 策略，您可以定义在 Web ACL 中首先运行的一组规则组和最后运行的一组规则组。在应用 Web ACL 的账户中，账户所有者可以添加规则和规则组，以便在两个 Firewall Manager 规则组集之间运行。
 - 对于 Amazon WAF Classic，您可以创建定义单个规则组的策略。
- Shield Advanced 策略 — 此策略将 Amazon Shield Advanced 保护以下事项，应用到指定的账户和资源。
- Amazon VPC 安全组策略 — 此类策略使您可以控制整个组织中使用的安全组，Amazon Organizations 并允许您在整个组织中强制执行一组基准规则。
- Network Firewall 策略-此策略将 Amazon Network Firewall 保护应用于您组织的 VPC。
- Amazon Route 53 Resolver DNS 防火墙政策 — 此策略对您组织的 VPC 应用 DNS 防火墙保护。
- Palo Alto Networks Cloud NGFW 政策 — 本政策将 Palo Alto Networks 云下一代防火墙 (NGFW) 保护和 Palo Alto Networks Cloud NGFW 规则堆栈应用于贵组织的 VPC。
- Fortigate 云原生防火墙 (CNF) 即服务政策 — 此政策将 Fortigate 云原生防火墙 (CNF) 作为服务保护使用。Fortigate CNF 是一种以云为中心的解决方案，它通过业界领先的高级威胁防御、智能 Web 应用程序防火墙 (WAF) 和 API 保护来阻止零日威胁并保护云基础架构。

Firewall Manager 策略特定于单个策略类型。如果要跨账户实施多个策略类型，您可以创建多个策略。您可以为每种类型创建多个策略。

如果您向创建的组织添加新帐户，Amazon Organizations Firewall Manager 会自动将策略应用到该账户中策略范围内的资源。

Amazon Firewall Manager 策略的常规设置

Amazon Firewall Manager 托管策略有一些常见的设置和行为。对于所有人，您可以指定名称并定义策略的范围，并且可以使用资源标记来控制策略范围。您可以选择不采取纠正措施的情况下查看不合规的账户和资源，也可以选择自动修复不合规的资源。

有关策略范围的信息，请参阅[Amazon Firewall Manager 策略范围 \(p. 440\)](#)。

创建 Amazon Firewall Manager 策略

创建策略的步骤因不同的策略类型而异。请确保使用适用于所需策略类型的过程。

Important

Amazon Firewall Manager 不支持亚马逊 Route 53 或 Amazon Global Accelerator。如果您想使用 Shield Advanced 保护这些资源，则不能使用 Firewall Manager 策略。而是应按照[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)中的说明操作。

主题

- [为 Amazon WAF 创建 Amazon Firewall Manager 策略 \(p. 423\)](#)
- [为 Amazon WAF Classic 创建 Amazon Firewall Manager 策略 \(p. 425\)](#)
- [为 Amazon Shield Advanced 创建 Amazon Firewall Manager 策略 \(p. 426\)](#)
- [创建 Amazon Firewall Manager 通用安全组策略 \(p. 428\)](#)

- [创建 Amazon Firewall Manager 内容审核安全组策略 \(p. 429\)](#)
- [创建 Amazon Firewall Manager 使用情况审核安全组策略 \(p. 431\)](#)
- [为 Amazon Network Firewall 创建 Amazon Firewall Manager 策略 \(p. 432\)](#)
- [为亚马逊 Route 53 Resolver DNS Firewall \(p. 435\)](#)
- [为帕洛阿尔托网络 Amazon Firewall Manager 制定政策 Palo Alto Networks Cloud NGFW \(p. 436\)](#)
- [为 Fortigate 云原生防火墙 \(CNF\) 即服务创建 Amazon Firewall Manager 策略 \(p. 438\)](#)

为 Amazon WAF 创建 Amazon Firewall Manager 策略

在 Firewall Manager Amazon WAF 策略中，您可以使用托管规则组，Amazon 由 Amazon Web Services Marketplace 卖家为您创建和维护。您也可以创建和使用自己的规则组。有关规则组的更多信息，请参阅[规则组 \(p. 23\)](#)。

如果您想使用自己的规则组，请在创建 Firewall Manager Amazon WAF 策略之前创建这些规则组。有关操作指南，请参阅[管理您自己的规则组 \(p. 78\)](#)。要使用单个自定义规则，您必须定义自己的规则组，再在其中定义您的规则，然后在策略中使用该规则组。

有关 Firewall Manager Amazon WAF 策略的信息，请参阅[Amazon WAF 策略 \(p. 444\)](#)。

为 Amazon WAF (控制台) 创建 Firewall Manager 策略

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Amazon WAF。
5. 对于区域，选择一个 Amazon Web Services 区域。要保护亚马逊 CloudFront 发行版，请选择全球。

要保护多个区域 (CloudFront 发行版除外) 中的资源，必须为每个区域创建单独的 Firewall Manager 策略。

6. 选择下一步。
7. 对于 Policies 名称，输入一个描述性名称。Firewall Manager 在其管理的 Web ACL 名称中包含策略名称。Web ACL 名称 FMManagedWebACL V2 - 后面是您在此处输入的策略名称和 Web ACL 创建时间戳 (以 UTC 毫秒为单位) 。 - 例如，FMManagedWebACL V2 - MyWAFPolicyName - 1621880374078。
8. 在 Policy rules (策略规则) 下，添加您希望 Amazon WAF 在 Web ACL 中最先评估和最后评估的规则组。要使用 Amazon WAF 托管规则组版本控制，请切换启用版本控制。各客户经理可以在最先运行的规则组和最后运行的规则组之间添加规则和规则组。有关在的 Firewall Manager 策略中使用 Amazon WAF 规则组的更多信息 Amazon WAF，请参阅[Amazon WAF 策略 \(p. 444\)](#)。

(可选) 要自定义 Web ACL 使用规则组的方式，请选择编辑。以下是常见的自定义设置：

- 对于托管规则组，改写部分或所有规则的规则操作。如果您没有为规则定义替代操作，则评估将使用在规则组内定义的规则操作。有关此选项的信息，请参阅[规则组中的操作替代 \(p. 14\)](#) 《Amazon WAF 开发者指南》。
- 某些托管规则组需要您提供其他配置。请参阅您的托管规则组提供商提供的文档。有关 Amazon 托管规则组的特定信息，请参阅[Amazon 的托管规则 Amazon WAF \(p. 32\)](#) 《Amazon WAF 开发者指南》。

完成设置后，选择“保存规则”。

9. 设置 Web ACL 的默认操作。这是 Web 请求与 Web ACL 中的任何规则均不匹配时执行的操作。Amazon 您可以使用“允许”操作添加自定义标头，也可以为“阻止”操作添加自定义响应。有关默认 Web ACL 操作的更多信息，请参阅[决定 Web ACL 的默认操作 \(p. 16\)](#)。有关设置自定义 Web 请求和响应的信息，请参阅[中的自定义 Web 请求和响应 Amazon WAF \(p. 118\)](#)。
10. 对于日志配置，选择启用日志记录以启用日志记录。日志记录提供有关由您的 Web ACL 分析的流量的详细信息。选择日志记录目的地，然后选择您配置的日志记录目标。必须选择名称以开头的日志目的地 `aws-waf-logs-`。有关配置 Amazon WAF 日志目的地的信息，请参见[为 Amazon WAF 策略配置日志 \(p. 445\)](#)。
11. (可选) 如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 Add (添加)。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为 REDACTED。
12. (可选) 如果您不想将所有请求发送到日志，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个过滤器，选择添加过滤器，然后选择您的筛选条件并指定要保留还是删除符合条件的请求。添加完过滤器后，如果需要，修改默认日志记录行为。有关更多信息，请参阅 Amazon WAF 开发人员指南中的[管理 Web ACL 的日志记录 \(p. 187\)](#)。
13. 您可以定义令牌域列表以启用受保护应用程序之间的令牌共享。令牌由 CAPTCHA 和 Challenge 操作以及您在使用防 Amazon WAF 欺诈控制账户接管 (ATP) 和 Amazon WAF 机器人控制的 Amazon 托管规则组时实现的应用程序集成 SDK 使用。

不允许使用公共后缀项。例如，您不能使用 `usa.gov` 或 `co.uk` 作为令牌域。

默认情况下，仅 Amazon WAF 接受受保护资源的域的令牌。如果您在此列表中添加令牌域，则 Amazon WAF 接受列表中所有域和关联资源域的令牌。有关更多信息，请参阅 Amazon WAF 开发人员指南中的[配置 Web ACL 令牌域列表 \(p. 138\)](#)。

您只能在编辑现有 Web ACL 时更改网页 ACL 的验证码和挑战免疫时间。您可以在 Firewall Manager 策略详细信息页面下找到这些设置。有关这些设置的信息，请参阅[时间戳到期：代币豁免时间 \(p. 137\)](#)。如果您更新现有策略中的验证码、挑战或令牌域列表设置，Firewall Manager 将使用新值覆盖您的本地 Web ACL。但是，如果您不更新策略的验证码、挑战或令牌域列表设置，则您的本地 Web ACL 中的值将保持不变。有关此选项的信息，请参阅[CAPTCHA 以及中的 Challenge 操作 Amazon WAF \(p. 175\)](#)《Amazon WAF 开发者指南》。

14. 对于 Policy action (策略操作)，如果要在组织中的每个适用账户内创建一个 Web ACL，但不将 Web ACL 应用于任何资源，请选择 Identify resources that don't comply with the policy rules, but don't auto remediate (识别不符合策略规则的资源，但不进行自动修复)。您随后可以更改此选项。

若要自动将策略应用于现有的范围内资源，请选择 Auto remediate any noncompliant resources (自动修复任何不合规的资源)。此选项会在 Amazon 组织中的每个适用账户内创建一个 Web ACL，并将 Web ACL 与账户中的资源关联。

当您选择“自动修复任何不合规的资源”时，对于未由其他有效的 Firewall Manager 策略管理的 Web ACL，也可以选择从作用域内资源中删除现有 Web ACL 关联。如果选择此选项，Firewall Manager 首先将策略的 Web ACL 与资源关联，然后删除先前的关联。如果资源与另一个由不同的活动 Firewall Manager 策略管理的 Web ACL 相关联，则此选择不会影响该关联。

15. 选择下一步。
16. 如果 Amazon Web Services 账户此政策适用于，请选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的 Amazon 组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要将策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

17. 对于资源类型，选择要保护的资源类型。
18. 对于 Resources (资源)，如果要仅保护（或排除）具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅[使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。

19. 选择下一步。
20. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
21. 选择下一步。
22. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

为Amazon WAF Classic 创建Amazon Firewall Manager策略

为Amazon WAF Classic (控制台) 创建Firewall Manager 策略

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Amazon WAF Classic。
5. 如果您已经创建了要添加到策略的Amazon WAF经典规则组，请选择创建Amazon Firewall Manager策略并添加现有规则组。如果要创建新规则组，请选择创建Firewall Manager 策略并添加新规则组。
6. 对于区域，选择一个Amazon Web Services 区域。要保护亚马逊 CloudFront 资源，请选择全球。

要保护多个区域（资源除外）中的 CloudFront 资源，必须为每个区域创建单独的Firewall Manager 策略。

7. 选择下一步。
8. 如果您要创建规则组，请按照[创建Amazon WAF经典规则组 \(p. 295\)](#)中的说明操作。在创建规则组后，请继续执行以下步骤。
9. 输入策略名称。
10. 如果您要添加现有规则组，请使用下拉菜单选择要添加的规则组，然后选择 Add rule group (添加规则组)。
11. 一个策略有两个可能的操作：Action set by rule group (由规则组设置的操作) 和 Count (计数)。如果您要测试策略和规则组，请将操作设置为 Count (计数)。此操作会覆盖该策略中的规则组所指定的任何阻止 操作。即，如果将策略的操作设置为 Count (计数)，则只会对这些请求进行计数而不会阻止它们。相反，如果将策略的操作设置为 Action set by rule group (由规则组设置的操作)，则会使用规则组规则的操作。选择适当的操作。
12. 选择下一步。

13. 如果Amazon Web Services 账户此政策适用于，请选择以下选项：

- 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
- 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要将策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

14. 选择要保护的资源的类型。

15. 如果您只想保护带特定标签的资源，或者排除带特定标签的资源，请选择 Use tags to include/exclude resources (使用标签来包含/排除资源)，输入标签，然后选择 Include (包含) 或 Exclude (排除)。您只能选择一个选项。

如果您输入了多个标签 (以逗号分隔)，并且某个资源带有任一这些标签，则会将该资源视为匹配项。

有关标签的更多信息，请参阅[使用标签编辑器](#)。

16. 如果您要将策略自动应用于现有资源，请选择 Create and apply this policy to existing and new resources (创建此策略并将其应用于现有资源和新资源)。

此选项在 Amazon 组织中的每个适用账户内创建一个 Web ACL，并将 Web ACL 与账户中的资源关联。此选项还将策略应用于符合上述条件 (资源类型和标签) 的所有新资源。或者，如果您选择 Create policy but do not apply the policy to existing or new resources (创建策略但不将策略应用于现有资源或新资源)，则 Firewall Manager 会在组织内的每个适用账户中创建一个 Web ACL，但不会将 Web ACL 应用于任何资源。您稍后必须将策略应用于资源。选择适当的选项。

17. 对于 Replace existing associated web ACLs (替换现有关联的 Web ACL)，您可以选择删除当前为范围内资源定义的任何 Web ACL 关联，然后将它们替换为与您使用此策略创建的 Web ACL 之间的关联。默认情况下，Firewall Manager 在添加新 Web ACL 关联之前不会删除现有的 Web ACL 关联。如果要删除现有关联，请选择此选项。

18. 选择下一步。

19. 查看新策略。要进行任何更改，请选择 Edit (编辑)。若您满意所创建的策略，请选择 Create and apply policy (创建并应用策略)。

为 Amazon Shield Advanced 创建Amazon Firewall Manager策略

为 Shield Advanced 创建Firewall Manager 策略 (控制台)

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。

3. 选择 Create policy (创建策略)。

4. 对于策略类型，选择 Shield Advanced。

要创建 Shield Advanced 政策，你必须订阅Shield 高级版。如果您尚未订阅，则会提示您订阅。有关订阅费用的信息，请参阅[Amazon Shield Advanced定价](#)。

5. 对于区域，选择一个Amazon Web Services 区域。要保护亚马逊 CloudFront发行版，请选择全球。

对于全局以外的区域选择，要保护多个区域中的资源，必须为每个区域创建单独的Firewall Manager 策略。

6. 选择下一步。

7. 对于 Name，输入一个描述性的名称。

8. 仅适用于全球区域策略，您可以选择是否要管理 Shield Advanced 自动应用层 DDoS 缓解措施。有关此 Shield Advanced 功能的信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

您可以选择启用或禁用自动缓解功能，也可以选择忽略以下事项。如果你选择忽略它，Firewall Manager 根本无法管理 Shield Advanced 保护的自动缓解措施。有关这些策略选项的更多信息，请参阅[自动缓解亚马逊 CloudFront发行版的应用层 DDoS \(p. 450\)](#)。

9. 对于策略操作，我们建议使用不自动修复不合规资源的选项来创建策略。禁用自动修复后，可以在应用新策略之前评估其影响。如果您对更改符合您的要求感到满意，则编辑策略并更改策略操作以启用自动修复。

若要自动将策略应用于现有的范围内资源，请选择 Auto remediate any noncompliant resources (自动修复任何不合规的资源)。此选项对Amazon组织内的每个适用账户以及账户中的每个适用资源应用Shield Advanced保护。

仅适用于全局区域策略，如果您选择“自动修复任何不合规的资源”，也可以选择让 Firewall Manager 自动将任何现有的经Amazon WAF典 Web ACL 关联替换为使用最新版本Amazon WAF (v2) 创建的 Web ACL 的新关联。如果您选择此选项，Firewall Manager 会在任何尚未为该策略创建新的空 Web ACL 的范围内的账户中创建新的空 Web ACL 后，删除与早期版本 Web ACL 的关联并创建与最新版本的 Web ACL 的新关联。有关此选项的更多信息，请参阅 [将Amazon WAF经典 Web ACL 替换为最新版本的 Web ACL \(p. 451\)](#)。

10. 选择下一步。

11. 如果Amazon Web Services 账户此政策适用于，请选择以下选项：

- 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
- 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

12. 选择要保护的资源的类型。

Firewall Manager 不支持亚马逊 Route 53 或Amazon Global Accelerator。如果您需要使用 Shield Advanced 来保护资源免受这些服务的侵害，则不能使用Firewall Manager 策略。取而代之的是，请遵循上的 Shield 高级指南[向 Amazon 资源添加 Amazon Shield Advanced 保护 \(p. 365\)](#)。

13. 如果您只想保护带有特定标签的资源，或者排除带有特定标签的资源，请选择“使用标签包含/排除资源”，输入以逗号分隔的标签，然后选择“包括”或“排除”。您只能选择一个选项。

如果您输入多个标签，并且资源具有任何这些标签，则将其视为匹配。

有关标签的更多信息，请参阅[使用标签编辑器](#)。

14. 选择下一步。
15. 对于策略标记，为Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
16. 选择下一步。
17. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

创建 Amazon Firewall Manager 通用安全组策略

有关常见安全组策略的工作原理的信息，请参阅[通用安全组策略 \(p. 452\)](#)。

要创建通用安全组策略，您必须已在您的 Firewall Manager 管理员帐户中创建了一个要用作策略主安全组的安全组。您可以通过 Amazon VPC (Amazon VPC) 或Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 [Amazon VPC 用户指南](#)中的[与安全组合作](#)。

创建 通用安全组策略 (控制台)

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Security group (安全组)。
5. 对于 Security group policy type (安全组策略类型)，选择 Common security groups (通用安全组)。
6. 对于区域，选择一个Amazon Web Services 区域。
7. 选择下一步。
8. 对于 Policy name (策略名称)，输入一个友好名称。
9. 对于策略规则，请执行以下操作：
 - a. 从规则选项中，选择要应用于安全组规则和策略范围内的资源的限制。如果您选择将标签从主安全组分配到此策略创建的安全组，则还必须选择识别并报告此策略创建的安全组何时变为不合规。

Important

Firewall Manager 不会将通过Amazon服务添加的系统标签分发到副本安全组中。系统标签以 aws: 为前缀。此外，如果策略的标签与组织的标签策略冲突，Firewall Manager 不会更新现有安全组的标签或创建新的安全组。有关标签策略的信息，请参阅Amazon Organizations用户指南中的[标签策略](#)。

- b. 对于主要安全组，选择添加主安全组，然后选择要使用的安全组。Firewall Manager 填充Firewall Manager 管理员帐户中所有 Amazon VPC 实例的主要安全组列表。策略的主安全组的默认最大数目为一。有关增加最大值的信息，请参阅[Amazon Firewall Manager 配额 \(p. 497\)](#)。
 - c. 对于 Policy action (策略操作)，建议使用不自动修复的选项来创建策略。这使您可以在应用新政策之前评估其影响。如果您对更改符合您的要求感到满意，则编辑策略并更改策略操作以启用对不合规资源的自动修复。
10. 选择下一步。

11. 如果Amazon Web Services 账户此政策适用于，请选择以下选项：

- 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
- 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

12. 对于资源类型，选择要保护的资源类型。

如果您选择 EC2 实例，则可以选择在每个 Amazon EC2 实例中包含所有弹性网络接口，或者只包含每个实例中的默认接口。如果您在任何 Amazon EC2 实例中有多个 elastic network interface，则选择包含所有接口的选项可让 Firewall Manager 将策略应用于所有接口。当您启用自动修复时，如果 Firewall Manager 无法将策略应用于 Amazon EC2 实例中的所有弹性网络接口，它会将该实例标记为不合规。

13. 对于资源，如果要策略应用于Amazon Web Services 账户和资源类型参数中的所有资源，请选择包括与所选资源类型匹配的所有资源。如果要包含或排除特定资源，请使用标记来指定资源，然后选择相应的选项并将标签添加到列表中。您可以将策略应用于除具有您指定所有标签的资源之外的所有资源，也可以仅将其应用于具有您指定的所有标签的资源。有关标记资源的更多信息，请参阅[使用标签编辑器](#)。

Note

如果您输入多个标签，则资源必须具有所有标签才能匹配。

14. 对于 Shared VPC resources (共享 VPC 资源)，如果除了账户拥有的 VPC 外，您要将策略应用于共享 VPC 中的资源，请选择 Include resources from shared VPCs (包括共享 VPC 中的资源)。

15. 选择下一步。

16. 查看策略设置，确保它们满足您的需求，然后选择 Create policy (创建策略)。

Firewall Manager 在范围内的每个 Amazon VPC 实例中创建主安全组的副本，但不得超过每个账户支持的 Amazon VPC 最大配额。Firewall Manager 将副本安全组与每个作用域内账户的策略范围内的资源相关联。有关此策略工作方式的更多信息，请参阅[通用安全组策略 \(p. 452\)](#)。

创建 Amazon Firewall Manager 内容审核安全组策略

有关内容审计安全组策略如何运作的信息，请参阅[内容审核安全组策略 \(p. 454\)](#)。

对于某些内容审计策略设置，必须提供审计安全组以供Firewall Manager 用作模板。例如，您的审计安全组可能包含您不允许在任何安全组中使用的所有规则。必须先使用您的 Firewall Manager 管理员帐户创建这些审计安全组，然后才能在策略中使用它们。您可以通过 Amazon VPC (Amazon VPC) 或Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 [Amazon VPC 用户指南](#) 中的[与安全组合作](#)。

创建内容审计安全组策略 (控制台)

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Security group (安全组)。
5. 对于安全组策略类型，选择审计和执行安全组规则。
6. 对于区域，选择一个Amazon Web Services 区域。
7. 选择下一步。
8. 对于 Policy name (策略名称)，输入一个友好名称。
9. 对于策略规则，请选择要使用的托管或自定义策略规则选项。
 - a. 对于配置托管式审计策略规则，执行以下操作：
 - i. 对于“配置要审核的安全组规则”，请选择要将审计策略应用到的安全组规则的类型。
 - ii. 如果您想执行诸如限制安全组中允许的协议、端口和 CIDR 范围设置之类的操作，请选择“审计过于宽松的安全组规则”，然后选择所需的选项。

对于使用协议列表的选择，您可以使用现有列表，也可以创建新列表。有关协议列表以及如何在策略中使用协议列表的信息，请参阅[托管列表 \(p. 441\)](#)和[使用托管列表 \(p. 442\)](#)。
 - iii. 如果您想对特定应用程序可以执行的操作施加限制，请选择“审计高风险应用程序”，然后选择所需的选项。

以下选择是相互排斥的：只能访问本地 CIDR 范围的应用程序和可以使用公有 CIDR 范围的应用程序。在任何策略中，您最多可以选择其中一个。

对于使用应用程序列表的选项，您可以使用现有列表，也可以创建新列表。有关应用程序列表以及如何在策略中使用它们的信息，请参阅[托管列表 \(p. 441\)](#)和[使用托管列表 \(p. 442\)](#)。
 - iv. 使用“覆盖”设置来显式覆盖策略中的其他设置。您可以选择始终允许或始终拒绝特定的安全组规则，无论这些规则是否符合您为该策略设置的其他选项。

对于此选项，您可以提供审计安全组作为允许的规则或拒绝的规则模板。对于审核安全组，选择添加审核安全组，然后选择要使用的安全组。Firewall Manager 填充 Firewall Manager 管理员账户中所有 Amazon VPC 实例的审计安全组列表。策略的审计安全组数量的默认最大配额为一。有关增加配额的信息，请参阅[Amazon Firewall Manager 配额 \(p. 497\)](#)。
 - b. 对于配置自定义策略规则，执行以下操作：
 - i. 从规则选项中，选择是只允许审计安全组中定义的规则，还是拒绝所有规则。有关此选择的信息，请参阅[内容审核安全组策略 \(p. 454\)](#)。
 - ii. 对于审核安全组，选择添加审核安全组，然后选择要使用的安全组。Firewall Manager 填充 Firewall Manager 管理员账户中所有 Amazon VPC 实例的审计安全组列表。策略的审计安全组数量的默认最大配额为一。有关增加配额的信息，请参阅[Amazon Firewall Manager 配额 \(p. 497\)](#)。
 - iii. 对于 Policy action (策略操作)，您必须使用不自动修复的选项来创建策略。这使您可以在应用新政策之前评估其影响。如果您对更改符合您的要求感到满意，请编辑策略并更改策略操作，以启用对不合规资源的自动修复。
10. 选择下一步。
11. 如果Amazon Web Services 账户此政策适用于，请选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添

加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

- 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

12. 对于资源类型，选择要保护的资源类型。
13. 对于资源，如果要策略应用于 Amazon Web Services 账户和资源类型参数中的所有资源，请选择包括与所选资源类型匹配的所有资源。如果要包含或排除特定资源，请使用标记来指定资源，然后选择相应的选项并将标签添加到列表中。您可以将策略应用于除具有您指定所有标签的资源之外的所有资源，也可以仅将其应用于具有您指定的所有标签的资源。有关标记资源的更多信息，请参阅[使用标签编辑器](#)。

Note

如果您输入多个标签，则资源必须具有所有标签才能匹配。

14. 选择下一步。
15. 查看策略设置，确保它们满足您的需求，然后选择 Create policy (创建策略)。

Firewall Manager 根据您的策略规则设置，将审计安全组与 Amazon 组织中的范围内的安全组进行比较。您可以在 Amazon Firewall Manager 策略控制台中查看策略状态。创建策略后，您可以对其进行编辑并启用自动补救以使您的审计安全组策略生效。有关此策略工作方式的更多信息，请参阅[内容审核安全组策略 \(p. 454\)](#)。

创建 Amazon Firewall Manager 使用情况审核安全组策略

有关使用情况审计安全组策略如何运作的信息，请参阅[使用情况审核安全组策略 \(p. 455\)](#)。

创建使用情况审核安全组策略 (控制台)

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于 Policy type (策略类型)，选择 Security group (安全组)。
5. 对于安全组策略类型，选择“审计和清理未使用的和冗余的安全组”。
6. 对于区域，选择一个 Amazon Web Services 区域。
7. 选择下一步。
8. 对于 Policy name (策略名称)，输入一个友好名称。
9. 对于 Policy rules (策略规则)，选择其中一个或全部两个可用选项。
 - 如果您选择此策略范围内的安全组，则必须至少由一个资源使用。，Firewall Manager 会删除其确定未使用的任何安全组。默认情况下，如果安全组在任意时间段内未使用，Firewall Manager 会将其视

为不符合此策略规则。您可以选择指定安全组在被视为不合规之前可以存在的分钟数。如果您选择此规则，则Firewall Manager 将在您保存策略时最后运行该规则。

- 如果您选择，则此策略范围内的安全组必须是唯一的。Firewall Manager 整合了冗余安全组，因此只有一个与任何资源相关联。如果您选择该策略，Firewall Manager 会在您保存策略时首先运行 Firewall Manager。
10. 对于 Policy action (策略操作)，建议使用不自动修复的选项来创建策略。这使您可以在应用新政策之前评估其影响。如果您对更改符合您的要求感到满意，则编辑策略并更改策略操作以启用对不合规资源的自动修复。
 11. 选择下一步。
 12. 如果Amazon Web Services 账户此政策适用于，请选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

13. 对于资源，如果要策略应用于Amazon Web Services 账户和资源类型参数中的所有资源，请选择“包括与所选 resource 类型匹配的所有资源”。如果要包含或排除特定资源，请使用标记来指定资源，然后选择相应的选项并将标签添加到列表中。您可以将策略应用于除具有您指定所有标签的资源之外的所有资源，也可以仅将其应用于具有您指定的所有标签的资源。有关标记资源的更多信息，请参阅[使用标签编辑器](#)。

Note

如果您输入多个标签，则资源必须具有所有标签才能匹配。

14. 选择下一步。
15. 如果您尚未将Firewall Manager 管理员帐户排除在策略范围之外，Firewall Manager 会提示您执行此操作。这样做会使 Firewall Manager 管理员帐户中的安全组（用于常见安全组策略和审计安全组策略）处于您的手动控制之下。在此对话框中选择你想要的选项。
16. 查看策略设置，确保它们满足您的需求，然后选择 Create policy (创建策略)。

如果您选择需要唯一的安全组，则Firewall Manager 会扫描每个作用域内的 Amazon VPC 实例中的冗余安全组。然后，如果您选择要求每个安全组至少由一个资源使用，Firewall Manager 会扫描在规则中指定的分钟内未使用的安全组。您可以在 Amazon Firewall Manager 策略控制台中查看策略状态。有关此策略工作方式的更多信息，请参阅[使用情况审核安全组策略 \(p. 455\)](#)。

为 Amazon Network Firewall 创建Amazon Firewall Manager策略

在 Firewall Manager Network Firewall 策略中，您可以使用自己在其中管理的规则组Amazon Network Firewall。有关管理规则组的信息，请参阅Network Firewall 开发人员指南中的[Amazon Network Firewall 规则组](#)。

有关Firewall Manager Network Firewall 策略的信息，请参见[Amazon Network Firewall 策略 \(p. 457\)](#)。

为 Amazon Network Firewall (控制台) 创建 Firewall Manager 策略

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
 3. 选择 Create policy (创建策略)。
 4. 对于 Policy type (策略类型)，选择 Amazon Network Firewall。
 5. 在“防火墙管理类型”下，选择您希望 Firewall Manager 如何管理策略的防火墙。从以下选项中进行选择：
 - 分布式-Firewall Manager 在策略范围内的每个 VPC 中创建和维护防火墙终端节点。
 - 集中化-Firewall Manager 在单个检查 VPC 中创建和维护终端节点。
 - 导入现有防火墙-Firewall Manager 使用资源集从 Network Firewall 导入现有防火墙。有关资源集的信息，请参见 [在 Firewall Manager 中使用资源集 \(p. 466\)](#)。
 6. 对于区域，选择一个 Amazon Web Services 区域。要保护多个区域中的资源，必须为每个区域创建单独的策略。
 7. 选择下一步。
 8. 对于 Policies 名称，输入一个描述性名称。Firewall Manager 在其创建的 Network Firewall 和防火墙策略的名称中包含策略名称。
 9. 在 Amazon Network Firewall 策略配置中，像在 Network Firewall 中一样配置防火墙策略。添加您的无状态和有状态规则组并指定策略的默认操作。您可以选择设置策略的状态规则评估顺序和默认操作以及日志配置。有关 Network Firewall 防火墙 [Amazon Network Firewall 策略](#) 管理的信息，请参阅 Amazon Network Firewall 开发人员指南中的防火墙策略。
- 创建 Firewall Manager Network Firewall 策略时，Firewall Manager 会为范围内的帐户创建防火墙策略。个人账户管理员可以将规则组添加到防火墙策略中，但他们无法更改您在此处提供的配置。
10. 选择下一步。
 11. 根据在上一步骤中选择的 Firewall 管理类型，执行以下某项操作之一，执行以下某项操作之一，执行以下某项操作之一，执行以下
 - 如果您使用分布式防火墙管理类型，请在防火墙 Amazon Firewall Manager 端点位置下的端点配置中，选择以下选项之一：
 - 自定义终端节点配置-Firewall Manager 在您指定的可用区内为策略范围内的每个 VPC 创建防火墙。每个 Firewall 至少包含一个 Firewall 端点。
 - 在可用区域下，选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
 - 如果要提供 CIDR 块供 Firewall Manager 用于 VPC 中的防火墙子网，则它们必须全部是 /28 CIDR 块。每行输入一个块。如果您省略这些 IP 地址，Firewall Manager 会从 VPC 中可用的 IP 地址中为您选择 IP 地址。

Note

Network Firewall Amazon Firewall Manager 策略会自动进行自动修复，因此您不会在此处看到选择不 auto 修复的选项。

- 自动端点配置-Firewall Manager 在您的 VPC 中有公有子网的可用区自动创建防火墙终端节点。
 - 对于防火墙端点配置，请指定您希望 Firewall Manager 如何管理防火墙端点。我们建议使用多个终端节点以实现高可用性。
- 如果您使用集中式防火墙管理类型，请在检查 VPC 配置下的 Amazon Firewall Manager 终端节点配置中，输入检查 VPC 所有者的 Amazon 账户 ID 和检查 VPC 的 VPC ID。

- 在可用区域下，选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
- 如果要提供 CIDR 块供 Firewall Manager 用于 VPC 中的防火墙子网，则它们必须全部是 /28 CIDR 块。每行输入一个块。如果您省略这些 IP 地址，Firewall Manager 会从 VPC 中可用的 IP 地址中为您选择 IP 地址。

Note

Network Firewall Amazon Firewall Manager 策略会自动进行自动修复，因此您不会在此处看到选择不 auto 修复的选项。

- 如果您使用导入现有防火墙管理类型，请在资源集中添加一个或多个资源集。资源集定义了贵组织账户拥有的现有 Network Firewall，您希望在此策略中集中管理这些防火墙。要向策略添加资源集，必须先使用控制台或 [PutResourceSet API](#) 创建资源集。有关资源集的信息，请参见 [在 Firewall Manager 中使用资源集 \(p. 466\)](#)。有关从 Network Firewall 导入现有防火墙的更多信息，请参见 [导入现有防火墙。 \(p. 458\)](#)
12. 选择下一步。
 13. 如果您的策略使用分布式防火墙管理类型，请在“路由管理”下选择 Firewall Manager 是否监视必须通过相应防火墙端点路由的流量并发出警报。

Note

如果您选择“监控”，则以后将无法将设置更改为“关闭”。监控会一直持续到您删除策略为止。

14. 对于流量类型，可以选择添加要路由流量以进行防火墙检查的流量端点。
15. 对于允许所需的跨可用区流量，如果您启用此选项，则对于没有自己的防火墙终端节点的可用区，Firewall Manager 会将流量发送出可用区进行检查，视为合规路由。具有终端节点的可用区必须始终检查自己的流量。
16. 选择下一步。
17. 对于政策范围，Amazon Web Services 账户在本政策适用范围内，选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的 Amazon 组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

18. Network Firewall 策略的资源类型是 VPC。
19. 对于 Resources (资源)，如果要仅保护 (或排除) 具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参见 [使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。

20. 选择下一步。
21. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参见 [使用标签编辑器](#)。
22. 选择下一步。

23. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

为亚马逊 Route 53 Resolver DNS Firewall

在 Firewall Manager DNS 防火墙策略中，您使用在 Amazon Route 53 Resolver DNS Firewall 中管理 有关管理规则组的信息，请参阅 Amazon Route 53 开发者指南 [中的 DNS 防火墙中管理规则组和规则](#)。

有关 Firewall Manager DNS 防火墙策略的信息，请参阅 [Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)。

为 Amazon Route 53 Resolver DNS 防火墙创建 Firewall Manager 策略

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于策略类型，选择 Amazon Route 53 Resolver DNS 防火墙。
5. 对于区域，选择一个 Amazon Web Services 区域。要保护多个区域中的资源，必须为每个区域创建单独的策略。
6. 选择下一步。
7. 对于 Policies 名称，输入一个描述性名称。
8. 在策略配置中，在 VPC 的规则组关联中添加您希望 DNS Firewall 首先和最后评估的规则组。您最多可以向策略添加两个规则组。

当您创建 Firewall Manager DNS 防火墙策略时，Firewall Manager 会使用您提供的关联优先级为范围内的 VPC 和账户创建规则组关联。个人账户经理可以在您的第一个关联和最后一个关联之间添加规则组关联，但他们无法更改您在此处定义的关联。有关更多信息，请参阅 [Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)：

9. 选择下一步。
10. 如果 Amazon Web Services 账户此政策适用于，请选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的 Amazon 组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您添加帐户到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

11. DNS 防火墙策略的资源类型是 VPC。
12. 对于 Resources (资源)，如果要仅保护（或排除）具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅[使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。
13. 选择下一步。
14. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
15. 选择下一步。
16. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

为帕洛阿尔托网络Amazon Firewall Manager制定政策 Palo Alto Networks Cloud NGFW

通过针对Palo Alto Networks云下一代防火墙（Palo Alto Networks Cloud NGFW）的Firewall Manager 策略，您可以使用Firewall Manager 部署 Palo Alto Networks Cloud NGFW 资源，并集中管理所有Amazon账户的 NGFW 规则堆栈。

有关Firewall Manager Palo Alto Networks Cloud NGFW 策略的信息，请参阅[帕洛阿尔托网络云 NGFW 政策 \(p. 464\)](#)。有关如何为Firewall Manager 配置和管理 Palo Alto Networks Cloud NGFW 的信息，请参阅Amazon文档中的 [Palo Alto Networks Palo Alto Networks Cloud NGFW](#)。

先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager先决条件 \(p. 403\)](#)介绍了这些步骤。在继续下一步之前，请先完成所有先决条件。

为 Palo Alto Networks Cloud NGFW（控制台）创建Firewall Manager 策略

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于策略类型，选择帕洛阿尔托网络 Palo Alto Networks Cloud NGFW。如果你还没有在Marketplace上订阅Palo Alto NAmazon etworks Cloud NGFW服务，则需要先订阅。要在Amazon Marketplace 中订阅，请选择查看Amazon Marketplace 详情。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定Firewall Manager 如何管理策略的端点。使用分布式模型，Firewall Manager 在策略范围内的每个 VPC 中维护防火墙终端节点。使用集中式模型，Firewall Manager 在检查 VPC 中维护单个端点。
6. 对于区域，选择一个Amazon Web Services 区域。要保护多个区域中的资源，必须为每个区域创建单独的策略。
7. 选择下一步。
8. 对于 Policies 名称，输入一个描述性名称。
9. 在策略配置中，选择 Palo Alto Networks Cloud NGFW 防火墙策略以与此策略关联。Palo Alto Networks Cloud NGFW 防火墙策略列表包含与您的 Palo Alto Networks Cloud NGFW 租户关联的所有帕洛阿尔托网络云 NGFW 防火墙策略。有关创建和管理 Palo Alto Networks Cloud NGFW 防火墙策略

的信息，请参阅[部署 Palo Alto Networks Cloud NGFW](#) 的 Palo Alto Networks Cloud NGFWAmazon 部署指南中的Amazon Firewall Manager主题。Amazon

10. 对于 Palo Alto Networks Palo Alto Networks Cloud NGFW 日志记录—— 可选，可以选择为您的策略记录哪种 Palo Alto Networks Cloud NGFW 日志类型。有关 Palo Alto Networks Cloud NGFW 日志类型的信息，请参阅 Palo Alto Networks [Palo Networks Cloud NGFWAmazon 部署指南](#)Amazon中的 [Palo Alto Networks Cloud NGFW 上](#) 的 Palo Alto

对于日志目标，请指定Firewall Manager 应在何时写入日志。

11. 选择下一步。
12. 在“配置第三方防火墙端点”下，执行以下操作之一，具体取决于您使用的是分布式部署模式还是集中式部署模型来创建防火墙终端节点：
 - 如果您为此策略使用分布式部署模型，请在可用区域下选择要在哪些可用区域中创建防火墙终端节点。您可以按可用区名称或可用区 ID 选择可用区。
 - 如果您为此策略使用集中部署模型，请在检查 VPC 配置下的Amazon Firewall Manager终端节点配置中，输入检查 VPC 所有者的Amazon账户 ID 和检查 VPC 的 VPC ID。
 - 在可用区域下，选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
13. 如果要提供 CIDR 块供Firewall Manager 用于 VPC 中的防火墙子网，则它们必须全部是 /28 CIDR 块。每行输入一个块。如果您省略这些 IP 地址，Firewall Manager 会从 VPC 中可用的 IP 地址中为您选择 IP 地址。

Note

Network Firewall Amazon Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不auto 修复的选项。

14. 选择下一步。
15. 对于政策范围，Amazon Web Services 账户在本政策适用范围内，选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的Amazon组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

16. Network Firewall 策略的资源类型是 VPC。
17. 对于 Resources (资源)，如果要仅保护（或排除）具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅[使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。

18. 对于“授予跨账户访问权限”，选择“下载Amazon CloudFormation模板”。这将下载一个可用于创建 Amazon CloudFormation堆栈的Amazon CloudFormation模板。此堆栈创建了一个Amazon Identity and Access Management角色，该角色授予Firewall Manager 跨账户权限，以管理 Palo Alto Networks Cloud NGFW 资源。有关堆栈的信息，请参阅《Amazon CloudFormation用户指南》中的使用[堆栈](#)。

19. 选择下一步。
20. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
21. 选择下一步。
22. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

为 Fortigate 云原生防火墙 (CNF) 即服务创建 Amazon Firewall Manager 策略

使用 Fortigate CNF 的 Firewall Manager 策略，您可以使用 Firewall Manager 在所有 Amazon 账户上部署和管理 Fortigate CNF 资源。

有关 Firewall Manager Fortigate CNF 策略的信息，请参阅[Fortigate 云原生防火墙 \(CNF\) 即服务策略 \(p. 464\)](#)。有关如何配置 Fortigate CNF 以与 Firewall Manager 一起使用的信息，请参阅[Fortinet 文档](#)。

先决条件

为 Amazon Firewall Manager 准备您的账户有几个必要步骤。[Amazon Firewall Manager 先决条件 \(p. 403\)](#) 介绍了这些步骤。在继续下一步之前，请先完成所有先决条件。

为 Fortigate CNF (控制台) 创建 Firewall Manager 策略

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy (创建策略)。
4. 对于策略类型，选择 Fortigate 云原生防火墙 (CNF) 即服务。如果你还没有在 [Amazon Marketplace 订阅 Fortigate CNF 服务](#)，你需要先订阅。要在 Amazon Marketplace 中订阅，请选择查看 Amazon Marketplace 详情。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定 Firewall Manager 如何管理策略的端点。使用分布式模型，Firewall Manager 在策略范围内的每个 VPC 中维护防火墙终端节点。使用集中式模型，Firewall Manager 在检查 VPC 中维护单个端点。
6. 对于区域，选择一个 Amazon Web Services 区域。要保护多个区域中的资源，必须为每个区域创建单独的策略。
7. 选择下一步。
8. 对于 Policies 名称，输入一个描述性名称。
9. 在策略配置中，选择要与此策略关联的 Fortigate CNF 防火墙策略。Fortigate CNF 防火墙策略列表包含与您的 Fortigate CNF 租户相关的所有 Fortigate CNF 防火墙策略。有关创建和管理 Fortigate CNF 租户的信息，请参阅 [Fortinet 文档](#)。
10. 选择下一步。
11. 在“配置第三方防火墙端点”下，执行以下操作之一，具体取决于您使用的是分布式部署模式还是集中式部署模型来创建防火墙终端节点：
 - 如果您为此策略使用分布式部署模型，请在可用区域下选择要在哪些可用区域中创建防火墙终端节点。您可以按可用区名称或可用区 ID 选择可用区。
 - 如果您为此策略使用集中部署模型，请在检查 VPC 配置下的 Amazon Firewall Manager 终端节点配置中，输入检查 VPC 所有者的 Amazon 账户 ID 和检查 VPC 的 VPC ID。

- 在可用区域下，选择要在哪些可用区域中创建防火墙端点。您可以按可用区名称或可用区 ID 选择可用区。
12. 如果要提供 CIDR 块供 Firewall Manager 用于 VPC 中的防火墙子网，则它们必须全部是 /28 CIDR 块。每行输入一个块。如果您省略这些 IP 地址，Firewall Manager 会从 VPC 中可用的 IP 地址中为您选择 IP 地址。

Note

Network Firewall Amazon Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不 auto 修复的选项。

13. 选择下一步。
14. 对于策略范围，Amazon Web Services 账户在本政策适用范围内，选择以下选项：
 - 如果您想将该政策应用于组织中的所有账户，请保留默认选择“包括我的 Amazon 组织下的所有账户”。
 - 如果只想将策略应用于特定账户或特定 Amazon Organizations 组织单位 (OU) 中的账户，请选择 Include only the specified accounts and organizational units (仅包括指定的账户和组织单位)，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
 - 如果要策略应用于除特定的一组账户或 Amazon Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 Exclude the specified accounts and organizational units, and include all others (排除指定的账户和组织单位，并包括所有其他账户和组织单位)，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新帐户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将策略应用于任何新帐户。再举一个例子，如果您包含 OU，则当您帐户添加到 OU 或其任何子 OU 时，Firewall Manager 会自动将策略应用于新帐户。

15. Network Firewall 策略的资源类型是 VPC。
16. 对于 Resources (资源)，如果要仅保护（或排除）具有特定标签的资源，请选择相应的选项，然后输入要包括或排除的标签。您只能选择一个选项。有关标签的更多信息，请参阅[使用标签编辑器](#)。

如果输入多个标签，则资源必须具有要包括或排除的所有标签。
17. 对于“授予跨账户访问权限”，选择“下载 Amazon CloudFormation 模板”。这将下载一个可用于创建 Amazon CloudFormation 堆栈的 Amazon CloudFormation 模板。该堆栈创建了一个 Amazon Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户权限，以管理 Fortigate CNF 资源。有关堆栈的信息，请参阅《Amazon CloudFormation 用户指南》中的使用[堆栈](#)。要创建堆栈，您需要 Fortigate CNF 门户网站中的账户 ID。
18. 选择下一步。
19. 对于策略标记，为 Firewall Manager 策略添加所需的任何识别标记。有关标签的更多信息，请参阅[使用标签编辑器](#)。
20. 选择下一步。
21. 查看新策略。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。若您满意所创建的策略，请选择 Create policy (创建策略)。

删除 Amazon Firewall Manager 策略

您可以通过执行以下步骤来删除 Firewall Manager 策略。

删除策略 (控制台)

1. 在导航窗格中，选择 Security policies (安全策略)。

2. 选择要删除的策略旁边的选项。
3. 选择删除。

Note

删除 Firewall Manager 通用安全组策略时，要删除该策略的副本安全组，请选择清理该策略创建的资源选项。否则，删除主实例后，副本将保留并需要在每个 Amazon VPC 实例中进行手动管理。

Important

当您删除 Firewall Manager Shield Advanced 策略时，该策略将被删除，但您的账户仍会订阅 Shield Advanced。

Amazon Firewall Manager策略范围

策略范围定义了政策的适用范围。您可以将集中控制的策略应用于组织内的所有账户和资源，也可以将集中控制的策略应用于Amazon Organizations您的账户和资源的子集。有关如何设置策略范围的说明，请参阅[创建 Amazon Firewall Manager 策略 \(p. 422\)](#)。

中的策略范围选项Amazon Firewall Manager

当您向组织添加新帐户或资源时，Firewall Manager 会根据您的每项策略的设置自动对其进行评估，并根据这些设置应用策略。例如，您可以选择将策略应用于除指定列表中的账户号码之外的所有账户；也可以选择仅将策略应用于列表中包含所有标签的资源。

Amazon Web Services 账户在范围内

您为定义受策略Amazon Web Services 账户影响者而提供的设置决定了要将策略应用到Amazon组织中的哪些账户。您可以选择以下方式应用策略：

- 发送到组织中的所有账户
- 仅应用到包括的账号和 Amazon Organizations 组织单位 (OU) 的特定列表
- 应用到除排除的账号和 Amazon Organizations 组织单位 (OU) 的特定列表之外的所有账户和组织单位

有关的信息Amazon Organizations，请参阅[《Amazon Organizations用户指南》](#)。

范围内的资源

与范围内的账户设置类似，您为资源提供的设置决定了要将策略应用于哪些范围内的资源类型。您可以选择以下操作之一：

- 所有资源
- 具有您指定的所有标签的资源
- 除具有您所指定所有标签的资源之外的所有资源

有关标记资源的更多信息，请参阅[使用标签编辑器](#)。

中的策略范围管理Amazon Firewall Manager

制定策略后，Firewall Manager 会根据策略范围持续对其进行管理，Amazon Web Services 账户并在添加新资源和资源时将其应用于新资源和资源。

Firewall Manager 如何Amazon Web Services 账户管理和资源

如果帐户或资源因任何原因超出范围，则Amazon Firewall Manager不会自动删除保护或删除 Firewall Manager 管理的资源，除非您选中“自动删除对离开策略范围的资源的保护”复选框。

Note

对于Amazon WAF传统策略，“自动删除对离开策略范围的资源的Amazon Shield Advanced保护”选项不可用。

选中此复选框指示Amazon Firewall Manager Firewall Manager 为账户管理的资源在这些账户离开策略范围时自动清理 Firewall Manager 为账户管理的资源。例如，当客户资源离开策略资源时，Firewall Manager 将取消 Firewall Manager 托管的 Web ACL 与受保护的客户端资源的关联。

要确定在客户端资源离开策略范围时应将哪些资源从保护中移除，Firewall Manager 遵循以下准则：

- 默认行为：
 - 关联的Amazon Config管理规则已删除。此行为与复选框无关。
 - 任何不包含任何资源的关联Amazon WAF网络访问控制列表 (Web ACL) 都将被删除。此行为与复选框无关。
 - 任何超出范围的受保护资源都将保持关联和受保护。例如，与 Web ACL 关联的Application Load Balancer 或 API 来自 API Gateway 的 API 仍与 Web ACL 关联，保护仍然有效。
- 选@@ 中“自动删除对离开策略范围的资源的保护”复选框：
 - 关联的Amazon Config管理规则已删除。此行为与复选框无关。
 - 任何不包含任何资源的关联Amazon WAF网络访问控制列表 (Web ACL) 都将被删除。此行为与复选框无关。
 - 任何超出范围的受保护资源都会在离开策略范围时自动取消关联并从保护中删除。例如，Elastic Inference 加速器或 Amazon EC2 实例在离开策略范围时会自动与复制的安全组断开关联。复制的安全组及其资源将自动从保护中删除。

托管列表

托管应用程序和协议列表简化了Amazon Firewall Manager内容审计安全组策略的配置和管理。您可以使用托管列表来定义您的策略允许和禁止的协议和应用程序。有关内容审计安全组策略的信息，请参阅[内容审核安全组策略 \(p. 454\)](#)。

您可以在内容审计安全组策略中使用以下类型的托管列表：

- Fi@@ rewall Manager 应用程序列表和协议列表 — Firewall Manager 管理这些列表。
 - 应用程序列表包括FMS-Default-Public-Access-Apps-Allowed和FMS-Default-Public-Access-Apps-Denied，其中描述了应允许或拒绝向公众开放的常用应用程序。
 - 协议列表包括FMS-Default-Protocols-Allowed应允许公众使用的常用协议列表。您可以使用 Firewall Manager 管理的任何列表，但不能对其进行编辑或删除。
- 自定义应用程序列表和协议列表-您可以管理这些列表。您可以使用所需的设置创建任一类型的列表。您可以完全控制自己的自定义管理列表，并且可以根据需要创建、编辑和删除它们。

Note

目前，当您删除自定义管理列表时，Firewall Manager 不会检查对该列表的引用。这意味着，即使活动策略正在使用自定义托管应用程序列表或协议列表，也可以将其删除。这可能导致策略停止运行。只有在确认任何有效的策略均未引用应用程序列表或协议列表后，才将其删除。

托管列表是Amazon资源。您可以标记自定义托管列表。您无法标记Firewall Manager 管理列表。

托管版本控制列表

自定义管理列表没有版本。编辑自定义列表时，引用该列表的策略会自动使用更新的列表。

Firewall Manager 管理的列表是版本控制的。Firewall Manager 服务团队根据需要发布新版本，以便将最佳安全实践应用于列表。

在策略中使用 Firewall Manager 管理列表时，您可以按如下方式选择版本控制策略：

- 最新可用版本-如果您没有为列表指定明确的版本设置，则您的策略会自动使用最新版本。这是通过控制台可用的唯一选项。
- 显式版本-如果您为列表指定版本，则您的策略将使用该版本。在您修改版本设置之前，您的策略将保持锁定在您指定的版本范围内。要指定版本，您必须在控制台之外定义策略，例如通过 CLI 或其中一个 SDK。

有关为列表选择版本设置的更多信息，请参阅[在内容审计安全组策略中使用托管列表 \(p. 442\)](#)。

在内容审计安全组策略中使用托管列表

创建内容审核安全组策略时，您可以选择使用托管审核策略规则。此选项的某些设置需要托管应用程序列表或协议列表。这些设置的示例包括安全组规则中允许的协议，应用程序可以访问互联网。

以下限制适用于使用托管列表的每个策略设置：

- 您可以为任何设置最多指定一个 Firewall Manager 托管列表。默认情况下，您最多可以指定一个自定义列表。自定义列表限制是软配额，因此您可以申请增加配额。有关更多信息，请参阅[Amazon Firewall Manager 配额 \(p. 497\)](#)：
- 在控制台中，如果您选择 Firewall Manager 管理列表，则无法指定版本。该政策将始终使用最新版本的列表。要指定版本，您必须在控制台之外定义策略，例如通过 CLI 或其中一个 SDK。有关 Firewall Manager 管理列表版本控制的信息，请参阅[托管版本控制列表 \(p. 441\)](#)。

有关通过控制台创建内容审核安全组策略的信息，请参阅[创建内容审核安全组策略 \(p. 429\)](#)。

创建自定义托管应用程序列表

创建自定义托管应用程序列表

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择应用程序列表。
3. 在应用程序列表页面中，选择创建应用程序列表。
4. 在创建应用程序列表页面中，为您的列表命名。不要使用前缀，fms- 因为这是为 Firewall Manager 保留的。
5. 通过提供协议和端口号或从类型下拉列表中选择应用程序来指定应用程序。为您的应用程序规范命名。
6. 根据需要选择“添加其他人”，然后填写申请信息，直到您完成列表。
7. （可选）将标签应用于列表。
8. 选择“保存”保存您的列表并返回“应用程序列表”页面。

创建自定义托管协议列表

创建自定义托管协议列表

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Policies listies。
3. 在协议列表页面中，选择创建协议列表。
4. 在协议列表创建页面中，为您的列表命名。不要使用前缀，fms- 因为这是为 Firewall Manager 保留的。
5. 指定协议。
6. 根据需要选择添加其他协议并填写协议信息，直到您完成列表。
7. （可选）将标签应用于列表。
8. 选择“保存”保存您的列表并返回“协议列表”页面。

查看托管列表

查看应用程序列表或协议列表

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择应用程序列表或协议列表。

该页面显示可供您使用的选定类型的所有列表。Firewall Manager 管理的列表的ManagedList列中有Y。

3. 要查看列表的详细信息，请选择其名称。详情页面显示列表的内容和所有标签。

对于Firewall Manager 管理列表，您还可以通过选择“版本”下拉列表来查看可用版本。

删除自定义托管列表

您可以删除自定义管理列表。您无法编辑或删除Firewall Manager 管理器管理的列表。

Note

目前，当您删除自定义管理列表时，Firewall Manager 不会检查对该列表的引用。这意味着，即使活动策略正在使用自定义托管应用程序列表或协议列表，也可以将其删除。这可能导致策略停止运行。只有在确认任何有效的策略未引用应用程序列表或协议列表后，才将其删除。

删除自定义托管应用程序或协议列表

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 通过执行以下操作，确保您要删除的列表未在任何审计安全组策略中使用：
 - a. 在导航窗格中，选择 Security policies (安全策略)。

- b. 在Amazon Firewall Manager策略页面中，选择并编辑您的审计安全组，并删除对要删除的自定义列表的任何引用。

如果您删除审计安全组策略中使用的自定义托管列表，则使用该列表的策略可能会停止运行。

3. 在导航窗格中，选择应用程序列表或协议列表，具体取决于要删除的列表类型。
4. 在列表页面中，选择要删除的自定义列表，然后选择 Delete (删除)。

Amazon WAF 策略

在Firewall ManagerAmazon WAF 策略中，您可以指定要在资源中使用的Amazon WAF规则组。当您应用策略时，Firewall Manager 会在策略范围内的每个账户中创建一个由Firewall Manager 管理的 Web ACL。在生成的 Web ACL 中，除了您通过Firewall Manager 定义的规则组外，个人账户管理员还可以添加规则和规则组。

当Firewall Manager 为策略创建 Web ACL 时，它会命名 Web ACLFMMManagedWebACLV2-*policy name-timestamp*。时间戳为UTC 毫秒。例如，FMMManagedWebACLV2-MyWAFPolicyName-1621880374078。

Amazon Firewall Manager为其为Amazon WAF策略创建的 Web ACL 和规则组启用采样和 Amazon CloudWatch 指标。

Note

如果配置了[高级自动应用层 DDoS 防护 \(p. 354\)](#)的资源进入Amazon WAF策略范围，Firewall Manager 将无法将该Amazon WAF策略创建的 Web ACL 关联到该资源。 >

Amazon WAF策略中的规则组

由Firewall ManagerAmazon WAF 策略管理的 Web ACL 包含三组规则。这些规则集为 Web ACL 中的规则和规则组提供了更高级的优先级划分机制：

- 第一个规则组，由您在Firewall ManagerAmazon WAF 策略中定义。Amazon WAF首先评估这些规则组。
- 由账户经理在 Web ACL 中定义的规则和规则组。Amazon WAF 会在中间评估任何客户托管的规则或规则组。
- 最后的规则组，由您在Firewall ManagerAmazon WAF 策略中定义。Amazon WAF最后评估这些规则组。

在其中的每个规则集中，Amazon WAF 会按照规则和规则组在规则集中的优先级设置照常评估规则和规则组。

在策略的“最先运行的规则组”集和“最后运行的规则组”集中，您只能添加规则组。您可以使用托管规则组，由 Amazon管理规则和Amazon Web Services Marketplace卖家为您创建和维护。您也可以管理和使用自己的规则组。有关所有这些操作的更多信息，请参阅[规则组 \(p. 23\)](#)。

如果您想使用自己的规则组，请在创建Firewall ManagerAmazon WAF 策略之前创建这些规则组。有关操作指南，请参阅[管理您自己的规则组 \(p. 78\)](#)。要使用单个自定义规则，您必须定义自己的规则组，再在其中定义您的规则，然后在策略中使用该规则组。

您通过Firewall Manager 管理的第一个和最后一个Amazon WAF规则组的名称分别以PREFMMManaged-或POSTFMMManaged-开头，后面是Firewall Manager 策略名称和规则组创建时间戳（以 UTC 毫秒为单位）。例如，PREFMMManaged-MyWAFPolicyName-1621880555123。

有关 Amazon WAF 如何评估 Web 请求的信息，请参阅[Web ACL 规则和规则组评估 \(p. 12\)](#)。

有关创建Firewall ManagerAmazon WAF 策略的过程，请参阅[Amazon WAF 创建Amazon Firewall Manager策略 \(p. 423\)](#)。

Firewall Manager 为您为 Amazon WAF 策略定义的规则组启用采样和 Amazon CloudWatch 指标。

个人账户所有者可以完全控制他们添加到策略的托管 Web ACL 中的任何规则或规则组的指标和采样配置。

限制

在 Amazon WAF 策略中使用规则组时，请注意以下限制。

- Firewall Manager 支持 Amazon WAF 机器人控制规则组，但以下情况除外：
 - 不支持机器人控制目标保护级别。
 - 仅支持 COUNT 规则操作覆盖。目前不支持其他规则操作替代类型。

有关中的机器人控制的信息 Amazon WAF，请参阅 [Amazon WAF 机器人控制 \(p. 142\)](#)。

为 Amazon WAF 策略配置日志

您可以为 Amazon WAF 策略启用集中日志记录，以获取有关组织内的 Web ACL 分析的流量的详细信息。日志中的信息包含从 Amazon 资源 Amazon WAF 收到请求的时间，有关请求的详细信息，以及每个请求所匹配的规则的操作。您可以将日志发送到 Amazon Kinesis Data Firehose 数据流或 Amazon Simple Storage Service (S3) 存储桶。有关 Amazon WAF 日志的信息，请参阅 [记录 Web ACL 流量 \(p. 180\)](#) Amazon WAF 开发者指南中的。

Note

Amazon Firewall Manager 支持此选项 Amazon WAFV2，不支持 Amazon WAF 经典版。

主题

- [日志记录目的地 \(p. 445\)](#)
- [启用日志记录 \(p. 448\)](#)
- [禁用日志记录 \(p. 449\)](#)

日志记录目的地

本部分将介绍您可以选择发送 Amazon WAF 策略日志的日志记录目的地。每个部分都提供了有关配置目的地类型日志记录的指导，以及有关特定于目的地类型的任何行为的信息。配置日志记录目的地后，您可以向 Firewall Manager Amazon WAF 策略提供其规范，以便开始对其进行日志记录。

Note

Firewall Manager 不会修改组织成员账户中的任何现有日志配置。

Amazon Kinesis Data Firehose

本主题提供有关将您的网络 ACL 流量日志发送到 Amazon Kinesis Data Firehose 数据流的信息。

当您启用 Amazon Kinesis Data Firehose 日志记录时，Firewall Manager 会将日志从您的策略的 Web ACL 发送到您在其中配置了存储目的地的 Amazon Kinesis Data Firehose。启用日志记录后，通过 Kinesis Data Firehose 的 HTTPS 端点将每个已配置的 Web ACL 的日志 Amazon WAF 传送到配置的存储目标。在使用之前，请测试您的交付流，以确保其吞吐量足以容纳您组织的日志。有关如何创建 Amazon Kinesis Data Firehose 和查看存储日志的更多信息，请参阅 [什么是 Amazon Kinesis Data Firehose ?](#)

您必须拥有以下权限才能成功启用 Kinesis 日志功能：

- iam:CreateServiceLinkedRole
- firehose:ListDeliveryStreams

- wafv2:PutLoggingConfiguration

当您在Amazon WAF策略上配置 Amazon Kinesis Data Firehose 日志目的地时，Firewall Manager 会在 Firewall Manager 管理员账户中为该策略创建 Web ACL，如下所示：

- 无论该帐户是否在策略范围内，Firewall Manager 都会在Firewall Manager 管理员帐户中创建 Web ACL。
- Web ACL 启用了带有日志名称的日志记录FMMangedWebACLV2-Logging`policy name-timestamp`，其中时间戳是为 Web ACL 启用日志的 UTC 时间，以毫秒为单位。例如，FMMangedWebACLV2-LoggingMyWAFPolicyName-1621880565180。Web ACL 没有规则组，也没有关联的资源。
- 根据Amazon WAF定价指南，您需要为 Web ACL 付费。有关更多信息，请参阅[Amazon WAF 定价](#)。
- 当您删除策略时，Firewall Manager 会删除 Web ACL。

有关服务相关角色和iam:CreateServiceLinkedRole权限的信息，请参阅[将服务相关角色用于 Amazon WAF \(p. 226\)](#)。

有关创建传输流的更多信息，请参阅[创建 Amazon Kinesis Data Firehose 传输流](#)。

Amazon Simple Storage Service 存储桶

本主题提供将 Web ACL 流量日志发送到 Amazon S3 存储桶的信息。

有关创建 Amazon S3 存储桶以满足日志记录和存储段命名要求的要求的信息，请参阅Amazon WAF开发者指南中的[Amazon Simple Storage Service](#)。

最终一致性

当您更改配置有 Amazon S3 日志记录目标的Amazon WAF策略时，Firewall Manager 会更新存储段策略以添加日志记录所需的权限。在这样做时，Firewall Manager 遵循亚马逊简单存储服务遵循的 last-writer-wins 语义和数据一致性模型。如果您同时在Firewall Manager 控制台或通过 [PutPolicy](#) API 对 Amazon S3 目标进行多个策略更新，则某些权限可能无法保存。有关 Amazon S3 数据一致性模型的更多信息，请参阅《[Amazon Simple Storage Service 用户指南](#)》中的[Amazon S3 数据一致性模型](#)。

向 Amazon S3 存储桶发布日志的权限

在Amazon WAF策略中为 Amazon S3 存储桶配置 Web ACL 流量记录需要以下权限设置。当您为 Amazon S3 配置为日志目的地以授予服务向存储桶发布日志的权限时，Firewall Manager 会自动将这些权限附加到您的 Amazon S3 存储桶。如果您想更细致地管理对日志记录和Firewall Manager 资源的访问权限，可以自己设置这些权限。有关管理权限的信息，请参阅 IAM 用户指南中的[Amazon资源访问管理](#)。有关Amazon WAF 托管策略的信息，请参阅[Amazon适用于 Amazon WAF 的托管策略 \(p. 222\)](#)。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForFirewallManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAc1CheckFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAc1",
      "Resource": "arn:aws:s3::aws-waf-example-bucket"
    },
    {
      "Sid": "AWSLogDeliveryWriteFMS",
      "Effect": "Allow",

```

```
        "Principal": {
            "Service": "delivery.logs.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3::aws-waf-logs-example-bucket/policy-id/AWSLogs/*",
        "Condition": {
            "StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control"
            }
        }
    }
}
]
```

为防止出现跨服务混淆的副手问题，您可以将[aws:SourceArn](#)和[aws:SourceAccount](#)全局条件上下文密钥添加到存储桶的策略中。要添加这些密钥，您可以修改 Firewall Manager 在配置日志目的地时为您创建的策略，或者如果您想要精细控制，则可以创建自己的策略。如果您将这些条件添加到您的日志目的地策略中，Firewall Manager 将不会验证或监控混乱的副手保护。有关混淆代理人问题的一般信息，请参阅[混淆代理人问题](#) 在 IAM 用户指南中。

当您添加sourceAccount添加sourceArn属性时，它会增加存储段策略的大小。如果您要添加一长串sourceAccount添加sourceArn属性，请注意不要超过 Amazon S3 [存储桶策略大小配额](#)。

以下示例说明了如何通过使用存储段策略中的aws:SourceArn和aws:SourceAccount全局条件上下文键防止混淆代理问题。*member-account-id*替换为组织中成员的账户 ID。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForFirewallManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAc1CheckFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3::aws-waf-logs-example-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "member-account-id",
            "member-account-id"
          ]
        },
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:logs:*:member-account-id:",
            "arn:aws:logs:*:member-account-id:"
          ]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryWriteFMS",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3::aws-waf-logs-example-bucket/policy-id/AWSLogs/*",
      "Condition": {
        "StringEquals": {
```

```
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceAccount": [
            "member-account-id",
            "member-account-id"
        ],
        "ArnLike": {
            "aws:SourceArn": [
                "arn:aws:logs:*:member-account-id-1:*",
                "arn:aws:logs:*:member-account-id-2:*"
            ]
        }
    }
}
```

服务器端加密

您可以启用 Amazon S3 服务器端加密或在 S3 存储桶上使用 Amazon Key Management Service 客户托管密钥。如果您选择在 Amazon S3 存储桶上使用 Amazon WAF 日志使用默认 Amazon S3 加密，则无需采取任何特殊措施。但是，如果您选择使用客户提供的加密密钥来加密您的 Amazon S3 静态数据，则必须在 Amazon Key Management Service 密钥策略中添加以下权限声明：

```
{
    "Sid": "Allow Logs Delivery to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

有关在 Amazon S3 中使用客户提供的加密密钥的详细信息，请参阅《Amazon S3 [Implement Storage Service User Guide](#)》中的“[使用具有客户提供密钥的服务器端加密 \(SSE-C\)](#)”的详细信息。

启用日志记录

以下过程介绍如何在 Firewall Manager 控制台中启用 Amazon WAF 策略日志功能。

启用 Amazon WAF 策略的日志记录

1. 在启用日志记录之前，必须按以下方式配置日志记录目标资源：

- Amazon Kinesis Data Streams-使用您的 Firewall Manager 管理员账户创建亚马逊 Kinesis Data Firehose。使用以前缀开头的名称 aws-waf-logs-。例如，aws-waf-logs-firewall-manager-central。使用 PUT 源和您正在操作的区域创建数据消防管。如果您要为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚州北部）创建 Firehose。在使用之前，请测试您的交付流，以确保其吞吐量足以容纳您组织的日志。有关更多信息，请参阅[创建 Amazon Kinesis Data Firehose 传输流](#)。
- Amazon Simple Storage Service 存储桶-根据 Amazon WAF 开发者指南中[亚马逊简单存储服务](#)主题中的指南创建 Amazon S3 存储桶。您还必须使用中列出的权限配置 Amazon S3 存储桶[向 Amazon S3 存储桶发布日志的权限 \(p. 446\)](#)。

2. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

3. 在导航窗格中，选择 Security Policies。
4. 选择要为其启用日志记录的Amazon WAF策略。有关 Amazon WAF 日志记录的更多信息，请参阅 [记录 Web ACL 流量 \(p. 180\)](#)。
5. 在策略详细信息选项卡的策略规则部分中，选择编辑。
6. 对于日志配置，选择启用日志记录以启用日志记录。日志记录提供有关由您的 Web ACL 分析的流量的详细信息。选择日志记录目的地，然后选择您配置的日志记录目标。必须选择名称以开头的日志目的地aws-waf-logs-。有关配置Amazon WAF日志目的地的信息，请参见[为Amazon WAF策略配置日志 \(p. 445\)](#)。
7. （可选）如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择Add (添加)。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为REDACTED。
8. （可选）如果您不想将所有请求发送到日志，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个过滤器，选择添加过滤器，然后选择您的筛选条件并指定要保留还是删除符合条件的请求。添加完过滤器后，如果需要，修改默认日志记录行为。有关更多信息，请参阅 Amazon WAF 开发人员指南中的 [管理 Web ACL 的日志记录 \(p. 187\)](#)。
9. 选择下一步。
10. 查看您的设置，然后选择“保存”以保存对策略所做的更改。

禁用日志记录

以下过程介绍如何在Firewall Manager 控制台中禁用Amazon WAF策略的日志记录。

禁用Amazon WAF策略的日志记录

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security Policies。
3. 选择要为其禁用日志记录的Amazon WAF策略。
4. 在策略详细信息选项卡的策略规则部分中，选择编辑。
5. 对于“记录配置状态”，选择“禁用”。
6. 选择下一步。
7. 查看您的设置，然后选择“保存”以保存对策略所做的更改。

Amazon Shield Advanced 策略

在应用启用auto 修复的 Firewall Manager Shield Advanced 策略时，对于每个尚未与Amazon WAF Web ACL 关联的作用域内资源，Firewall Manager 会关联一个空Amazon WAF Web ACL。空的 Web ACL 仅用于 Shield 监视目的。如果您随后将任何其他 Web ACL 关联到该资源，则Firewall Manager 会删除空的 Web ACL 关联。

Note

当Amazon WAF策略范围内的资源进入配置了[自动应用层 DDoS 缓解的 Shield Advanced 策略的范围时](#)，[Firewall Manager 只有在关联Amazon WAF策略创建的 Web ACL 后才会应用 \(p. 354\)](#) Shield Advanced 保护。

如何Amazon Firewall Manager管理Shield 政策中的范围变更

帐户和资源可能会由于许多更改而超出Amazon Firewall Manager Shield Advanced 政策的范围，例如策略范围设置的更改、资源标签的更改以及从组织中删除帐户。有关策略范围设置的一般信息，请参阅[Amazon Firewall Manager策略范围 \(p. 440\)](#)。

使用Amazon Firewall Manager Shield Advanced 策略时，如果帐户或资源超出范围，Firewall Manager 将停止监视该帐户或资源。

如果账户因被从组织中移除而超出范围，则该账户将继续订阅 Shield Advanced。由于该账户不再是整合账单系列的一部分，因此该账户将按比例收取 Shield Advanced 订阅费。另一方面，超出范围但仍留在组织中的账户不会产生额外费用。

如果资源超出范围，它将继续受到 Shield Advanced 的保护，并继续收取 Shield Advanced 的数据传输费用。

自动缓解亚马逊 CloudFront发行版的应用层 DDoS

当您为 Shield Advanced 策略应用于亚马逊 CloudFront 发行版时，您可以选择在策略中配置 Shield Advanced 自动应用层 DDoS 缓解措施。

有关 Shield Advanced 自动缓解的信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

Shield Advanced 自动缓解应用层 DDoS

- 自动应用层 DDoS 缓解仅适用于亚马逊 CloudFront 资源。

因此，您只能为为全球区域创建的 Shield Advanced 策略选择此选项，用于亚马逊 CloudFront 分配。

- 自动应用层 DDoS 缓解仅适用于使用最新版本Amazon WAF (v2) 创建的 Web ACL。

因此，如果您的策略使用Amazon WAF经典 Web ACL，则需要将该策略替换为新策略，新策略将自动使用最新版本的策略，或者让 Firewall Manager 为现有策略创建新版本的 Web ACL 并切换到使用它们。Amazon WAF有关选项的更多信息，请参阅[将Amazon WAF经典 Web ACL 替换为最新版本的 Web ACL \(p. 451\)](#)。

自动缓解配置

Firewall Manager Shield Advanced 策略的自动应用层 DDoS 缓解选项将 Shield Advanced 自动缓解功能应用于策略范围内的帐户和资源。有关此 Shield Advanced 功能的详细信息，请参阅[Shield Advanced 自动应用层 DDoS \(p. 354\)](#)。

您可以选择让 Firewall Manager 为策略范围内的 CloudFront发行版启用或禁用自动缓解功能，也可以选择让策略忽略 Shield Advanced 自动防护设置：

- 启用 — 如果您选择启用自动缓解，则还应指定缓解 Shield Advanced 规则应计入还是阻止匹配的 Web 请求。如果范围内的资源未启用自动缓解功能，或者使用的规则操作与您为策略指定的规则操作不匹配，Firewall Manager 会将这些资源标记为不合规。如果您将策略配置为自动修复，Firewall Manager 会根据需要更新不合规的资源。
- 禁用-如果您选择禁用自动缓解，Firewall Manager 会将范围内的资源标记为不合规，前提是这些资源启用了自动缓解。如果您将策略配置为自动修复，Firewall Manager 会根据需要更新不合规的资源。

- 忽略-如果您选择忽略自动缓解，Firewall Manager 在为该策略执行修复活动时不会考虑任何自动缓解设置。此设置允许您通过 Shield Advanced 在资源级别启用或禁用自动缓解功能，而不会被Firewall Manager 覆盖这些设置。

将Amazon WAF经典 Web ACL 替换为最新版本的 Web ACL

自动应用层 DDoS 缓解仅适用于使用最新版本Amazon WAF (v2) 创建的 Web ACL。

要确定您的 Shield Advanced 策略的网页 ACL 版本，请参阅[确定 Shield Advanced 策略使用的版本 \(p. 451\)](#)。

如果您想在 Shield Advanced 策略中使用自动缓解，并且您的策略当前使用Amazon WAF经典 Web ACL，则可以创建新的 Shield Advanced 策略来替换当前的 Shield Advanced 策略，也可以使用本节中描述的选项将早期版本的 Web ACL 替换为当前 Shield Advanced 策略中的新 (v2) Web ACL。新策略始终使用最新版本的创建 Web ACLAmazon WAF。如果您替换了整个策略，则在删除策略时，也可以让Firewall Manager 删除所有早期版本的 Web ACL。本节的其余部分描述了替换现有策略内的 Web ACL 的选项。

当您修改亚马逊 CloudFront 资源的现有 Shield Advanced 策略时，Firewall Manager 可以在任何还没有 v2 Web ACL 的作用域内账户中自动为该策略创建一个新的空Amazon WAF (v2) Web ACL。当Firewall Manager 创建新的 Web ACL 时，如果该策略已在同一账户中具有经Amazon WAF典 Web ACL，则Firewall Manager 使用与现有 Web ACL 相同的默认操作设置来配置新版本的 Web ACL。如果没有现有的经Amazon WAF典 Web ACL，则Firewall Manager 在新的 Web ACLAllow 中将默认操作设置为。Firewall Manager 创建新的 Web ACL 后，您可以根据需要通过Amazon WAF控制台对其进行自定义。

当您选择以下任一策略配置选项时，Firewall Manager 会为尚未拥有新的 (v2) Web ACL 的作用域内帐户创建新的 (v2) Web ACL：

- 当您启用或禁用自动应用层 DDoS 缓解时。仅此选择仅会导致Firewall Manager 创建新的 Web ACL，而不会替换策略范围内资源上的任何现有Amazon WAF经典 Web ACL 关联。
- 当您选择自动修复的策略操作并选择将Amazon WAF经典 Web ACL 替换为Amazon WAF (v2) Web ACL 的选项时。无论您为应用层 DDoS 自动缓解选择了何种配置，您都可以选择替换早期版本的 Web ACL。

选择替换选项时，Firewall Manager 会根据需要创建新版本的 Web ACL，然后对策略的作用域内资源执行以下操作：

- 如果资源与任何其他活动Firewall Manager 策略中的 Web ACL 相关联，则Firewall Manager 将不影响该关联。
- 对于任何其他情况，Firewall Manager 都会删除与经Amazon WAF典 Web ACL 的任何关联，并将资源与策略的Amazon WAF (v2) Web ACL 关联。

您可以根据需要选择让Firewall Manager 将早期版本的 Web ACL 替换为新版本的 Web ACL。如果您之前自定义了策略的Amazon WAF经典 Web ACL，则可以在选择让Firewall Manager 执行替换步骤之前，将新版本的 Web ACL 更新为类似设置。

您可以通过相同版本的控制台访问策略的任一版本的 Web ACLAmazon WAF 或Amazon WAF Classic。

在您删除策略本身之前，Firewall Manager 不会删除任何替换的Amazon WAF经典 Web ACL。策略不再使用经Amazon WAF典 Web ACL 后，可以根据需要将其删除。

确定 Shield Advanced 策略使用的版本

您可以通过查看策略的Amazon Config服务关联规则中的参数密钥来确定Amazon WAF您的 Firewall Manager Shield Advanced 策略使用的版本。如果使用的Amazon WAF版本是最新版本，则参数键包括policyId和webAclArn。如果是早期版本Amazon WAF Classic，则参数键包括webAclId和resourceTypes。

该Amazon Config规则仅列出策略当前在作用域内资源中使用的 Web ACL 的密钥。

确定Amazon WAF您的 Firewall Manager Shield Manager Shield

1. 检索 Shield Advanced 策略的策略 ID :

- Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。
- 在导航窗格中，选择 Security Policies。
- 为策略选择区域。对于 CloudFront 发行版来说，这是Global。
- 找到所需的策略并复制其策略 ID 的值。

策略ID示例：1111111-2222-3333-4444-a55aa5aaa555。

2. 通过将策略 ID 附加到字符串来创建策略的Amazon Config规则名称FMManagedShieldConfigRule。

示例Amazon Config规则名称:FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555。

3. 在参数中搜索名为policyId和的密钥的关联Amazon Config规则webAclArn :

- 通过以下网址打开 Amazon Config 控制台：<https://console.aws.amazon.com/config/>。
- 在导航窗格中，选择 Rules (规则)。
- 在列表中找到您的Firewall Manager 策略的Amazon Config规则名称并将其选中。此规则的页面将打开此页。
- 在“规则详细信息”下的“参数”部分，查看密钥。如果您找到名为policyId和的密钥webAclArn，则该策略将使用使用最新版本创建的 Web ACLAmazon WAF。如果您找到名为webAclId和的密钥resourceTypes，则该策略将使用使用早期版本 CAamazon WAF classic 创建的 Web ACL。

安全组策略

您可以使用Amazon Firewall Manager安全组策略来管理您的组织的Amazon Virtual Private Cloud 安全组 Amazon Organizations。您可以将集中控制的安全组策略应用于整个组织或部分账户和资源。您还可以通过审核和使用安全组策略来监控和管理组织中正在使用的安全组策略。

Firewall Manager 会持续维护您的策略，并在整个组织中添加或更新帐户和资源时将其应用于这些帐户和资源。有关的信息Amazon Organizations，请参阅《[Amazon Organizations用户指南](#)》。有关 Amazon [Virtual Private Cloud Virtual VPC 安全组](#)的信息，请参阅《[Amazon VPC 用户指南](#)》中的 VPC 的安全组。

您可以使用 Firewall Manager 安全组策略在整个Amazon组织中执行以下操作：

- 将通用安全组应用到指定的账户和资源。
- 审计安全组规则，以查找和修正不合规的规则。
- 审计安全组的使用情况，以清理未使用的和冗余的安全组。

本节介绍Firewall Manager 安全组策略的工作原理，并提供使用指南。有关创建安全组策略的过程，请参阅[创建 Amazon Firewall Manager 策略 \(p. 422\)](#)。

通用安全组策略

Firewall Manager 通过通用安全组策略在组织中提供集中控制的安全组与账户和资源的关联。您可以指定在企业中应用策略的位置和方式。

您可以将常见的安全组策略应用于以下资源类型：

- Amazon Elastic Compute Cloud (Amazon EC2)
- 弹性网络接口

- Application Load Balancer
- 经典负载均衡器

有关使用控制台创建通用安全组策略的指南，请参阅[创建通用安全组策略 \(p. 428\)](#)。

共享 VPC

在通用安全组策略的策略范围设置中，可以选择包括共享 VPC。此选项包括由另一个账户拥有并与范围内账户共享的 VPC。始终包括范围内账户拥有的 VPC。有关共享 VPC 的信息，请参阅[Amazon VPC 用户指南中的使用共享 VPC](#)。

以下注意事项适用于包含共享 VPC。这些是关于安全组策略的一般注意事项的补充[安全组策略限制 \(p. 456\)](#)。

- Firewall Manager 将主安全组复制到每个作用域内账户的 VPC 中。对于共享 VPC，Firewall Manager 会为与之共享 VPC 的每个作用域内账户复制一次主安全组。这可能会导致单个共享 VPC 中存在多个副本。
- 创建新的共享 VPC 时，在 Firewall Manager 安全组策略详细信息中不会看到该共享 VPC，直到您在 VPC 中创建了至少一个策略范围内的资源。
- 当您在启用了共享 VPC 的策略中禁用共享 VPC 时，在共享 VPC 中，Firewall Manager 会删除与任何资源均不关联的副本安全组。Firewall Manager 将剩余的副本安全组保留在原处，但停止对其进行管理。删除这些其余的安全组时，需要在每个共享 VPC 实例中执行手动管理。

主要安全组

对于每种常见安全组策略，您 Amazon Firewall Manager 提供一个或多个主要安全组：

- 主要安全组必须由 Firewall Manager 管理员账户创建，并且可以位于该账户中的任何 Amazon VPC 实例中。
- 您可以通过 Amazon Virtual VPC (Amazon VPC) 或 Amazon Elastic Cloud (Amazon EC2) 管理主要安全组。有关信息，请参阅[Amazon VPC 用户指南中的与安全组合作](#)。
- 您可以将一个或多个安全组命名为 Firewall Manager 安全组策略的主安全组。默认情况下，策略中允许的安全组数量为一，但您可以提交增加安全组的请求。有关信息，请参阅[Amazon Firewall Manager 配额 \(p. 497\)](#)。

策略规则设置

您可以为常用安全组策略的安全组和资源选择以下一种或多种变更控制行为：

- 识别并报告本地用户对副本安全组所做的任何更改。
- 取消任何其他安全组与策略范围内的 Amazon 资源的关联。
- 将标签从主组分配到副本安全组。

Important

Firewall Manager 不会将通过 Amazon 服务添加的系统标签分发到副本安全组中。系统标签以 `aws:` 为前缀。此外，如果策略的标签与组织的标签策略冲突，Firewall Manager 不会更新现有安全组的标签或创建新的安全组。有关标签策略的信息，请参阅 Amazon Organizations 用户指南中的[标签策略](#)。

策略创建和管理

当您创建通用安全组策略时，Firewall Manager 会将主要安全组复制到策略范围内的每个 Amazon VPC 实例，并将复制的安全组与策略范围内的账户和资源关联起来。修改主安全组时，Firewall Manager 会将更改传播到副本。

删除常见安全组策略时，您可以选择是否清理该策略创建的资源。对于Firewall Manager 常见安全组，这些资源是副本安全组。除非您想在删除策略后手动管理每个副本，否则请选择清理选项。在大多数情况下，选择清理选项是最简单的方法。

如何管理副本

Amazon VPC 实例中的副本安全组像其他 Amazon VPC 安全组一样进行管理。有关信息，请参阅 [《Amazon VPC 用户指南》中的 VPC 的安全组](#)。

内容审核安全组策略

使用Amazon Firewall Manager内容审核安全组策略来检查和管理组织的安全组中使用的规则。根据您在策略中定义的范围，内容审计安全组策略适用于Amazon组织中使用的所有客户创建的安全组。

有关使用控制台创建内容审计安全组策略的指导，请参阅[创建内容审核安全组策略 \(p. 429\)](#)。

策略范围资源类型

您可以将内容审计安全组策略应用于以下资源类型：

- Amazon Elastic Compute Cloud (Amazon EC2)
- 弹性网络接口
- Amazon VPC 安全组

如果安全组明确位于策略范围内，或者与范围内的资源相关联，则将其视为策略的范围。

策略规则选项

您可以对每个内容审计策略使用托管策略规则或自定义策略规则，但不能同时使用两者。

- 托管策略规则-在具有托管规则的策略中，您可以使用应用程序和协议列表来指定策略允许的内容和拒绝的内容。您可以使用由Firewall Manager 管理的列表。您也可以创建和使用自己的应用程序和协议列表。有关这些类型的列表以及您的自定义列表管理选项的信息，请参阅[托管列表 \(p. 441\)](#)。
- 自定义策略规则-在具有自定义策略规则的策略中，您可以指定现有安全组作为策略的审计安全组。您可以使用审计安全组规则作为模板来定义策略允许或拒绝的规则。

审计安全组

必须先使用您的 Firewall Manager 管理员帐户创建审计安全组，然后才能在策略中使用它们。您可以通过 Amazon VPC (Amazon VPC) 或Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 [Amazon VPC 用户指南](#)中的[与安全组合作](#)。

Firewall Manager 仅将您用于内容审计安全组策略的安全组用作策略范围内的安全组的比较参考。Firewall Manager 不会将其与组织中的任何资源相关联。

您在审计安全组中定义规则的方式取决于您在策略规则设置中的选择：

- 托管策略规则-对于托管策略规则设置，您可以使用审计安全组来覆盖策略中的其他设置，明确允许或拒绝否则可能会产生其他合规性结果的规则。
 - 如果您选择始终允许在审计安全组中定义的规则，则无论其他策略设置如何，任何与审计安全组中定义的规则相匹配的规则都被视为符合该策略。
 - 如果您选择始终拒绝在审计安全组中定义的规则，则无论其他策略设置如何，任何与审计安全组中定义的规则相匹配的规则都被视为不符合该策略。
- 自定义策略规则-对于自定义策略规则设置，审计安全组提供范围内的安全组规则中可接受或不可接受的示例：

创建审计安全组策略时，必须禁用自动修复。建议的做法是在启用自动补救之前查看策略创建的影响。查看

受审计安全组策略影响的安全组

您组织中由客户创建的所有安全组都有资格进入审计安全组策略的范围。

副本安全组不是客户创建的，因此没有资格直接进入审计安全组策略的范围。但是，由于策略的自动补救活

使用情景审核它个组策略

使用Amazon Firewall Manager使用情况审计安全组策略监控组织中是否存在未使用和安全的安全组，并可

1 合并冗余安全组（如果选择了该选项）。

- Amazon VPC 安全组

Firewall Manager 如何修复冗余安全组

要将安全组视为冗余，它们必须设置完全相同的规则并且位于相同的 Amazon VPC 实例中。要修复冗余安全

Note

如果你还选择删除未使用的安全组，则Firewall Manager 接下来会执行此操作。这可能导致删除可

Firewall Manager 如何修复未使用的安全组

要使安全组被视为未使用，任何资源都必须在策略规则指定的最小分钟数内未使用这些安全组。默认情况

默认账户规范

当您通过控制台创建使用情况审计安全组策略时，Firewall Manager 会自动选择排除指定帐户并包括所有其

安全组策略的最佳实践

本节列出了使用管理安全组的建议Amazon Firewall Manager。

排除Firewall Manager 管理员帐户

设置策略范围时，排除Firewall Manager 管理员帐户。当您通过控制台创建使用情况审计安全组策略时，这是默认选项。

从禁用自动修复开始

对于内容或使用情况审计安全组策略，请先禁用自动修复。查看策略详细信息以确定自动补救将产生的影响。在您确定进行了所需的更改时，请编辑策略以启用自动修复。

如果您还使用外部资源来管理安全组，则可以避免冲突

如果您使用Firewall Manager 以外的工具或服务来管理安全组，请注意避免Firewall Manager 中的设置与外部源中的设置发生冲突。如果您使用自动修复而您的设置发生冲突，则可能会创建一个冲突补救循环，从而消耗双方的资源。

例如，假设您配置了另一项服务来维护一组Amazon资源的安全组，并且配置了 Firewall Manager 策略来为部分或全部相同资源维护不同的安全组。如果您将任一端配置为禁止任何其他安全组与作用域内的资源相关联，则该端将删除另一方维护的安全组关联。如果双方都以这种方式配置，则最终可能会出现相互冲突的解除关联和关联的循环。

此外，假设您创建了 Firewall Manager 审计策略来强制执行与其他服务的安全组配置冲突的安全组配置。Firewall Manager 审计策略应用的补救措施可以更新或删除该安全组，使其与其他服务不兼容。如果将其他服务配置为监视和自动修复发现的任何问题，它将重新创建或更新安全组，使其再次不符合Firewall Manager 审计策略。如果将 Firewall Manager 审计策略配置为自动修复，它将再次更新或删除外部安全组，依此类推。

为避免此类冲突，请在Firewall Manager 任何外部来源之间创建相互排斥的配置。

您可以使用标记将外部安全组排除在Firewall Manager 策略的自动修复范围之外。为此，请向外部源管理的安全组或其他资源添加一个或多个标签。然后，当您定义 Firewall Manager 策略范围时，在资源规范中排除带有您添加的一个或多个标签的资源。

同样，在您的外部工具或服务中，将 Firewall Manager 管理的安全组排除在任何管理或审计活动之外。要么不要导入Firewall Manager 资源，要么使用Firewall Manager 特定的标记将其排除在外部管理之外。

安全组策略限制

本节列出了使用Amazon Firewall Manager安全组策略的限制：

- 不支持更新使用 Fargate 服务类型创建的 Amazon EC2 弹性网络接口的安全组。但是，您可以使用 Amazon EC2 服务类型更新 Amazon ECS 弹性网络接口的安全组。
- Firewall Manager 不支持由Amazon Relational Database Service 创建的 Amazon EC2 弹性网络接口的安全组。
- 更新Amazon ECS 弹性网络接口只能用于使用滚动更新 (Amazon ECS) 部署控制器的 Amazon ECS 服务。对于其他 Amazon ECS 部署控制器，例如 CODE_DEPLOY 或外部控制器，Firewall Manager 目前无法更新弹性网络接口。
- 使用 Amazon EC2 弹性网络接口的安全组，Firewall Manager 无法立即看到对安全组的更改。Firewall Manager 通常会在几个小时内检测到更改，但检测可能会延迟多达六个小时。
- Firewall Manager 不支持更新网络负载均衡器的弹性网络接口中的安全组。
- Firewall Manager 不支持常见安全组策略中的安全组引用。

安全组策略使用案例

您可以使用 Amazon Firewall Manager 常见的安全组策略自动配置主机防火墙，以实现 Amazon VPC 实例之间的通信。本节列出了标准的 Amazon VPC 架构，并描述了如何使用 Firewall Manager 常见安全组策略保护每个架构。这些安全组策略可以帮助您应用一组统一的规则来选择不同账户中的资源，并避免在 Amazon Elastic Compute Cloud 和 Amazon VPC 中按账户进行配置。

使用 Firewall Manager 常见安全组策略，您可以仅标记与其他 Amazon VPC 中的实例通信所需的 EC2 弹性网络接口。这样，同一 Amazon VPC 中的其他实例就会变得更加安全和隔离。

用例：监视和控制对应用程序负载均衡器和经典负载均衡器的请求

您可以使用 Firewall Manager 的通用安全组策略来定义您的作用域内负载均衡器应处理哪些请求。您可以通过 Firewall Manager 控制台进行配置。只有符合安全组入站规则的请求才能到达您的负载均衡器，负载均衡器只会分发符合出站规则请求。

用例：可访问互联网的公共 Amazon VPC

您可以使用 Firewall Manager 通用安全组策略来保护公有 Amazon VPC，例如，仅允许入站端口 443。这与仅允许公共 VPC 的入站 HTTPS 流量相同。您可以标记 VPC 中的公共资源（例如，“publicVPC”），然后将 Firewall Manager 策略范围设置为仅带有该标签的资源。Firewall Manager 自动将策略应用于这些资源。

用例：公有和私有 Amazon VPC 实例

您可以对公共资源使用相同的通用安全组策略，如先前用例中针对可访问互联网的公用 Amazon VPC 实例所建议的那样。您可以使用第二个通用安全组策略来限制公共资源和私有资源之间的通信。使用类似“PublicPrivate”的内容标记公有和私有 Amazon VPC 实例中的资源，以将第二个策略应用于它们。您可以使用第三个策略来定义私有资源与其他公司或私有 Amazon VPC 实例之间允许的通信。对于此策略，您可以在私有资源上使用其他识别标签。

用例：中心和分支 Amazon VPC 实例

您可以使用通用安全组策略来定义中心 Amazon VPC 实例和分支 Amazon VPC 实例之间的通信。您可以使用第二个策略来定义从每个分支 Amazon VPC 实例到中心 Amazon VPC 实例的通信。

用例：Amazon EC2 实例的默认网络接口

您可以使用通用安全组策略仅允许标准通信，例如内部 SSH 和 Patch/OS 更新服务，并禁止其他不安全的通信。

用例：识别具有开放权限的资源

您可以使用审计安全组策略来识别组织内有权与公共 IP 地址通信或拥有属于第三方供应商的 IP 地址的所有资源。

Amazon Network Firewall 策略

您可以使用 Amazon Firewall Manager Network Amazon Network Firewall 策略来管理组织内的 Amazon Virtual Private Cloud VPC 的防火墙 Amazon Organizations。您可以将集中控制的防火墙应用于整个组织或部分账户和 VPC。

Network Firewall 为您的 VPC 中的公共子网提供网络流量过滤保护。Firewall Manager 根据您的策略定义的防火墙管理类型创建和管理您的防火墙。Firewall Manager 提供以下防火墙管理模型：

- 分布式-对于策略范围内的每个账户和 VPC，Firewall Manager 会创建 Network Firewall 并将防火墙终端节点部署到 VPC 子网，以过滤网络流量。
- 集中式-Firewall Manager 在单个 Amazon VPC 中创建单个 Network Firewall 防火墙。

- 导入现有防火墙-Firewall Manager 在单个Firewall Manager 策略中导入现有防火墙进行管理。您可以对由您的策略管理的导入的防火墙应用其他规则，以确保您的防火墙符合您的安全标准。

Note

Firewall Manager Network Firewall 策略是Firewall Manager 策略，用于管理组织内的 VPC 的 Network Firewall 保护。

Network Firewall 保护是在Network Firewall 服务中的资源中指定的，这些资源称为防火墙策略。

有关使用 Network Firewall 的信息，请参阅[Amazon Network Firewall开发人员指南](#)。

以下各节涵盖了使用Firewall Manager Network Firewall 策略的要求，并描述了这些策略的工作原理。有关创建策略的过程，请参阅[为 Amazon Network Firewall 创建Amazon Firewall Manager策略 \(p. 432\)](#)。

必须启用资源共享

Network Firewall 策略在组织中的账户之间共享Network Firewall 规则组。要使此功能起作用，您必须启用资源共享Amazon Organizations。有关如何启用资源共享的信息，请参阅[Network Firewall 和 DNS 防火墙策略的资源共享 \(p. 465\)](#)。

您必须定义Network Firewall 规则组

指定新的Network Firewall 策略时，定义防火墙策略的方法与Amazon Network Firewall直接使用时相同。您可以指定要添加的无状态规则组、默认无状态操作和有状态的规则组。您的规则组必须已经存在于 Firewall Manager 管理员帐户中，您才能将其包含在策略中。有关创建Network Firewall 规则组的信息，请参阅[Amazon Network Firewall规则组](#)。

Firewall Manager 如何创建防火墙端点

您的策略中的防火墙管理类型决定了Firewall Manager 如何创建防火墙。您的策略可以创建分布式防火墙、集中式防火墙，也可以导入现有的防火墙：

- 分布式-使用分布式部署模型，Firewall Manager 为策略范围内的每个 VPC 创建终端节点。您可以通过指定要在哪些可用区域中创建防火墙端点来自定义终端节点位置，或者Firewall Manager 可以在具有公共子网的可用区域中自动创建终端节点。如果您手动选择可用区，则可以选择限制每个可用区允许的 CIDR 集。如果您决定让 Firewall Manager 自动创建终端节点，则还必须指定该服务是在您的 VPC 中创建单个端点还是多个防火墙端点。
 - 对于多个防火墙端点，Firewall Manager 会在每个可用区域部署防火墙终端节点，在该可用区中，您的子网中有 Internet 网关或Firewall Manager 创建的防火墙端点路由。这是网络Firewall 策略的默认选项。
 - 对于单个防火墙端点，Firewall Manager 在任何具有 Internet 网关路由的子网的单个可用区中部署防火墙端点。使用此选项，其他区域的流量需要跨越区域边界才能被防火墙过滤。

Note

对于这两个选项，都必须有一个与包含 IPv4/PrefixList 路由的路由表关联的子网。Firewall Manager 不检查任何其他资源。

- 集中化-使用集中部署模式，Firewall Manager 在检查 VPC 内创建一个或多个防火墙端点。检查 VPC 是中央 VPC，Firewall Manager 在其中启动您的终端节点。使用集中式部署模型时，还可以指定要在哪些可用区域中创建防火墙端点。创建策略后，您无法更改检查 VPC。要使用不同的检查 VPC，您必须创建新的策略。
- 导入现有防火墙-导入现有防火墙时，您可以通过向策略中添加一个或多个资源集来选择要在策略中管理的防火墙。资源集是资源的集合，在本例中为 Network Firewall 中的现有防火墙，由组织中的帐户管理。在策略中使用资源集之前，必须首先创建资源集。有关Firewall Manager 资源集的信息，请参见[在Firewall Manager 中使用资源集 \(p. 466\)](#)。

使用导入的防火墙时以下事项，使用导入的防火墙时以下事项

- 如果导入的防火墙变得不合规，Firewall Manager 将尝试自动解决违规问题，以下情况除外：
 - 如果防火墙管理器和Network Firewall 策略的有状态或无状态默认操作不匹配。

- 如果导入的防火墙的防火墙策略中的规则组与Firewall Manager 策略中的规则组具有相同的优先级。
- 如果导入的防火墙使用的防火墙策略与不属于策略资源集的防火墙相关联。之所以会发生这种情况，是因为防火墙只能有一个防火墙策略，但是单个防火墙策略可以与多个防火墙相关联。
- 如果属于导入的防火墙的防火墙策略的预先存在的规则组也在 Firewall Manager 策略中指定，则被赋予不同的优先级。
- 如果您在策略中启用资源清理，Firewall Manager 会从资源集范围内的防火墙中删除 FMS 导入策略中的规则组。
- 由Firewall Manager 管理的防火墙导入现有的防火墙一次只能由一个策略管理。如果将相同的资源集添加到多个导入网络防火墙策略中，则资源集中的防火墙将由该资源集添加到的第一个策略管理，第二个策略将忽略该资源集中的防火墙。

如果您使用分布式或集中式防火墙管理更改策略的可用区域列表，Firewall Manager 将尝试清理过去创建但目前不在策略范围内的任何端点。只有在没有引用范围外端点的路由表路由时，Firewall Manager 才会删除终端节点。如果 Firewall Manager 发现无法删除这些端点，它会将防火墙子网标记为不合规，并将继续尝试删除该端点，直到可以安全删除为止。

Firewall Manager 如何管理您的防火墙子网

防火墙子网是Firewall Manager 为过滤网络流量的防火墙终端节点创建的 VPC 子网。每个Firewall 端点都必须部署在专用 VPC 子网中。Firewall Manager 在策略范围内的每个 VPC 中创建至少一个防火墙子网。

对于使用具有自动端点配置的分布式部署模型的策略，Firewall Manager 仅在具有带有 Internet 网关路由的子网的可用区域中创建防火墙子网，或者子网具有指向 Firewall Manager 为其策略创建的防火墙端点的路由。有关更多信息，请参阅 [Amazon VPC 用户指南](#) 中的 [VPC 和子网](#)。

对于使用分布式或集中式模型的策略，您可以指定Firewall Manager 在哪些可用区域中创建防火墙端点，Firewall Manager 会在这些特定的可用区域中创建终端节点，无论可用区中是否有其他资源。

首次定义Network Firewall 策略时，需要指定Firewall Manager 如何管理范围内的每个 VPC 中的防火墙子网。以后您不能更改此选项。

对于使用具有自动端点配置的分布式部署模型的策略，可以在以下选项中进行选择：

- 为每个具有公共子网的可用区部署防火墙子网。这是默认行为。这为您的流量过滤保护提供了高可用性。
- 在一个可用区中部署单个防火墙子网。通过此选择，Firewall Manager 可识别 VPC 中公有子网最多的区域，并在那里创建防火墙子网。单一防火墙端点过滤 VPC 的所有网络流量。这可以降低防火墙成本，但它的可用性不高，并且需要来自其他区域的流量跨越区域边界才能进行过滤。

对于使用具有自定义端点配置的分布式部署模型或集中部署模型的策略，Firewall Manager 会在策略范围内的指定可用区域中创建子网。

您可以提供 VPC CIDR 块供Firewall Manager 用于防火墙子网，也可以将防火墙终端地址的选择留给 Firewall Manager 来决定。

- 如果您不提供 CIDR 块，Firewall Manager 会查询您的 VPC 以获取可用的 IP 地址。
- 如果您提供 CIDR 块列表，Firewall Manager 将仅在您提供的 CIDR 块中搜索新的子网。必须使用 /28 CIDR 块。对于 Firewall Manager 创建的每个防火墙子网，它会遍历您的 CIDR 阻止列表，并使用它找到的第一个适用于可用区域和 VPC 且具有可用地址的防火墙子网。如果 Firewall Manager 无法在 VPC 中找到开放空间（有或没有限制），则该服务不会在 VPC 中创建防火墙。

如果 Firewall Manager 无法在可用区创建所需的防火墙子网，则会将该子网标记为不符合策略。当区域处于这种状态时，该区域的流量必须跨越区域边界才能被另一个区域中的终端节点过滤。这与单一防火墙子网场景类似。

Firewall Manager 如何管理您的Network Firewall 资源

在Firewall Manager 中定义策略时，您需要提供标准Amazon Network Firewall防火墙策略的网络流量过滤行为。您可以添加无状态和有状态的Network Firewall 规则组，并为不匹配任何无状态规则的数据包指定默认操作。有关使用中的防火墙策略的信息Amazon Network Firewall，请参阅[Amazon Network Firewall防火墙策略](#)。

对于分布式和集中式策略，当您保存Network Firewall 策略时，Firewall Manager 会在策略范围内的每个VPC 中创建防火墙和防火墙策略。Firewall Manager 通过连接以下值来命名这些Network Firewall 资源：

- 固定字符串，可以是FMManagedNetworkFirewall或FMManagedNetworkFirewallPolicy，具体取决于资源类型。
- Firewall Manager 策略名称。这是您在创建策略时分配的名称。
- Firewall Manager 策略 ID。这是Firewall Manager 策略的Amazon资源 ID。
- Amazon VPC ID。这是Firewall Manager 创建防火墙和防火墙策略的 VPC 的Amazon资源 ID。

以下显示了由Firewall Manager 管理的防火墙的示例名称：

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

下面是一个示例 Firewall 策略名称：

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

创建策略后，VPC 中的成员账户无法覆盖您的防火墙策略设置或规则组，但他们可以将规则组添加到Firewall Manager 创建的防火墙策略中。

Firewall Manager 如何管理和监视您的策略的 VPC 路由表

Note

使用集中部署模型的策略目前不支持路由表管理。

当Firewall Manager 创建您的防火墙终端节点时，它还会为它们创建 VPC 路由表。但是，Firewall Manager 不管理您的 VPC 路由表。您必须配置 VPC 路由表以将网络流量定向到Firewall Manager 创建的防火墙终端节点。使用 Amazon VPC 入口路由增强功能，更改您的路由表，通过新的防火墙终端节点路由流量。您的更改必须在要保护的子网和外部位置之间插入防火墙端点。您需要执行的确切路由取决于您的架构及其组件。

目前，Firewall Manager 允许监视您的 VPC 路由表路由，以查看任何发往互联网网关的流量，即绕过防火墙的流量。Firewall Manager 不支持其他目标网关，例如 NAT 网关。

有关管理 VPC 的路由表的信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的[“管理 VPC 的路由表”](#)。有关管理Network Firewall [路由表的信息，请参阅Amazon Network Firewall开发者指南Amazon Network Firewall中的路由表配置](#)。

当您启用策略监控时，Firewall Manager 会持续监控 VPC 路由配置，并提醒您绕过该 VPC 的防火墙检查的流量。如果子网有防火墙端点路由，Firewall Manager 会查找以下路由：

- 向网络Firewall 端点发送流量的路由。
- 将流量从Network Firewall 端点转发到互联网网关的路由。
- 从互联网网关到Network Firewall 端点的入站路由。
- 来自防火墙子网的路由。

如果子网有Network Firewall 路由，但Network Firewall 和您的互联网网关路由表中有非对称路由，Firewall Manager 会将该子网报告为不合规。Firewall Manager 还会在Firewall Manager 创建的防火墙路由表以及子网的路由表中检测到指向 Internet 网关的路由，并将其报告为不合规。Network Firewall 子网路由表和您的互联网网关路由表中的其他路由也被报告为不合规。根据违规类型，Firewall Manager 会建议采取补救措施以

使路由配置合规。Firewall Manager 并非在所有情况下都提供建议。例如，如果您的客户子网的防火墙端点是在 Firewall Manager 之外创建的，Firewall Manager 不会建议采取补救措施。

默认情况下，Firewall Manager 会将任何跨越可用区边界的流量标记为不合规以供检查。但是，如果您选择在 VPC 中自动创建单个终端节点，Firewall Manager 不会将跨越可用区边界的流量标记为不合规。

对于使用具有自定义终端节点配置的分布式部署模型的策略，您可以选择将从没有防火墙终端节点的可用区跨越可用区边界的流量标记为合规还是不合规。

Note

- Firewall Manager 不建议对非 IPv4 路由（例如 IPv6 和前缀列表路由）采取补救措施。
- 使用 `DisassociateRouteTable` API 调用发出的调用最长可能需要在 12 小时后才会被检测到。
- Firewall Manager 为包含防火墙端点的子网创建 Network Firewall 路由表。Firewall Manager 假设此路由表仅包含有效的互联网网关和 VPC 默认路由。此路由表中任何额外或无效的路由都被视为不合规。

配置 Firewall Manager 策略时，如果选择监控模式，Firewall Manager 会提供有关您的资源的资源违规和补救详细信息。您可以使用这些建议的补救措施来修复路由表中的路由问题。如果您选择关闭模式，Firewall Manager 不会为您监视路由表内容。使用此选项，您可以自己管理 VPC 路由表。有关这些资源违规的更多信息，请参阅[查看 Amazon Firewall Manager 策略的合规性信息 \(p. 467\)](#)。

Warning

如果您在创建策略时在 Amazon Network Firewall 路由配置下选择监控，则无法为该策略将其关闭。但是，如果您选择 Off，则可以稍后将其启用。

为 Amazon Network Firewall 策略配置日志

您可以启用 Network Firewall 策略的集中日志记录，以获取有关组织内流量的详细信息。您可以选择流量记录来捕获网络流量，也可以选择警报日志来报告与规则操作设置为 DROP 或的规则相匹配的流量 ALERT。有关 Amazon Network Firewall 日志记录的更多信息，请参阅《Amazon Network Firewall 开发人员指南》Amazon Network Firewall [中的记录网络流量](#)。

您将日志从策略的 Network Firewall 发送到 Amazon S3 存储桶。启用日志记录后，通过更新防火墙设置，将日志 Amazon Network Firewall 传输到带有预留 Amazon Firewall Manager 前缀的选定 Amazon S3 存储桶，从而为每个配置的 Network Firewall 提供日志 `<policy-name>-<policy-id>`。

Note

Firewall Manager 使用此前缀来确定日志配置是由 Firewall Manager 添加的，还是由账户所有者添加的。如果账户所有者尝试使用保留的前缀进行自己的自定义日志记录，则该前缀将被 Firewall Manager 策略中的日志配置所覆盖。

有关如何创建 Amazon S3 存储桶和查看存储日志的更多信息，请参阅[什么是 Amazon S3？](#)在 Amazon Simple 存储服务用户指南中。

要启用日志记录，您必须满足以下要求：

- 您在 Firewall Manager 策略中指定的 Amazon S3 必须是存在的。
- 您必须拥有以下权限：
 - `logs:CreateLogDelivery`
 - `s3:GetBucketPolicy`
 - `s3:PutBucketPolicy`
- 如果作为您的日志记录目标的 Amazon S3 存储桶使用服务器端加密以及存储在中的 Amazon Key Management Service 密钥，则必须将以下策略添加到 Amazon KMS 客户管理的密钥中，以允许 Firewall Manager 登录到您的 CloudWatch 日志日志组：

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "delivery.logs.amazonaws.com"
  },
  "Action": [
    "kms:Encrypt*",
    "kms:Decrypt*",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:Describe*"
  ],
  "Resource": "*"
}
```

请注意，只有 Firewall Manager 管理员帐户中的存储段可用于 Amazon Network Firewall 集中日志。

在 Network Firewall 策略上启用集中登录时，Firewall Manager 会对您的帐户执行以下操作：

- Firewall Manager 更新选定 S3 存储桶的权限以允许日志传输。
- Firewall Manager 在 S3 存储桶中为策略范围内的每个成员帐户创建目录。每个帐户的日志都可以在以下网址找到 <bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>。

启用 Network Firewall 策略的日志记录

1. 使用您的 Firewall Manager 管理员帐户创建 Amazon S3 存储桶。有关更多信息，请参阅《《Amazon Simple Storage Service Service Service》》。
2. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员帐户的信息，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

3. 在导航窗格中，选择 Security Policies。
4. 选择要为其启用日志记录的网络 Firewall 策略。有关 Amazon Network Firewall 日志记录的更多信息，请参阅《Amazon Network Firewall 开发者指南》Amazon Network Firewall [中的记录网络流量](#)。
5. 在策略详细信息选项卡的策略规则部分中，选择编辑。
6. 要启用和聚合日志，请在日志配置下选择一个或多个选项：
 - 启用和聚合流日志
 - 启用和汇总警报日志
7. 选择要将日志传输到其中的 Amazon S3 存储桶。您必须为启用的每种日志类型选择一个存储桶。您可针对两种日志类型使用同一存储桶。
8. （可选）如果您希望将自定义成员帐户创建的日志记录替换为策略的日志配置，请选择覆盖现有的日志配置。
9. 选择下一步。
10. 查看您的设置，然后选择“保存”以保存对策略所做的更改。

禁用 Network Firewall 策略的日志记录

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security Policies。
3. 选择要为其禁用日志记录的网络 Firewall 策略。
4. 在策略详细信息选项卡的策略规则部分中，选择编辑。
5. 在“记录配置状态”下，取消选择“启用和聚合流日志”以及“启用和聚合警报日志”（如果已选择）。
6. 选择下一步。
7. 查看您的设置，然后选择“保存”以保存对策略所做的更改。

Amazon Resolver DNS 防火墙策略

您可以使用 Amazon Firewall Manager DNS 防火墙策略来管理组织内的 Amazon Route 53 Resolver DNS 防火墙规则组与您的 Amazon Virtual Private Cloud VPC 之间的关联 Amazon Organizations。您可以将集中控制的规则组应用于整个组织，也可以应用于账户和 VPC 的选定子集。

DNS 防火墙为您的 VPC 的出站 DNS 流量提供筛选和调节。您可以在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，并将规则组关联到您的 VPC。当您应用 Firewall Manager 策略时，对于策略范围内的每个账户和 VPC，Firewall Manager 会使用您在 Firewall Manager 策略中指定的关联优先级设置，在策略中的每个 DNS 防火墙规则组与策略范围内的每个 VPC 之间创建关联。

有关使用 DNS 防火墙的信息，请参阅[亚马逊 Route 53 开发者指南中的 Amazon Route 53 Resolver DNS 防火墙](#)。

以下部分涵盖了使用 Firewall Manager DNS 防火墙策略的要求，并描述了这些策略的工作原理。有关创建策略的过程，请参阅[为亚马逊 Route 53 Resolver DNS Firewall \(p. 435\)](#)。

必须启用资源共享

DNS 防火墙策略在组织中的账户之间共享 DNS 防火墙规则组。要使此功能起作用，您必须启用资源共享 Amazon Organizations。有关如何启用资源共享的信息，请参阅[Network Firewall 和 DNS 防火墙策略的资源共享 \(p. 465\)](#)。

您必须定义 DNS Firewall 规则组

指定新的 DNS 防火墙策略时，定义规则组的方式与直接使用 Amazon Route 53 Resolver DNS 防火墙时相同。您的规则组必须已经存在于 Firewall Manager 管理员帐户中，您才能将其包含在策略中。有关创建 DNS 防火墙规则组的信息，请参阅[DNS 防火墙规则组和规则](#)。

您可以定义最低和最高优先级的规则组关联

您通过 Firewall Manager DNS 防火墙策略管理的 DNS 防火墙规则组关联包含您的 VPC 的最低优先级关联和最高优先级的关联。在您的策略配置中，这些规则组显示为第一个和最后一个规则组。

DNS 防火墙按以下顺序过滤 VPC 的 DNS 流量：

1. 第一个规则组，由您在 Firewall Manager DNS Firewall 策略中定义。有效值在 1 到 99 之间。
2. 个人账户管理员通过 DNS 防火墙关联的 DNS 防火墙规则组。
3. 最后一个规则组，由您在 Firewall Manager DNS Firewall 策略中定义。有效值在 9901 到 10000 之间。

删除规则组

要从 Firewall Manager DNS 防火墙策略中删除规则组，必须执行以下步骤：

1. 取消共享中的规则组Amazon Resource Access Manager。要取消共享您拥有的规则组，必须从资源共享中将其删除。您可以使用Amazon RAM控制台或Amazon CLI 完成该操作。有关取消共享资源的信息，请参阅《Amazon RAM用户指南》中的[Amazon RAM “更新资源共享”](#)。
2. 使用 DNS 防火墙控制台或Amazon CLI 删除规则组。
3. 从您的Firewall Manager DNS Firewall 策略中删除规则

Firewall Manager 如何命名其创建的规则组关联

保存 DNS 防火墙策略时，如果您启用了自动修复，Firewall Manager 将在您在策略中提供的规则组与该策略范围内的 VPC 之间创建 DNS 防火墙关联。Firewall Manager 通过连接以下值来命名这些关联：

- 固定字符串，FMManaged_。
- FiFirewall Manager 策略 ID。这是Firewall Manager 策略的Amazon资源 ID。

以下显示了由Firewall Manager 管理的防火墙的示例名称：

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

创建策略后，如果 VPC 中的账户所有者覆盖了您的防火墙策略设置或规则组关联，则 Firewall Manager 会将该策略标记为不合规并尝试提出补救措施。账户所有者可以将其他 DNS 防火墙规则组关联到 DNS 防火墙策略范围内的 VPC。由个人账户所有者创建的任何关联都必须在您的第一个和最后一个规则组关联之间设置优先级。

帕洛阿尔托网络云 NGFW 政策

Palo Alto Networks 云下一代防火墙 (NGFW) 是一项可用于Amazon Firewall Manager策略的第三方防火墙服务。使用适用于Firewall Manager 的 Palo Alto Networks Cloud NGFW，您可以在所有Amazon账户中创建和集中部署 Palo Alto Networks Cloud NGFW 资源和规则堆栈。

要将 Palo Alto Networks Cloud NGFW 与Firewall Manager 一起使用，请先在Marketplace 上订阅 [Palo Alto Networks Cloud NGFW 即用即付](#) 服务。订阅后，您可以在 Palo Alto Networks Cloud NGFW 服务中执行一系列步骤，以配置您的账户和 Cloud NGFW 设置。然后，创建Firewall Manager Cloud FMS 策略，以集中部署和管理 Palo Alto Networks Cloud NGFW 资源和规则，涵盖Organizations 内所有账户。Amazon

有关创建Firewall Manager 策略的过程，请参阅[为帕洛阿尔托网络Amazon Firewall Manager制定政策 Palo Alto Networks Cloud NGFW \(p. 436\)](#)。有关如何为Firewall Manager 配置和管理 Palo Alto Networks Cloud NGFW 的信息，请参阅Amazon文档中的 [Palo Alto Networks Palo Alto Networks Cloud NGFW](#)。

Fortigate 云原生防火墙 (CNF) 即服务策略

Fortigate 云原生防火墙 (CNF) 即服务是可用于Amazon Firewall Manager策略的第三方防火墙服务。Fortigate CNF 是下一代防火墙服务，可帮助您轻松地保护云网络和管理安全策略。使用 Fortigate CNF for Firewall Manager，您可以在所有Amazon账户中创建和集中部署 Fortigate CNF 资源和策略集。

要将Fortigate CNF与Firewall Manager 一起使用，您首先要在Marketplace 上订阅[Fortigate Cloud Native Firewall \(CNF \) 即服务](#)。订阅后，您可以在 Fortigate CNF 服务中执行一系列步骤来配置您的全局策略集和其他设置。然后，您创建Firewall Manager 策略，以集中部署和管理Amazon Organizations 中所有账户的 Fortigate CNF 资源。

有关创建 Fortigate CNF Firewall Manager 策略的过程，请参阅[Fortigate 云原生防火墙 \(CNF\) 即服务创建Amazon Firewall Manager策略 \(p. 438\)](#)。有关如何配置和管理与Firewall Manager 一起使用的 Fortigate CNF 的信息，请参阅 [Fortigate CNF 文档](#)。

Network Firewall 和 DNS 防火墙策略的资源共享

要管理 Firewall Manager Network Firewall 和 DNS 防火墙策略，必须使用 in 启用资源共Amazon Organizations享Amazon Resource Access Manager。这样，当您创建这些策略类型时，Firewall Manager 可以在您的账户中部署保护。

要启用资源共享，请按照《Amazon Resource Access Manager用户指南》中的“[启用共享Amazon Organizations](#)对象”中的说明进行操作。

资源共享问题

在使用Amazon RAM资源共享时，或者在制定需要资源共享的 Firewall Manager 策略时，您可能会遇到资源共享问题。

这些问题的示例包括：

- 当您按照说明启用共享时，在Amazon RAM控制台中，“启用共享对象”选项显示Amazon Organizations为灰色且不可选择。
- 当您在 Firewall Manager 中制定需要资源共享的策略时，该策略被标记为不合规，您会看到指示资源共享或Amazon RAM未启用资源共享的消息。

如果您遇到资源共享问题，以下事项，尝试以下事项，尝试将其启用。

重试启用资源共享

- 再次尝试使用以下选项之一启用共享：
 - （选项）通过Amazon RAM控制台，按照《Amazon Resource Access Manager用户指南》中的“[启用共享对象](#)”Amazon Organizations 中的说明进行操作。
 - （选项）使用Amazon RAM API 调用EnableSharingWithAwsOrganization。请参阅以下文档[EnableSharingWithAwsOrganization](#)。

在Firewall Manager 中使用资源集

Amazon Firewall Manager资源集是资源的集合，例如防火墙，您可以将这些资源组合在一起并在Firewall Manager 策略中进行管理。资源集使组织中的成员能够精细控制策略中要管理的资源。要使用资源集，请在控制台中或使用 [PutResourceSet](#)API 创建资源集，然后将该资源集添加到您的Firewall Manager 策略中。

您可以为以下资源和安全策略类型创建和管理资源集：

资源类型	Firewall Manager 安全策略类型
Amazon Network Firewall-防火墙	Network Firewall 策略-使用资源集从Network Firewall 导入现有防火墙。有关在Network Firewall 策略中使用资源集的信息，请参阅过程中的 导入现有防火墙 (p. 458) 为 Amazon Network Firewall 创建 Amazon Firewall Manager策略 (p. 432) 步骤。

以下部分涵盖了创建和删除资源集的要求。

主题

- [在Firewall Manager 中使用资源集时的注意事项 \(p. 466\)](#)
- [创建资源集 \(p. 466\)](#)
- [删除资源集 \(p. 467\)](#)

在Firewall Manager 中使用资源集时的注意事项

请注意以下使用资源集时的注意事项

对不存在资源的引用

当您使用 Amazon Resource Name (ARN) 时，Firewall Manager 会验证 Amazon 资源名称 (ARN) 的格式是否正确，但Firewall Manager 不检查引用的资源是否存在。如果资源不存在尚未通过 ARN 验证，Firewall Manager 会将资源引用包含在资源集中。如果稍后创建了具有相同 ARN 的新资源，Firewall Manager 会将资源集关联策略中的规则组应用到新资源。

已删除资源

删除资源集中的资源后，对该资源的引用将保留在资源集中，直到Firewall Manager 管理员将其删除。

离开Amazon Organizations组织的成员账户拥有的资源

如果成员账户离开组织，则对该成员账户拥有的资源的任何引用都将保留在资源集中，但将不再受该资源集关联的任何策略管理。

与多个策略的关联

一个资源集可以与多个策略相关联，但并非所有策略类型都支持管理同一资源的多个策略。有关不支持的场景的信息，请参阅特定策略类型的文档。

创建资源集

创建资源集 (控制台)

1. Amazon Web Services Management Console使用您的Firewall Manager 管理员帐户登录，然后在上打开Firewall Manager 控制台<https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择资源集。
3. 选择“创建资源集”。
4. 对于 Resourcegroup，输入资源集的描述。
5. （可选）输入资源集的描述。
6. 选择下一步。
7. 对于选择资源，选择 Amazon 账户 ID，然后选择选择资源，将此账户拥有和管理的资源添加到资源集中。选择资源后，选择“添加”将资源添加到资源集中。
8. 选择下一步。
9. 对于资源集标签，为资源集添加所需的任何识别标签。有关标签的更多信息，请参阅[使用标签编辑器](#)。
10. 选择下一步。
11. 查看新资源集。要进行任何更改，请在要更改的区域中选择 Edit (编辑)。此操作会将您返回到创建向导中的相应步骤。当您对资源集感到满意时，请选择创建资源集。

删除资源集

在删除资源集之前，必须先取消该资源集与使用该资源集的所有策略的关联。您可以使用控制台或 [PutPolicyAPI](#) 取消策略详细信息页面中的资源组的关联。

删除资源集 (控制台)

1. 在导航窗格中，选择资源集。
2. 选中想要删除的资源集旁边的选项。
3. 选择 Delete (删除)。

查看 Amazon Firewall Manager 策略的合规性信息

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](#)。

对于所有 Amazon Firewall Manager 策略，您可以查看策略范围内账户和资源的合规性状态。如果策略中的设置反映在帐户或资源的设置中，则该帐户或资源符合 Firewall Manager 策略。每种策略类型都有自己的合规性要求，可以在定义策略时调整这些要求。对于某些策略，您还可以查看范围内的资源的详细违规信息，以帮助您更好地了解和管理安全风险。

查看策略的合规性

1. Amazon Web Services Management Console 使用您的 Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台 <https://console.amazonaws.cn/wafv2/fmsv2>。

Note

有关设置 Firewall Manager 管理员账户的信息，请参阅 [Amazon Firewall Manager 先决条件 \(p. 403\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择一个策略。在策略页面的帐户和资源选项卡中，Firewall Manager 列出了组织中的帐户，按策略范围内的帐户和范围外的帐户分组。

策略范围内的帐户窗格列出了每个帐户的合规状态。合规状态表示该策略已成功应用于该帐户的所有范围内的资源。不合规状态表示该策略尚未应用于该帐户的一个或多个范围内的资源。

4. 选择不合规的帐户。在帐户页面中，Firewall Manager 列出了每个不合规资源的 ID 和类型以及该资源违反策略的原因。

Note

对于资源类型 `AWS::EC2::NetworkInterface` (ENI) 和 `AWS::EC2::Instance`，Firewall Manager 可能会显示有限数量的不合规资源。要列出其他不合规的资源，请修复最初为该帐户显示的资源。

5. 如果 Firewall Manager 策略类型是内容审计安全组策略，则可以访问资源的详细违规信息。

要查看违规详细信息，请选择资源。

Note

在添加详细的资源违规页面之前，Firewall Manager 发现不合规的资源可能没有违规详细信息。

在资源页面中，Firewall Manager 根据资源类型列出了有关违规的具体详细信息。

- **AWS::EC2::NetworkInterface**(ENI) — Firewall Manager 显示有关资源不符合的安全组的信息。选择安全组以查看有关它的更多详细信息。
- **AWS::EC2::Instance**— Firewall Manager 显示连接到不合规的 EC2 实例的 ENI。它还显示有关资源不符合的安全组的信息。选择安全组以查看有关它的更多详细信息。
- **AWS::EC2::SecurityGroup**— Firewall Manager 显示以下违规详细信息：
 - 不合规安全组规则-违规的规则，包括其协议、端口范围、IP CIDR 范围和描述。
 - 引用规则-不合规安全组规则违反的审计安全组规则及其详细信息。
 - 违规原因 — 对不合规调查结果的解释。
 - 补救措施-建议采取的措施。如果 Firewall Manager 无法确定安全修复操作，则此字段为空。
- **AWS::EC2::Subnet**— 这用于 Network Firewall 策略。Firewall Manager 显示子网 ID、VPC ID 和可用区。如果适用，Firewall Manager 会包含有关违规的其他信息，例如违规发生的原因或子网应关联的路由表的 ID。违规描述组件包含对资源预期状态和当前不合规状态的描述，以及对导致差异的原因的描述 (如果有)。

例如，子网的预期状态可能是“子网应在其可用区中包含一个 Amazon Network Firewall 子网”，当前状态可能是“ID 为 subnet-1234 的子网在可用区 us-east-1e 中缺少 Network Firewall 子网”，描述可能是“由于没有可用的 CIDR 块，Firewall Manager 无法在该可用区中创建子网”。

- 路由管理违规-对于使用监控模式的Network Firewall 策略，Firewall Manager 会显示基本子网信息，以及子网、Internet 网关和Network Firewall 子网路由表中的预期和实际路由。Firewall Manager 会提醒您，如果实际路由与路由表中的预期路由不匹配，则存在违规行为。
- 路由管理违规的补救措施-对于使用监控模式的Network Firewall 策略，Firewall Manager 建议对存在违规的路由配置采取可能的补救措施。

Example — 路线管理违规和补救建议

子网应通过防火墙端点发送流量，但当前子网将流量直接发送到互联网网关。这是违反路线管理的行为。在这种情况下，建议的补救措施可能是有序操作列表。第一项建议是向Network Firewall 子网的路由表中添加所需的路由，以将传出流量定向到互联网网关，并将来自 VPC 内目的地的传入流量定向到`local`。第二个建议是替换子网路由表中的互联网网关路由或无效的Network Firewall 路由，将传出流量定向到防火墙端点。第三项建议是向互联网网关的路由表中添加所需的路由，以将传入流量定向到防火墙端点。

- **AWS::EC2:InternetGateway**— 这用于启用了监控模式的Network Firewall 策略。
 - 路由管理违规-如果互联网网关未与路由表关联，或者互联网网关路由表中存在无效的路由，则互联网网关不合规。
 - 路由管理违规的补救措施 — Firewall Manager 建议可能的补救措施，以纠正路径管理违规行为。

Example 1 — 路线管理违规和补救建议

互联网网关与路由表无关。建议的补救措施可能是有序操作的列表。第一个操作是创建路由表。第二个操作是将路由表与互联网网关关联。第三个操作是将所需的路由添加到互联网网关路由表中。

Example 2 — 路线管理违规和补救建议

Internet 网关与有效的路由表相关联，但路由配置不正确。建议的补救措施可能是有序操作列表。第一个建议是删除无效路由。第二个是将所需的路由添加到互联网网关路由表中。

- **AWS::NetworkFirewall::FirewallPolicy**— 这用于Network Firewall 策略。Firewall Manager 显示有关Network Firewall 策略的信息，该策略已被修改使其不合规。该信息提供了预期的防火墙策略及其在客户账户中找到的策略，因此您可以比较无状态和有状态的规则组名称和优先级设置、自定义操作名称和默认无状态操作设置。违规描述组件包含对资源预期状态和当前不合规状态的描述，以及对导致差异的原因的描述（如果有）。
- **AWS::EC2::VPC**— 这用于 DNS 防火墙策略。Firewall Manager 显示有关在Firewall Manager DNS 防火墙策略范围内且不符合该策略的 VPC 的信息。提供的信息包括预计与 VPC 关联的预期规则组 and 实际规则组。违规描述组件包含对资源预期状态和当前不合规状态的描述，以及对导致差异的原因的描述（如果有）。

Amazon Firewall Manager 结果

Amazon Firewall Manager为不合规的资源以及它检测到并发送的攻击创建调查结果Amazon Security Hub。有关 Security Hub 发现结果的信息，请参阅[中的调查结果Amazon Security Hub](#)。

当您使用Security Hub 和Firewall Manager 时，Firewall Manager 会自动将您的发现发送到Security Hub。有关开始使用 Security Hub 的信息，请参阅[Amazon Security Hub用户指南Amazon Security Hub](#)中的[设置](#)。

如何查看我的 Firewall Manager 调查结果？

要在 Security Hub 中查看Firewall Manager 查找结果，请按照在 [Security Hub 中使用查找结果中的](#) 指导进行操作，并使用以下设置创建筛选器：

- 属性设置为“产品名称”。
- 运算符设置为 EQUALS。
- 值设置为Firewall Manager。此设置区分大小写。

我可以禁用这个吗？

您可以通过 Security Hub 控制台禁用将 Amazon Firewall Manager 发现结果与 Security Hub 集成。在导航栏中选择“集成”，然后在“Firewall Manager”窗格中选择“禁用集成”。有关更多信息，请参阅 [Amazon Security Hub 用户指南](#)。

Amazon Firewall Manager 查找类型

- [Amazon WAF 策略结果 \(p. 470\)](#)
- [Amazon Shield Advanced 策略结果 \(p. 470\)](#)
- [安全组通用策略结果 \(p. 471\)](#)
- [安全组内容审核策略结果 \(p. 471\)](#)
- [安全组使用情况审核策略结果 \(p. 471\)](#)
- [ALED 53 Resolver DNS Firewall \(p. 472\)](#)

Amazon WAF 策略结果

您可以使用 Firewall Manager Amazon WAF 策略将 Amazon WAF 规则组应用于中的资源 Amazon Organizations。有关更多信息，请参阅 [使用 Amazon Firewall Manager 策略 \(p. 422\)](#)。

资源缺少 Firewall Manager 管理的 Web ACL。

根据 Firewall Manager 策略，Amazon 资源没有 Amazon Firewall Manager 托管 Web ACL 关联。您可以对策略启用 Firewall Manager 修复来纠正此问题。

- 严重性-80
- 状态设置-PASSESED/FALED
- 更新-如果 Firewall Manager 执行修复操作，它将更新调查结果，严重性将从降HIGH至INFORMATIONAL。如果您执行补救措施，Firewall Manager 将不会更新调查结果。

Firewall Manager 托管的 Web ACL 有配置错误的规则组。

根据 Firewall Manager 策略，由 Firewall Manager 管理的 Web ACL 中的规则组配置不正确。这意味着 Web ACL 缺少策略所需的规则组。您可以对策略启用 Firewall Manager 修复来纠正此问题。

- 严重性-80
- 状态设置-PASSESED/FALED
- 更新-如果 Firewall Manager 执行修复操作，它将更新调查结果，严重性将从降HIGH至INFORMATIONAL。如果您执行补救措施，Firewall Manager 将不会更新调查结果。

Amazon Shield Advanced 策略结果

有关 Amazon Shield Advanced 策略的信息，请参阅 [安全组策略 \(p. 452\)](#)。

资源缺少 Shield 高级保护。

根据 Firewall Manager 政策，本应具有 Shield Advanced 保护的 Amazon 资源没有。您可以在策略上启用 Firewall Manager 修复，这将启用对资源的保护。

- 严重性-60
- 状态设置-PASSESED/FALED
- 更新-如果 Firewall Manager 执行修复操作，它将更新调查结果，严重性将从降HIGH至INFORMATIONAL。如果您执行补救措施，Firewall Manager 将不会更新调查结果。

Shield Advanced 检测到针对监控资源的攻击

Shield Advanced 检测到对受保护Amazon资源的攻击。您可以在该策略上启用Firewall Manager 修复。

- 严重性-70
- 状态设置-无
- 更新-Firewall Manager 不更新此发现。

安全组通用策略结果

有关安全组常用策略的信息，请参阅[安全组策略 \(p. 452\)](#)。

资源的安全组配置不正确。

根据 Firewall Manager 策略，Firewall Manager 已发现一项资源缺少Firewall Manager 管理的安全组关联，而防火墙管理器应具有的安全组关联。您可以在策略上启用 Firewall Manager 修复，这会根据策略设置创建关联。

- 严重性-70
- 状态设置-PASSESED/FALED
- 更新-Firewall Manager 更新了此发现。

Firewall Manager 副本安全组与主安全组不同步。

根据其通用安全组策略，Firewall Manager 副本安全组与其主安全组不同步。您可以在策略上启用 Firewall Manager 修复，该策略会将副本安全组与主安全组同步。

- 严重性-80
- 状态设置-PASSESED/FALED
- 更新-Firewall Manager 更新了此发现。

安全组内容审核策略结果

有关安全组内容审计策略的信息，请参阅[安全组策略 \(p. 452\)](#)。

安全组与内容审计安全组不一致。

Firewall Manager 安全组内容审计策略已识别出不合规的安全组。这是客户创建的安全组，在内容审计策略的范围内，不符合策略及其审计安全组定义的设置。您可以对策略启用 Firewall Manager 修复，这会修改不合规的安全组以使其合规。

- 严重性-70
- 状态设置-PASSESED/FALED
- 更新-Firewall Manager 更新了此发现。

安全组使用情况审核策略结果

有关安全组使用情况审计策略的信息，请参阅[安全组策略 \(p. 452\)](#)。

Firewall Manager 发现冗余安全组。

Firewall Manager 安全组使用情况审计发现了一个冗余安全组。这是一个安全组，其规则设置与同一 Amazon Virtual Private Cloud 实例中的另一个安全组相同。您可以对使用情况审计策略启用 Firewall Manager 自动修复，用单个安全组替换冗余安全组。

- 严重性-30
- 状态设置-无
- 更新-Firewall Manager 不更新此发现。

Firewall Manager 发现未使用的安全组。

Firewall Manager 安全组使用情况审计发现了一个未使用的安全组。这是一个未被任何 Firewall Manager 通用安全组策略引用的安全组。您可以对使用情况审计策略启用 Firewall Manager 自动修复，这将删除未使用的安全组。

- 严重性-30
- 状态设置-无
- 更新-Firewall Manager 不更新此发现。

ALED 53 Resolver DNS Firewall

有关 DNS Firewall 策略的信息，请参阅[Amazon Resolver DNS 防火墙策略 \(p. 463\)](#)。

资源缺少 DNS 防火墙保护

VPC 缺少 Firewall Manager DNS 防火墙策略中定义的 DNS 防火墙规则组关联。调查结果列出了策略指定的规则组。

- 严重性-80

Amazon Firewall Manager 中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业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。[责任共担模型](#)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 Web Services 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，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解如何应用于合规性计划范围内的Amazon服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用时应用防火共担模型。以下主题说明如何配置以实现您的安全性和合规性目标。您还将了解如何使用其他Amazon服务来帮助您监控和保护 Fificate Firewall Manager 资源。

主题

- [Firewall Manager \(p. 473\)](#)
- [适用于 Amazon Firewall Manager 的 Identity and Access Management \(p. 473\)](#)
- [中的日志记录和监控 \(p. 496\)](#)
- [Firewall Manager 合规性验证 \(p. 497\)](#)
- [Firewall Manager 中的弹性 \(p. 497\)](#)
- [Amazon Firewall Manager 中的基础设施安全性 \(p. 497\)](#)

Firewall Manager

Amazon [责任共担模式](#) 适用于 Amazon Firewall Manager 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 Amazon Web Services 使用控制台、API、或 Amazon SDK 处理 Firewall Manager 或其他时。Amazon CLI 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。

Firewall Manager 实体（例如策略）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

适用于 Amazon Firewall Manager 的 Identity and Access Management

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）来使用 Firewall Manager 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题

- [受众 \(p. 210\)](#)
- [使用身份进行身份验证 \(p. 211\)](#)
- [使用策略管理访问 \(p. 212\)](#)
- [Amazon Firewall Manager 如何与 IAM 协同工作 \(p. 476\)](#)
- [适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)
- [Amazon 适用于 Amazon Firewall Manager 的托管策略 \(p. 485\)](#)
- [对 Amazon Firewall Manager 身份和访问进行故障排除 \(p. 492\)](#)
- [为 Firewall Manager 使用服务相关角色 \(p. 493\)](#)
- [防止跨服务混淆代理 \(p. 494\)](#)

受众

使用 Amazon Identity and Access Management (IAM) 的方式因您可以在 Firewall Manager 中执行的操作而异。

服务用户-如果您使用 Firewall Manager 服务来完成作业，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Firewall Manager 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Firewall Manager 中的功能，请参阅[对 Amazon Shield 身份和访问进行故障排除 \(p. 396\)](#)。

服务管理员 — 如果您在公司负责管理 Firewall Manager 的资源，您可能对 Firewall Manager 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Firewall Manager 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Firewall Manager 搭配使用的更多信息，请参阅[Amazon Shield 如何与 IAM 协同工作 \(p. 387\)](#)。

IAM 管理员 — 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理 Firewall Manager 的访问的详细信息。要查看您可在 IAM 中使用的 Firewall Manager 基于身份的策略策略，请参阅[适用于 Amazon Shield 的基于身份的策略示例 \(p. 392\)](#)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包 (SDK) 和命令行界面 (CLI)，以便使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅 Amazon 一般参考中的[签名版本 4 签名流程](#)。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的[在 Amazon 中使用多重身份验证 \(MFA\)](#)。

Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 Amazon Account Management 参考指南 中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

IAM 用户和组

[IAM 用户](#)是 Amazon Web Services 账户内对某个人或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[对于需要长期凭证的使用场景定期轮换访问密钥](#)。

[IAM 组](#)是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的[何时创建 IAM 用户（而不是角色）](#)。

IAM 角色

IAM 角色是Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过[切换角色](#)，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以担任角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的[使用 IAM 角色](#)。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access (联合用户访问) – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色信息，请参阅《IAM 用户指南》中的[为第三方身份提供商创建角色](#)。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人 (可信主体) 访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源 (而不是使用角色作为代理)。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。
- 跨服务访问 – 某些 Amazon Web Services使用其它 Amazon Web Services中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
 - 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的[Amazon Firewall Manager 的操作、资源和条件键](#)。
 - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 **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](#)。
 - 服务相关角色 – 服务相关角色是与 Amazon Web Service关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户 中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的[使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限](#)。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的[何时创建 IAM 角色 \(而不是用户 \)](#)。

使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体 (用户、根用户或角色会话) 发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南 中的[JSON 策略概览](#)。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 iam:GetRole 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 [创建 IAM policy](#)。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到 Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的[在托管式策略与内联策略之间进行选择](#)。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 Amazon 托管式策略。

访问控制列表 (ACL)

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Simple Storage Service (Amazon S3)、Amazon WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的[访问控制列表 \(ACL\) 概览](#)。

其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 Principal 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 [IAM 实体的权限边界](#)。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 Amazon Web Services 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 [SCP 的工作原理](#)。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

Amazon Firewall Manager 如何与 IAM 协同工作

在使用 IAM 管理 Firewall Manager 的访问之前，您应该了解哪些 IAM 功能可用于 Firewall Manager。

您可以与 Amazon Firewall Manager 搭配使用的 IAM 功能

IAM 功能	FiFirewall Manager
基于身份的策略 (p. 477)	是
基于资源的策略 (p. 477)	否
策略操作 (p. 478)	是
策略资源 (p. 478)	是
策略条件键 (特定于服务) (p. 479)	否
ACL (p. 479)	否
ABAC (策略中的标签) (p. 480)	是
临时凭证 (p. 480)	是
委托人权限 (p. 480)	是
服务角色 (p. 480)	部分
服务相关角色 (p. 481)	是

要大致了解 Firewall Manager 和其他 Amazon 服务如何与大多数 IAM 功能一起使用，[请参阅 IAM 用户指南中的与 IAM 一起使用的 Amazon 服务](#)。

Firewall Manager 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

要查看 Firewall Manager 基于身份的策略的策略的策略的策略，请参阅[适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)。

Firewall Manager 的基于身份的策略示例

要查看 Firewall Manager 基于身份的策略的策略的策略的策略，请参阅[适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)。

Firewall

支持基于资源的策略。	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service (Amazon S3) 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。主体可以包括账户、用户、角色、联合身份用户或 Amazon Web Services。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 Amazon Web Services 账户中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的[IAM 角色与基于资源的策略有何不同](#)。

FiFirewall Manager

支持策略操作	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

要查看 Firewall Manager 的[操作的列表](#)，请参阅[服务授权参考Amazon Firewall Manager中的定义](#)的操作。

Firewall Manager 中的策略操作在操作前使用以下前缀：

```
fms
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [  
    "fms:action1",  
    "fms:action2"  
]
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 Describe 开头的所有操作，包括以下操作：

```
"Action": "fms:Describe"
```

要查看 Firewall Manager 基于身份的策略的策略的策略的策略，请参阅[适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)。

FiFirewall Manager

支持策略资源	是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN \)](#) 指定资源。对于支持特定资源类型 (称为资源级权限) 的操作，您可以执行此操作。

对于不支持资源级权限的操作 (如列出操作)，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"

```

要查看 Firewall Manager 资源类型及其 ARN 的列表，请参阅服务授权参考Amazon Firewall Manager中的[由定义的资源](#)。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 [Amazon Firewall Manager 定义的操作](#)。

要查看 Firewall Manager 基于身份的策略的策略的策略的策略，请参阅[适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)。

Firewall

支持特定于服务的策略条件键	否

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素 (或 Condition 块) 中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用[条件运算符](#) (例如，等于或小于) 的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。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](#)。

Amazon支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 [Amazon 全局条件上下文键](#)。

要查看 Firewall Manager 条件键的列表，请参阅服务授权参考Amazon Firewall Manager中的[的条件键](#)。要了解您可以对哪些操作和资源使用条件键，请参阅 [Amazon Firewall Manager 定义的操作](#)。

要查看 Firewall Manager 基于身份的策略的策略的策略的策略，请参阅[适用于 Amazon Firewall Manager 的基于身份的策略示例 \(p. 481\)](#)。

Firewall Manager

支持 ACL	否

访问控制列表 (ACL) 控制哪些主体 (账户成员、用户或角色) 有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带有 ABAC 的 ABAC

支持 ABAC (策略中的标签)	是

基于属性的访问控制 (ABAC) 是一种授权策略, 该策略基于属性来定义权限。在 Amazon 中, 这些属性称为标签。您可以将标签附加到 IAM 实体 (用户或角色) 以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略, 以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用, 并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问, 您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的 [条件元素](#) 中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键, 则对于该服务, 该值为 Yes (是)。如果某个服务仅对于部分资源类型支持所有这三个条件键, 则该值为 Partial (部分)。

有关 ABAC 的更多信息, 请参阅《IAM 用户指南》中的 [什么是 ABAC?](#)。要查看设置 ABAC 步骤的教程, 请参阅《IAM 用户指南》中的 [使用基于属性的访问控制 \(ABAC\)](#)。

将临时凭证与 Firewall Manager

支持临时凭证	是

某些 Amazon Web Services 在您使用临时凭证登录时无法正常工作。有关更多信息, 包括 Amazon Web Services 与临时凭证配合使用, 请参阅 IAM 用户指南中的 [使用 IAM 的 Amazon Web Services](#)。

如果您不使用用户名和密码而用其它方法登录到 Amazon Web Services Management Console, 则使用临时凭证。例如, 当您使用贵公司的单点登录 (SSO) 链接访问 Amazon 时, 该过程将自动创建临时凭证。当您以用户身份登录控制台, 然后切换角色时, 您还会自动创建临时凭证。有关切换角色的更多信息, 请参阅《IAM 用户指南》中的 [切换到角色 \(控制台\)](#)。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后, 您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证, 而不是使用长期访问密钥。有关更多信息, 请参阅 [IAM 中的临时安全凭证](#)。

Firewall Manager 的跨服务主体

支持委托人权限	是

当您使用 IAM 用户或角色在 Amazon 中执行操作时, 您将被视为委托人。策略向主体授予权限。使用某些服务时, 您可能会执行一个操作, 此操作然后在不同服务中触发另一个操作。在这种情况下, 您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作, 请参阅服务授权参考中的 [Amazon Firewall Manager 的操作、资源和条件键](#)。

Fi Firewall Manager

支持服务角色	部分

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](#)。

Warning

更改服务角色的权限可能会破坏 Firewall Manager 的功能。仅当 Firewall Manager 提供相关指导时才编辑服务角色。

在 Firewall Manager

要在 Firewall Manager 中使用 [PutNotificationChannel](#) API 操作，您必须选择一个角色来允许 Firewall Manager 访问 Amazon SNS，这样该服务才能代表您发布 Amazon SNS 消息。有关更多信息，请参阅《Amazon Firewall Manager API 参考》中的 [PutNotificationChannel](#)。

下面显示了一个示例 SNS 主题权限设置。要将此策略用您自己的自定义角色，请将 `AWSServiceRoleForFMS` Amazon 资源名称 (ARN) 替换为 `SnsRoleName` ARN。

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

有关 Firewall Manager 操作和资源的更多信息，请参阅 Amazon Identity and Access Management 指南主题 [操作定义者 Amazon Firewall Manager](#)

Firewall

支持服务相关角色	是

服务相关角色是一种与 Amazon Web Service 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅 [能够与 IAM 搭配使用的 Amazon 服务](#)。在表中查找服务相关角色列中包含 Yes 的表。选择 Yes 链接以查看该服务的服务相关角色文档。

适用于 Amazon Firewall Manager 的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Firewall Manager 资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执行任务。要用户用户在其需要的资源上执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的 [创建 IAM policy](#)。

有关 Firewall Manager 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考 Amazon Firewall Manager 中的 [的操作、资源和条件键](#)。

主题

- [策略最佳实践 \(p. 482\)](#)
- [使用 Firewall Manager 控制台 \(p. 482\)](#)
- [允许用户查看他们自己的权限 \(p. 482\)](#)

- [授予对您的Firewall Manager 安全组的读取权限 \(p. 483\)](#)
- [授予对Amazon Firewall Manager资源的完全访问权限 \(p. 483\)](#)

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Firewall Manager 资源。这些操作可能会使 Amazon Web Services 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- Amazon 托管策略及转向最低权限许可入门 - 要开始向用户和工作负载授予权限，请使用 Amazon 托管策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 [Amazon 托管策略](#)或[工作职能的 Amazon 托管策略](#)。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Service（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [IAM Access Analyzer 策略验证](#)。
- Require multi-factor authentication (MFA) [需要多重身份验证 (MFA)] – 如果您所处的场景要求您的 Amazon Web Services 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的[配置受 MFA 保护的 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用Firewall Manager 控制台

要访问 Amazon Firewall Manager 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的中的 Firewall Manager 资源的详细信息Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍可使用 Firewall Manager 控制台，请同时将 Firewall Manager [ConsoleAccess](#) 或 [ReadOnly](#) Amazon 托管策略添加到实体。有关更多信息，请参阅 IAM 用户指南中的[为用户添加权限](#)。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",

```

```
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
```

授予对您的Firewall Manager 安全组的读取权限

Firewall Manager 允许跨账户资源访问，但它不允许您创建跨账户资源保护。您只能在拥有这些资源的账户内为资源创建保护。

以下是授予对所有资源执行fms:Getfms:List、和ec2:DescribeSecurityGroups操作的权限的示例策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "fms:Get*",
        "fms:List*",
        "ec2:DescribeSecurityGroups"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

授予对Amazon Firewall Manager资源的完全访问权限

如果您在使用托管策略创建或管理 Firewall Manager 策略时遇到困难，请遵循本指南AWSFMAAdminFullAccess。有关使用的托管策略的信息Amazon Firewall Manager，请参阅。

此政策不包括在中设置亚马逊简单通知服务通知的权限Amazon Firewall Manager。有关如何设置亚马逊简单通知服务的访问权限的信息，请参阅[设置亚马逊简单通知服务的访问权限](#)。

使用以下策略向您的账户授予完全管理访问权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
"Action":[
  "fms:*",
  "waf:*",
  "waf-regional:*",
  "elasticloadbalancing:SetWebACL",
  "firehose:ListDeliveryStreams",
  "organizations:DescribeAccount",
  "organizations:DescribeOrganization",
  "organizations:ListRoots",
  "organizations:ListChildren",
  "organizations:ListAccounts",
  "organizations:ListAccountsForParent",
  "organizations:ListOrganizationalUnitsForParent",
  "shield:GetSubscriptionState",
  "route53resolver:ListFirewallRuleGroups",
  "route53resolver:GetFirewallRuleGroup",
  "wafv2:ListRuleGroups",
  "wafv2:ListAvailableManagedRuleGroups",
  "wafv2:CheckCapacity",
  "wafv2:PutLoggingConfiguration",
  "wafv2:ListAvailableManagedRuleGroupVersions",
  "network-firewall:DescribeRuleGroup",
  "network-firewall:DescribeRuleGroupMetadata",
  "network-firewall:ListRuleGroups",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeRegions"
],
"Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:PutBucketPolicy",
    "s3:GetBucketPolicy"
  ],
  "Resource": [
    "arn:aws:s3:::aws-waf-logs-*"
  ]
},
{
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "iam:AWSServiceName": [
        "fms.amazonaws.com"
      ]
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "organizations:ServicePrincipal": [
        "fms.amazonaws.com"
      ]
    }
  }
}
```

```
}  
  }  
]  
}
```

权限详情

此策略包含以下权限。：

- `fms:*`:
可让您使用Amazon Firewall Manager资源。
- `waf:*`, `waf-regional:*`:
可让您使用Amazon WAF策略。
- `waf:*`, `waf-regional:*`:
可让您使用Amazon WAF策略。
- `elasticloadbalancing:SetWebACL`:
可让您将 Web 访问控制列表 (ACL) 与 Elastic 负载均衡器相关联。
- `firehose:ListDeliveryStreams`:
允许您查看Amazon WAF日志。
- `organizations:DescribeAccount`, `organizations:DescribeOrganization`, `organizations:ListRoots`, `organizations:ListChildren`, `organizations:ListAccounts`, `organizations:ListAccountsForParent`, `organizations:ListOrganizationalUnitsForParent`:
可让您与OrganizationsAmazon 合作。
- `shield:GetSubscriptionState`:
允许您查看Amazon Shield策略的订阅状态。
- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup`:
允许您在适用于 VPC 的 Route 53 私有 DNS 策略中使用适用于 VPC 的 Route 53 私有 DNS 规则组。
- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`, `wafv2:PutLoggingConfiguration`, `wafv2:ListAvailableManagedRuleGroupVersions`:
可让您使用Amazon WAFV2策略。
- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`, `network-firewall:ListRuleGroups`:
可让您使用Amazon Network Firewall策略。
- `ec2:DescribeAvailabilityZones`:
允许您查看Amazon Network Firewall策略的可用区。
- `ec2:DescribeRegions`:
允许您在Amazon Firewall Manager控制台中查看策略的区域。

Amazon适用于 Amazon Firewall Manager 的托管策略

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 Web Services 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 Web Services 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，服务最有可能更新 Amazon 托管策略。服务不会从 Amazon 托管策略中删除权限，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，ViewOnlyAccess Amazon 托管策略提供对许多 Amazon Web Services 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：AWSFMAdminFullAccess

使用 AWSFMAdminFullAccess Amazon 托管策略，以允许您的管理员访问 Amazon Firewall Manager 资源，包括所有 Firewall Manager 策略类型。此策略不包括在中设置亚马逊简单通知服务通知的权限 Amazon Firewall Manager。有关如何设置亚马逊简单通知服务的访问权限的信息，请参阅 [设置亚马逊简单通知服务的访问权限](#)。

权限详情

此策略根据权限集分为多个语句。

- Amazon Firewall Manager 策略资源-允许对中的 Amazon Firewall Manager 资源（包括所有 Firewall Manager 策略类型）的完全管理权限。
- 将 Amazon WAF 日志写入亚马逊简单存储服务-允许 Firewall Manager 在 Amazon S3 中写入和读取 Amazon WAF 日志。
- 创建服务链接角色 — 允许管理员创建服务相关角色以允许 Firewall Manager 访问其他服务中的资源。此权限允许创建服务相关角色仅供 Firewall Manager 使用。有关 Firewall Manager 如何使用服务相关角色的信息，请参阅 [Firewall Manager 使用服务相关角色 \(p. 493\)](#)。
- Amazon Organizations — 允许管理员为中的组织使用 Firewall Manager Amazon Organizations。为 Firewall Manager 启用可信访问权限 Amazon Organizations，管理员帐户的成员可以查看其 Firewall Manager。有关 Amazon Organizations 与一起使用的信息 Amazon Firewall Manager，请参阅《Amazon Organizations 用户指南》中的 [Amazon Organizations 与其他 Amazon 服务一起使用](#)。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fms:*",
        "waf:*",
        "waf-regional:*",
        "elasticloadbalancing:SetWebACL",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",

```

```
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:PutLoggingConfiguration",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:PutBucketPolicy",
      "s3:GetBucketPolicy"
    ],
    "Resource": [
      "arn:aws:s3:::aws-waf-logs-*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": [
          "fms.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:EnableAWSServiceAccess",
      "organizations:ListDelegatedAdministrators",
      "organizations:RegisterDelegatedAdministrator",
      "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "fms.amazonaws.com"
        ]
      }
    }
  }
]
}
```

此策略包含以下权限：

- fms:*

可让您使用Amazon Firewall Manager资源。

- waf:*, waf-regional:*

可让您使用Amazon WAF策略。

- elasticloadbalancing:SetWebACL:

可让您将 Web 访问控制列表 (ACL) 与弹性负载均衡器。

- `firehose:ListDeliveryStreams`:

允许您查看Amazon WAF日志。

- `organizations:DescribeAccount`, `organizations:DescribeOrganization`,
`organizations:ListRoots`, `organizations:ListChildren`,
`organizations:ListAccounts`, `organizations:ListAccountsForParent`,
`organizations:ListOrganizationalUnitsForParent`:

可让您与OrganizationsAmazon 合作。

- `shield:GetSubscriptionState`:

允许您查看Amazon Shield策略的订阅状态。

- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup`:

允许您在适用于 VPC 的 Route 53 私有 DNS 策略中使用适用于 VPC 的 Route 53 私有 DNS 规则组。

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`,
`wafv2:PutLoggingConfiguration`, `wafv2:ListAvailableManagedRuleGroupVersions`:

可让您使用Amazon WAFV2策略。

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`,
`network-firewall:ListRuleGroups`:

可让您使用Amazon Network Firewall策略。

- `ec2:DescribeAvailabilityZones`:

允许您查看Amazon Network Firewall策略的可用区。

- `ec2:DescribeRegions`:

允许您在Amazon Firewall Manager控制台中查看策略的区域。

- `s3:GetBucketPolicy`:

可让您获取适用于Amazon WAF日志的 Amazon S3 存储桶策略。

- `ListDelegatedAdministrators`:

允许您列出亚马逊 OpenSearch 服务委托管理员。

Amazon托管策略：FMSServiceRolePolicy

此策略Amazon Firewall Manager允许您在防火墙管理器和集成服务中代表您管理Amazon资源。此策略附加到 `AWSServiceRoleForFMS` 服务相关角色。有关 service-linked role 服务相关角色的更多信息，请参阅[为 Firewall Manager 使用服务相关角色 \(p. 493\)](#)。

有关策略的详细信息，请参阅 [FMS](#) 上的 IAM 控制台ServiceRolePolicy。

Amazon托管策略：AWSFMAdminReadOnlyAccess

授予对所有Amazon Firewall Manager 资源的只读访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fms:Get*",

```

```
        "fms:List*",
        "waf:Get*",
        "waf:List*",
        "waf-regional:Get*",
        "waf-regional:List*",
        "firehose:ListDeliveryStreams",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListOrganizationalUnitsForParent",
        "shield:GetSubscriptionState",
        "route53resolver:ListFirewallRuleGroups",
        "route53resolver:GetFirewallRuleGroup",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
        "wafv2:CheckCapacity",
        "wafv2:ListAvailableManagedRuleGroupVersions",
        "network-firewall:DescribeRuleGroup",
        "network-firewall:DescribeRuleGroupMetadata",
        "network-firewall:ListRuleGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeRegions"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketPolicy"
    ],
    "Resource": [
      "arn:aws:s3:::aws-waf-logs-*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "fms.amazonaws.com"
        ]
      }
    }
  }
]
}
```

此策略包含以下权限：

- fms:*

允许您查看Amazon Firewall Manager资源。

- waf:Get*, waf-regional:Get*

让你获取Amazon WAF政策。

- waf:List*, waf-regional:List*

允许您列出Amazon WAF策略。

- `firehose:ListDeliveryStreams:`

允许您列出Amazon WAF日志。

- `organizations:DescribeOrganization`, `organizations:DescribeAccount`,
`organizations:DescribeOrganization`, `organizations:ListRoots`,
`organizations:ListChildren`, `organizations:ListAccounts`,
`organizations:ListAccountsForParent`,
`organizations:ListOrganizationalUnitsForParent:`

允许您查看Amazon Organizations 资源。

- `shield:GetSubscriptionState:`

允许您获取Amazon Shield策略的订阅状态。

- `route53resolver:ListFirewallRuleGroups`, `route53resolver:GetFirewallRuleGroup:`

允许您在 Route 53 适用于 VPC 的私有 DNS 策略中获取并列出 VPC 规则组的 Route 53 私有 DNS。

- `wafv2:ListRuleGroups`, `wafv2:ListAvailableManagedRuleGroups`, `wafv2:CheckCapacity`,
`wafv2:ListAvailableManagedRuleGroupVersions:`

允许您列出Amazon WAFV2规则组、Amazon WAFV2策略中的Amazon托管规则组、Amazon WAFV2规则组容量和Amazon WAFV2Amazon托管规则组版本。

- `network-firewall:DescribeRuleGroup`, `network-firewall:DescribeRuleGroupMetadata`,
`network-firewall:ListRuleGroups:`

允许您查看Amazon Network Firewall规则组和规则组元数据。

- `ec2:DescribeAvailabilityZones:`

允许您查看Amazon Network Firewall策略的可用区。

- `ec2:DescribeRegions:`

允许您在Amazon Firewall Manager控制台中查看策略的区域。

- `s3:GetBucketPolicy:`

可让您获取适用于Amazon WAF日志的 Amazon S3 存储桶策略。

- `ListDelegatedAdministrators:`

允许您在中列出委派的管理员Amazon Organizations。

Amazon托管策略：AWSFMMemberReadOnlyAccess

授予对Amazon Firewall Manager成员资源的只读访问权限。有关策略的详细信息，请参阅 IAM 控制台，网址为[AWSFMMemberReadOnlyAccess](#)。

Firewall Manager 更新到Amazon托管策略

查看有关Firewall Manager 的Amazon托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动警报，请订阅 Firewall Manager 文档历史记录页面上的 RSS 源，网址为[文档历史记录 \(p. 525\)](#)。

更改	说明	日期
FMSServiceRolePolicy (p. 488) — 更新的政策	添加了允许Firewall Manager 描述 Amazon EC2 实例和网络接口属性的权限。 在 IAM 控制台中查看更新的政策：FMSServiceRolePolicy。	2022 年 11 月 15 日
AWSFMAdminReadOnlyAccess (p. 488) — 更新的政策	添加了对支持Amazon WAFV2、Shield、Network Firewall、DNS 防火墙、Amazon VPC 安全组和策略的权限。 在 IAM 控制台中查看更新的政策：AWSFMAdminReadOnlyAccess。	2022 年 11 月 2 日
AWSFMAdminFullAccess (p. 486) — 更新的政策	添加了对支持Amazon WAFV2、Shield、Network Firewall、DNS 防火墙、Amazon VPC 安全组和策略的权限。删除了Amazon SNS 权限。 在 IAM 控制台中查看更新的政策：AWSFMAdminFullAccess。	2022 年 10 月 21 日
FMSServiceRolePolicy— Amazon Firewall Manager 第三方 防火墙策略的新权限	此更改允许Firewall Manager 创建和删除与第三方防火墙策略关联的 Amazon EC2 VPC 终端节点。	2022 年 3 月 30 日
FMSServiceRolePolicy— Amazon Network Firewall 策略的 新权限	为Network Firewall 策略添加了支持部署防火墙的新权限。新权限允许为策略范围内的账户检索有关可用区域的信息。	2022 年 2 月 16 日
FMSServiceRolePolicy— Amazon Shield 策略的新权限	添加了检索Amazon WAF区域和 Amazon WAF全球资源标签的新权限。添加了使用资源 ARN 检索 Web ACL 的Amazon WAF区域权限。添加了支持 Shield 自动应用层 DDoS 缓解的权限。	2022 年 1 月 7 日
FMSServiceRolePolicy— Amazon Shield 策略的新权限	添加了检索 Elastic Load Bload Balanccess	2021 年 11 月 18 日
FMSServiceRolePolicy— 安全 组和Amazon Network Firewall 策略的新权限	添加了新权限以启用Amazon Network Firewall策略的集中日志记录。此外，还添加了只读 Amazon EC2 权限，以支持对 Config 服务的更改，这些更改会影响Amazon Firewall Manager 查询资源以获取安全组策略的方式。	2021 年 9 月 29 日
FMSServiceRolePolicy— Amazon WAF 资源的 ARN 格式	更新了FMSServiceRolePolicy以标准化Amazon WAF资源的 ARN 格式。更新后的 ARN 格式	2021 年 8 月 12 日

更改	说明	日期
	为arn:aws:waf:*:*:*和arn:aws:waf-regional:*:*:*。	
FMSServiceRolePolicy— 中国的其他地区	Amazon Firewall Manager已在中国FMSServiceRolePolicy的BJS 和 ZHY 区域启用。	2021 年 8 月 12 日
FMSServiceRolePolicy— 对现有策略的更新	添加了允许Amazon Firewall Manager管理Amazon Route 53 Resolver DNS 防火墙的新权限。 此更改允许Firewall Manager 配置Amazon Route 53 Resolver DNS 防火墙关联。这允许您使用Firewall Manager 为整个组织中的 VPC 提供 DNS 防火墙保护 Amazon Organizations。	2021 年 3 月 17 日
Firewall Manager 已开启跟踪更改	FiFirewall Manager 已开始跟踪其 Amazon托管策略的更改。	2021 年 3 月 2 日

对 Amazon Firewall Manager 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Firewall Manager 和 IAM 时可能遇到的常见问题。

主题

- [我无权在Firewall Manager 中执行操作 \(p. 492\)](#)
- [我无权执行 iam : PassRole \(p. 492\)](#)
- [我希望允许我的之外的人员访问我的 FAmazon Web Services 账户 irewall Manager 资源 \(p. 493\)](#)

我无权在Firewall Manager 中执行操作

如果您收到一个错误，表明您无权执行某个操作，则必须更新策略以允许您执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 fms:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
fms:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 fms:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到一个错误，表明您无权执行操作，则必须更新策略以允许您将角色传递给 Firewall Manager。iam:PassRole

有些 Amazon Web Services允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Firewall Manager 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。管理员是向您提供登录凭证的人。

我希望允许我的之外的人员访问我的 FAmazon Web Services 账户 irewall Manager 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Firewall Manager 是否支持这些功能，请参阅[Amazon Shield 如何与 IAM 协同工作 \(p. 387\)](#)。
- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的[为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限](#)。
- 要了解如何为第三方 Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的[为第三方拥有的 Amazon Web Services 账户提供访问权限](#)。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的[为经过外部身份验证的用户 \(联合身份验证\) 提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的[IAM 角色与基于资源的策略有何不同](#)。

为 Firewall Manager 使用服务相关角色

Amazon Firewall Manager 使用 Amazon Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色是一种与 Firewall Manager 直接关联的独特类型的 IAM 角色。服务相关角色由 Firewall Manager 预定义，并包含服务调用其他角色所需的一切权限。Amazon 服务代表您。

服务相关角色可让您更轻松设置 Firewall Manager，因为您不必手动添加必要的权限。Firewall Manager 定义其服务相关角色的权限，除非另外定义，否则只有 Firewall Manager 可以代入该角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这将保护您的 Firewall Manager 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅[使用 IAM 的 Amazon 服务](#)并查找 Service-Linked Role (服务相关角色) 列中显示为 Yes (是) 的服务。请选择 Yes 与查看该服务的[服务相关角色文档](#)的链接。

Firewall Manager 的服务相关角色权限

FMS Firewall Manager 使用服务相关角色 AWSServiceRoleForFMS。

Amazon Firewall Manager 使用此服务相关角色将日志写入 Amazon Kinesis Data Firehose。仅当您在 Amazon Firewall Manager 中启用日志记录时，才会使用此角色。有关更多信息，请参阅[记录 Web ACL 流量 \(p. 180\)](#)。

这些区域有：AWSServiceRoleForFMS 服务相关角色信任服务来代入该角色。fms.amazonaws.com。

角色的权限策略允许 Firewall Manager 对指定的资源完成以下操作：

- 操作：`firehose:PutRecord`和`firehose:PutRecordBatch`Amazon Kinesis Data Firehose 数据流资源上名称以“aws-fms-logs-”开头的 Amazon Kinesis Data Firehose 数据流资源。例如，aws-fms-logs-us-east-2-analytics。

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](#)。

为 Firewall Manager 创建服务相关角色

无需手动创建服务相关角色。启用 Firewall Manager 时，登录 Amazon Web Services Management Console，或者您可以做 `PutLoggingConfiguration` 请求在 Firewall Manager CLI 或 Firewall Manager API 中，Firewall Manager 为您创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

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。当您启用防火墙管理器日志记录时，Firewall Manager 会再次为您创建服务相关角色。

为 Firewall Manager 编辑服务相关角色

Firewall Manager 不允许您编辑 `AWSServiceRoleForFMS` 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参见《IAM 用户指南》中的[编辑服务相关角色](#)。

为 Firewall Manager 删除服务相关角色

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，您必须先清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 Firewall Manager 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。

使用 IAM 删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 `AWSServiceRoleForFMS` 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](#)。

Firewall Manager 服务相关角色的受支持区域

Firewall Manager 支持在该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 [Firewall Manager 终端节点和配额](#)。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 Amazon 中，跨服务模拟可能会导致混淆代理问题。一个服务（呼叫服务）调用另一项服务（所谓的“服务”）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况，Amazon 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务委托人有权访问账户中的资源。

我们建议在资源策略中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全局条件上下文键，以限制 Amazon Firewall Manager 为其他服务提供的资源访问权限。如果您只希望将一个资源与跨服务访问相关联，请使用 `aws:SourceArn`。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 `aws:SourceAccount`。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符字符 (*) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:fms:*:account-id:*`。

如果 `aws:SourceArn` 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文密钥来限制权限。

的价值 `aws:SourceArn` 必须是 Amazon Firewall Manager 管理员 `Amazonaccount`。

以下示例演示如何使用 `aws:SourceArn` 防 Firewall Manager 中的全局条件上下文键，以防止混淆的副问题。

以下示例演示如何通过使用 `aws:SourceArn` Firewall Manager 角色信任策略中的全局条件上下文键。Replace ## 和 *account-id* 用你自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"
        ]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

中的日志记录和监控

监控是保持和 Firewall Manager 和您的可靠性、可用性和性能的重要方面Amazon解决方案。你应该从你的所有部分收集监控数据Amazon使用解决方案，您可以更轻松地调试出现的多点故障。Amazon提供了多种工具来监控 Firewall Manager 资源并对潜在的事件做出响应：

亚马逊 CloudWatch Alarms

使用 CloudWatch 使用警报，您可在指定时间段内监控某个指标。如果指标超出给定阈值，CloudWatch 发送通知到 Amazon SNS 主题或Amazon Auto Scaling政策。有关更多信息，请参阅 [使用亚马逊进行监控 CloudWatch \(p. 501\)](#)。

Amazon CloudTrail 日志

CloudTrail 提供了用户、角色或用户所执行操作的记录AmazonFirewall Manager 中的服务。使用 CloudTrail 收集的信息，您可以确定向 Firewall Manager 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。有关更多信息，请参阅[使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)。

Firewall Manager 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](#)。

Firewall Manager 中的弹性

Amazon 全球基础设施围绕 Amazon Web Services 区域和可用区构建。Amazon Web Services 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。

有关 Amazon Web Services 区域和可用区的更多信息，请参阅 [Amazon 全球基础设施](#)。

Amazon Firewall Manager 中的基础设施安全性

作为托管服务，Amazon Firewall Manager 受保护 Amazon 中描述的全局网络安全程序 [Amazon Web Services：安全过程概述](#) 白皮书。

你用 Amazon 使用发布的 API 调用通过网络访问 Firewall Manager。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 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，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [Amazon Security Token Service](#) (Amazon STS) 生成临时安全凭证来对请求进行签名。

Amazon Firewall Manager 配额

Amazon Firewall Manager 受以下配额（以前称为限制）所限。

Amazon Firewall Manager 有您可以增加的默认配额和固定配额。

Firewall Manager 管理的安全组策略受标准 Amazon VPC 配额的约束。有关更多信息，请参阅 [Amazon VPC 用户指南中的 Amazon VPC 配额](#)。

每个 Firewall Manager Network Firewall 策略都会创建具有关联防火墙策略及其规则组的 Network Firewall 防火墙。这些 Network Firewall 资源受限于《Network Firewall 开发人员指南》中按 [Amazon Network Firewall 配额](#) 列出的配额。

软配额

Amazon Firewall Manager对每个区域的实体数量有默认配额。您可以[请求提高](#)这些配额。

所有策略类型

资源	每个区域的默认限额
每个组织的账户数Amazon Organizations	可变。发送到账户的邀请将计入此配额。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则撤销此计数。
中每个组织的Firewall Manager 策略Amazon Organizations	20。区域规格Global和US East (N. Virginia) Region指的是同一个区域，因此此限制适用于两个区域的合并策略总数。
每个 Firewall Manager 策略范围内的组织单位	20
如果您明确包括和排除单个帐户，则帐户将在 Firewall Manager 策略的范围内	200
如果您未明确包括或排除单个帐户，则帐户属于Firewall Manager 策略的范围	2,500
每个 Firewall Manager 策略的包含或排除资源的标签数	8
每个账户的最大资源集数量。	20
每个资源集的最大资源数。	100
每个Firewall Manager 策略的最大资源集数。	5

通用安全组策略

资源	每个区域的默认限额
每个策略的主安全组	1
每个账户每个策略作用域内的 Amazon VPC 实例数	100

内容审核安全组策略

资源	每个区域的默认限额
每个策略的审计安全组	1
每个应用程序列表的应用程序数	50
策略中任何设置的自定义托管应用程序列表	1
每个账户的自定义托管式应用程序列表数	10
每个协议列表的协议数	5

资源	每个区域的默认限额
策略中任何设置的自定义托管协议列表	1
每个账户的自定义托管式协议列表数	10

Amazon WAF 策略

资源	每个区域的默认限额
Amazon WAF每个Firewall Manager 管理员帐户的规则组	100
Amazon WAF每个Firewall Manager 管理员帐户的经典规则组	10
每个 Amazon WAF 策略的规则组数	50
Amazon WAF策略中规则组的 Web ACL 总容量单位 (WCU)	1500

DNS 防火墙策略

资源	每个区域的默认限额
每个策略的 DNS Firewall 规则组数	2

硬配额

以下与相关的每个区域的配额Amazon Firewall Manager无法更改。

Network Firewall 策略

资源	每个区域的配额
可针对单个策略自动修复的 VPC 数量。	1000
您可以为单个策略提供的 IPV4 CIDR 数量。	50

安全组内容审计策略

资源	每个区域的配额
策略中任何设置的 Firewall Manager 托管应用程序列表	1
策略中任何设置的 Firewall Manager 管理协议列表	1

Amazon WAF经典政策

资源	每个区域的配额
Amazon WAF每个策略的经典规则组	2：客户创建的 1 个规则组和 1 个 Amazon Web Services Marketplace 规则组
Amazon WAF每个Firewall ManagerAmazon WAF 经典规则组的经典规则	10

监控 Amazon WAF、Amazon Firewall Manager 和 Amazon Shield Advanced

监控是保持服务的可靠性、可用性和性能的重要方面。

Note

有关使用 Shield Advanced 监控您的 Shield Advanced 资源和识别可能 [Amazon Shield \(p. 329\)](#) 的 DDoS 事件的信息，请参阅

在开始监控这些服务时，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 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？

下一步，通过在不同时间和不同负载条件下测量性能，在您的环境中建立正常性能的基准。在监控 Amazon WAF Firewall Manager、Shield Advanced 和相关服务时，存储历史监控数据，以便将此数据与当前性能数据进行比较，确定正常性能模式和性能异常，并设计解决问题的方法。

对于 Amazon WAF，至少应监控以下几项以建立基准：

- 允许的 Web 请求数
- 阻止的 Web 请求数

主题

- [监控工具 \(p. 500\)](#)
- [使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)

监控工具

Amazon 为您提供了各种可用于监控 Amazon WAF 和 Amazon Shield Advanced 的工具。您可以配置其中的一些工具来为您执行监控任务，但其他工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动化监控工具来监控 Amazon WAF 和 Amazon Shield Advanced 并在出现错误时报告：

- 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。具体操作是：通知已发送到 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略。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 CloudFront 活动](#)。

Note

CloudWatch 未启用指标和警报Amazon Firewall Manager。

您不仅可以使用 CloudWatch 中所述监控Amazon WAF和Shield 高级指标[使用亚马逊进行监控 CloudWatch \(p. 501\)](#)，还应该 CloudWatch 用于监控受保护资源的活动。有关更多信息，请参阅下列内容：

- CloudWatch在《亚马逊 CloudFront 开发者指南》中[@@ 使用监控 CloudFront 活动](#)
- API Gateway 开发者指南中的 Amazon API Gateway [中的日志记录和监控](#)
- CloudWatch 《弹性负载平衡用户指南》中应用程序负载均衡器的[指标](#)
- 《Amazon AppSync开发者指南》中的[@@ 监控和登录](#)
- 《Amazon Cognito 开发者指南》中的 Amazon Cognito [中的日志记录和监控](#)
- [查看流式传输到日志的 App Runner CloudWatch 日志](#)和[查看《Amazon App Runner开发者指南》CloudWatch中报告的 App Runner 服务指标](#)
- Amazon CloudWatch Logs — 监控、存储和访问来自Amazon CloudTrail或其他来源的日志文件。有关更多信息，请参阅[什么是 Amazon CloudWatch Logs ?](#)。
- Amazon CloudWatch Events — 自动执行Amazon服务并自动响应系统事件。Amazon服务中的 CloudWatch 事件将近实时传输到 Events，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 Event CloudWatch s ?](#)
- Amazon CloudTrail日志监控 — 在账户间共享日志文件，通过将 CloudTrail 日志文件发送到 Log CloudWatch s 对它们进行实时监控，在 Java 中编写日志处理应用程序，以及验证您的日志文件在交付后未发生更改 CloudTrail。有关更多信息[使用 Amazon CloudTrail 记录 API 调用 \(p. 509\)](#)，请参阅《Amazon CloudTrail用户指南》中的“[使用 CloudTrail 日志文件](#)”。
- Amazon Config— 查看Amazon账户中Amazon资源的配置，包括资源如何相互关联以及过去的配置方式，这样您就可以看到配置和关系如何随着时间的推移而变化。

手动监控工具

监控Amazon WAF的另一个重要环Amazon Shield Advanced是手动监控 CloudWatch 告警未覆盖的项目。您可以查看 Shield Advan CloudWatch ced 和其他Amazon Web Services Management Console仪表板，以查看您的Amazon环境状态。Amazon WAF建议还查看 Web ACL 和规则的日志文件。

- 例如，要查看 Amazon WAF 控制面板：
 - 在 Web ACLsAmazon WAF 页的 Requests 选项卡上，查看总请求数和与您创建的每个规则匹配的请求数的图表。有关更多信息，请参阅[查看 Web 请求示例 \(p. 205\)](#)：
- 查看 CloudWatch 主页上的以下内容：
 - 当前告警和状态
 - 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：

- 创建[自定义控制面板](#)以监控您关注的服务。
- 绘制指标数据图，以排除问题并弄清楚趋势。
- 搜索并浏览您的所有 Amazon 资源指标。
- 创建和编辑告警接收有关问题的通知。

使用亚马逊进行监控 CloudWatch

您可以使用 Amazon 监控 Web 请求、Web ACL 和规则 CloudWatch，此工具可从Amazon WAF原始数据收集原始数据，近实时处理Amazon Shield Advanced为便于读取的指标。您可以使用Amazon 的统计数据

CloudWatch 来了解您的 Web 应用程序或服务的执行情况。有关更多信息，请参阅《亚马逊 CloudWatch 用户指南》CloudWatch 中的[内容](#)。

Note

CloudWatch Firewall Manager 器的指标和警报未启用。

创建 Amazon CloudWatch 警报

您可以创建 Amazon CloudWatch 告警，在告警改变状态时发送 Amazon SNS 消息。警报会监控某个指标在一定时间段 (由您指定) 的变化情况，并根据相对于指定阈值的指标值每隔若干个时间段执行一项或多项操作。操作是一个发送到 Amazon SNS 主题或 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。

Amazon WAF 和 Amazon Shield Advanced 的指标与维度

指标的分组首先依据服务命名空间，然后依据每个命名空间内的各种维度组合。

- 命 Amazon WAF 名空间是 AWS/WAFV2
- Shield 高级命名空间是 AWS/DDoSProtection

Note

Amazon WAF 每分钟报告一次指标。
Shield Advanced 在活动期间每分钟报告一次指标，其他时间则不那么频繁。

使用以下流程查看 Amazon WAF 和的指标 Amazon Shield Advanced。

使用 CloudWatch 控制台查看指标

1. 登录 Amazon Web Services Management Console 并打开 CloudWatch 主机，[网址为 https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/)。
2. 如果需要，可将区域更改为 Amazon 资源所在的区域。为 CloudFront 选择 US East (N. Virginia) 区域。
3. 在导航窗格的“指标”下，选择“所有指标”，然后在“浏览”选项卡下搜索服务。

使用 Amazon CLI 查看指标

- 对于 AWS/WAFV2，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

对于 Shield Advanced，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

Amazon WAF 指标和维度

Amazon WAF 每分钟报告一次指标。Amazon WAF 在 AWS/WAFV2 命名空间中提供以下指标和维度。

Web ACL、规则组和规则指标

指标	描述
AllowedRequests	允许的 Web 请求数。 报告标准：有非零值。 有效统计数据：Sum
BlockedRequests	阻止的 Web 请求数。 报告标准：有非零值。 有效统计数据：Sum
CountedRequests	计数的 Web 请求数。 报告标准：有非零值。 已计数的 Web 请求是至少匹配了一个规则的请求。请求计数通常用于测试。 有效统计数据：Sum
CaptchaRequests	应用了验证码控制的网络请求数量。 报告标准：有非零值。 CAPTCHA 网络请求是与具有CAPTCHA操作设置的规则相匹配的请求。此指标记录所有匹配的请求，无论它们是否具有有效的 CAPTCHA 令牌。 有效统计数据：Sum
RequestsWithValidCaptchaToken	应用了 CAPTCHA 控件且具有有效 CAPTCHA 令牌的网络请求数量。 报告标准：有非零值。 有效统计数据：Sum
ChallengeRequests	应用了质询控制的 Web 请求数量。 报告标准：有非零值。 质询 Web 请求是与具有Challenge操作设置的规则相匹配的请求。该指标记录所有匹配的请求，无论它们是否具有有效的质询令牌。 有效统计数据：Sum
RequestsWithValidChallengeToken	应用了质询控制且具有有效质询令牌的 Web 请求的数量。 报告标准：有非零值。 有效统计数据：Sum
PassedRequests	通过的请求数。这仅用于在不匹配任何规则组规则的情况下通过规则组评估的请求。

指标	描述
	报告标准：有非零值。 通过的请求是指与规则组中任何规则都不匹配的请求。 有效统计数据：Sum

Web ACL、规则组和规则维度

维度	描述
Region	除亚马逊 CloudFront 发行版以外的所有受保护资源类型均为必填项。
Rule	下列情况之一： • Rule 的指标名称。 • ALL，表示 WebACL 或 RuleGroup 中的所有规则。 • Default_Action（仅当与 WebACL 维度结合使用时），它表示分配给任何请求的操作，其评估未因 Web ACL 中的规则操作而终止。
RuleGroup	RuleGroup 的指标名称。
WebACL	WebACL 的指标名称。

Note

对于任何单个 Web 请求，最多 Amazon WAF 发出 100 个标签的指标。您的 Web ACL 评估可以应用 100 多个标签并与 100 多个标签进行匹配，但只有前 100 个标签会反映在这些指标中。

有关标签的信息，请参见 [网络请求上的标签 \(p. 123\)](#)。

标签指标

指标	描述
AllowedRequests	Web 请求上 Allow 应用了操作设置的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
BlockedRequests	Web 请求上 Block 应用了操作设置的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
CountedRequests	由具有 Count 操作设置的规则组规则添加到 Web 请求的标签数量。 此指标仅适用于规则组的所有者，适用于规则组内部的规则。对于其他情况，计数标签指标将汇总到应用于请求的终止操作中，例如 Allow 或 Block。

指标	描述
	报告标准：有非零值。 有效统计数据：Sum
CaptchaRequests	已应用终止CAPTCHA操作的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
ChallengeRequests	已应用终止Challenge操作的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum

标签维度

维度	描述
Region	除亚马逊 CloudFront发行版以外的所有受保护资源类型均为必填项。
WebACL	WebACL 的指标名称。
RuleGroup	RuleGroup 的指标名称。用于指标CountedRequests。
LabelNamespace	添加到请求的标签的命名空间前缀。
Label	添加到请求的标签的名称。

免费机器人可见度指标

指标	描述
SampleAllowedRequests	具有Allow操作的抽样请求的百分比。 报告标准：有非零值。 有效统计数据：Sum
SampleBlockedRequests	具有Block操作的抽样请求的百分比。 报告标准：有非零值。 有效统计数据：Sum

免费机器人可见度尺寸

维度	描述
Region	除亚马逊 CloudFront发行版以外的所有受保护资源类型均为必填项。

维度	描述
WebACL	WebACL 的指标名称。
BotCategory	检测到的机器人类别的指标名称，基于 Web 请求标签。

Amazon Shield Advanced 指标和警报

此部分会讨论 Amazon Shield Advanced 提供的指标和警报。

Amazon Shield Advanced 指标

与没有事件发生时，Shield Advanced CloudWatch 在 DDoS 事件期间向亚马逊报告 Amazon 资源指标的频率更高。Shield Advanced 在活动期间每分钟报告一次指标，然后在活动结束后立即报告一次。虽然没有事件在进行中，但 Shield Advanced 会在分配给资源的时间每天报告一次指标。此定期报告使指标保持活动状态并可用于自定义 CloudWatch 警报。

Shield Advanced 报告了美国东部（弗吉尼亚北部）区域 us-east-1 的指标，内容如下：

- 亚马逊 CloudFront 和亚马逊 Route 53 的全球服务。
- 保护组。有关保护组的信息，请参阅[Amazon Shield Advanced 保护 \(p. 368\)](#)。

检测指标

Shield Advanced 在 AWS/DDoSProtection 命名空间中提供以下检测指标和维度。

检测指标

指标	描述
DDoSDetected	指示特定 Amazon 资源名称 (ARN) 的 DDoS 事件是否正在进行中。 该指标在事件期间的值为非零。
DDoSAttackBitsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的位数。此指标仅适用于网络和传输层（第 3 层和第 4 层）DDoS 事件。 该指标在事件期间的值为非零。 单位：位
DDoSAttackPacketsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的数据包数。此指标仅适用于网络和传输层（第 3 层和第 4 层）DDoS 事件。 该指标在事件期间的值为非零。 单位：数据包
DDoSAttackRequestsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的请求数。该指标仅适用于第 7 层 DDoS 事件。仅针对最重要的第 7 层事件报告指标。 该指标在事件期间的值为非零。 单位：请求

Shield Advanced 发布的指标没有其他维度。其余检测指标包括以下列表中与攻击类型对应的 AttackVector 维度：

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYN Flood
- UDPFragment
- UDPTraffic
- UDPReflection

风险防范

Shield Advanced 在 AWS/DDoSProtection 命名空间中提供以下缓解指标和维度。

风险防范

指标	描述
VolumePacketsPerSecond	为响应检测到的事件而部署的缓解措施每秒丢弃或传递的数据包数。 单位：数据包

风险防范

维度	描述
ResourceArn	Amazon Resource Name (ARN)
MitigationAction	应用缓解的结果。可能的值为 Pass 或 Drop。

热门贡献者指标

Shield Advanced 在 AWS/DDoSProtection 命名空间中提供以下缓解指标和维度。

热门贡献者指标

指标	描述
VolumePacketsPerSecond	主要贡献者每秒的数据包数。

指标	描述
	单位：数据包
VolumeBitsPerSecond	最大贡献者的每秒比特数。 单位：比特

Shield Advanced 按维度组合发布了主要贡献者指标，这些指标代表了事件贡献者的特征。您可以使用以下任何维度组合来查看任何主要贡献者指标：

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

主要贡献者维度

维度	描述
ResourceArn	Amazon 资源名称 (ARN)。
Protocol	IP 协议名称，TCP或为UDP。
SourcePort	源 TCP 或 UDP 端口。
DestinationPort	目标 TCP 或 UDP 端口。
SourceIp	源 IP 地址。
SourceAsn	源自治系统号 (ASN)。
TcpFlags	TCP 数据包中存在的标志组合，由短划线 (-) 分隔。监控标志是ACK、FIN、RST、SYN。此维度值始终按字母顺序显示。例如：ACK-FIN-RST-SYN、ACK-SYN 和 FIN-RST。

创建 Amazon Shield Advanced 警报

您可以将Amazon Shield Advanced指标用于亚马逊 CloudWatch 警报。CloudWatch 发送通知或自动更改正在监控的资源。

有关创建 CloudWatch 警报的详细说明，请参阅[亚马逊 CloudWatch 用户指南](#)。在 CloudWatch 控制台上创建警报时，要使用 Shield Advanced 指标，请在选择“创建警报”后，选择AWSDDOSProtectionMetrics。然后，您可以根据特定的流量创建警报，也可以在指标为非零时触发警报。第二个选项会对Shield Advanced观察到的任何潜在攻击触发警报。

Note

仅适用AWSDDOSProtectionMetrics于 Shield Advanced 客户。

有关更多信息，请参阅《亚马逊 CloudWatch 用户指南》CloudWatch中的[内容](#)。

Amazon Firewall Manager 通知

Amazon Firewall Manager 不记录指标，因此您无法专门为 Firewall Manager 创建 Amazon CloudWatch 警报。但是，您可以配置 Amazon SNS 通知以提醒您注意潜在的攻击。要在 Firewall Manager 中创建 Amazon SNS 通知，请参阅 [第 4 步：配置 Amazon SNS 通知和 Amazon CloudWatch 警报 \(p. 412\)](#)。

使用 Amazon CloudTrail 记录 API 调用

Amazon WAF、Amazon Shield Advanced、和与集成 Amazon CloudTrail，后 Amazon Firewall Manager 者是提供用户、角色或服务所采取操作的记录的记录的 Amazon 服务。CloudTrail 将这些服务的 API 调用子集作为事件捕获，包括来自、Shield Advanced 或 Firewall Manager 控制台的调用和对 Shield Advanced API 的代码调用。Amazon WAF、Amazon WAF 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 Shield Advanced Amazon S3 存储桶或 Firewall Manager 的事件）。Amazon WAF 如果您不配置跟踪，则仍可在 Event history（事件历史记录 CloudTrail）中查看最新事件。使用收集的信息 CloudTrail，您可以确定向这些服务发出的请求、发出请求的 IP 地址、请求的发出者、发出请求的时间以及其他详细信息。

要了解 CloudTrail 更多信息（包括如何对其进行配置和启用），请参阅 [Amazon CloudTrail 用户指南](#)。

CloudTrail 在您创建账户 Amazon Web Services 账户时启用。当 Shield Advanced Firewall Manager 在 CloudTrail 中 Amazon WAF 发生受支持的事件活动时，该活动将记录在 Event history（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 [使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您中的事件（包括 Shield Advanced Amazon Web Services 账户、Amazon WAF、Firewall Manager 事件），请创建跟踪。通过跟踪，可 CloudTrail 将日志文件传送到 Amazon S3 存储桶。在控制台创建跟踪时，跟踪默认应用于所有区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送到您指定的 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操作。有关更多信息，请参阅下列内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [为配置 Amazon SNS 通知 CloudTrail](#)
- [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](#)

Amazon CloudTrail 中的 Amazon WAF 信息

所有 Amazon WAF 操作由 Amazon CloudTrail 记录，并且在 [Amazon WAF API 参考](#) 中正式记载。例如，对 ListWebACL、UpdateWebACL 和 DeleteWebACL 的调用将在 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：

- 使用根用户凭证发出的
- 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 userIdentity 元素](#)。

示例：Amazon WAF 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。Amazon 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 Amazon WAF Web ACL 操作 CloudTrail 的日志条目示例。

示例：CloudTrail 的日志条目 CreateWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    }
  },
  "description": "foo",
  "rules": [
    {
      "name": "foo",
      "priority": 1,
      "statement": {
        "geoMatchStatement": {
          "countryCodes": [
            "AF",
            "AF"
          ]
        }
      },
      "action": {
        "block": {}
      },
      "visibilityConfig": {
        "sampledRequestsEnabled": true,
        "cloudWatchMetricsEnabled": true,
        "metricName": "foo"
      }
    }
  ]
}
```

```
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-west-2:112233445566:global/webacl/foo/ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afdl1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

示例：CloudTrail 的日志条目GetWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
}
```



```
"eventType": "AwsApiCall",  
"apiVersion": "2019-04-23",  
"recipientAccountId": "112233445566"  
}
```

示例：CloudTrail 的日志条目UpdateWebACL

```
{  
  "eventVersion": "1.05",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "principalId",  
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",  
    "accountId": "112233445566",  
    "accessKeyId": "accessKeyId",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "principalId",  
        "arn": "arn:aws:iam::112233445566:role/Admin",  
        "accountId": "112233445566",  
        "userName": "Admin"  
      },  
      "webIdFederationData": {},  
      "attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2019-11-06T19:17:20Z"  
      }  
    }  
  },  
  "eventTime": "2019-11-06T19:20:56Z",  
  "eventSource": "wafv2.amazonaws.com",  
  "eventName": "UpdateWebACL",  
  "awsRegion": "us-west-2",  
  "sourceIPAddress": "10.0.0.1",  
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML,  
like Gecko) Chrome/78.0.3904.87 Safari/537.36",  
  "requestParameters": {  
    "name": "foo",  
    "scope": "CLOUDFRONT",  
    "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",  
    "defaultAction": {  
      "block": {}  
    }  
  },  
  "description": "foo",  
  "rules": [  
    {  
      "name": "foo",  
      "priority": 1,  
      "statement": {  
        "geoMatchStatement": {  
          "countryCodes": [  
            "AF"  
          ]  
        }  
      },  
      "action": {  
        "block": {}  
      },  
      "visibilityConfig": {  
        "sampledRequestsEnabled": true,  
        "cloudWatchMetricsEnabled": true,  
        "metricName": "foo"  
      }  
    }  
  ]  
}
```

```
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

示例：CloudTrail 的日志条目DeleteWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/sheqiang-Isengard",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbc976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

示例：Amazon WAF Classic 日志文件条目

Amazon WAF Classic 是 Amazon WAF 的以前版本。有关信息，请参阅 [Amazon WAF Classic \(p. 238\)](#)。

日志条目演示了 CreateRule、GetRule、UpdateRule 和 DeleteRule 操作：

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "Amazon Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "19434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [
            ],
            "name": "0923ab32-7229-49f0-a0e3-66c81example"
          ],
          "changeToken": "19434322-8685-4ed2-9c5b-9410bexample"
        },
        "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
        "eventID": "923f4321-d378-4619-9b72-4605bexample",
        "eventType": "AwsApiCall",
        "apiVersion": "2015-08-24",
        "recipientAccountId": "777777777777"
      },
      {
        "eventVersion": "1.03",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDAIEP4IT4TPDEXAMPLE",
          "arn": "arn:aws:iam::777777777777:user/nate",
          "accountId": "777777777777",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "userName": "nate"
        },
        "eventTime": "2016-04-25T21:35:22Z",
        "eventSource": "waf.amazonaws.com",
        "eventName": "GetRule",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "Amazon Internal",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
          "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
        }
      }
    ]
  }
}
```

```
    },
    "responseElements": null,
    "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
    "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
      "accountId": "777777777777",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "nate"
    },
    "eventTime": "2016-04-25T21:35:13Z",
    "eventSource": "waf.amazonaws.com",
    "eventName": "UpdateRule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "Amazon Internal",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
      "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
      "updates": [
        {
          "predicate": {
            "type": "SizeConstraint",
            "dataId": "9239c032-bbbe-4b80-909b-782c0example",
            "negated": false
          },
          "action": "INSERT"
        }
      ]
    },
    "responseElements": {
      "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
    },
    "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
    "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
      "accountId": "777777777777",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "nate"
    },
    "eventTime": "2016-04-25T21:35:28Z",
    "eventSource": "waf.amazonaws.com",
    "eventName": "DeleteRule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "Amazon Internal",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "changeToken": "fd232003-62de-4ea3-853d-52932example",
      "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
    }
  }
}
```

```
    },
    "responseElements": {
      "changeToken": "fd232003-62de-4ea3-853d-52932example"
    },
    "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
    "eventID": "a3236565-1a1a-4475-978e-81c12example",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  }
]
}
```

Amazon Shield Advanced中的信息 CloudTrail

Amazon Shield Advanced支持在 CloudTrail 日志文件中将以下操作记录为事件：

- [ListAttacks](#)
- [DescribeAttack](#)
- [CreateProtection](#)
- [DescribeProtection](#)
- [DeleteProtection](#)
- [ListProtections](#)
- [CreateSubscription](#)
- [DescribeSubscription](#)
- [GetSubscriptionState](#)

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：

- 使用根用户凭证发出的
- 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 userIdentity 元素](#)。

示例：Shield Id Advanced 日志

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。

下面的示例显示了一个 CloudTrail，该条目说明了DeleteProtection和ListProtections操作。

```
[
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "1234567890987654321231",
      "arn": "arn:aws:iam::123456789012:user:SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
```

```
    "userName": "SampleUser"
  },
  "eventTime": "2018-01-10T21:31:14Z",
  "eventSource": "shield.amazonaws.com",
  "eventName": "DeleteProtection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
  "requestParameters": {
    "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
  },
  "responseElements": null,
  "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
  "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
  "eventType": "AwsApiCall",
  "apiVersion": "AWSShield_20160616",
  "recipientAccountId": "123456789012"
},
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789098765432123",
    "arn": "arn:aws:iam::123456789012:user:SampleUser",
    "accountId": "123456789012",
    "accessKeyId": "1AFGDT647FHU83JHFI81H",
    "userName": "SampleUser"
  },
  "eventTime": "2018-01-10T21:30:03Z",
  "eventSource": "shield.amazonaws.com",
  "eventName": "ListProtections",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "Amazon Internal",
  "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
  "requestParameters": null,
  "responseElements": null,
  "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
  "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
  "eventType": "AwsApiCall",
  "apiVersion": "AWSShield_20160616",
  "recipientAccountId": "123456789012"
}
]
```

Amazon Firewall Manager中的信息 CloudTrail

Amazon Firewall Manager支持在 CloudTrail 日志文件中将以下操作记录为事件：

- [AssociateAdminAccount](#)
- [DeleteNotificationChannel](#)
- [DeletePolicy](#)
- [DisassociateAdminAccount](#)
- [PutNotificationChannel](#)
- [PutPolicy](#)
- [GetAdminAccount](#)
- [GetComplianceDetail](#)
- [GetNotificationChannel](#)
- [GetPolicy](#)
- [ListComplianceStatus](#)

- [ListPolicies](#)

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：

- 使用根用户凭证发出的
- 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 userIdentity 元素](#)。

示例：Firewall Manager 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。

下面的示例显示了一个 GetAdminAccount--> 操作 CloudTrail 的日志条目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890987654321231",
    "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
    "accountId": "123456789012",
    "accessKeyId": "1AFGDT647FHU83JHFI81H",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated":
        "false",
        "creationDate":
        "2018-04-14T02:51:50Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId":
        "1234567890987654321231",
        "arn":
        "arn:aws:iam::123456789012:role/Admin",
        "accountId":
        "123456789012",
        "userName": "Admin"
      }
    },
    "eventTime": "2018-04-14T03:12:35Z",
    "eventSource": "fms.amazonaws.com",
    "eventName": "GetAdminAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "console.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
    "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-01-01",
    "recipientAccountId": "123456789012"
  }
```

```
}
```

使用 Amazon WAF 和 Amazon Shield Advanced API

本节介绍如何向 Amazon WAF 和 Shield Advanced API 发出请求，以便在中创建和管理匹配集、规则和 Web ACL，Amazon WAF 以及您在 Shield Advanced 中的订阅和保护。在本部分中，您将了解请求的组成部分、响应的内容以及如何验证请求。

主题

- [使用 Amazon 软件开发工具包 \(p. 520\)](#)
- [向 Amazon WAF 或 Shield Advanced 发出 HT \(p. 520\)](#)
- [HTTP 响应 \(p. 522\)](#)
- [对请求进行身份验证 \(p. 523\)](#)

使用 Amazon 软件开发工具包

如果 Amazon 为您使用的语言提供了开发工具包，请使用该开发工具包而不是尝试使用 API 自行操作。软件开发工具包让身份验证变得更简单，可轻松与您的开发环境集成以及让您轻松访问 Shield Advanced 命令。Amazon WAF 有关 Amazon 开发工具包的更多信息，请参阅[设置 \(p. 3\)](#)主题中的[下载工具 \(p. 3\)](#)。

向 Amazon WAF 或 Shield Advanced 发出 HT

Amazon WAF 根据 [RFC 2616](#) 的定义，Shield Advanced 请求是 HTTPS 请求。与任何 HTTP 请求一样，对 Amazon WAF 或 Shield Advanced 的请求包含请求方法、URI、请求标头和请求正文。响应包含 HTTP 状态码、响应标题，有时候包含响应主体。

请求 URI

请求 URI 始终是一个正斜杠 /。

HTTP 标头

Amazon WAF 而且 Shield Advanced 要求在 HTTP 请求的标头中包含以下信息：

Host (必需)

指定资源创建位置的终端节点。有关终端节点的信息，请参阅[Amazon 服务终端节点](#)。例如，CloudFront 分配的 Host 标题值为 `waf.amazonaws.com:443`。Amazon WAF

x-amz-date 或日期 (必填)

用于创建 Authorization 标头中包含的签名的日期。采用 ISO 8601 标准格式以 UTC 时间指定日期，如下示例所示：

```
x-amz-date: 20151007T174952Z
```

必须包含 x-amz-date 或 Date。(有些 HTTP 客户端库不允许设置 Date 标头。) 当存在 x-amz-date 标头时，Amazon WAF 在验证请求身份时会忽略所有 Date 标头。

当接收请求时，时间戳必须在 Amazon 系统时间的 15 分钟内。如果不在此时间范围内，请求将失败，并出现 RequestExpired 错误代码，以防止其他人重放您的请求。

Authorization (必需)

请求身份验证所需的信息。有关构建此标头的更多信息，请参阅[对请求进行身份验证 \(p. 523\)](#)。

X-Amz-Target (必需)

AWSWAF_ 或 AWSShield_、无标点的 API 版本、句点 (.) 以及操作名称的联接，例如：

AWSWAF_20150824.CreateWebACL

Content-Type (条件性)

指定内容类型为 JSON，并指定 JSON 的版本，如下示例所示：

```
Content-Type: application/x-amz-json-1.1
```

条件：POST 请求时为必填项。

Content-Length (条件性)

符合 RFC 2616 的消息的长度（不带标头）。

条件：必需，如果请求主体本身包含信息（大多数工具包自动添加此标题）。

以下示例为在 Amazon WAF 中创建 Web ACL 所用的 HTTP 请求的标头：

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
                Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
                SignedHeaders=host;x-amz-date;x-amz-target,
                Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

HTTP 请求正文

许多 Amazon WAF Shield Advanced API 操作都要求您在请求正文中包含 JSON 格式的数据。

以下示例请求使用简单的 JSON 语句更新，IPSet 使其包含 IP 地址 192.0.2.44（以 CIDR 表示法表示为 192.0.2.44/32）：

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
                Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
                SignedHeaders=host;x-amz-date;x-amz-target,
                Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive
```

```
{
  "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
  "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
  "Updates": [
    {
      "Action": "INSERT",
      "IPSetDescriptor": {
        "Type": "IPv4",
        "Value": "192.0.2.44/32"
      }
    }
  ]
}
```

HTTP 响应

AllAmazon WAF 和 Shield Advanced API 操作在响应中都包含 JSON 格式的数据。

以下是 HTTP 响应中的一些重要标头，以及您在应用程序中对其进行处理的方法 (如适用)：

HTTP/1.1

此标头后跟状态代码。状态代码 200 表示操作成功。

类型：字符串

x-amzn-RequestId

例如，由 Amazon WAF 或 Shield Advanced 创建的唯一标识您的请求的值 K2QH8DN0U907N97FNA2GDLL80BVV4KQNS05AEMVJF66Q9ASUAAJG。如果您在使用 Amazon WAF 时遇到问题，Amazon 可以使用此值来排除故障。

类型：字符串

内容长度

响应正文的长度 (以字节为单位)。

类型：字符串

日期

Amazon WAF 或 Shield Advanced 回复的日期和时间，例如，格林尼治标准时间 2015 年 10 月 7 日星期三 12:00:00。

类型：字符串

错误响应

如果请求导致错误，HTTP 响应将包含以下值：

- 作为响应正文的 JSON 错误文档
- Content-Type
- 合适的 3xx、4xx 或 5xx HTTP 状态代码

下面是 JSON 错误文档的示例：

```
HTTP/1.1 400 Bad Request
```

```
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message": "1 validation error detected: Value null at 'TargetString' failed to satisfy
constraint: Member must not be null"}
```

对请求进行身份验证

如果 Amazon 为您使用的语言提供了开发工具包，建议您使用该开发工具包。与使用 Amazon WAF 或 Shield Advanced API 相比，所有 Amazon 开发工具包都会大大简化签名请求的过程，从而为您节省大量时间。此外，开发工具包还可轻松与您的开发环境集成，并让您轻松访问相关命令。

Amazon WAF 而且 Shield Advanced 要求您通过签署请求来对发送的每个请求进行身份验证。要对请求进行签名，您需要使用加密哈希函数计算出数字签名，此函数可根据输入返回一个哈希值。输入内容包括您的请求文本和秘密访问密钥。哈希函数返回哈希值，您将该值包含在请求中，作为签名。该签名是您的请求的 Authorization 标头的一部分。

收到您的请求后，Amazon WAFShield Advanced 会使用您在为请求签名时使用的相同哈希函数和输入来重新计算签名。如果得出的签名与请求中的签名相匹配，Amazon WAF 则 Shield Advanced 会处理请求。如果不匹配，则拒绝请求。

Amazon WAFShield Advanced 支持使用[Amazon 签名版本 4](#) 进行身份验证。计算签名的过程可分为三个任务：

[任务 1：创建规范请求](#)

按照 Amazon Web Services 一般参考中的[任务 1：针对签名版本 4 创建规范请求](#) 中所述，以规范格式创建 HTTP 请求。

[任务 2：创建待签字符串](#)

创建一个字符串，将该字符串用作您的加密哈希函数输入值中的一项。该字符串称为“待签字符串”，是以下值的结合：

- 哈希算法的名称
- 请求日期
- 凭证范围字符串
- 来自上一任务的规范请求

凭证范围字符串本身是日期、区域和服务信息的结合。

对于 X-Amz-Credential 参数，指定以下内容：

- 您要请求发送到的终端节点的代码，即 us-east-2
- waf (表示服务缩写)

例如：

X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/aws4_request

[任务 3：创建签名](#)

使用接受两种输入字符串的加密哈希函数为您的请求创建签名：

- 您的待签字符串，来自任务 2。
- 派生密钥。派生密钥的计算方法是，以您的秘密访问密钥为开始并使用证书范围字符串来创建一系列基于哈希的消息身份验证代码 (HMAC)。

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。

以下资源可用于 Amazon WAF、Amazon Shield Advanced 和 Amazon Firewall Manager。

- [实施指南Amazon WAF](#) — 技术出版物，其中包含最新的实施建议Amazon WAF，以保护现有和新的 Web 应用程序。
- [Amazon开发论坛](#)-基于社区的论坛，在这里可以讨论与此Amazon服务和其他服务有关的技术问题。
- [Amazon WAF开发@@ 论坛](#)-基于社区的论坛，供开发人员讨论与之相关的技术问题Amazon WAF。
- [Shield Advan cer Forum](#) — 基于社区的论坛，供开发人员讨论与 Sheld Advancer 有关的技术问题。
- [Amazon WAF产品信息-提供](#)有关的信息的主要网页Amazon WAF，包括功能、定价等信息。
- [Shild Advancer 产品信息](#)-提供 Shield Advancer 相关信息（包括功能、定价等信息）的主要网页。

以下资源可用于Amazon Web Services。

- [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](#)— 提供有关的信息的主要网页Amazon Web Services Support one-on-one，这是一个快速响应支持渠道，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

本页列出了对此文档的重大更改。

在服务可用的 Amazon 区域会不时逐步地推出服务功能。我们仅在第一次发布时更新了此文档。我们不提供有关区域可用性的信息，也不会宣布后续区域支持情况。要了解服务功能的区域可用性以及订阅更新通知，请参阅 [Amazon 有哪些新增功能？](#)

变更	说明	日期
中的新Amazon WAF政策规则选项Amazon Firewall Manager (p. 423)	Amazon Firewall Manager 增加了对Amazon WAF欺诈控制账户接管预防 (ATP) 和 Amazon WAF机器人控制 Amazon管理规则组、Amazon S3 日志记录目标、规则操作替代CAPTCHA和Challenge规则操作以及令牌域列表的支持。	2023 月月月月月月
Firewall Manager 支持 Amazon S3 存储桶作为Amazon WAF日志记录目的地 (p. 445)	现在，您可以将 Amazon S3 存储桶用作Amazon WAF策略中的日志目标。	2023 月月月月月月
Amazon WAF管理政策变更 (p. 223)	更新了AWSWAFFullAccessPolicyAWSWAFConsoleFullAccess、AWSWAFReadOnlyPolicy和AWSWAFConsoleReadOnlyAccess，以将Amazon App Runner服务添加到您可以保护的资源类型中 Amazon WAF。	2023 月月月月月月
添加了有关在安全组策略中使用标签的警告 (p. 428)	如果策略的标签与组织的标签策略冲突，Firewall Manager 不会更新现有安全组的标签或创建新的安全组。	2023 月月月月月月
更新服务角色信息 (p. 481)	更新了如何在Firewall Manager 中使用服务角色。	2023 年 3 月 8 日
更新了取消Firewall Manager 管理员帐户更改资格的指南 (p. 407)	阐明了从组织中删除具有Firewall Manager 策略的帐户时会发生什么。	2023 年 3 月 6 日
更正了有关基于速率的规则如何执行速率限制的信息 (p. 95)	带有缩小范围语句的基于速率的规则仅限与规则的范围缩小语句相匹配的速率限制请求。我们指出，该限制适用于所有对任何速率有限的 IP 地址的请求。	2023 年 3 月 1 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了 PHP 应用程序规则组的管理规则。	2023 年 2 月 27 日
添加了对Amazon App Runner的支持Amazon WAF (p. 5)	现在，您可以将Amazon WAF Web ACL 与Amazon App Runner 服务相关联。此更改仅在最新版本的中可用，在Amazon WAF Classic 中不可用。Amazon WAF	2023 年 2 月 23 日

更新了 IAM 指南Amazon Firewall Manager (p. 473)	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践 。	2023 年 2 月 16 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon管理规则 Amazon WAF更新了规则组AWSManagedRulesATPRuleSet，在保护 Amazon CloudFront 发行版的 Web ACL 中添加了登录响应检查。	2023 年 2 月 15 日
Amazon WAF欺诈控制账户接管预防 (ATP) 登录响应检查 (p. 155)	对于受保护的 CloudFront 发行版，您现在可以使用 ATP 阻止最近提交了过多失败登录尝试的客户的新登录尝试。	2023 年 2 月 15 日
更新的Amazon托管规则Amazon WAF (p. 68)	更新了核心规则集。	2023 年 1 月 25 日
智能威胁缓解的最佳实践 (p. 135)	添加了有关实现机器人控制、ATP 和其他智能威胁缓解功能的最佳实践的章节。	2023 年 1 月 20 日
如何检查 HTTP/2 伪标头 (p. 106)	添加了一个将 HTTP/2 伪标头映射到其相应的 Web 请求组件的部分。	2023 年 1 月 20 日
更新了Amazon WAF Classic IAM 指南 (p. 310)	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践 。	2023 年 1 月 3 日
更新了 IAM 指南Amazon WAF (p. 210)	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践 。	2023 年 1 月 3 日
更新了 IAM 指南Amazon Shield (p. 383)	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践 。	2023 年 1 月 3 日
更新Amazon Route 53 Resolver DNS (p. 463)	添加了有关删除 Amazon Route 53 Resolver DNS Firewall 规则	2022 年 12 月 29 日
Firewall Manager 中Amazon WAF规则组的限制 (p. 445)	为Firewall Manager 中的Amazon WAF规则组添加了限制。	2022 年 12 月 29 日
更新的Amazon托管规则Amazon WAF (p. 68)	更新了 Linux 操作系统规则集。	2022 年 12 月 15 日
更新的Amazon托管规则Amazon WAF (p. 68)	更新了核心规则集。	2022 年 12 月 5 日
Firewall Manager 增加了对Fortigate 云原生防火墙 (CNF) 即服务策略的支持 (p. 464)	Firewall Manager 现在支持 Fortigate CNF 策略。	2022 年 12 月 2 日
取消了 DNS 防火墙策略的Amazon Config要求 (p. 404)	对于 DNS 防火墙策略，您现在只需要为资源类型 EC2 VPC 启用 Config 即可。	2022 年 11 月 17 日

Amazon Firewall Manager 托管式策略更新 (p. 490)	已更新 FMSServiceRolePolicy。	2022 年 11 月 15 日
Amazon WAF 验证码拼图的语言扩展 (p. 175)	CAPTCHA 拼图现在提供多种语言的书面说明。每个音频拼图中的说明仍然仅以英文提供。	2022 年 11 月 11 日
资源集的新 Firewall Manager 配额 (p. 498)	为资源集添加了新的配额。	2022 年 11 月 8 日
添加对资源集的支持 (p. 466)	您可以创建资源集，对要在 Firewall Manager 策略中管理的资源进行分组。	2022 年 11 月 8 日
添加对从 Network Firewall 导入防火墙的支持 (p. 422)	现在，您可以使用资源集导入和管理 Network Firewall 策略中的现有防火墙。	2022 年 11 月 8 日
Amazon Firewall Manager 托管式策略更新 (p. 490)	已更新 AWSFMAdminReadOnlyAccess。	2022 年 11 月 2 日
地理匹配声明现在为国家和地区的请求添加了标签 (p. 87)	现在，您可以通过将地理匹配与标签匹配相结合，在区域级别管理地理请求来源。	2022 年 10 月 31 日
重命名了顶级部分：托管保护 (p. 130)	该部分现在被命名为 Amazon WAF 智能威胁缓解，与我们的营销页面一致。	2022 年 10 月 27 日
Bot Control 托管规则组中的新的目标保护级别 (p. 49)	Bot Control 托管规则组现在为高级机器人检测和缓解提供了额外的有针对性的规则。此保护级别需要支付额外费用。	2022 年 10 月 27 日
关于 Amazon WAF 代币的新章节 (p. 136)	了解如何 Amazon WAF 使用代币来智能缓解威胁。	2022 年 10 月 27 日
添加了有关更新 Firewall Manager Network Firewall 策略的重要说明 (p. 457)	更新 Firewall Manager 策略时，该策略创建的所有 Network Firewall 策略都将使用 Firewall Manager 策略的 Network Firewall 策略配置进行更新。	2022 年 10 月 27 日
规则组中的操作替代 (p. 14)	现在，您可以将规则组中规则的操作改写为任何规则操作设置。与之前的 Count 操作改写一样，您可以将改写应用于规则组中的所有规则和单个规则。	2022 年 10 月 27 日
Amazon WAF 新 Challenge 规则操作选项 (p. 175)	您可以将规则配置为使用 Challenge，以验证请求是否由浏览器发送。	2022 年 10 月 27 日
Amazon WAF 允许在多个受保护的的应用程序之间共享令牌 (p. 138)	通过为 Web ACL 配置令牌域列表，可以在多个受保护的的应用程序中启用令牌的使用。	2022 年 10 月 27 日
所有标题规范均不区分大小写 (p. 103)	将所有标题的规范更改为不区分大小写。这与单标题行为相匹配。	2022 年 10 月 26 日

Amazon Firewall Manager 政策变更 (p. 483)	更新了手动授予 Amazon Firewall Manager 资源完全访问权限的策略列表。	2022 年 10 月 21 日
Amazon Firewall Manager 管理政策变更 (p. 490)	对的更正 AWSFMAdminFullAccess。	2022 年 10 月 21 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	更新了已知的错误输入规则组。	2022 年 10 月 20 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	更新了已知的错误输入规则组。	2022 年 10 月 5 日
更新移 Amazon WAF 动 SDK 规范 (p. 169)	将的默认值 tokenRefreshDelaySec 从 600 (10 分钟) 降低到 300 (5 分钟)。	2022 年 9 月 30 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	更正了本文档中为以下规则组提供的标签名称：POSIX 操作系统、PHP 应用程序、WordPress 应用程序。	2022 年 9 月 19 日
中的新 Amazon WAF 策略规则选项 Amazon Firewall Manager (p. 423)	Amazon Firewall Manager 现在支持对 Amazon WAF 策略中默认 Web 操作的自定义 Web 请求和响应。	2022 年 9 月 9 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	Amazon Amazon WAF 更新了以下规则组的管理规则：IP 信誉。	2022 年 8 月 30 日
Amazon WAF 管理政策变更 (p. 223)	更新 AWSWAFFullAccessPolicy、AWSWAFConsoleFullAccessAWSWAFReadOnlyAccess 和，AWSWAFConsoleReadOnlyAccess 将 Amazon Cognito 用户池添加到您可以保护的资源类型中 Amazon WAF。	2022 年 8 月 25 日
Amazon WAF 欺诈控制账户收购预防 (ATP) (p. 155)	现在，您可以将 Amazon WAF 欺诈控制账户防盗用 (ATP) 功能与亚马逊配送一起 CloudFront 使用。	2022 年 8 月 24 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	Amazon Amazon WAF 更新了以下规则组的管理规则：已知的错误输入。	2022 年 8 月 22 日
更新的 Amazon 托管规则 Amazon WAF (p. 68)	Amazon Amazon WAF 更新了以下规则组的管理规则：AWSManagedRulesATPRuleSet。	2022 年 8 月 11 日
添加了对 Amazon Cognito 用户池的支持 Amazon WAF (p. 5)	现在，您可以将一个 Amazon WAF Web ACL 与 Amazon Cognito 用户池相关联。此更改仅在最新版本的中可用，在 Amazon WAF Classic 中不可用。Amazon WAF	2022 年 8 月 11 日

添加了关于版本化Amazon托管规则组部署的章节 (p. 61)	添加了记录版本化Amazon托管规则组部署的新章节。本节包含有关在候选版本部署期间如何命名默认版本的信息。	2022 年 7 月 29 日
更新了配置Network Firewall 策略日志记录的要求 (p. 461)	添加了使用加密的 Amazon S3 存储桶作为日志目标的Network Firewall 策略的要求。	2022 年 7 月 26 日
SQLi 规则语句的灵敏度级别选项 (p. 99)	现在，您可以提高 SQL 注入规则语句的敏感度。这不会改变现有语句的行为，其敏感度级别默认为 LOW。	2022 年 7 月 15 日
添加了Network Firewall 策略配置选项 (p. 432)	Firewall Manager 现在支持 Network Firewall 防火墙策略配置中的状态评估顺序和默认操作。	2022 年 7 月 14 日
Firewall Manager 安全组策略规则设置的更新 (p. 452)	Firewall Manager 现在支持从主要安全组向副本安全组分配标签。	2022 年 7 月 7 日
Amazon Shield指南的更新 (p. 336)	扩展了 Shield 指南中的信息，以描述 Shield 如何缓解事件。	2022 年 6 月 20 日
更新了测试和调整Amazon WAF保护的指南 (p. 200)	测试和调整Amazon WAF的一般指南已更新，现在是顶级主题。	2022 年 6 月 20 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon WAF更新了以下规则组的管理规则：核心规则集 (CRS)。	2022 年 6 月 9 日
新的Firewall Manager 混乱了副手的指导 (p. 494)	添加了有关如何防止Firewall Manager 出现混乱的副手问题的指南。	2022 年 6 月 1 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon WAF更新了以下规则组的管理规则：核心规则集 (CRS)。	2022 年 5 月 24 日
新的Amazon WAF请求组件：Headers和Cookies (p. 102)	现在，您可以检查 Web 请求中的 cookie，除了检查单个标头外，还可以检查 Web 请求中的所有标头。	2022 年 4 月 29 日
Amazon WAF处理超大尺寸的车身请求组件 (p. 107)	现在，您可以在检查正文的规则中指定Amazon WAF应如何处理超大的请求正文。您在此版本之前创建的用于检查正文的规则的行为与处理超大尺寸的新Continue选项相匹配。	2022 年 4 月 29 日
Amazon WAFAmazon S3 日志策略变更 (p. 182)	更新了 Amazon S3 日志权限策略和示例。	2022 年 4 月 12 日

应用程序Application Load Balancer 自动应用层 DDoS 缓解选项现已可用Amazon Shield Advanced (p. 354)	Shield Advanced 现在支持应用程序负载均衡器的自动应用层 DDoS 缓解，使其可用于所有应用层保护。您可以将 Shield Advanced 配置为自动计算或阻止作为应用层 DDoS 攻击一部分的网络请求，这些请求是针对受保护资源的 DDoS 攻击的一部分。	2022 年 4 月 8 日
为托管规则组添加了当前默认版本设置的指示器 (p. 24)	托管规则组版本列表现在指示当前默认版本是哪个版本。	2022 年 4 月 8 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：Amazon WAF机器人控制。	2022 年 4 月 6 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 年 3 月 31 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 年 3 月 30 日
Firewall Manager 增加了对帕洛阿尔托网络云下一代防火墙 (NGFW) 的支持 (p. 464)	Firewall Manager 现在支持 Palo Alto Networks 云下一代防火墙 (NGFW)。	2022 年 3 月 30 日
将对帕洛阿尔托网络 Palo Alto Networks Cloud NGFW 的支持添加到Amazon Firewall Manager (p. 422)	Amazon Firewall Manager现在支持 Palo Alto Networks 的云下一代防火墙 (NGFW) 策略。	2022 年 3 月 30 日
Amazon Shield指南的更新 (p. 329)	扩展了 Shield 指南中的信息，以描述 Shield 如何进行事件检测，并提供 DDoS 弹性架构的示例。	2022 年 3 月 16 日
Amazon Shield指南的更新 (p. 329)	扩展了 Shield 指南中的信息，改进了各个章节的组织结构。主要更改见以下Shield 指南部分：Shield 响应小组 (SRT) 支持Amazon Shield Advanced、中的资源保护和 DDoS 事件的可见性。	2022 年 2 月 28 日
Firewall Manager 现在支持 Network Firewall 集中部署模型 (p. 432)	添加了一个新程序，说明如何配置使用分布式和集中式部署模型的策略。	2022 年 2 月 24 日
Firewall Manager 增加了对 Amazon Network Firewall集中部署模型的支持 (p. 457)	现在，您可以将Amazon Network Firewall策略配置为使用分布式或集中式部署模型。使用分布式部署模型，Firewall Manager 在策略范围内的每个 VPC 中创建和维护防火墙终端节点。使用集中部署模式，Firewall Manager 在单个检查 VPC 中创建和维护防火墙终端节点。	2022 年 2 月 24 日

将对Amazon WAF托管规则组版本控制的支持添加到Amazon Firewall Manager (p. 408)	Amazon Firewall Manager现在支持Firewall ManagerAmazon WAF策略中的Amazon WAF托管规则组版本控制。	2022 年 2 月 18 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到FMSServiceRolePolicy。	2022 年 2 月 16 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：IP 信誉列表。	2022 年 2 月 15 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon管理规则Amazon WAF添加了Amazon WAF欺诈控制账户防盗用 (ATP) 规则组AWSManagedRulesATPRuleSet。	2022 年 2 月 15 日
对Amazon WAF指南组织结构的更改 (p. 5)	为托管保护添加了新的顶级部分。将验证码部分从“规则”下移至新的托管保护部分下。将标签部分从规则下移至其自己的顶级分区。	2022 年 2 月 15 日
Amazon WAF应用程序集成 SDK (p. 164)	使用Amazon WAF JavaScript 和移动应用程序集成 SDK 将您的客户端应用程序与Managed Rules 规则组集成AWSManagedRulesBotControlRuleSet , AWSManagedRulesATPRuleSet并增强规则组的检测。Amazon	2022 年 2 月 15 日
Amazon WAF欺诈控制账户收购预防 (ATP) (p. 155)	您可以使用新的 FAmazon WAF Fraud Control 账户接管预防 (ATP) 管理规则组检测和阻止账户接管尝试AWSManagedRulesATPRuleSet。	2022 年 2 月 15 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 年 1 月 28 日
Amazon WAF管理政策变更 (p. 223)	已更新新AWSWAFFullAccessPolicy并AWSWAFConsoleFullAccess更正了日志权限。	2022 年 1 月 11 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：核心规则集 (CRS)、SQLi 数据库。	2022 年 1 月 10 日
Firewall Manager 支持 Shield 高级自动应用层 DDoS 缓解 (p. 450)	Firewall Manager Shield Amazon CloudFront 资源的高级策略现在包括支持自动缓解应用层 DDoS。	2022 年 1 月 7 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到FMSServiceRolePolicy。	2022 年 1 月 7 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 年 1 月 7 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 年 1 月 7 日

更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：已知的错误输入。	2022 月 月 月 月 月 月 月
新的Amazon Shield Advanced服务相关角色 (p. 398)	添加了AWSServiceRoleForAWSShield以支持自动应用层 DDoS 缓解功能。	2021 年 12 月 1 日
新的Amazon Shield托管策略 (p. 396)	添加了AWSShieldServiceRolePolicy以支持自动应用层 DDoS 缓解功能。	2021 年 12 月 1 日
自动应用层 DDoS 缓解选项现在已在 for 中可Amazon Shield Advanced用CloudFront (p. 354)	Shield Advanced 现在支持亚马逊 CloudFront发行版的自动应用层 DDoS 缓解措施。您可以将 Shield Advanced 配置为自动计数或屏蔽作为 CloudFront分布层应用层 DDoS 攻击一部分的 Web 请求。	2021 年 12 月 1 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新了以下规则组的管理规则：核心规则集 (CRS)、Windows 操作系统、Linux 操作系统和 IP 信誉列表。	2021 年 11 月 23 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到FMSServiceRolePolicy。	2021 年 11 月 18 日
扩展了以下的日志选项Amazon WAF (p. 180)	现在，您可以将 Web ACL 流量记录至 Amazon CloudWatch Simple Simple Simple Simple Simple Storage Service (Amazon S3) imple S 这些选项是对 Amazon Kinesis Data Firehose 的现有日志记录选项的补充。	2021 年 11 月 15 日
Amazon WAF管理政策变更 (p. 223)	已更新AWSWAFFullAccessPolicyAWSWAFConsoleFullAccess并支持其他日志记录目的地。	2021 年 11 月 15 日
Amazon WAF新CAPTCHA规则操作选项 (p. 175)	您可以配置规则以针对网络请求运行验证码，并根据需要向客户端发送验证码问题。	2021 年 11 月 8 日
更新的Amazon托管规则Amazon WAF (p. 68)	AmazonAmazon WAF更新核心规则集 (CRS) 规则组的管理规则。	2021 年 10 月 27 日
更新的Amazon托管规则Amazon WAF (p. 32)	现在，所有Amazon托管规则组都支持标签。规则描述包括标签规范。	2021 年 10 月 25 日
Firewall Manager 支持Network Firewall 日志过滤 (p. 461)	Amazon Firewall Manager现在支持Network Firewall 策略的日志过滤。	2021 年 10 月 4 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到FMSServiceRolePolicy。	2021 年 9 月 29 日

添加了正则表达式匹配语句 (p. 97)	现在，您可以将 Web 请求与单个正则表达式进行匹配。	2021 年 9 月 22 日
规则组内部基于费率的Amazon WAF规则 (p. 95)	现在，您可以在规则组内 Amazon WAF定义基于费率的规则。中Amazon Firewall Manager，Amazon WAF策略完全支持此功能。	2021 年 9 月 13 日
Firewall Manager 支持Amazon WAF日志过滤 (p. 445)	Amazon Firewall Manager现在支持Amazon WAF策略的日志过滤。	2021 年 8 月 31 日
自动删除中的 out-of-scope 资源保护Amazon Firewall Manager (p. 440)	Amazon Firewall Manager允许您自动删除离开策略范围的资源的保护。	2021 年 8 月 25 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到FMSServiceRolePolicy。	2021 年 8 月 12 日
向托管规则组添加了版本控制 (p. 24)	托管规则组提供者现在可以对其规则组进行版本控制。	2021 年 8 月 9 日
修改Amazon Firewall Manager管理员要求 (p. 403)	您可以使用组织的管理帐户作为 Firewall Manager 管理员帐户。这是不允许的。	2021 年 8 月 2 日
Firewall Manager 配额增加 (p. 498)	将您可以在 Firewall Manager 策略范围内拥有的 Amazon VPC 实例数量从 10 月月月月 2 月 2 月 2 月月月月 2 月 2 月 2 月	2021 年 7 月 28 日
Amazon Firewall Manager支持 Amazon Network Firewall路由表监控 (p. 444)	Amazon Firewall Manager现在支持路由表监控，并针对路由配置错误的Amazon Network Firewall策略向安全管理员提供补救措施建议。	2021 年 7 月 8 日
Amazon WAF其他文本转换选项 (p. 107)	在检查请求之前，还可以将其他文本转换应用于 Web 请求组件。	2021 年 6 月 24 日
修改了Firewall ManagerAmazon WAF 策略资源的命名 (p. 444)	Firewall Manager 为您的Amazon WAF策略管理的 Web ACL、规则组和日志记录的命名已更改。	2021 年 5 月 26 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon管理规则Amazon WAF增加了对 IP 信誉列表标签的支持，并删除了亚马逊 IP 信誉列表规则名称上的后缀。	2021 年 5 月 4 日
添加对Amazon Organizations委派管理员的支持 (p. 403)	设置Amazon Firewall Manager管理员帐户时，Firewall Manager 现在会将该帐户指定为防火墙管理器的Amazon Organizations委派管理员。通过此更改，在设置 Firewall Manager 管理员帐户时，必须提供组织管理帐户以外的成员帐户。此更改不会影响您的现有设置。	2021 年 4 月 30 日

更新的Amazon托管规则Amazon WAF (p. 68)	Amazon WAF 添加了 Amazon WAF Bot Control 规则组的托管规则	2021 年 4 月 1 日
在规则组Count中将单个规则操作设置为 (p. 14)	现在，您可以将规则组中的单个规则操作设置为 Count。规则组级别的现有改写信息已更正。	2021 年 4 月 1 日
托管规则组的范围缩小声明 (p. 110)	现在，您可以像使用基于速率的语句一样，对托管规则组使用范围缩小语句。	2021 年 4 月 1 日
日志过滤 (p. 180)	现在，您可以根据规则操作和标签筛选您记录的 Web ACL 流量。	2021 年 4 月 1 日
Amazon WAF网络请求上的标签 (p. 123)	您可以配置规则，为匹配的 Web 请求添加标签，并在其他规则添加的标签上进行匹配。	2021 年 4 月 1 日
Amazon WAF机器人控制 (p. 142)	您可以使用新的 Bot Control 功能监视和控制 Amazon WAF 机器人流量，该功能将机器人控制托管规则组与 Web 请求标签、范围缩小语句和日志筛选相结合。	2021 年 4 月 1 日
Firewall Mirewall 管理器支持 Amazon Route (p. 463)	Amazon Firewall Manager 支持集中管理您的 VPC 的 Amazon Route 53 Resolver DNS 防火墙出站 DNS 流量过滤。	2021 年 3 月 31 日
自定义请求和响应处理 (p. 118)	您可以为 Amazon WAF 未阻塞的 Web 请求添加自定义标头，也可以为阻塞的 Amazon WAF Web 请求发送自定义响应。这适用于 Web ACL 默认操作和规则操作设置。	2021 年 3 月 29 日
Amazon Firewall Manager管理策略变更 (p. 490)	更新到 FMSServiceRolePolicy。	2021 月月月月月月
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon WAF 更新了以下规则组的管理规则：核心规则集 (CRS)、管理员保护、已知的错误输入和 Linux 操作系统。	2021 年 3 月 3 日
Amazon Shield托管策略变更跟踪 (p. 396)	Shield 为其 Amazon 托管策略开启了跟踪更改。	2021 年 3 月 3 日
Amazon Firewall Manager托管策略变更跟踪 (p. 490)	Firewall Manager 为其 Amazon 托管策略开启了跟踪更改。	2021 年 3 月 2 日
Amazon WAF托管策略变更跟踪 (p. 223)	Amazon WAF 为其 Amazon 托管策略开启了跟踪更改。	2021 年 3 月 1 日
检查已解析的 JSON 请求正文 (p. 105)	添加了检查已解析和筛选 JSON 的 Web 请求正文的选项。这是对以纯文本形式检查 Web 请求正文的现有选项的补充。	2021 年 2 月 12 日

Firewall Manager 支持Amazon Network Firewall策略 (p. 457)	Amazon Firewall Manager支持集中管理您的 VPC 的Amazon Network Firewall网络流量过滤。	2020 年 11 月 17 日
添加对Amazon Shield Advanced 保护组的支持 (p. 368)	现在，您可以将受保护的资源分组到逻辑组中，并共同管理它们的保护。	2020 年 11 月 13 日
添加了对Amazon AppSync的支持 Amazon WAF (p. 5)	现在，您可以将Amazon WAF Web ACL 与Amazon AppSync GraphQL API 关联起来。此更改仅在最新版本的中可用，在Amazon WAF Classic 中不可用。Amazon WAF	2020 年 10 月 1 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon用于Amazon WAF更新 Windows 操作系统规则集的托管规则。	2020 年 9 月 23 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon用于Amazon WAF更新规则集 PHP 应用程序和 POSIX 操作系统的托管规则。	2020 年 9 月 16 日
更新了Amazon Shield控制台 (p. 343)	Amazon Shield提供了新的控制台选项，改善了用户体验。文档中的控制台指南适用于新控制台。	2020 年 9 月 1 日
Firewall Manager 对常见安全组策略的更新 (p. 457)	Amazon Firewall Manager现在，通过控制台实现，常见安全组策略支持应用程序负载均衡器和 Classic Load Bancer 资源类型。新选项可在通用策略的策略范围设置中找到。	2020 年 8 月 11 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon用于Amazon WAF更新核心规则集的管理规则。	2020 年 8 月 7 日
Firewall Manager 支持Amazon WAF日志配置 (p. 445)	Amazon Firewall Manager现在支持Amazon WAF策略的集中日志配置。	2020 年 7 月 30 日
在 Web 请求中指定 IP 地址位置 (p. 110)	添加了使用您指定的 HTTP 标头中的 IP 地址，而不是使用 Web 请求源。备用标头通常为X-Forwarded-For (XFF)，但您可以指定任何标头名称。您可以使用此选项进行 IP 集匹配、地理匹配和基于速率的规则计数聚合。	2020 年 7 月 9 日
Firewall Manager 更新内容审计安全组策略 (p. 454)	Amazon Firewall Manager扩展了内容审计安全组策略的功能，包括托管规则选项，该选项使用托管应用程序和协议列表以及资源违规的详细信息。	2020 年 7 月 7 日

Firewall Manager 管理列表 (p. 441)	Amazon Firewall Manager现在支持托管应用程序和协议列表。Firewall Manager 管理一些列表，您可以创建和管理自己的列表。	2020 年 7 月 7 日
Firewall Manager 支持常见安全组策略中的共享 VPC (p. 452)	现在，Amazon Firewall Manager 支持在共享 VPC 中使用通用安全组策略。除了在范围内账户拥有的 VPC 中使用这些策略之外，还可以执行该操作。	2020 年 5 月 26 日
更新的Amazon托管规则Amazon WAF (p. 32)	在“Amazon托管规则”中为每条规则添加了文档Amazon WAF。	2020 年 5 月 20 日
更新的Amazon托管规则Amazon WAF (p. 68)	Amazon用于Amazon WAF更新Linux 操作系统规则组的管理规则。	2020 年 5 月 19 日
添加对将Amazon WAF经典资源迁移到Amazon WAF (v2) 的支持 (p. 232)	现在，您可以使用控制台或 API 导出您的Amazon WAF经典资源，以便迁移到最新版本的Amazon WAF。	2020 年 4 月 27 日
在策略范围内增加对Amazon Organizations组织单位的支持 (p. 422)	Amazon Firewall Manager 现在支持使用 Amazon Organizations 组织单位 (OU) 指定策略范围。除了包括或排除特定账户外，您还可以使用 OU 在范围中包括或排除账户。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。	2020 年 4 月 6 日
将对Amazon WAF (v2) 的支持添加到Amazon Firewall Manager (p. 422)	Amazon Firewall Manager除了之前的版本外Amazon WAF，现在还支持最新版本的Amazon WAF Classic。	2020 年 3 月 31 日
更新Amazon Firewall Manager常见安全组策略	Amazon Firewall Manager通用安全组策略现在可以选择将该策略应用于您作用域内的 Amazon EC2 实例中的所有弹性网络接口。您仍然可以选择仅将策略应用于默认弹性网络接口。	2020 年 3 月 11 日
更新的Amazon托管规则Amazon WAF	Amazon用于Amazon WAF添加规则组的管理AWSManagedRulesAnonymousIpList规则。	2020 年 3 月 6 日
更新的Amazon托管规则Amazon WAF	Amazon用于Amazon WAF更新 WordPress 应用程序和规则组的管理AWSManagedRulesCommonRuleSet规则。	2020 年 3 月 3 日

在Amazon Shield Advanced保护选项中添加了亚马逊 Route 53 运行状况检查 (p. 358)	Shield Advanced 现在支持使用亚马逊 Route 53 运行状况检查关联，以提高威胁检测和缓解的准确性。	2020 年 2 月 14 日
更新的Amazon托管规则Amazon WAF	Amazon的管理规则更新Amazon WAF了 SQL 数据库规则组，增加了检查消息 URI 的功能。	2020 年 1 月 23 日
Firewall Manager 安全组使用情况审计策略的新选项	Firewall Manager 为安全组使用审计策略提供了一个新选项。现在，您可以设置安全组在被视为不合规之前必须保持未使用状态的最小分钟数。默认情况下，此分钟数设置为零。	2020 年 1 月 14 日
Firewall ManagerAmazon WAF策略的新选项	Firewall Manager 为Amazon WAF策略提供了一个新的选项。现在，您可以选择从范围内资源删除所有现有 Web ACL 关联，然后再将策略的新 Web ACL 与这些资源关联。	2020 年 1 月 14 日
更新的Amazon托管规则Amazon WAF	Amazon的管理规则更新Amazon WAF了核心规则集和 SQL 数据库规则组中规则的文本转换。	2019 年 12 月 20 日
Amazon Firewall Manager 与 Amazon Security Hub 集成	Amazon Firewall Manager 现在为不符合要求的资源以及攻击创建结果，并将其发送到 Amazon Security Hub。	2019 年 12 月 18 日
Amazon WAF版本 2 的发布	《Amazon WAF 开发人员指南》的新版本。您可以管理 JSON 格式的 Web ACL 或规则组。扩展的功能包括逻辑规则语句、规则语句嵌套以及对 IP 地址和地址范围的完整 CIDR 支持。规则不再是 Amazon 资源，而仅存在于 Web ACL 或规则组的上下文中。对于现有客户，该服务的先前版本现在称为Amazon WAF Classic。在 API、SDK 和 CLI 中，CAmazon WAF lassic 保留其命名方案，根据上下文的Amazon WAF不同，在引用最新版本时添加了“V2”或“v2”。Amazon WAF无法访问在Amazon WAF Classic 中创建的Amazon资源。要在 Amazon WAF 中使用这些资源，您需要迁移它们。	2019 年 11 月 25 日
Amazon的管理规则规则组Amazon WAF	添加了Amazon托管规则规则组。这些对于 Amazon WAF 客户是免费的。	2019 年 11 月 25 日
Amazon Firewall Manager支持Amazon Virtual Private C	添加了对 Amazon VPC 安全组的支持。	2019 年 10 月 10 日

Amazon Firewall Manager 支持 Amazon Shield Advanced	在 Firewall Manager 中添加了对 Shield 高级的支持。	2019 年 3 月 15 日
教程：创建分层策略	增加了有关在 Amazon Firewall Manager 中创建分层策略的教程。	2019 年 2 月 11 日
规则组中的规则级别控制	您现在可以从 Amazon Web Services Marketplace 规则组以及您自己的规则组中排除单个规则。	2018 年 12 月 12 日
Amazon Shield Advanced 支持 Amazon Global Accelerator 标准加速器	Shield Advanced 现在可以保护 Amazon Global Accelerator 标准加速器了。	2018 年 11 月 26 日
Amazon WAF 支持 Amazon API Gateway	Amazon WAF 现在可以保护 Amazon API Gateway	2018 年 10 月 25 日
扩展 Amazon 盾高级入门向导	新向导提供了创建基于费率的规则和亚马逊 CloudWatch 活动的机会。	2018 年 8 月 31 日
Amazon WAF 记录	启用日志记录，以获取有关 Web ACL 对流量进行分析的详细信息。	2018 年 8 月 31 日
Support 条件中的查询参数	创建条件时，您现在可以在请求中搜索特定的参数。	2018 年 6 月 5 日
Shield 高级入门向导	引入一个新的简化流程来订阅 Amazon Shield Advanced。	2018 年 6 月 5 日
扩展了允许的 CIDR 范围	在创建 IP 匹配条件时，Amazon WAF 现在支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。	2018 年 6 月 5 日

2018 年之前的更新

下表描述了在 2018 年之前的更新。

更改	API 版本	描述	发行日期
更新	2016-08-24	Amazon Web Services Marketplace 规则组	2017 年 11 月
更新	2016-08-24	弹性 IP 地址的 Shield 高级支持	2017 年 11 月
更新	2016-08-24	全球威胁控制面板	2017 年 11 月
更新	2016-08-24	能够抵御 DDoS 的网站教程	2017 年 10 月
更新	2016-08-24	地理和正则表达式条件	2017 年 10 月

Amazon WAF、Amazon Firewall Manager
和 Amazon Shield Advanced 开发人员指南
2018 年之前的更新

更改	API 版本	描述	发行日期
更新	2016-08-24	基于速率的规则	2017 年 6 月
更新	2016-08-24	重新企业	2017 年 4 月
更新	2016-08-24	添加了有关 DDOS 保护和 Application Load Balancer 支持的信息。	2016 年 11 月
新功能	2015-08-24	现在，您可以将所有 API 调用记录 Amazon WAF 到 Amazon CloudTrail through，该 Amazon 服务记录您的账户的 API 调用并将日志文件传送到您的 S3 存储桶。CloudTrail 日志可用于启用安全分析、跟踪 Amazon 资源变更和帮助您进行合规性审计。通过集成 Amazon WAF 和，CloudTrail 您可以确定哪些请求是向 Amazon WAF API 发出的、发出每个请求的源 IP 地址、何人发出的请求以及时间等。 如果您已经在使用 Amazon CloudTrail，则将开始在 CloudTrail 日志中看到 Amazon WAF API 调用。如果您尚未启用 CloudTrail 您的帐户，则可以 CloudTrail 从中将其启用 Amazon Web Services Management Console。启用不收取额外费用 CloudTrail，但使用 Amazon S3 和 Amazon SNS 的标准费率适用。	2016 年 4 月 28 日
新功能	2015-08-24	您现在可以使用 Amazon WAF 对表现为包含恶意脚本（称为跨站点脚本或 XSS）的请求进行允许、阻止或计数。攻击者有时会将恶意脚本插入到 Web 请求中，企图利用 Web 应用程序中的漏洞。有关更多信息，请参阅 跨站点脚本攻击规则语句 (p. 101) ：	2016 年 3 月 29 日
新功能	2015-08-24	在此版本中，Amazon WAF 添加了以下功能： - 您可以将 Amazon WAF 配置为基于请求的指定部分的长度（如查询字符串或 URI）对 Web 请求进行允许、阻止或计数。有关更多信息，请参阅 大小约束规则语句 (p. 99)： - 您可以将 Amazon WAF 配置为基于请求正文中的内容对 Web 请求进行允许、阻止或计数。这是请求中包含您要作为 HTTP 请求正文发送到 Web 服务器的任何附加数据（如来自表单的数据）的部分。此功能适用于字符串匹配条件、SQL 注入匹配条件以及第一个项目符号中提到的新的大小约束条件。有关更多信息，请参阅 网络请求组件 (p. 102)：	2016 年 1 月 27 日
新功能	2015-08-24	现在，您可以使用 Amazon WAF 控制台选择要与 Web ACL 关联的 CloudFront 发行版。有关更多信息，请参阅 关联或取消关联 Web ACL 和 CloudFront 分发 。	2015 年 11 月 16 日
首次发布	2015-08-24	这是 Amazon WAF 开发人员指南的首次发布。	2015 年 10 月 6 日

Amazon词汇表

有关最新Amazon术语，请参阅《Amazon一般参考》中的[Amazon术语表](#)。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。