

---

# AWS WAF、AWS Firewall Manager 和 AWS Shield Advanced

开发人员指南

API 版本 2015-08-24



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

Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

## Table of Contents

AWS WAF、AWS Shield 和 AWS Firewall Manager 是什么？	1
AWS Shield	1
AWS Firewall Manager	2
我应该如何选择？	2
设置	3
步骤 1：注册 AWS 账户	3
步骤 2：创建 IAM 用户	3
步骤 3：下载工具	4
AWS WAF	6
AWS WAF 如何工作	6
AWS WAF 定价	8
AWS WAF 入门	9
步骤 1：设置 AWS WAF	9
步骤 2：创建 Web ACL	9
步骤 3：创建 IP 匹配条件	10
步骤 4：创建地理匹配条件	10
步骤 5：创建字符串匹配条件	11
步骤 5A：创建正则表达式条件 (可选)	12
步骤 6：创建 SQL 注入匹配条件	13
步骤 7：(可选) 创建其他条件	14
步骤 8：创建规则并添加条件	14
步骤 8：向 Web ACL 中添加规则	15
步骤 9：清除资源	16
教程	18
教程：针对常见攻击快速设置 AWS WAF 保护	18
教程：阻止提交恶意请求的 IP 地址	23
教程：使用 AWS 服务实施能够抵御 DDoS 的网站	28
博客教程	46
创建和配置 Web 访问控制列表 (Web ACL)	46
使用条件	47
使用规则	73
使用 Web ACL	77
列出根据基于速率的规则而阻止的 IP 地址	84
AWS WAF 如何使用 Amazon CloudFront 功能	85
结合使用 AWS WAF 与 CloudFront 自定义错误页面	85
结合使用 AWS WAF 与 CloudFront 地理限制	85
选择 CloudFront 响应的 HTTP 方法	86
身份验证和访问控制	86
身份验证	86
访问控制	87
AWS Identity and Access Management	87
访问管理概述	88
使用基于身份的策略 (IAM 策略)	91
AWS WAF API 权限参考	95
AWS WAF 限制	102
AWS Firewall Manager	104
AWS Firewall Manager 定价	104
AWS Firewall Manager 先决条件	104
步骤 1：加入 AWS Organizations	105
步骤 2：设置 AWS Firewall Manager 管理员账户	105
步骤 3：启用 AWS Config	105

AWS Firewall Manager 入门 .....	106
步骤 1：完成前提条件 .....	106
步骤 2：创建规则 .....	106
步骤 3：创建规则组 .....	106
步骤 4：创建并应用 AWS Firewall Manager 策略 .....	107
AWS Firewall Manager 限制 .....	108
使用规则组 .....	108
创建规则组 .....	109
在规则组中添加和删除规则 .....	109
使用 AWS Firewall Manager 策略 .....	110
创建 AWS Firewall Manager 策略 .....	110
删除 AWS Firewall Manager 策略 .....	111
查看资源的策略合规性 .....	111
指定另一个账户作为 AWS Firewall Manager 管理员账户 .....	112
关闭 AWS Firewall Manager 管理员账户 .....	112
AWS Shield .....	114
AWS Shield 的工作原理 .....	114
AWS Shield Standard .....	114
AWS Shield Advanced .....	114
DDoS 攻击的类型 .....	115
关于 AWS DDoS 响应团队 (DRT) .....	115
帮我选择一个防护计划 .....	116
AWS Shield Advanced 使用案例示例 .....	118
AWS Shield Advanced 定价 .....	118
AWS Shield Advanced 和 AWS Shield Standard 定价 .....	118
AWS Shield Advanced 入门 .....	119
步骤 1：激活 AWS Shield Advanced .....	119
步骤 2：指定要保护的资源 .....	120
步骤 3：( 可选 ) 向 DDoS 响应团队授权 .....	120
步骤 4：在 CloudWatch 中创建 DDoS 控制面板并设置 CloudWatch 警报 .....	121
步骤 5：部署 AWS WAF 规则 .....	121
步骤 6：监控全球威胁环境控制面板 .....	122
向更多 AWS 资源添加 AWS Shield Advanced 防护 .....	122
从 AWS 资源中删除 AWS Shield Advanced .....	123
编辑 AWS Shield Advanced 设置 .....	123
AWS Shield Advanced：请求服务抵扣金额 .....	123
AWS Shield Advanced 限制 .....	124
监控 .....	125
监控工具 .....	125
自动化工具 .....	125
手动工具 .....	126
使用 Amazon CloudWatch 进行监控 .....	126
创建警报 .....	126
指标与维度 .....	126
AWS WAF 指标 .....	127
AWS WAF 维度 .....	128
Shield Advanced 指标 .....	128
使用 AWS CloudTrail 记录 API 调用 .....	130
CloudTrail 中的 AWS WAF 信息 .....	130
CloudTrail 中的 AWS Shield Advanced 信息 .....	133
CloudTrail 中的 AWS Firewall Manager 信息 .....	134
响应 DDoS 攻击 .....	136
审查 DDoS 事件 .....	136
Shield Advanced 详细信息报告 .....	137
跨 AWS 监控威胁 .....	137
使用 AWS WAF 和 AWS Shield Advanced API .....	139
使用 AWS SDKs .....	139

向 AWS WAF 或 Shield Advanced 发出 HTTPS 请求 .....	139
请求 URI .....	139
HTTP 标头 .....	139
HTTP 请求正文 .....	140
HTTP 响应 .....	141
错误响应 .....	141
对请求进行身份验证 .....	142
AWS WAF 和 AWS Shield Advanced PCI DSS 合规性 .....	144
资源 .....	145
AWS 资源 .....	145
文档历史记录 .....	146
早期更新 .....	146
AWS 词汇表 .....	148

# AWS WAF、AWS Shield 和 AWS Firewall Manager 是什么？

AWS WAF 是一种 Web 应用程序防火墙，让您能够监控转发到 Amazon CloudFront 或 应用程序负载均衡器的 HTTP 和 HTTPS 请求。利用 AWS WAF 还可控制对您的内容的访问。根据您指定的条件 (如请求源自的 IP 地址或查询字符串的值)，CloudFront 或 应用程序负载均衡器 会使用所请求的内容或使用 HTTP 403 状态代码 (禁止) 来响应请求。您还可以配置 CloudFront 以在请求被阻止时返回自定义错误页面。

在最基本的情况下，AWS WAF 允许您选择以下行为之一：

- 允许您指定的请求之外的所有请求 – 当您希望 CloudFront 或 应用程序负载均衡器 为公共网站提供内容、但同时又想阻止来自攻击者的请求时，此行为很有用。
- 阻止您指定的请求之外的所有请求 – 当您要为其用户可通过 Web 请求中的属性 (如他们用于浏览网站的 IP 地址) 轻松识别的受限网站提供内容时，此行为很有用。
- 对与您指定的属性匹配的请求计数 – 当您要根据 Web 请求中的新属性允许或阻止请求时，首先可将 AWS WAF 配置为对与属性匹配的请求计数，而不允许或阻止这些请求。这样，您便可以确保不会意外将 AWS WAF 配置为阻止进入网站的所有流量。当您确信已指定正确的属性后，可以更改行为以允许或阻止请求。

使用 AWS WAF 有几个优势：

- 使用您指定的条件针对 Web 攻击提供额外保护。您可以使用 Web 请求的如下特征来定义条件：
  - 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 (特定字符串或与正则表达式 (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)。
- 规则可以允许、阻止或统计满足指定条件的 Web 请求。或者，规则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。
- 可以重复用于多个 Web 应用程序的规则。
- 实时指标和采样的 Web 请求。
- 使用 AWS WAF API 的自动化管理。

## AWS Shield

您可以使用 AWS WAF Web 访问控制列表 (Web ACL) 来帮助最大程度地降低分布式拒绝服务 (DDoS) 攻击的影响。为了实现针对 DDoS 攻击的额外保护，AWS 还提供了 AWS Shield Standard 和 AWS Shield Advanced。AWS Shield Standard 是自动包含的，除了已为 AWS WAF 和其他 AWS 服务支付的费用外，无任何附加成本。AWS Shield Advanced 可为您的 Amazon EC2 实例、Elastic Load Balancing 负载均衡器、CloudFront 分配和 Route 53 托管区域提供扩展的 DDoS 攻击保护。AWS Shield Advanced 会产生额外费用。

有关 AWS Shield Standard 和 AWS Shield Advanced 的更多信息，请参阅 [AWS Shield \(p. 114\)](#)。

## AWS Firewall Manager

AWS Firewall Manager 可简化跨多个账户和多种资源的 AWS WAF 管理和维护任务。利用 Firewall Manager，您只需设置您的防火墙规则一次。该服务会跨您的账户和资源自动应用规则，即使您添加了新资源。

有关 Firewall Manager 的更多信息，请参阅 [AWS Firewall Manager \(p. 104\)](#)。

## 我应该如何选择？

您可以将 [AWS WAF \(p. 6\)](#)、[AWS Firewall Manager \(p. 104\)](#) 和 [AWS Shield \(p. 114\)](#) 一起使用来创建全面的安全解决方案。

一切都从 AWS WAF 入手。您可以使用 AWS Firewall Manager 自动执行然后简化 AWS WAF 管理。Shield Advanced 在 AWS WAF 的基础上添加了额外功能，例如来自 DDoS 响应团队 (DRT) 的专属支持和高级报告。

如果您希望对添加到您的资源的保护进行精细控制，单独使用 AWS WAF 是正确的选择。如果您希望跨账户使用 AWS WAF、加快您的 AWS WAF 配置或自动执行新资源的保护，请将 Firewall Manager 与 AWS WAF 结合使用。

最后，如果您拥有高可见性网站或容易遭受频繁的 DDoS 攻击，则应考虑购买 Shield Advanced 提供的额外功能。

# 设置

本主题介绍准备使用 AWS WAF、AWS Firewall Manager 和 AWS Shield Advanced 的预备步骤 (如创建 AWS 账户)。我们不会因为设置此账户和其他预备项目而对您收费。您只需为使用的 AWS 服务付费。

完成这些步骤后，请参阅 [AWS WAF 入门 \(p. 9\)](#) 继续开始使用 AWS WAF。

## Note

AWS Shield Standard 随 AWS WAF 提供，无需额外设置。有关更多信息，请参阅 [AWS Shield 的工作原理 \(p. 114\)](#)。

首次使用 AWS WAF 或 AWS Shield Advanced 前，请完成以下任务：

- [步骤 1：注册 AWS 账户 \(p. 3\)](#)
- [步骤 2：创建 IAM 用户 \(p. 3\)](#)
- [步骤 3：下载工具 \(p. 4\)](#)

## 步骤 1：注册 AWS 账户

当您注册 Amazon Web Services (AWS) 时，您的 AWS 账户会自动注册 AWS 中的所有服务，包括 AWS WAF。您只需为使用的服务付费。

如果您已有 AWS 账户，请跳到下一个任务。如果您还没有 AWS 账户，请使用以下步骤创建。

### 注册 AWS

1. 打开 <https://aws.amazon.com/> 并选择 Sign Up。
2. 按照页面上的说明操作。

作为注册流程的一部分，您会收到一个电话，需要您使用电话键盘输入一个 PIN 码。

请记住您的 AWS 账号，因为在下一个任务中您会用到它。

## 步骤 2：创建 IAM 用户

要使用 AWS WAF 控制台，您必须登录以确认您有权执行 AWS WAF 操作。您可以使用您的 AWS 账户的根凭证，但不建议这样做。为提高您的账户的安全性和控制能力，建议您使用 AWS Identity and Access Management (IAM) 执行以下操作：

- 为您自己或您的公司创建一个 IAM 用户账户。
- 将该 IAM 用户账户添加到具有管理权限的 IAM 组，或直接向该 IAM 用户账户授予管理权限。

您随后可以使用专用 URL 和该 IAM 用户的凭证登录 AWS WAF 控制台 (和其他服务控制台)。您还可以将其他用户添加到该 IAM 用户账户，并控制它们对 AWS 服务和您的资源的访问级别。

## Note

有关使用 [AWS Command Line Interface \(AWS CLI\)](#)、[Windows PowerShell 工具](#)、[AWS 开发工具包](#) 或 AWS WAF API 创建用于访问 AWS WAF 的访问密钥的信息，请参阅 [管理 IAM 用户的访问密钥](#)。



如果您已注册 AWS 但尚未为自己创建 IAM 用户，则可以使用 IAM 控制台创建。如果您不熟悉如何使用控制台，请参阅[使用 AWS 管理控制台](#)中的概述内容。

为您自己创建一个 IAM 用户并将该用户添加到管理员组

1. 使用 AWS 账户电子邮件地址和密码，以 [AWS 账户根用户](#) 身份登录到 IAM 控制台 (<https://console.aws.amazon.com/iam/>)。

**Note**

强烈建议您遵守以下使用 **Administrator** IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数[账户和服务管理任务](#)时才作为根用户登录。

2. 在控制台的导航窗格中，选择 Users，然后选择 Add user。
3. 对于 User name，键入 **Administrator**。
4. 选中 AWS 管理控制台 access 旁边的复选框，选择 Custom password，然后在文本框中键入新用户的密码。您可以选择 Require password reset (需要重置密码) 以强制用户在下次登录时创建新密码。
5. 选择 Next: Permissions。
6. 在设置权限页面上，选择将用户添加到组。
7. 选择 Create group。
8. 在 Create group (创建组) 对话框中，对于 Group name (组名称)，键入 **Administrators**。
9. 对于 Filter policies (筛选策略)，选中 AWS managed - job function (AWS 托管 - 工作职能) 的复选框。
10. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group。
11. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh 以在列表中查看该组。
12. 选择 Next: Review 以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user。

您可使用此相同的流程创建更多的组 and 用户，并允许您的用户访问 AWS 账户资源。要了解有关使用策略限制用户对特定 AWS 资源的权限的信息，请参阅[访问管理](#)和[示例策略](#)。

要以此新 IAM 用户的身份登录，请先从 AWS 控制台注销。然后使用以下 URL，其中 `your_aws_account_id` 是您的不带连字符的 AWS 账号。例如，如果您的 AWS 账号是 1234-5678-9012，则您的 AWS 账户 ID 是 123456789012：

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

输入您刚创建的 IAM 用户名和密码。登录后，导航栏显示 `your_user_name @ your_aws_account_id`。

如果不希望您的登录页面 URL 包含您的 AWS 账户 ID，可以创建账户别名。从 IAM 控制面板上，选择 Customize，输入别名，如您的公司名称。要在创建账户别名后登录，请使用以下 URL：

```
https://your_account_alias.signin.aws.amazon.com/console/
```

要验证您的账户的 IAM 用户登录链接，请打开 IAM 控制台，检查控制面板上 IAM users sign-in link 下面的内容。

完成这些步骤后，您可以在此处停止并转到[AWS WAF 入门 \(p. 9\)](#)，使用控制台继续开始使用 AWS WAF。如果您要使用 AWS WAF API 以编程方式访问 AWS WAF，请继续下一步骤[步骤 3：下载工具 \(p. 4\)](#)。

## 步骤 3：下载工具

AWS 管理控制台包含一个用于 AWS WAF 的控制台，但是如果您要以编程方式访问 AWS WAF，则以下文档和工具会对您有所帮助：

- 如果您要调用 AWS WAF API 而不必处理低级别详细信息 (如汇编原始 HTTP 请求)，则可以使用 AWS 开发工具包。AWS 开发工具包提供用于封装 AWS WAF 和其他 AWS 服务的功能的函数和数据类型。要下载 AWS 开发工具包，请参阅还包含先决条件和安装说明的适用页面：

- [Java](#)
- [JavaScript](#)
- [.NET](#)
- [Node.js](#)
- [PHP](#)
- [Python](#)
- [Ruby](#)

有关 AWS 开发工具包的完整列表，请参阅[适用于 Amazon Web Services 的工具](#)。

- 如果 AWS 没有为您使用的编程语言提供开发工具包，请参阅 [AWS WAF API 参考](#)中记录的 AWS WAF 支持的操作。
- AWS Command Line Interface (AWS CLI) 支持 AWS WAF。利用 AWS CLI，您可以从命令行控制多个 AWS 服务并通过脚本自动执行这些服务。有关更多信息，请参阅 [AWS Command Line Interface](#)。
- 适用于 Windows PowerShell 的 AWS 工具支持 AWS WAF。有关更多信息，请参阅[适用于 PowerShell 的 AWS 工具 Cmdlet Reference](#)。

# AWS WAF

AWS WAF 是一种 Web 应用程序防火墙，让您能够监控转发到 Amazon CloudFront 或 应用程序负载均衡器的 HTTP 和 HTTPS 请求。利用 AWS WAF 还可控制对您的内容的访问。根据您的指定条件 (如请求源自的 IP 地址或查询字符串的值)，CloudFront 或 应用程序负载均衡器 会使用所请求的内容或使用 HTTP 403 状态代码 (禁止) 来响应请求。您还可以配置 CloudFront 以在请求被阻止时返回自定义错误页面。

## 主题

- [AWS WAF 如何工作 \(p. 6\)](#)
- [AWS WAF 定价 \(p. 8\)](#)
- [AWS WAF 入门 \(p. 9\)](#)
- [教程 \(p. 18\)](#)
- [创建和配置 Web 访问控制列表 \(Web ACL\) \(p. 46\)](#)
- [列出根据基于速率的规则而阻止的 IP 地址 \(p. 84\)](#)
- [AWS WAF 如何使用 Amazon CloudFront 功能 \(p. 85\)](#)
- [AWS WAF 的身份验证和访问控制 \(p. 86\)](#)
- [AWS WAF 限制 \(p. 102\)](#)

## AWS WAF 如何工作

您可使用 AWS WAF 控制 Amazon CloudFront 或 应用程序负载均衡器 响应 Web 请求的方式。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。

## 条件

条件定义您希望 AWS WAF 在 Web 请求中监视的基本特征：

- 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。AWS WAF 提供了两种类型的规则：  
常规规则

常规规则仅使用条件来锁定特定请求。例如，根据您的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。

当一个规则中包括多个条件时，如本例所示，AWS WAF 会查找匹配所有条件的请求，即，它通过 AND 将条件合并在一起。

## 基于速率的规则

基于速率的规则类似于常规规则，但增加了速率限制。基于速率的规则会每五分钟统计一次来自指定 IP 地址的请求。如果请求数超过速率限制，则规则会触发操作。

您可以将条件与速率限制结合起来。这样，如果请求匹配所有条件，且请求数在任一五分钟周期内超过速率限制，则规则将触发 Web ACL 中所指定的操作。

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 15000。当请求既符合上述两个条件又超过每 5 分钟 15000 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）。

不符合上述两个条件的请求不会计入速率限制，也不会被此规则阻止。

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 是 Starts with。
- Value to match 是 login。

还要将 RateLimit 指定为 15000。

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。

### Important

应至少向常规规则中添加一个条件。不含任何条件的常规规则不能匹配任何请求，因此，也永远不会触发该规则的操作（允许、计数、阻止）。

但是，对于基于速率的规则而言，条件是可选的。如果您没有在基于速率的规则中添加任何条件，AWS WAF 则假定所有请求都匹配该规则，因此，当请求来自同一个 IP 地址时，将计入速率限制中。若来自同一 IP 地址的请求数超过速率限制，则会触发规则的操作（计数或阻止）。

## 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）和默认操作：

### 每个规则的操作

当 Web 请求匹配一个规则中的所有条件时，AWS WAF 要么阻止该请求，要么允许其转发到 CloudFront 或 应用程序负载均衡器。您可以指定希望 AWS WAF 为每个规则执行的操作。

AWS WAF 按照规则列出的顺序，将请求与 Web ACL 中的规则进行比较。AWS WAF 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，则 AWS WAF 会根据先列出的规则来允许或阻止该请求。

如果您要先测试新规则，然后再开始使用它，则还可以将 AWS WAF 配置为对满足规则的所有条件的请求进行计数。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 AWS WAF 是允许还是阻止不匹配 Web ACL 中任何规则中所有条件的请求。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该规则中的所有三个条件，并且默认操作是 ALLOW，则 AWS WAF 会将该请求转发到 CloudFront 或 应用程序负载均衡器，服务会使用请求的对象进行响应。

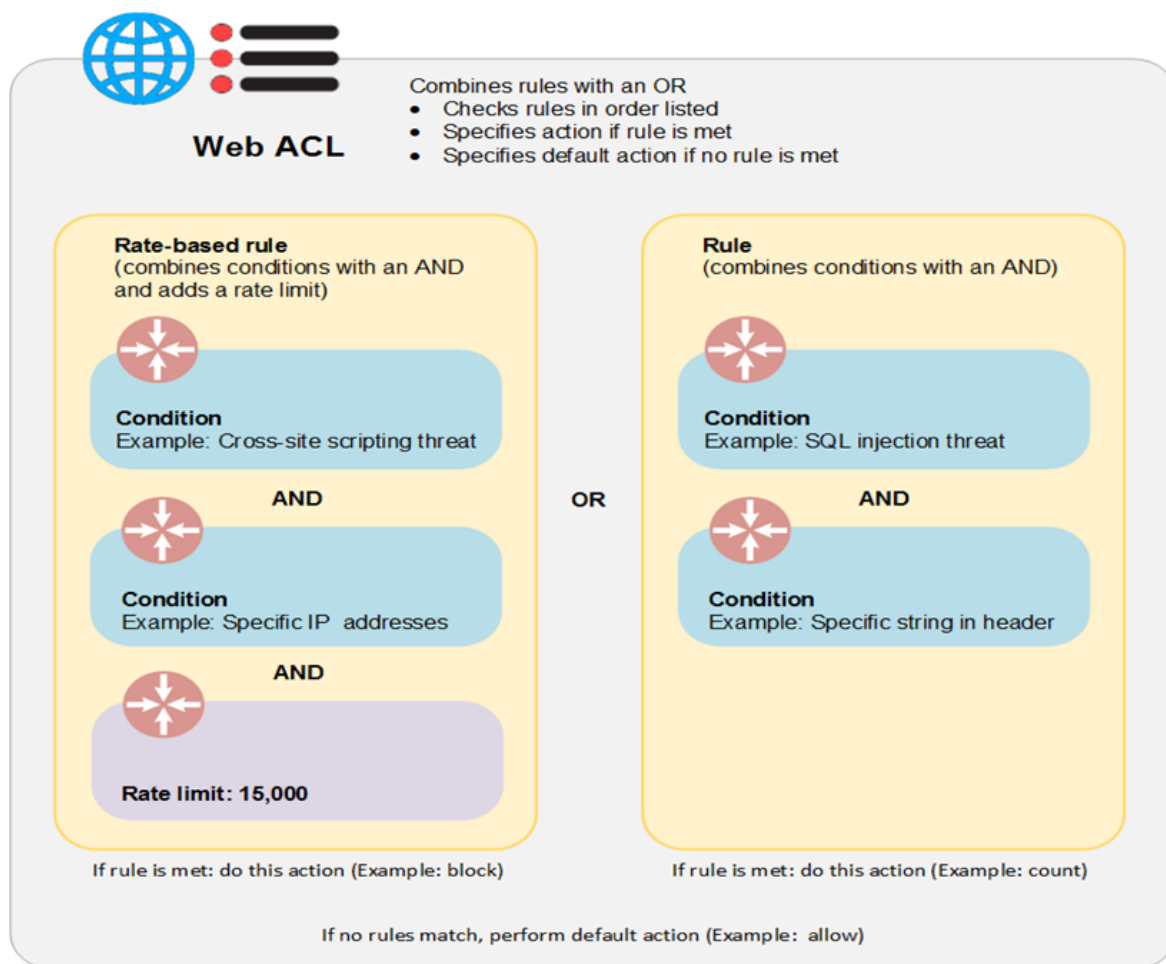
如果您向 Web ACL 中添加两个或更多规则，则仅当有请求不满足任一规则的所有条件时，AWS WAF 才执行默认操作。例如，假设您添加另一个只包含一个条件的规则：

- 在 User-Agent 标头中包含值 BIGBadBot 的请求。

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，AWS WAF 才执行默认操作。

在极少数情况下，AWS WAF 可能会遇到内部错误，该错误会延迟对 CloudFront 或 应用程序负载均衡器 有关允许还是阻止请求的响应。在这些情况下，CloudFront 或 应用程序负载均衡器 通常会提供内容。

下图显示 AWS WAF 如何检查规则并基于这些规则执行操作。



## AWS WAF 定价

使用 AWS WAF 时，您只需为您创建的 Web ACL 和规则以及为 AWS WAF 检查的 HTTP 请求数付费。有关更多信息，请参阅 [AWS WAF 定价](#)。

## AWS WAF 入门

本教程介绍如何使用 AWS WAF 执行以下任务：

- 设置 AWS WAF。
- 使用 AWS WAF 控制台创建 Web 访问控制列表 (Web ACL)，并指定用于筛选 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 请求必须与规则中的所有条件匹配，AWS WAF 才能基于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 AWS WAF 在 Web 请求不与任何规则匹配时执行的操作。
- 选择您希望 AWS WAF 针对其检查 Web 请求的 Amazon CloudFront 分配。本教程只介绍 CloudFront 的操作步骤，但 应用程序负载均衡器 的操作步骤基本相同。适用于 CloudFront 的 AWS WAF 在所有区域都可用。用于 应用程序负载均衡器 的 AWS WAF 现在在 [AWS 区域和终端节点](#) 中所列的区域中可用。

### Note

对于在本教程中创建的资源，AWS 向您收取的费用通常少于每日 0.25 USD。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 AWS WAF \(p. 9\)](#)
- [步骤 2：创建 Web ACL \(p. 9\)](#)
- [步骤 3：创建 IP 匹配条件 \(p. 10\)](#)
- [步骤 4：创建地理匹配条件 \(p. 10\)](#)
- [步骤 5：创建字符串匹配条件 \(p. 11\)](#)
- [步骤 5A：创建正则表达式条件 \(可选\) \(p. 12\)](#)
- [步骤 6：创建 SQL 注入匹配条件 \(p. 13\)](#)
- [步骤 7：\(可选\) 创建其他条件 \(p. 14\)](#)
- [步骤 8：创建规则并添加条件 \(p. 14\)](#)
- [步骤 8：向 Web ACL 中添加规则 \(p. 15\)](#)
- [步骤 9：清除资源 \(p. 16\)](#)

## 步骤 1：设置 AWS WAF

如果您已注册 AWS 账户并已创建 IAM 用户 (如[设置 \(p. 3\)](#)中所述)，请转到[步骤 2：创建 Web ACL \(p. 9\)](#)。

如果未执行这些操作，请转到[设置 \(p. 3\)](#)并至少执行前两个步骤。(您可以暂时跳过下载工具，因为本入门主题侧重于使用 AWS WAF 控制台。)

## 步骤 2：创建 Web ACL

AWS WAF 控制台会指导您完成一系列操作，以配置 AWS WAF 基于指定条件 (如请求的来源 IP 地址或请求中的值) 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 如果这是您首次使用 AWS WAF，请选择 Go to AWS WAF，然后选择 Configure Web ACL。

如果您以前使用过 AWS WAF，请在导航窗格中选择 Web ACLs，然后选择 Create web ACL。

3. 在 Name web ACL 页面上，对于 Web ACL name，键入一个名称。

#### Note

Web ACL 在创建之后无法更改名称。

4. 对于 CloudWatch metric name，键入一个名称。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。

5. 对于 Region，选择一个区域。如果您要将此 Web ACL 与 CloudFront 分配关联，请选择 Global (CloudFront)。
6. 对于 AWS 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 \(p. 52\)](#)。

### 创建 IP 匹配条件

1. 在 Create conditions 页面上，对于 IP match conditions，选择 Create condition。
2. 在 Create IP match condition 对话框中，对于 Name，键入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_!@#%&\*},./。
3. 对于 Address，键入 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。)

AWS WAF 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。AWS WAF 支持 IPv6 地址范围：/16、/24、/32、/48、/56、/64 和 /128。(要指定一个 IP 地址，如 192.0.2.44，请键入 192.0.2.44/32。) 不支持其他范围。

有关 CIDR 表示法的更多信息，请参阅维基百科文章 [Classless Inter-Domain Routing](#)。

4. 选择 Create。

## 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 \(p. 54\)](#)。



### 创建地理匹配条件

1. 在 Create conditions 页面上，对于 Geo match conditions，选择 Create condition。
2. 在 Create geo match condition 对话框中，对于 Name，键入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_!@#%&\*},./。
3. 选择位置类型和国家/地区。Location type 目前只能选择 Country。
4. 选择 Add location。
5. 选择 Create。

## 步骤 5：创建字符串匹配条件

字符串匹配条件标识您希望 AWS WAF 在请求中搜索的字符串 (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，您会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 \(p. 63\)](#)。

### 创建字符串匹配条件

1. 在 Create conditions 页面上，对于 String match conditions，选择 Create condition。
2. 在 Create string match condition 对话框中，键入下列值：

名称

键入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_!@#%&\*},./。

类型

选择 String match。

Part of the request to filter on

选择 Web 请求中您希望 AWS WAF 在其中检查指定字符串的部分。

对于此示例，选择 Header。

### Note

如果选择 Body 作为 Part of the request to filter on 的值，则 AWS WAF 只检查前 8192 个字节 (8 KB)，因为 CloudFront 只转发前 8192 个字节进行检查。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。(AWS WAF 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 \(p. 55\)](#)。

Header (在“Part of the request to filter on”为“Header”时是必需的)

因为您对 Part of the request to filter on 选择了 Header，所以必须指定您希望 AWS WAF 检查哪个标头。键入 User-Agent。(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。

对于此示例，选择 Exactly matches，表示 AWS WAF 检查 Web 请求中与您指定的值完全相同的标头值。



## Transformation

为试图绕过 AWS WAF，攻击者会在 Web 请求中使用不寻常的格式，例如通过添加空格或通过部分或所有请求进行 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 中键入的值已进行了 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 AWS WAF 在 Part of the request to filter on 所指定的 Web 请求部分中搜索的值。

对于此示例，键入 BadBot。AWS WAF 将在 Web 请求的 User-Agent 标头中检查值 BadBot。

Value to match 的最大长度是 50 个字符。如果您要指定 base64 编码值，则最大长度是 50 个字符 (编码前)。

3. 如果您希望 AWS WAF 在 Web 请求中检查多个值 (如包含 BadBot 的 User-Agent 标头和包含 BadParameter 的查询字符串)，则您有两个选择：
  - 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，二者的相似之处在于它标识您希望 AWS WAF 在请求中搜索的字符串 (如标头或查询字符串中的指定值)。主要区别在于您使用正则表达式 (regex) 来指定您希望 AWS WAF 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 \(p. 68\)](#)。

### 创建正则表达式匹配条件

1. 在 Create conditions 页面上，对于 String match conditions，选择 Create condition。
2. 在 Create string match condition 对话框中，键入下列值：

名称

键入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_! "# + \*},./。

类型

选择 Regex match。

Part of the request to filter on

选择 Web 请求中您希望 AWS WAF 在其中检查指定字符串的部分。

对于此示例，选择 Body。

#### Note

如果选择 Body 作为 Part of the request to filter on 的值，则 AWS WAF 只检查前 8192 个字节 (8 KB)，因为 CloudFront 只转发前 8192 个字节进行检查。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。(AWS WAF 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 \(p. 55\)](#)。

Transformation

为试图绕过 AWS WAF，攻击者会在 Web 请求中使用不寻常的格式，例如通过添加空格或通过部分或所有请求进行 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

键入名称，然后指定您希望 AWS WAF 搜索的正则表达式模式。

接下来，键入正则表达式 `l[a@]mAB[a@]dRequest`。AWS WAF 会在 Web 请求的 `User-Agent` 标头中检查值：

- `lAmABadRequest`
- `lAmAB@dRequest`
- `l@mABadRequest`
- `l@mAB@dRequest`

3. 选择 Create pattern set and add filter。
4. 选择 Create。

## 步骤 6：创建 SQL 注入匹配条件

SQL 注入匹配条件标识 Web 请求中您希望 AWS WAF 在其中检查恶意 SQL 代码的部分 (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 \(p. 60\)](#)。

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 对话框中，键入下列值：

名称

键入名称。

Part of the request to filter on

选择 Web 请求中您希望 AWS WAF 在其中检查恶意 SQL 代码的部分。

对于此示例，选择 Query string。

#### Note

如果选择 Body 作为 Part of the request to filter on 的值，则 AWS WAF 只检查前 8192 个字节 (8 KB)，因为 CloudFront 只转发前 8192 个字节进行检查。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。(AWS WAF 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 \(p. 55\)](#)。

Transformation

对于此示例，选择 URL decode。

攻击者会使用不寻常的格式 (如 URL 编码) 试图绕过 AWS WAF。URL decode 选项会在 AWS WAF 检查请求之前消除 Web 请求中的某些格式设置。

您只能指定一个类型的文本转换。

3. 选择 Create。
4. 选择 Next。

## 步骤 7：(可选) 创建其他条件

AWS WAF 还提供其他条件，包括：

- 大小约束条件 – 标识 Web 请求中您希望 AWS WAF 检查长度的部分 (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 \(p. 55\)](#)。
- 跨站点脚本匹配条件 – 标识 Web 请求中您希望 AWS WAF 在其中检查恶意脚本的部分 (如标头或查询字符串)。有关更多信息，请参阅 [使用跨站点脚本匹配条件 \(p. 48\)](#)。

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 \(p. 14\)](#)。

## 步骤 8：创建规则并添加条件

您可以创建规则以指定希望 AWS WAF 在 Web 请求中搜索的条件。如果您将多个条件添加到一个规则，则 Web 请求必须与该规则中的所有条件匹配，AWS WAF 才会基于该规则允许或阻止请求。

#### Note

有关规则的更多信息，请参阅[使用规则 \(p. 73\)](#)。

创建规则并添加条件

1. 在 Create rules 页面上，选择 Create rule。
2. 在 Create rule 对话框中，键入下列值：

名称

键入名称。

CloudWatch metric name

为 AWS WAF 将创建并与规则关联的 CloudWatch 指标键入名称。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` 或 `Rate based rule`。基于速率的规则与常规规则基本相同，但还考虑到每五分钟来自标识的 IP 地址的请求数。有关这些规则类型的更多信息，请参见 [AWS WAF 如何工作 \(p. 6\)](#)。对于此示例，选择 `Regular rule`。

#### Rate limit

如果要创建基于速率的规则，则输入五分钟周期内可允许的来自一个 IP 地址的最大请求数。

3. 对于要添加到规则的第一个条件，指定以下设置：

- 选择您是希望 AWS WAF 基于 Web 请求与条件中的设置匹配还是不匹配来允许还是阻止请求。

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`。

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`。

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`。

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`。

14. 对于 `Default action`，选择 `Allow all requests that don't match any rules`。

15. 选择 `Review and create`。

## 步骤 8：向 Web ACL 中添加规则

向 Web ACL 中添加规则时，您可指定以下设置：

- 您希望 AWS WAF 对匹配规则中所有条件的 Web 请求执行的操作：允许、阻止或计数。
- Web ACL 的默认操作。这是您希望 AWS WAF 对不 与规则中的所有条件匹配的 Web 请求执行的操作：允许或阻止请求。

AWS WAF 开始阻止与以下所有条件 (和您可能添加的任何其他条件) 匹配的 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

AWS WAF 允许 CloudFront 响应不满足所有这三个条件的任何请求。

## 步骤 9：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 AWS WAF 费用，您应清除所创建的 AWS WAF 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，AWS 向您收取的费用通常少于每日 0.25 USD。完成后，建议您删除资源以防止产生不必要的费用。

### 删除 AWS WAF 进行收费的对象

1. 取消 Web ACL 与 CloudFront 分配的关联：
  - a. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
  - b. 选择要删除的 Web ACL。
  - c. 在右窗格中，在 Rules 选项卡上，转到 AWS resources using this web ACL 部分。对于 Web ACL 所关联的 CloudFront 分配，选择 Type 列中的 x。
2. 从规则中删除条件：
  - a. 在导航窗格中，选择 Rules。
  - 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。
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. 选择在教程中创建的 Web ACL。
  - 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。

- b. 选择在教程中创建的规则。
- c. 选择 Delete。
- d. 在 Delete 对话框中，再次选择 Delete 以确认。

AWS WAF 不对条件收取费用，但如果您要完成清除，请执行以下过程以从条件中删除筛选条件并删除条件。

#### 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 AWS WAF 控制台的导航窗格中，选择 IP addresses。
  - 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。

## 教程

本部分包含指向预配置的模板以及三个教程的链接，其中提供了可在 AWS WAF 中执行的常见任务的完整解决方案。这些教程演示了如何结合使用多种 AWS 服务，以自动配置 AWS WAF 来响应 CloudFront 流量。其目的在于提供一般性指导。教程中的解决方案不适合直接在生产环境中使用，须经过仔细的审查并针对商业环境的独特因素进行适应性修改。

### AWS WAF 预配置保护

您可以利用预配置模板快速开始使用 AWS WAF。该模板包含一组 AWS WAF 规则，设计用于阻止基于 Web 的常见攻击。您可以通过自定义模板来满足自己的业务需求。

该模板中的规则可帮助防范恶意机器人、SQL 注入、跨站点脚本 (XSS)、HTTP 泛洪和其他已知攻击。部署该模板之后，AWS WAF 便开始阻止发往您的 CloudFront 分配或应用程序负载均衡器、与您的 Web 访问控制列表 (Web ACL) 中的预配置规则匹配的 Web 请求。除了您配置的其他 Web ACL 外，您还可以使用此自动化解决方案。有关更多信息，请参阅 [AWS WAF 安全自动化](#)。

### 教程

- [教程：针对常见攻击快速设置 AWS WAF 保护 \(p. 18\)](#)
- [教程：阻止提交恶意请求的 IP 地址 \(p. 23\)](#)
- [教程：使用 AWS 服务实施能够抵御 DDoS 的网站 \(p. 28\)](#)

## 教程：针对常见攻击快速设置 AWS WAF 保护

本教程向您展示如何使用 [AWS CloudFormation](#) 快速配置 AWS WAF 以防范下列常见攻击：

- 跨站点脚本攻击 – 攻击者有时将脚本插入 Web 请求，企图利用 Web 应用程序中的漏洞。跨站点脚本匹配条件识别 Web 请求中您希望 AWS WAF 检查可能包含恶意代码的部分，如 URI 或查询字符串。
- SQL 注入攻击 – 攻击者有时将恶意 SQL 代码插入 Web 请求，企图从您的数据库中提取数据。SQL 注入匹配条件可识别 Web 请求中您希望 AWS WAF 检查可能的恶意 SQL 代码的部分。
- 来自已知不良 IP 地址的攻击 – 您可以使用 IP 匹配条件根据请求所源自的 IP 地址来允许、阻止 Web 请求或对其计数。一个 IP 匹配条件最多可列出您指定的 1000 个 IP 地址或 IP 地址范围。

### Note

本教程假定您拥有可用于为 Web 应用程序提供内容的 CloudFront 分配。如果您没有 CloudFront 分配，请参阅 Amazon CloudFront 开发人员指南 中的 [使用 CloudFront 控制台创建或更新 Web 分配](#)。

### 主题

- [解决方案概述 \(p. 18\)](#)
- [步骤 1：创建可针对常见攻击设置 AWS WAF 保护的 AWS CloudFormation 堆栈 \(p. 20\)](#)
- [步骤 2：将 Web ACL 与 CloudFront 分配关联 \(p. 21\)](#)
- [步骤 3：\(可选\) 向 IP 匹配条件中添加 IP 地址 \(p. 22\)](#)
- [步骤 4：\(可选\) 更新 Web ACL 以阻止较大的正文 \(p. 22\)](#)
- [步骤 5：\(可选\) 删除您的 AWS CloudFormation 堆栈 \(p. 23\)](#)
- [相关资源 \(p. 23\)](#)

## 解决方案概述

AWS CloudFormation 使用模板来设置以下 AWS WAF 条件、规则和 Web ACL。



## 条件

AWS CloudFormation 会创建以下条件。

### IP 匹配条件

筛选来自已知不良 IP 地址的请求。该条件使您很容易将 IP 添加到列表中，以阻止其访问您的网站。如果您收到来自一个或多个 IP 地址的大量不良请求，则可能要执行此操作。如果要根据请求来自的 IP 地址允许、阻止请求或对请求计数，请参阅本教程后面的[步骤 3：\(可选\) 向 IP 匹配条件中添加 IP 地址 \(p. 22\)](#)。

条件的名称是 `prefixManualBlockSet`，其中 `prefix` 是在创建 AWS CloudFormation 堆栈时为 Web ACL 指定的名称。

### 大小约束条件

筛选正文长度超过 8192 字节的请求。AWS WAF 仅对您在筛选器中指定的请求部分的前 8192 字节进行计算。如果有效的请求正文从不会超过 8192 字节，则可使用大小约束条件来捕获可能漏掉的恶意请求。

在本教程中，AWS CloudFormation 将 AWS WAF 配置为对正文长度超过 8192 字节的请求只进行计数，而不会阻止。如果请求中的正文从不会超过该长度，您可以将配置更改为阻止正文超过该长度的请求。有关如何查看超过 8192 字节的请求计数以及如何更改 Web ACL 以阻止正文超过 8192 字节的请求的信息，请参阅[步骤 4：\(可选\) 更新 Web ACL 以阻止较大的正文 \(p. 22\)](#)。

条件的名称是 `prefixLargeBodyMatch`，其中 `prefix` 是在创建 AWS CloudFormation 堆栈时为 Web ACL 指定的名称。

### SQL 注入条件

筛选可能包含恶意 SQL 代码的请求。该条件包括用于对请求的以下部分进行计算的筛选器：

- 查询字符串 (URL 解码转换)
- URI (URL 解码转换)
- 正文 (URL 解码转换)
- 正文 (HTML 解码转换)

条件的名称是 `prefixSqliMatch`，其中 `prefix` 是在创建 AWS CloudFormation 堆栈时为 Web ACL 指定的名称。

### 跨站点脚本条件

筛选可能包含恶意脚本的请求。该条件包括用于对请求的以下部分进行计算的筛选器：

- 查询字符串 (URL 解码转换)
- URI (URL 解码转换)
- 正文 (URL 解码转换)
- 正文 (HTML 解码转换)

条件的名称是 `prefixXssMatch`，其中 `prefix` 是在创建 AWS CloudFormation 堆栈时为 Web ACL 指定的名称。

## 规则

当您创建 AWS CloudFormation 堆栈时，AWS CloudFormation 将创建以下规则并向每个规则中添加相应条件：

### `prefixManualIPBlockRule`

AWS CloudFormation 将 `prefixManualBlockSet` 条件添加到此规则中。



### **prefixSizeMatchRule**

AWS CloudFormation 将 **prefixLargeBodyMatch** 条件添加到此规则中。

### **prefixSqliRule**

AWS CloudFormation 将 **prefixSqliMatch** 条件添加到此规则中。

### **prefixXssRule**

AWS CloudFormation 将 **prefixXssMatch** 条件添加到此规则中。

## Web ACL

AWS CloudFormation 创建 Web ACL，它具有您在创建 AWS CloudFormation 堆栈时指定的名称。Web ACL 包含具有指定设置的以下规则：

### **prefixManualIPBlockRule**

默认情况下，此规则中的条件不包含任何 IP 地址。如果要根据请求来自的 IP 地址允许、阻止请求或对请求计数，请参阅本教程后面的 [步骤 3：\(可选\) 向 IP 匹配条件中添加 IP 地址 \(p. 22\)](#)。

### **prefixSizeMatchRule**

默认情况下，AWS WAF 对正文长度超过 8192 字节的请求计数。

### **prefixSqliRule**

AWS WAF 根据此规则中的设置来阻止请求。

### **prefixXssRule**

AWS WAF 根据此规则中的设置来阻止请求。

## 要求

本教程假定您拥有可用于为 Web 应用程序提供内容的 CloudFront 分配。如果您没有 CloudFront 分配，请参阅 Amazon CloudFront 开发人员指南 中的 [使用 CloudFront 控制台创建或更新 Web 分配](#)。本教程还使用 AWS CloudFormation 简化配置过程。有关更多信息，请参阅 [AWS CloudFormation 用户指南](#)。

## 估计时间

如果您已有 CloudFront 分配，完成本教程的预计时间为 15 分钟；如果需要创建 CloudFront 分配，则预计时间为 30 分钟。

## 成本

您在本教程期间创建的资源具有关联的成本。完成本教程后，您可以删除资源以停止产生费用。有关更多信息，请参阅 [AWS WAF 定价](#) 和 [Amazon CloudFront 定价](#)。

## 步骤 1：创建可针对常见攻击设置 AWS WAF 保护的 AWS CloudFormation 堆栈

在下面的过程中，您将使用 AWS CloudFormation 模板创建一个可针对常见攻击设置 AWS WAF 保护的堆栈。

### Important

当您创建用于部署此解决方案的 AWS CloudFormation 堆栈时，即开始为各种服务引发费用。费用将持续累积，直至您删除 AWS CloudFormation 堆栈。有关更多信息，请参阅 [步骤 5：\(可选\) 删除您的 AWS CloudFormation 堆栈 \(p. 23\)](#)。

## 创建 AWS CloudFormation 堆栈以阻止提交不良请求的 IP 地址

1. 要开始创建 AWS CloudFormation 堆栈，请选择要在其中创建 AWS 资源的区域对应的链接：
  - [在美国东部（弗吉尼亚北部）创建堆栈](#)
  - [在美国西部（俄勒冈）创建堆栈](#)
  - [在欧洲（爱尔兰）创建堆栈](#)
  - [在亚太区域（东京）创建堆栈](#)
2. 如果尚未登录 AWS 管理控制台，在提示时登录。
3. 在 Select Template 页面上，选择 Specify an Amazon S3 template URL。对于模板 URL，请键入 **`https://s3.amazonaws.com/cloudformation-examples/community/common-attacks.json`**。
4. 选择 Next。
5. 在 Specify Details 页面上，指定下列值：

### 堆栈名称

您可以使用默认名称 (CommonAttackProtection)，或更改该名称。堆栈名称不得包含空格，且必须是 AWS 账户内的唯一名称。

### 名称

为 AWS CloudFormation 将创建的 Web ACL 指定名称。您指定的名称也用作 AWS CloudFormation 将创建的条件和规则的前缀，以便于您找到所有相关对象。

6. 选择 Next。
7. (可选) 在 Options 页面上，输入标签和高级设置，或将这些框保留为空。
8. 选择 Next。
9. 在 Review 页面上，检查配置，然后选择 Create。

选择 Create 后，AWS CloudFormation 将创建在 [解决方案概述 \(p. 18\)](#) 中提到的 AWS WAF 资源。

## 步骤 2：将 Web ACL 与 CloudFront 分配关联

在 AWS CloudFormation 创建堆栈后，您必须关联您的 CloudFront 分配以激活 AWS WAF。

### Note

您可以将 Web ACL 与任何所需数量的分配相关联，但是，您仅可以将一个 Web ACL 与给定分配相关联。

### 将一个 Web ACL 与一个 CloudFront 分配相关联

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与 CloudFront 分配关联的 Web ACL。
4. 在规则选项卡中，在 使用此 Web ACL 的 AWS 资源下，选择添加关联。
5. 系统提示时，使用资源列表选择您想将此 Web ACL 与之关联的分配。
6. 选择 Add。
7. 要将此 Web ACL 与其他 CloudFront 关联，请重复步骤 4 到步骤 6。

## 步骤 3：(可选) 向 IP 匹配条件中添加 IP 地址

在您创建 AWS CloudFormation 堆栈时，AWS CloudFormation 为您创建了 IP 匹配条件，将其添加到规则，再将该规则添加到 Web ACL，并将 Web ACL 配置为根据 IP 地址阻止请求。但 IP 匹配条件不包含任何 IP 地址。如果要根据 IP 地址阻止请求，请执行以下过程。

编辑 AWS CloudFormation 参数值

1. 打开 AWS WAF 控制台 <https://console.aws.amazon.com/waf/>。
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. 采用 CIDR 表示法键入 IP 地址或范围。以下是两个示例：
    - 要指定 IP 地址 192.0.2.44，请键入 192.0.2.44/32。
    - 要指定从 192.0.2.0 到 192.0.2.255 的 IP 地址范围，请键入 192.0.2.0/24。

AWS WAF 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。AWS WAF 支持 IPv6 地址范围：/16、/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 [Classless Inter-Domain Routing](#)。

### Note

AWS WAF 同时支持 IPv4 和 IPv6 IP 地址。

- c. 要添加更多 IP 地址，请选择 Add another IP address，然后键入值。
- d. 选择 Add。

## 步骤 4：(可选) 更新 Web ACL 以阻止较大的正文

在您创建 AWS CloudFormation 堆栈时，AWS CloudFormation 创建了一个大小约束条件，用于筛选请求正文长度大于 8192 字节的请求。此外，它还将该条件添加到规则中，并将规则添加到 Web ACL。在本示例中，AWS CloudFormation 将 Web ACL 配置为对请求计数，但不阻止请求。当您要确保不会意外阻止有效请求时，此配置很有用。

如果要阻止长度超过 8192 字节的请求，请执行以下过程。

为 Web ACL 中的规则更改操作

1. 打开 AWS WAF 控制台 <https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL。
4. 在右窗格中，选择 Rules 选项卡。
5. 选择 Edit Web ACL。
6. 要更改 `prefixLargeBodyMatchRule` 的操作，请选择首选选项。( `prefix` 是您为 Web ACL 的名称指定的值。)
7. 选择 Save changes。

## 步骤 5：(可选) 删除您的 AWS CloudFormation 堆栈

如果您要停止针对常见攻击的保护 (如[解决方案概述](#) (p. 18)中所述)，请删除您在[步骤 1：创建可针对常见攻击设置 AWS WAF 保护的 AWS CloudFormation 堆栈](#) (p. 20)中创建的 AWS CloudFormation 堆栈。此操作会删除 AWS CloudFormation 创建的 AWS WAF 资源，并停止这些资源的 AWS 费用。

删除 AWS CloudFormation 堆栈

1. 登录 AWS 管理控制台并通过以下网址打开 AWS CloudFormation 控制台：<https://console.aws.amazon.com/cloudformation>。
2. 选中堆栈对应的复选框。默认名称为 CommonAttackProtection。
3. 选择 Delete Stack。
4. 选择 Yes, Delete 以确认。
5. 要跟踪堆栈删除的进度，请选中堆栈对应的复选框，然后在底部窗格中选择 Events 选项卡。

## 相关资源

如需包括 Lambda 函数和 AWS CloudFormation 模板的 AWS WAF 示例以及 SDK 用法示例，请转到位于<https://github.com/aws-labs/aws-waf-sample> 的 GitHub。

## 教程：阻止提交恶意请求的 IP 地址

使用 [AWS Lambda](#) 时，您可以设置一个阈值，以规定您的 Web 应用程序能够容许、来自给定 IP 地址的每分钟恶意请求数。您的 CloudFront 源会对恶意请求返回以下 HTTP 40x 状态代码：

- 400, Bad Request
- 403, Forbidden
- 404, Not Found
- 405, Method Not Allowed

如果用户 (基于 IP 地址) 超出此错误代码阈值，Lambda 会自动更新您的 AWS WAF 规则以阻止 IP 地址，并指定应将来自这些 IP 地址的请求阻止多长时间。

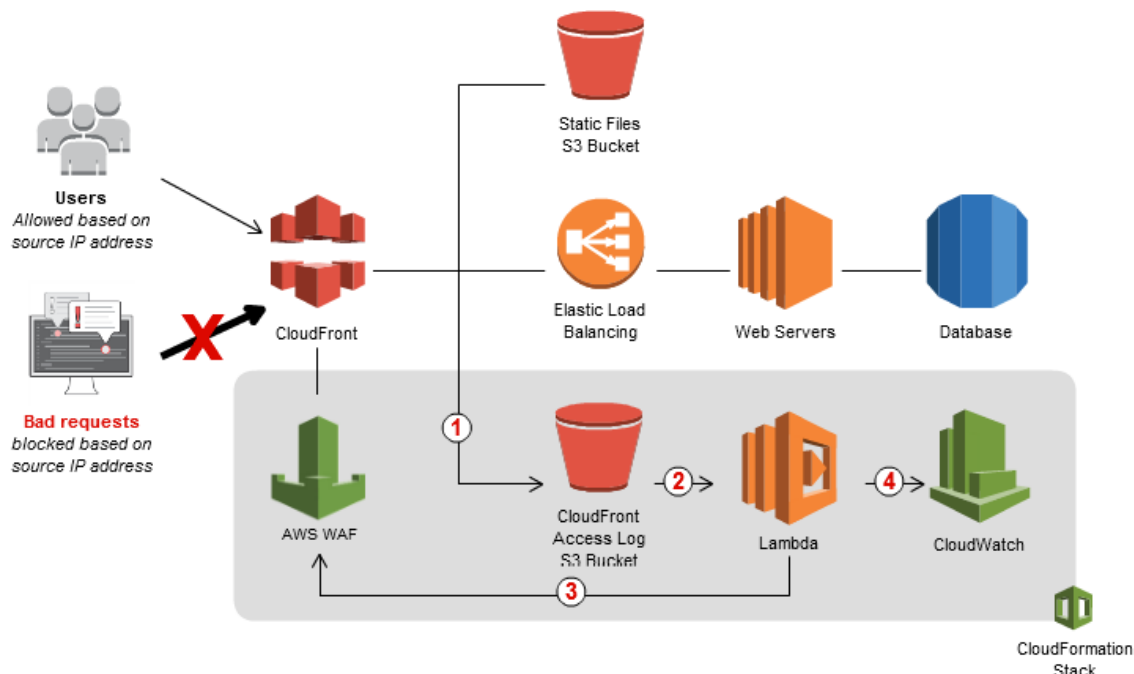
本教程演示如何使用 [AWS CloudFormation](#) 模板指定请求阈值和阻止请求的时间。本教程还使用 CloudFront [访问日志](#) (存储在 [Amazon S3](#) 中) 在请求由 CloudFront 和 [Amazon CloudWatch](#) 指标服务时对请求计数。

主题

- [解决方案概述](#) (p. 23)
- [步骤 1：创建用于阻止提交恶意请求的 IP 地址的 AWS CloudFormation 堆栈](#) (p. 25)
- [步骤 2：将 Web ACL 与 CloudFront 分配关联](#) (p. 26)
- [步骤 3：\(可选\) 编辑 AWS CloudFormation 参数值](#) (p. 27)
- [步骤 4：\(可选\) 测试阈值和 IP 规则](#) (p. 27)
- [步骤 5：\(可选\) 删除您的 AWS CloudFormation 堆栈](#) (p. 28)
- [相关资源](#) (p. 28)

## 解决方案概述

下图显示了如何将 AWS WAF 与 AWS Lambda 结合使用来阻止来自特定 IP 地址的请求。



1. 当 CloudFront 代表您的 Web 应用程序接收请求时，它会将访问日志发送到 Amazon S3 存储桶，其中包含有关请求的详细信息。
2. 对于存储在 Amazon S3 存储桶中的每个新的访问日志，都会触发 Lambda 函数。Lambda 函数分析日志文件并查找导致错误代码 400、403、404 和 405 的请求。然后，该函数对恶意请求计数，并将结果临时存储在您用于访问日志的 Amazon S3 存储桶中的 `current_outstanding_requesters.json` 中。
3. Lambda 函数将更新 AWS WAF 规则，以便在您指定的时间段内阻止 `current_outstanding_requesters.json` 中列出的 IP 地址。当此阻止期限到期时，AWS WAF 将允许这些 IP 地址再次访问您的应用程序，但会继续监控来自这些 IP 地址的请求。
4. Lambda 函数会在 CloudWatch 中发布执行指标，如分析的请求数和被阻止的 IP 地址数。

根据您在教程中配置的设置，AWS CloudFormation 模板会在 AWS WAF 中创建一个 Web 访问控制列表 (Web ACL) 和两个独立规则，用于阻止和监控来自 IP 地址的请求。这两个规则定义如下：

- 自动阻止 – 此规则添加超出每分钟请求限制的 IP 地址。将一直阻止来自这些 IP 地址的新请求，直到 Lambda 在指定的到期时间段后从阻止列表中删除这些 IP 地址。默认值为四个小时。
- 手动阻止 – 此规则手动将 IP 地址添加到自动阻止列表中。将永久阻止这些 IP 地址；仅当您从阻止列表中将其删除后，它们才能访问 Web 应用程序。您可以使用此列表来阻止已知不良 IP 地址或经常添加到自动阻止规则中的 IP 地址。

要求：本教程假定您已拥有用于为 Web 应用程序提供内容的 CloudFront 分配。如果您没有 CloudFront 分配，请参阅 Amazon CloudFront 开发人员指南 中的[使用 CloudFront 控制台创建或更新 Web 分配](#)。本教程还使用 AWS CloudFormation 简化配置过程。有关更多信息，请参阅[AWS CloudFormation 用户指南](#)。

估计时间：如果您已有 CloudFront 分配，完成本教程的预计时间为 15 分钟；如果需要创建 CloudFront 分配，则预计时间为 30 分钟。

估算费用：

- AWS WAF
  - 每个 Web ACL 每月 5.00 USD (本教程创建一个 Web ACL)
  - 每个规则每月 1.00 USD (x2，AWS CloudFormation 为本教程创建了两个规则)

- 每百万请求 0.60 USD
- AWS Lambda – 每个新 CloudFront 访问日志表示一个新请求，并且会触发本教程创建的 Lambda 函数。Lambda 费用包括以下内容：
  - 请求 – 前一百万个请求免费，然后 Lambda 对后面每一百万个请求收取 0.20 USD。CloudFront 一个小时内会为分配提交若干次访问日志。
  - 每秒使用的内存 – 每秒使用的内存，每 GB 收费 0.00001667 USD。
- Amazon S3 – Amazon S3 会对存储 CloudFront 访问日志收费。日志大小和存储费用取决于 CloudFront 接收的对于您的对象的请求数。有关更多信息，请参阅 [Amazon S3 定价](#)。
- CloudFront – 对于此解决方案，您不会产生任何额外的 CloudFront 费用。有关更多信息，请参阅 [Amazon CloudFront Pricing](#)。

## 步骤 1：创建用于阻止提交恶意请求的 IP 地址的 AWS CloudFormation 堆栈

在下面的过程中，您将使用 AWS CloudFormation 模板创建一个堆栈，用于启动 Lambda、CloudFront、Amazon S3、AWS WAF 和 CloudWatch 所需的 AWS 资源。

### Important

当您创建用于部署此解决方案的 AWS CloudFormation 堆栈时，即开始为各种服务引发费用。费用将持续累积，直至您删除 AWS CloudFormation 堆栈。有关更多信息，请参阅 [步骤 5：\(可选\) 删除您的 AWS CloudFormation 堆栈 \(p. 28\)](#)。

创建 AWS CloudFormation 堆栈以阻止提交不良请求的 IP 地址

1. 要开始创建 AWS CloudFormation 堆栈，请选择要在其中创建 AWS 资源的区域对应的链接：
  - [在美国东部 \(弗吉尼亚北部\) 创建堆栈](#)
  - [在美国西部 \(俄勒冈\) 创建堆栈](#)
  - [在欧洲 \(爱尔兰\) 创建堆栈](#)
  - [在亚太区域 \(东京\) 创建堆栈](#)
2. 如果尚未登录 AWS 管理控制台，在提示时登录。
3. 在 Select Template 页面上，选择的 URL 会自动显示在 Specify an Amazon S3 template URL 下面。选择 Next。
4. 在 Specify Details 页面上，指定下列值：

### 堆栈名称

您可以使用默认名称 (BadBehavingIP)，也可以更改该名称。堆栈名称不得包含空格，且必须是 AWS 账户内的唯一名称。

### Create CloudFront Access Log Bucket

选择 yes 为 CloudFront 访问日志创建一个新的 Amazon S3 存储桶；如果您已有用 CloudFront 访问日志的 Amazon S3 存储桶，则选择 no。

### CloudFront Access Log Bucket Name

键入希望 CloudFront 存放访问日志的 Amazon S3 存储桶的名称。如果对 Create CloudFront Access Log Bucket 选择 no，则将此框保留为空。

### Request Threshold

键入每分钟可从一个 IP 地址发出而不会被阻止的最大请求数。默认值为 400。

### WAF Block Period

指定 IP 地址在超出阈值后被阻止的时间 (以分钟为单位)。默认值为 240 分钟 (四小时)。



5. 选择 Next。
6. (可选) 在 Options 页面上，输入标签和高级设置，或将这些框保留为空。
7. 选择 Next。
8. 在 Review 页面上，选中 I acknowledge 复选框，然后选择 Create。

选择 Create 后，AWS CloudFormation 会创建运行解决方案所必需的 AWS 资源。

- Lambda 函数
- AWS WAF Web ACL (名为 Malicious Requesters)，包含已配置的必要规则
- CloudWatch 自定义指标
- Amazon S3 存储桶，具有您在步骤 6 的 CloudFront Access Log Bucket Name 字段中指定的名称，如果对 Create CloudFront Access Log Bucket 选择了 yes

## 步骤 2：将 Web ACL 与 CloudFront 分配关联

在 AWS CloudFormation 创建堆栈后，您必须关联 CloudFront 分配以激活 AWS WAF 并更新 Amazon S3 存储桶，以启用事件通知。

### Note

如果您已经在使用 AWS WAF 监控 CloudFront 请求，并且已为您监控的分配启用日志记录，则可跳过第一个步骤。

### Note

您可以将 Web ACL 与任何所需数量的分配相关联，但是，您仅可以将一个 Web ACL 与给定分配相关联。

将一个 Web ACL 与一个 CloudFront 分配相关联

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与 CloudFront 分配关联的 Web ACL。
4. 在规则选项卡中，在使用此 Web ACL 的 AWS 资源下，选择添加关联。
5. 系统提示时，使用资源列表选择您想将此 Web ACL 与之关联的分配。
6. 选择 Add。
7. 要将此 Web ACL 与其他 CloudFront 关联，请重复步骤 4 到步骤 6。

如果您已经拥有 CloudFront 访问日志的 Amazon S3 存储桶 (如果您在上述流程中为创建 CloudFront 访问日志存储桶选择了否)，那么在将新日志文件添加到存储桶中时，则会启用 Amazon S3 事件通知以触发 Lambda 函数。有关更多信息，请参阅 Amazon Simple Storage Service 控制台用户指南 中的 [启用事件通知](#)。

### Note

如果您选择让 AWS CloudFormation 创建存储桶，则 AWS CloudFormation 也会为存储桶启用事件通知。

要启用 Amazon S3 事件通知

1. 通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。

2. 选择要为 CloudFront 访问日志使用的存储桶。
3. 选择属性并展开活动。
4. 指定以下值：

Name

为事件键入一个名称，如 LambdaNotificationsForWAFBadRequests。名称中不得含有空格。

事件

选择 ObjectCreated(All)。

前缀

将字段留空。

后缀

键入 gz。

发送至

选择 Lambda 函数。

Lambda 函数

选择 BadBehavingIP 或您为 AWS CloudFormation 堆栈指定的名称。

5. 选择 Save。

## 步骤 3：(可选) 编辑 AWS CloudFormation 参数值

如果要在创建 AWS CloudFormation 堆栈后更改参数 (例如，如果要更改阈值或阻止 IP 的时间)，您可以更新 AWS CloudFormation 堆栈。

编辑 AWS CloudFormation 参数值

1. 通过以下网址打开 AWS CloudFormation 控制台：<https://console.aws.amazon.com/cloudformation>。
2. 在堆栈列表中，选择要更新的运行堆栈，如果在创建堆栈时接受默认值，则为 BadBehavingIP。
3. 选择 Actions，然后选择 Update Stack。
4. 在 Select Template 页面上，选择 Use current template，然后选择 Next。
5. 在 Specify Details 页面上，适当更改 Error Code Blacklisting Parameters 的值。

Request Threshold

键入可以发出而不会被阻止的新的最大请求数。

WAF Block Period

指定当来自某 IP 地址的请求数超过 Request Threshold 值时，您希望 AWS WAF 阻止该 IP 地址的新的时间长度值 (以分钟为单位)。

6. 在 Options 页面上，选择 Next。
7. 在 Review 页面上，选中 I acknowledge 复选框，然后选择 Update。

AWS CloudFormation 将更新堆栈，以反映新的参数值。

## 步骤 4：(可选) 测试阈值和 IP 规则

要测试您的解决方案，您可以等到 CloudFront 生成新的访问日志文件，或通过将示例访问日志文件上传到您指定的用于接收日志文件的 Amazon S3 存储桶来模拟此过程。



### 测试阈值和 IP 规则

1. 从 AWS 网站下载示例 CloudFront [访问日志文件](#)。
2. 通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。
3. 选择您用于此教程的 CloudFront 访问日志的 Amazon S3 存储桶。
4. 选择 Upload。
5. 选择 Add Files，选择示例访问日志文件，然后选择 Start Upload。

上传结束后，执行以下过程以确认 IP 地址是否已自动填充在 AWS WAF Auto Block 规则中。Lambda 需要几秒钟来处理日志文件和更新规则。

### 查看 Auto Block 规则中的 IP 地址

1. 打开 AWS WAF 控制台 <https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Rules。
3. 选择 Auto Block 规则。
4. 确认 Auto Block 规则包括一个包含 IP 地址的 IP 匹配条件。

## 步骤 5：(可选) 删除您的 AWS CloudFormation 堆栈

如果您要停止阻止提交恶意请求的 IP 地址，请删除您在[步骤 1：创建用于阻止提交恶意请求的 IP 地址的 AWS CloudFormation 堆栈 \(p. 25\)](#)中创建的 AWS CloudFormation 堆栈。此操作会删除 AWS CloudFormation 创建的 AWS 资源，并停止这些资源的 AWS 费用。

### 删除 AWS CloudFormation 堆栈

1. 登录 AWS 管理控制台并通过以下网址打开 AWS CloudFormation 控制台：<https://console.aws.amazon.com/cloudformation>。
2. 选中堆栈对应的复选框。默认名称为 BadBehavingIP。
3. 选择 Delete Stack。
4. 选择 Yes, Delete 以确认。
5. 要跟踪堆栈删除的进度，请选择堆栈对应的复选框，然后选择底部窗格中的 Events 选项卡。

## 相关资源

如需包括 Lambda 函数和 AWS CloudFormation 模板的 AWS WAF 示例以及 SDK 用法示例，请转到位于 <https://github.com/aws-labs/aws-waf-sample> 的 GitHub。

## 教程：使用 AWS 服务实施能够抵御 DDoS 的网站

本教程将提供有关设置可抵御分布式拒绝服务 (DDoS) 攻击的网站的分步指导。DDoS 攻击可能会使您的网站涌入大量流量，导致合法用户无法访问网站，甚至导致您的网站因流量过大而崩溃。

### 主题

- [概述 \(p. 29\)](#)
- [架构 \(p. 29\)](#)
- [先决条件 \(p. 30\)](#)
- [步骤 1：使用 Amazon EC2 启动虚拟服务器 \(p. 34\)](#)

- [步骤 2：使用 Elastic Load Balancing 扩展您的流量 \(p. 37\)](#)
- [步骤 3：使用 Amazon CloudFront 提高性能和吸收攻击 \(p. 39\)](#)
- [步骤 4：使用 Route 53 注册域名并实施 DNS 服务 \(p. 40\)](#)
- [步骤 5：使用 AWS WAF 检测和筛选恶意 Web 请求 \(p. 42\)](#)
- [其他最佳实践 \(p. 45\)](#)

## 概述

本教程向您介绍如何结合使用多个 AWS 服务来构建具有弹性的、高度安全的网站。例如，您将了解如何执行以下操作：

- 使用负载均衡器和边缘服务器，它们将流量分配到跨区域和可用区的多个实例并帮助保护您的实例免受基于 SSL 的攻击
- 使用超额预配容量等技术来缓解基础设施 (第 3 层和第 4 层) DDoS 攻击
- 使用 Web 应用程序防火墙来监控 HTTP 和 HTTPS 请求，并控制对您的内容的访问

本教程介绍如何集成 AWS 服务，如 Amazon EC2、Elastic Load Balancing、CloudFront、Route 53 和 AWS WAF。虽然本教程设计为端到端解决方案，但如果您已在使用其中一些 AWS 服务，则不必完成每个步骤。例如，如果您已向 Route 53 注册了您的网站域，并使用 Route 53 作为您的 DNS 服务，则可以跳过这些步骤。

本教程旨在帮助您快速启动每个 AWS 服务。因此，它没有涵盖所有可能的选项。有关每个服务的详细信息，请参阅 [AWS 文档](#)。对于很多步骤，本教程提供了要输入的特定值。通常，您应使用这些值。但有些情况下，请使用符合您需要的域名，例如您网站的域名。

本教程的每个主要步骤简要介绍了以下内容：

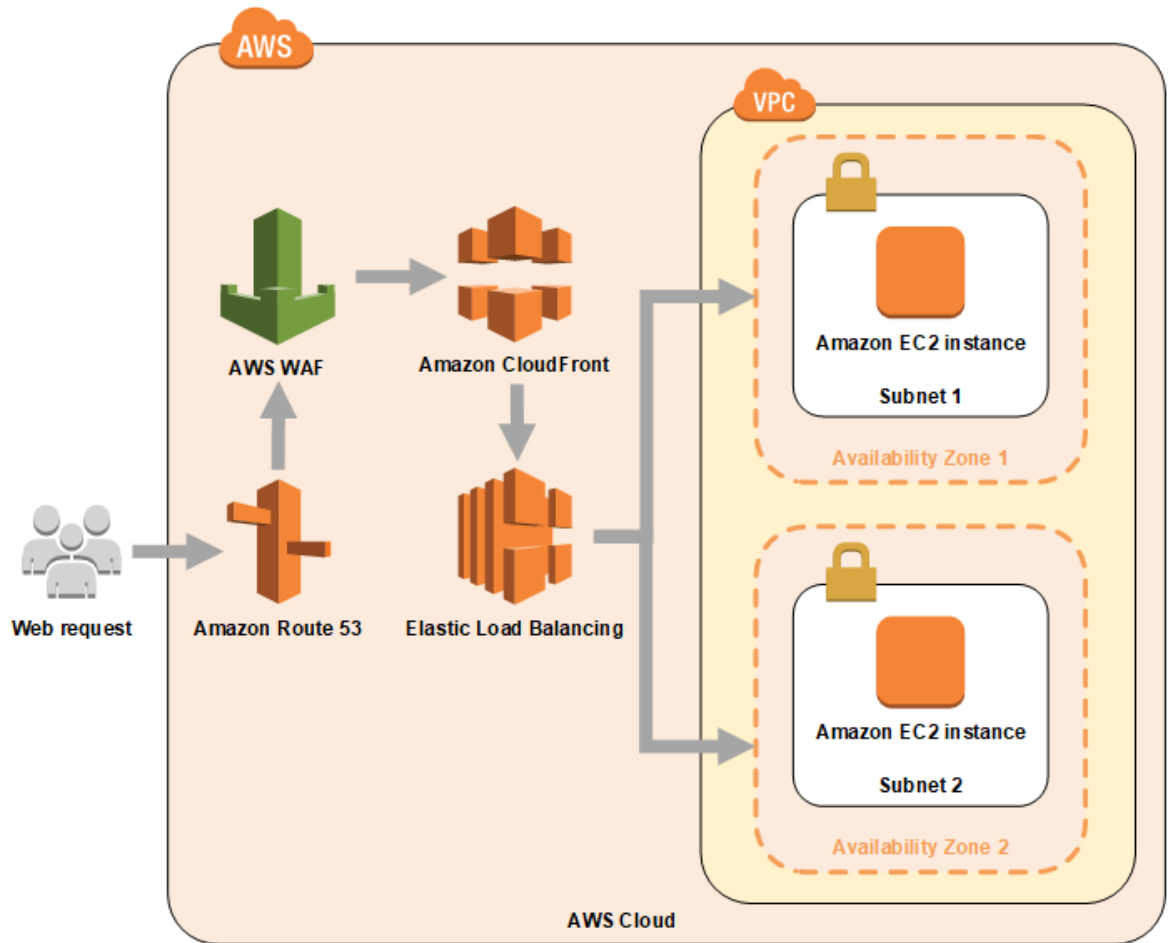
- 您在做什么
- 您为什么这样做 (即，这样做对于抵御 DDoS 攻击有何帮助)
- 如何做

### Important

您负责承担本教程中所实施的 AWS 服务的费用。有关完整详细信息，请参阅您在本解决方案中使用的每个 AWS 服务的定价 [webest-practicesage](#)。您可以在 [云产品页面](#) 上找到指向每个服务的链接。

## 架构

下图显示了本教程中部署的架构。



要开始，请转到[先决条件](#) (p. 30)。

## 先决条件

以下任务不是专门针对 DDoS 防护，但是完成本教程所必需的。

### 主题

- [注册 AWS](#) (p. 30)
- [创建 IAM 用户](#) (p. 31)
- [创建密钥对](#) (p. 32)
- [创建具有两个子网的 Virtual Private Cloud \(VPC\)](#) (p. 32)
- [创建安全组](#) (p. 33)

## 注册 AWS

当您注册 Amazon Web Services (AWS) 时，您的 AWS 账户会自动注册 AWS 中的所有服务。您只需为使用的服务付费。

如果您已有一个 AWS 账户，请跳到下一个任务。如果您还没有 AWS 账户，请使用以下步骤创建。

### 创建 AWS 账户

1. 打开 <https://aws.amazon.com/>，然后选择 Create an AWS Account。

## Note

如果您之前已登录 AWS 管理控制台，则可能无法在浏览器中执行此操作。在此情况下，请选择 Sign in to a different account，然后选择 Create a new AWS account。

2. 按照屏幕上的说明进行操作。

作为注册流程的一部分，您会收到一个电话，需要您使用电话键盘输入一个 PIN 码。

请记住您的 AWS 账号，因为在下一个任务中您会用到它。

## 创建 IAM 用户

要访问 AWS 服务和资源，您必须提供凭证。虽然可以使用您在第一次打开 AWS 账户时所创建的用户名和密码登录，但出于安全考虑，我们强烈建议您通过 AWS Identity and Access Management (IAM) 服务创建新凭证，并且使用这些凭证登录。

如果您注册了 AWS 但没有为自己创建一个 IAM 用户，则可以使用以下过程来创建一个。

为您自己创建一个 IAM 用户并将该用户添加到管理员组

1. 登录 AWS 管理控制台 并通过以下网址打开 IAM 控制台 <https://console.aws.amazon.com/iam/>。
2. 在导航窗格中，选择 Users，然后选择 Add user。
3. 对于 User name，键入用户名，例如 **Administrator**。名称可包含字母、数字以及以下字符：加号 (+)、等号 (=)、逗号 (,)、句点 (.)、at 符号 (@)、下划线 (\_) 和连字符 (-)。名称不区分大小写，且最大长度可为 64 个字符。
4. 选中 AWS 管理控制台 access 旁边的复选框，选择 Custom password，然后在文本框中键入新用户的密码。
5. 选择 Next: Permissions。
6. 在 Set permissions for user 页面上，选择 Add user to group。
7. 选择 Create group。
8. 在 Create group 对话框中，为新组键入名称。名称可包含字母、数字以及以下字符：加号 (+)、等号 (=)、逗号 (,)、句点 (.)、at 符号 (@)、下划线 (\_) 和连字符 (-)。名称不区分大小写，且最大长度可为 128 个字符。
9. 对于 Filter，选择 Job function。
10. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group。
11. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh 以在列表中查看该组。
12. 选择 Next: Review 以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user。

要以这一新的 IAM 用户身份登录，请从 AWS 控制台退出，然后使用以下 URL，其中 `your_aws_account_id` 是您的不带连字符的 AWS 账号 (例如，如果您的 AWS 账号是 1234-5678-9012，则您的 AWS 账户 ID 是 123456789012)：

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

输入您刚创建的 IAM 用户名 (而不是电子邮件地址) 和密码。登录后，导航栏显示 `your_user_name @ your_aws_account_id`。

要为您的账户验证 IAM 用户的登录链接，请打开 IAM 控制台并在控制面板的 IAM users sign-in link (IAM 用户登录链接) 下进行检查。

有关 IAM 的更多信息，请参阅 [IAM 用户指南](#)。

## 创建密钥对

密钥对 是一组用于证明个人身份的安全凭证。密钥对包含您创建的私有密钥和公有密钥。您可以使用密钥对来登录您的 Amazon EC2 实例，这是 AWS 云中的虚拟服务器。在您初次启动实例时指定密钥对的名称。

### 创建密钥对

1. 使用您在上节中创建的 URL 登录到 AWS。
2. 从 AWS 控制面板中，选择 EC2 以打开 Amazon EC2 控制台。
3. 从导航栏中，选择密钥对区域。您可以选择向您提供的任何区域，无需理会您身处的位置。但是，密钥对是特定于区域的；例如，如果您计划在美国西部（俄勒冈）区域中启动实例，则必须在 美国西部（俄勒冈）区域 中创建实例的密钥对。在本教程中，考虑选择 美国西部（俄勒冈）区域。

#### Note

在本教程的后面，我们使用 AWS Lambda 和 Amazon API Gateway，它们目前仅在特定的 AWS 区域中可用。因此，请确保您选择了 Lambda 和 Amazon API Gateway 在其中都可用的 AWS 区域。上面建议的 美国西部（俄勒冈） 支持本教程中使用的所有服务。有关最新的服务可用性信息，请参阅[按区域提供的 AWS 服务](#)。

4. 在导航窗格中的 NETWORK & SECURITY 下，选择 Key Pairs。

#### Tip

导航窗格位于控制台的左侧。如果您看不到窗格，它可能被最小化了；请选择箭头展开该窗格。您可能必须向下滚动才能看到 Key Pairs 链接。

5. 选择 Create Key Pair。
6. 在 Create Key Pair 对话框的 Key pair name 字段中键入新密钥对的名称，然后选择 Create。使用一个容易记住的名称（如您的 IAM 用户名）后跟 -key-pair 加区域名称。例如，me-key-pair-uswest2。
7. 您的浏览器会自动下载私有密钥文件。基本文件名是您为密钥对指定的名称，文件扩展名为 .pem。将私有密钥文件保存在安全位置。

#### Important

这是您保存私有密钥文件的唯一机会。启动实例时，您必须提供密钥对的名称；每次连接到实例时，必须提供相应的私有密钥。

有关更多信息，请参阅 [Amazon EC2 密钥对](#)。

## 创建具有两个子网的 Virtual Private Cloud (VPC)

Amazon VPC 允许您在已经定义的虚拟网络内启动 AWS 资源。在本教程中，您的 VPC 将包含两个托管您的网站的 Amazon EC2 实例以及两个连接到这些实例的子网。

有关 Amazon VPC 的更多信息，请参阅 [Amazon VPC 是什么？](#)（在 Amazon VPC 用户指南 中）。

### 创建非默认 VPC

1. 打开 Amazon VPC 控制台 <https://console.aws.amazon.com/vpc/>。
2. 从导航栏中，为 VPC 选择区域。VPC 特定于某一区域，因此您应选择已创建密钥对的区域。在本教程中，我们使用 美国西部（俄勒冈）区域。
3. 在 VPC 控制面板上，选择 Start VPC Wizard。
4. 在 Step 1: Select a VPC Configuration 页面上，确保选中 VPC with a Single Public Subnet，然后选择 Select。
5. 在 Step 2: VPC with a Single Public Subnet 页面上，指定以下详细信息：
  - 对于 VPC name，键入您的 VPC 的友好名称。

- 对于 Availability Zone，选择 us-west-2a。
  - 对于 Subnet name，键入 subnet-1。
  - 保留其他默认配置设置。
6. 选择 Create VPC。在确认页面上，请选择 OK。

### 向您的 VPC 中添加第二个子网

为了提高可用性，在本教程的后面，您将配置负载均衡器以在两个不同的可用区中使用不同的子网。在上一步中创建您的 Amazon VPC 时，您在可用区中创建了第一个子网。您现在必须在不同的可用区中添加第二个子网。两个可用区必须位于同一 AWS 区域中。

### 向您的 Amazon VPC 中添加第二个子网

1. 通过以下网址打开 Amazon VPC 控制台：<https://console.aws.amazon.com/vpc/>。
2. 在导航窗格中，选择 Subnets、Create Subnet。
3. 指定以下子网详细信息：
  - 对于 Name tag，为子网提供一个名称。例如，键入 subnet-2。这样做可创建具有 Name 键以及您指定的值的标签。
  - 对于 VPC，选择您在前面的步骤中刚创建的 VPC。
  - 对于 Availability Zone，选择您的子网将位于的可用区。这应该不同于您在本教程的前面使用您的 VPC 创建的可用区。本教程使用 us-west-2a 作为示例。因此这次选择非 us-west-2a 的可用区，如 us-west-2b。
  - 对于 IPv4 CIDR block，为此第二个子网指定 IPv4 CIDR 块。您必须在 VPC 范围内为子网指定 IPv4 CIDR 块。两个子网的 IP 地址不能重叠。假定您在设置 VPC 时使用的是默认值，您的第一个子网使用的 CIDR 块为 10.0.0.0/24。因此对于此第二个 CIDR 块，您可以使用 10.0.1.0/24。有关更多信息，请参阅[针对 IPv4 的 VPC 和子网大小调整](#)。
4. 选择 Yes, create。
5. 在子网页面上，选择您创建的第一个子网 subnet-1。
6. 在详细信息窗格中，在 Route Table 选项卡上，记下路由表 ID。它以 rtb- 开头。
7. 在子网页面上，选择您创建的第二个子网 subnet-2。
8. 在详细信息窗格上，选择 Edit。
9. 您的第二个子网必须与您的第一个子网使用同一路由表。对于 Change to，选择之前记下的路由表的名称。
10. 选择 Save。

## 创建安全组

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

### 先决条件

您需要使用本地计算机的公有 IPv4 地址。Amazon EC2 控制台中的安全组编辑器可以为您自动检测公有 IPv4 地址。或者，您可以在 Internet 浏览器中使用搜索短语“what is my IP address”。如果您通过 Internet 服务提供商 (ISP) 连接或者在不使用静态 IP 地址的情况下从防火墙后面连接，则必须找出客户端计算机使用的 IP 地址范围。

### 为您的 VPC 创建具有最小特权的

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。



2. 从导航栏中选择安全组的区域。安全组特定于某一区域，因此您应选择已创建密钥对的区域 美国西部（俄勒冈）。
3. 在导航窗格中，选择 Security Groups。
4. 选择 Create Security Group。
5. 键入新安全组的名称和描述。使用一个容易记住的名称（如您的 IAM 用户名称）后跟 \_SG\_ 加区域名称。例如，me\_SG\_uswest2。
6. 在 VPC 列表中，选择您在本教程的前面创建的 VPC。
7. 在 Inbound 选项卡上，创建以下规则（为每个新规则选择 Add Rule）：
  - 从 Type 列表中选择 HTTP，确保 Source 设置为 Anywhere (0.0.0.0/0)。
  - 从 Type 列表中选择 HTTPS，确保 Source 设置为 Anywhere (0.0.0.0/0)。
  - 从 Type 列表中选择 RDP。在 Source 框中，选择 MyIP 以便使用本地计算机的公有 IPv4 地址自动填充该字段。或者，选择自定义并使用 CIDR 表示法指定计算机的公有 IPv4 地址或网络。要采用 CIDR 表示法指定单个 IP 地址，请添加路由前缀 /32，例如 203.0.113.25/32。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 203.0.113.0/24。

#### Warning

出于安全原因，我们不建议您允许从所有 IPv4 地址 (0.0.0.0/0) 对您的实例进行 RDP 访问（以测试为目的的短暂访问除外）。

8. 在添加了所有规则后，选择 Create。

下一步: [步骤 1：使用 Amazon EC2 启动虚拟服务器 \(p. 34\)](#)。

## 步骤 1：使用 Amazon EC2 启动虚拟服务器

您可以使用超额预配容量等技术来缓解基础设施（第 3 层和第 4 层）DDoS 攻击。也就是说，您可以扩展网站来吸收更大的流量，而无需进行巨额投资，也不会产生不必要的复杂性。您可以使用 Amazon EC2 启动虚拟服务器（称为实例）并在您的需求发生变化时快速扩展或收缩。需要时，您可以通过向网站添加实例来横向扩展。还可以选择使用较大的实例进行纵向扩展。在本教程的此步骤中，您将在 美国西部（俄勒冈）区域 中创建一个 c4.xlarge Amazon EC2 Windows 实例，其中包括 10 GB 网络接口和增强联网。

#### Important

您负责承担本教程中所实施的 AWS 服务的费用。有关 EC2 费用的完整详细信息，请参阅 [Amazon EC2 定价页面](#)。

#### 主题

- [创建 Amazon EC2 实例 \(p. 34\)](#)
- [连接到您的实例 \(p. 35\)](#)
- [安装 Web 服务器并托管您的网站 \(p. 36\)](#)
- [启动第二个 EC2 实例 \(p. 36\)](#)
- [测试网站 \(p. 37\)](#)

## 创建 Amazon EC2 实例

您在此处创建的 Amazon EC2 实例将托管您的网站。

#### 启动实例

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航窗格中，选择“美国西部（俄勒冈）”区域（或您为您的 VPC 选择的任何区域）。
3. 从 Amazon EC2 控制面板中，选择 Launch Instance。

4. Choose an Amazon Machine Image (AMI) 页面显示一组称为 Amazon 系统映像 (AMI) 的基本配置，作为您的实例的模板。选择适用于 Windows Server 2016 R2 Base 的 AMI。
5. 在 Choose an Instance Type 页面上，选择 c4.8xlarge 类型。此类型提供了 10 GB 网络接口和对增强联网的支持。
6. 选择 Review and Launch。
7. 选择 Edit Instance Details。
8. 对于 Network，选择您在先决条件步骤“[创建具有两个子网的 Virtual Private Cloud \(VPC\) \(p. 32\)](#)”中创建的 VPC。
9. 对于 Subnet，选择您在创建 VPC 时创建并命名的 subnet-1。
10. 对于 Auto-assign Public IP，选择 Enable。
11. 选择 Review and Launch。
12. 在 Review Instance Launch 页面上的 Security Groups 下，使用以下步骤来选择您在先决条件步骤“[创建安全组 \(p. 33\)](#)”中创建的安全组。
  - a. 选择 Edit security groups。
  - b. 在 Configure Security Group 页面上，确保 Select an existing security group 处于选中状态。
  - c. 从现有安全组列表中选择您之前创建的安全组，然后选择 Review and Launch。
13. 在 Review Instance Launch 页面上，选择 Launch。
14. 当系统提示提供密钥对时，选择 Choose an existing key pair，然后选择您在先决条件步骤“[创建密钥对 \(p. 32\)](#)”中创建的密钥对。

#### Warning

请勿选择 Proceed without a key pair (在没有密钥对的情况下继续) 选项。如果您没有使用密钥对启动实例，就不能连接到该实例。

选中确认复选框，然后选择 Launch Instances。

15. 确认页面会让您知道自己的实例已启动。选择 View Instances 以关闭确认页面并返回控制台。
16. 在 Instances 页面上，您可以查看启动状态。启动实例只需很短的时间。启动实例时，其初始状态为 pending。实例启动后，其状态变为 running，并且会收到一个公有 DNS 名称。(如果 Public DNS (IPv4) 列已隐藏，请选择页面右上角的“Show/Hide”图标，然后选择 Public DNS (IPv4)。)记下您的公有 IPv4 地址。您在本教程的后面需要此值。
17. 需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查；您可以在 Status Checks 列中查看此信息。

## 连接到您的实例

您将使用 Microsoft 远程桌面连接到您的实例。如果您从 Microsoft Windows 计算机进行连接，则已安装远程桌面。如果您使用的是其他操作系统，可能需要先安装远程桌面，然后再执行以下过程。

### 使用 RDP 客户端连接到 Windows 实例

1. 在 Amazon EC2 控制台中，选择实例，然后选择 Connect。
2. 在 Connect To Your Instance 对话框中，选择 Get Password (密码在实例启动几分钟之后才可用)。
3. 选择 Browse 并导航至您启动实例时所创建的私有密钥文件。选择文件并选择打开，以便将文件的全部内容复制到 Contents 字段。
4. 选择 Decrypt Password。控制台将在 Connect To Your Instance (连接到您的实例) 对话框中显示实例的默认管理员密码，会将先前显示的 Get Password (获取密码) 链接替换为实际密码。
5. 记录下默认管理员密码，或将其复制到剪贴板。需要使用此密码连接实例。
6. 选择 Download Remote Desktop File。您的浏览器会提示您打开或保存 .rdp 文件。两种选择都可以。完成后，可选择 Close 以关闭 Connect To Your Instance 对话框。



- 如果已打开 .rdp 文件，您将看到 Remote Desktop Connection 对话框。
  - 如果已保存 .rdp 文件，请导航至下载目录，然后打开 .rdp 文件以显示该对话框。
7. 您可能看到一条警告，指出远程连接发布者未知。您可以继续连接到您的实例。
  8. 当收到系统提示时，使用操作系统的管理员账户和您之前记录或复制的密码连接到并登录该实例。

#### Note

有时复制和粘贴内容可能会损坏数据。如果您在登录时遇到“Password Failed (密码失败)”错误，请尝试手动键入密码。

9. 由于自签名证书的固有特性，您可能会看到一条警告，指出无法验证该安全证书。请使用以下步骤验证远程计算机的标识；或者，如果您信任该证书，则直接选择 Yes 或 Continue 以继续操作。
  - a. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 View certificate。如果您正在 Mac 上使用 Microsoft Remote Desktop，请选择 Show Certificate。
  - b. 选择 Details 选项卡，并向下滚动到 Thumbprint 条目 (在 Windows PC 上) 或 SHA1 Fingerprints 条目 (在 Mac 上)。这是远程计算机的安全证书的唯一标识符。
  - c. 在 Amazon EC2 控制台中，选择该实例，选择 Actions，然后选择 Get System Log。
  - d. 在系统日志输出中，查找标记为 RDP-CERTIFICATE-Thumbprint 的条目。如果此值与 thumbprint 或证书指纹匹配，则表示您已验证了远程计算机的标识。
  - e. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请返回到 Certificate 对话框并选择 OK。如果您正在 Mac 上使用 Microsoft Remote Desktop，请返回到 Verify Certificate 并选择 Continue。
  - f. [Windows] 在 Remote Desktop Connection 窗口中选择 Yes 连接到您的实例。  
  
[Mac OS] 使用默认 Administrator 账户和您先前记录或复制的默认管理员密码，按提示登录。您可能需要切换空间才能看到登录屏幕。有关空间的更多信息，请参阅 <http://support.apple.com/kb/PH14155>。
  - g. 如果您在尝试连接到您的实例时收到错误，请参阅[远程桌面无法连接到远程计算机](#)。

## 安装 Web 服务器并托管您的网站

下一步是在您的 Amazon EC2 实例上安装 Web 托管服务并构建您的网站。有多个适用于 Web 服务器的选项，如 Microsoft Internet Information Server (IIS) (它已是您的实例的一部分)、Apache HTTP Server for Windows 等。

安装 Web 服务器并配置您的网站不在本教程的讨论范围之内。请参阅适当的产品文档来在您的实例上实施 Web 服务器。但是，作为示例，一般来说，安装 IIS 的步骤如下：

- 连接到您的实例，如前所述。
- 使用 Windows Server Manager，选择 Add roles and features。
- 选择 Role-based or feature-based installation。
- 选择 Web Server (IIS) 并开始安装过程。
- 安装完成后，构建您的网站。

## 启动第二个 EC2 实例

您现在必须重复此过程 (启动另一个 EC2 实例并构建您的网站) 来创建您的第一个 EC2 实例的副本。这是在本教程的稍后阶段启用负载均衡所必需的。

按照刚才所述的所有相同步骤来启动实例。请务必按照前面的步骤编辑第二个实例详细信息和安全组。在编辑实例详细信息时，请注意以下几点：

- 选择与您的第一个实例相同的 VPC，即您在先决条件中创建的 VPC。

- 对于 Subnet，选择 subnet-2。这是您在先决条件步骤中创建的第二个子网。这不是用于您的第一个实例的相同子网。
- 对于 Auto-assign Public IP，选择 Enable。

在启动第二个 Amazon EC2 实例后，安装与第一个 EC2 实例相同的 Web 托管服务和文件。

## 测试网站

您现在应该能够使用每个实例的公有地址查看您的网站。

测试您的 Amazon EC2 实例和网站

1. 在 Amazon EC2 控制台中，选中第一个实例旁边的复选框。
2. 在详细信息窗格中，记下公有 DNS 地址。
3. 在 Web 浏览器中输入此地址。您应定向到您的网站。
4. 对第二个实例重复这些步骤。

下一步: [步骤 2：使用 Elastic Load Balancing 扩展您的流量 \(p. 37\)](#)。

## 步骤 2：使用 Elastic Load Balancing 扩展您的流量

Elastic Load Balancing 针对应用层攻击提供了额外保护。Elastic Load Balancing 将流量分配到多个 Amazon EC2 实例。使用 Elastic Load Balancing 以及 CloudFront (在本教程的后面讨论)，SSL 协商由负载均衡器和 CloudFront 边缘服务器处理，这有助于保护您的 Amazon EC2 实例免受基于 SSL 的攻击。

### Important

您负责承担本教程中所实施的 AWS 服务的费用。有关 Elastic Load Balancing 费用的完整详细信息，请参阅 [Elastic Load Balancing 定价页面](#)。

### 主题

- [开始前的准备工作 \(p. 37\)](#)
- [创建负载均衡器 \(p. 37\)](#)
- [测试负载均衡器 \(p. 38\)](#)

## 开始前的准备工作

请确保您在本教程的前面启动的 Amazon EC2 实例处于 Active 状态。

## 创建负载均衡器

接下来，配置自动将流量路由到您的两个 Amazon EC2 实例的负载均衡器。

### 创建负载均衡器

1. 打开 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在导航栏上，选择您为 EC2 实例选择的同一个区域。
3. 在导航窗格上的 LOAD BALANCING 下，选择 Target Groups。
4. 选择 Create target group。
5. 为目标组指定名称、协议、端口和 VPC，然后选择 Create。在本教程中，使用以下值：
  - Name : MyWebServers
  - Protocol : HTTP
  - Port : 80

- Target type : Instance
  - VPC : 包含您的 EC2 实例的 VPC
  - 保留其他设置。
6. 选择新目标组。
  7. 在 Targets 选项卡上，选择 Edit。
  8. 对于 Instances，选择您在本教程的前面创建的两个实例。选择 Add to registered，然后选择 Save。

实例的状态为 `initial`，直至实例注册并通过运行状况检查，然后，实例的状态将成为 `unused`，直至您将目标组配置为从负载均衡器接收流量。
  9. 在导航窗格中的 LOAD BALANCING 下，选择 Load Balancers。
  10. 选择 Create Load Balancer。
  11. 对于 Select load balancer type，选择 Application Load Balancer。
  12. 选择 Create。
  13. 完成 Configure Load Balancer 页面，如下所示：
    - a. 对于 Name，键入负载均衡器的名称。
    - b. 对于 Scheme，选择 Internet-facing。面向 Internet 的负载均衡器将来自客户端的请求通过 Internet 路由到目标。内部负载均衡器使用私有 IP 地址将请求路由到目标。
    - c. 对于 Listeners，默认值是负责接收端口 80 上的 HTTP 流量的侦听器。
    - d. 对于 Availability Zones，选择用于 EC2 实例的 VPC。选择至少两个可用区。如果可用区有一个子网，则将选择此子网。如果可用区有多个子网，请选择子网之一。您只能为每个可用区域选择一个子网。
    - e. 选择 Next: Configure Security Settings。
  14. 目前，忽略有关创建安全侦听器组的消息。选择 Next: Configure Security Groups。
  15. 完成 Configure Security Groups 页面，如下所示：
    - a. 选择 Create a new security group。
    - b. 为安全组键入名称和描述，或者保留默认名称和描述。此新安全组包含一条规则，该规则允许将流量传送到在 Configure Load Balancer 页面上为负载均衡器选择的端口。
    - c. 选择 Next: Configure Routing。
  16. 完成 Configure Routing 页面，如下所示：
    - a. 对于 Target group，选择 Existing target group。
    - b. 对于 Name，选择您之前创建的目标组。
    - c. 选择 Next: Register Targets。
  17. 在 Register Targets 页面上，在 Registered instances 下会显示向目标组注册的实例。在完成向导之前，您无法修改向目标组注册的目标。选择 Next: Review。
  18. 在 Review 页面上，选择 Create。
  19. 在您收到已成功创建负载均衡器的通知后，选择 Close。

## 测试负载均衡器

您现在应该能够使用负载均衡器的 DNS 名称查看您的网站。

### 测试负载均衡器

1. 在 Amazon EC2 控制台上的导航窗格中，选择 Load Balancers。
2. 选中您的负载均衡器旁边的框。
3. 在详细信息窗格中，记下 DNS 名称。
4. 在 Web 浏览器中输入此地址。您应定向到您的网站。

### Important

如果您对网站进行更改，则必须对两个 EC2 实例进行相同的更改。负载均衡器可以从任一实例提供内容，因此两个实例完全相同非常重要。

下一步: [步骤 3：使用 Amazon CloudFront 提高性能和吸收攻击 \(p. 39\)](#).

## 步骤 3：使用 Amazon CloudFront 提高性能和吸收攻击

高度扩展的多样化 Internet 连接可以显著地缩短网站的响应时间、更好地吸收 DDoS 攻击和隔离故障。Amazon CloudFront 边缘服务器以及 Route 53 提供了实现这些好处所需的网络基础设施的附加层。从通常比您的 EC2 源服务器离用户更近的位置提供您的内容和解析 DNS 查询。这减少了您的源 EC2 服务器上的负载。

### Important

您负责承担本教程中所实施的 AWS 服务的费用。有关 CloudFront 费用的完整详细信息，请参阅 [CloudFront 定价页面](#)。

### 主题

- [使用 Amazon CloudFront 分发您的内容 \(p. 39\)](#)

## 使用 Amazon CloudFront 分发您的内容

Amazon CloudFront 是一种内容分发网络 (CDN) 服务，可用于交付您的整个网站，包括静态、动态、流媒体和交互内容。您可以使用持久 TCP 连接和可变生存时间 (TTL) 来加快内容分发速度，即使内容不能在边缘站点缓存也是如此。这允许您使用 CloudFront 来保护您的 Web 应用程序，即使您不提供静态内容。

CloudFront 仅接受格式正确的连接，以防止许多常见的 DDoS 攻击 (如 [SYN 泛洪](#) 和 [UDP 反射](#) 攻击) 到达您的源。CloudFront 可自动关闭异常缓慢的连接，这可能指示潜在的 DDoS 攻击。

另外，DDoS 攻击在地理上与源相隔离，这可防止流量影响其他位置。您还可以使用 CloudFront 地理限制功能来阻止特定地理位置的用户访问您的内容。如果您想要阻止来自您不希望为用户提供服务的地理位置的攻击，这可能非常有用。

所有这些功能都可以极大地提高您在大型 DDoS 攻击期间继续为用户提供流量的能力。

### 实施 Amazon CloudFront

1. 通过以下网址打开 CloudFront 控制台：<https://console.aws.amazon.com/cloudfront/>。
2. 选择 Create Distribution。
3. 在 Select a delivery method for your content 页面上的 Web 部分中，选择 Get Started。
4. 在 Create Distribution 页面上，对于 Origin name，键入您在本教程的前面创建的负载均衡器的名称。要查找名称，请转到 Amazon EC2 控制面板，然后选择导航窗格中的 Load Balancers。选择您之前创建的负载均衡器。
5. 接受 Origin Settings 字段的其余部分的所有默认值。
6. 在 Default Cache Behavior Settings 下，接受默认值，CloudFront 将执行以下操作：
  - 将对您的分配使用 CloudFront URL 的所有请求 (例如，<http://d111111abcdef8.cloudfront.net/image.jpg>) 转发到您之前指定的负载均衡器
  - 允许用户使用 HTTP 或 HTTPS 访问您的对象
  - 响应对象请求
  - 在 CloudFront 边缘站点缓存您的对象 24 小时
  - 仅将默认请求标头转发到您的源，并且不基于标头中的值来缓存对象
  - 允许每个人查看您的内容
  - 不自动压缩您的内容

有关更多信息，请参阅[缓存行为设置](#)。

- 在 Distribution Settings 下，接受默认值，但以下情况除外：

#### 价格级别

选择与您想要为 CloudFront 服务支付的最高价对应的价格级别。默认情况下，CloudFront 从所有 CloudFront 区域的节点位置提供您的对象。

有关价格级别以及您的价格级别选择如何影响分配的 CloudFront 性能的更多信息，请参阅[选择 CloudFront 分配的价格级别](#)。有关 CloudFront 定价的信息，包括价格级别如何映射到 CloudFront 区域，请参阅[Amazon CloudFront 定价](#)。

#### AWS WAF Web ACL

选择 None。您将在本教程的后面配置 AWS WAF。

#### 备用域名 (CNAME) (可选)

指定要用于您的网站的 URL 的域名。例如，您可以输入 `example.com`。

#### 默认根对象 (可选)

当查看器请求分配 `http://example.com/` 的根 URL 而不是分配 `http://example.com/product-description.html` 中的对象时，您希望 CloudFront 从您的源（例如，`index.html`）中请求的对象。指定一个默认根对象，以避免公开分配的内容。

#### 评论 (可选)

输入您想与分配一起保存的任何评论。

- 选择 Create Distribution。
- 在 CloudFront 创建了分配后，分配的 Status 列的值将从 InProgress 更改为 Deployed。如果您选择启用分配，其将准备处理请求。这应该需要不到 15 分钟的时间。

CloudFront 指派给分配的域名将出现在分配列表中。（它同时也出现在选定分配的“General”选项卡上。）记下此名称和分配 ID，因为您将在本教程的稍后阶段用到它们。

- 在 CloudFront 控制台上，记下您刚刚创建的分配的 ID。您将在本教程的后面需要此 ID。

### 测试您的 CloudFront 分配

- 在 CloudFront 控制台上，选择您刚刚创建的分配的 ID。这会打开此分配的详细信息页面。记下域名。
- 在浏览器中打开该域名。您应该看到您的网站。可能需要大约 15 分钟时间才能使分配处于活动状态。如果您获得指示您的源关闭了连接的错误，请等待更长时间，然后重试。您可能还必须在浏览器中刷新页面。

下一步: [步骤 4：使用 Route 53 注册域名并实施 DNS 服务 \(p. 40\)](#)。

## 步骤 4：使用 Route 53 注册域名并实施 DNS 服务

您可以使用 Route 53 为您的网站注册域名，将 Internet 流量路由到您的域的资源，并检查您的 Web 服务器的运行状况以验证它是否可访问、可用且正常运行。Route 53 通过跨多个 DNS 服务器提供冗余和负载均衡来帮助防范 DDoS 攻击。Route 53 还可以检测 DNS 查询中的异常并优先考虑用户的已知可靠的请求，并且通过扩展名忽略来自可能不太可靠的源的请求。

#### Important

您负责承担本教程中所实施的 AWS 服务的费用。有关 Route 53 费用的完整详细信息，请参阅[Route 53 定价页面](#)。



## 主题

- [使用 Route 53 注册域 \(p. 41\)](#)
- [创建记录 \(p. 42\)](#)

## 使用 Route 53 注册域

如果您是第一次托管网站，则本教程中的下一步是使用 Route 53 注册域。以下是执行此操作的步骤。

### Important

如果已向其他注册商注册了您的域，则您必须从其他注册商的 DNS 服务迁移您的现有域以改为使用 Route 53 作为 DNS 服务。本教程不介绍该转移过程。您必须执行四个步骤来转移现有域，而不是执行本教程中所述的 Route 53 过程：

- 创建一个托管区域
- 从您的 DNS 服务提供商那里获取当前的 DNS 配置
- 创建资源记录集
- 更新您的注册商的名称服务器

有关从其他注册商转移现有域注册的更多信息，请参阅[转移域](#)。

### 使用 Route 53 注册新域

1. 登录 AWS 管理控制台并通过以下网址打开 Route 53 控制台：<https://console.aws.amazon.com/route53/>。
2. 在 Domain Registration 下，选择 Get Started Now。
3. 选择 Register Domain。
4. 键入要注册的域名，选择 Check 来了解该域名是否可用。例如，本教程假定您注册域名 `example.com`。

有关如何指定除 a-z、0-9 和 - (连字符) 以外的字符以及如何指定国际化域名的信息，请参阅[DNS 域名格式](#)。

5. 如果该域可用，则选择 Add to cart。域名将出现在您的购物车中。
6. 在购物车中，选择域要注册的年数。
7. 要注册多个域，请重复步骤 4 到 6。
8. 选择 Continue (继续)。
9. 在 Contact Details for Your n Domains 页面上，输入域注册者、管理员和技术联系人的联系信息。您在此处输入的值将应用于您要注册的所有域。
10. 对于某些顶级域 (TLD)，我们需要收集更多信息。对于这些 TLD，请在 Postal/Zip Code 字段后输入适用的值。
11. 选择是否要向 WHOIS 查询隐藏您的联系人信息。有关更多信息，请参阅以下主题：
  - [为域的联系信息启用或禁用隐私保护](#)
  - [可向 Route 53 注册的域](#)
12. 选择 Continue (继续)。
13. 检查您输入的信息，阅读服务条款，并选中相应复选框，以确认您已阅读服务条款。
14. 选择 Complete Purchase。

对于[通用 TLD](#)，我们通常向域注册者发送一封电子邮件，以确认可以通过您指定的电子邮件地址访问注册联系人。(如果我们已确认该电子邮件地址有效，将不发送电子邮件。)电子邮件来自以下电子邮件地址之一：

- [noreply@registrar.amazon.com](mailto:noreply@registrar.amazon.com) – 用于 Amazon Registrar 注册的 TLD。
- [noreply@domainnameverification.net](mailto:noreply@domainnameverification.net) – 用于我们的注册商合作者 Gandi 注册的 TLD。要确定您的 TLD 的注册商是谁，请参阅[可向 Route 53 注册的域](#)。

### Important

注册联系人必须按照电子邮件中的说明来验证已收到电子邮件，否则我们必须按照 ICANN 的要求暂停该域。域被暂停后，将无法在 Internet 上访问该域。

对于所有 TLD，当您的域注册获得批准后，您都将收到一封电子邮件。要确定您的请求的当前状态，请参阅[查看域注册的状态](#)。

## 创建记录

下一步是创建告诉 Route 53 您要如何为域和子域路由流量的记录。

### 创建记录

1. 登录 AWS 管理控制台并通过以下网址打开 Route 53 控制台：<https://console.aws.amazon.com/route53/>。
2. 在导航窗格中，选择 Hosted zones。
3. 因为您使用 Route 53 注册域，所以 Route 53 会自动为您创建托管区域。选择此托管区域。
4. 选择 Create Record Set。
5. 输入适用的值：
  - 对于 Name，保留原样 (它应已为 example.com)。
  - 对于 Type，选择 A – IPv4 address。
  - 对于 Alias，选择 Yes。
  - 对于 Alias Target，键入您在本教程的前面创建的 CloudFront 分配的域名。
6. 选择 Create。

### Note

您的新记录需要一定时间才会传播到 Route 53 DNS 服务器。更改通常在 60 秒内传播到所有 Route 53 名称服务器。

### 测试 Route 53 记录

1. 在浏览器中打开您添加到记录中的域名，例如 example.com。
2. 您应该看到您的网站。

下一步: [步骤 5：使用 AWS WAF 检测和筛选恶意 Web 请求 \(p. 42\)](#)。

## 步骤 5：使用 AWS WAF 检测和筛选恶意 Web 请求

您可以使用 Web 应用程序防火墙 (WAF) 来保护 Web 应用程序免遭试图利用网站中的漏洞的攻击。常见示例包括 SQL 注入或跨站点请求伪造。您还可以使用防火墙来检测和缓解 Web 应用层 DDoS 攻击。

AWS WAF 是一种 Web 应用程序防火墙服务，让您能够监控转发到 Amazon CloudFront 或 Application Load Balancer 的 HTTP 和 HTTPS 请求。利用 AWS WAF 还可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)，CloudFront 会使用所请求的内容或使用 HTTP 状态代码 403 (禁止) 来响应请求。



有些攻击由伪装成正常用户流量的 Web 流量组成。要缓解此类型的攻击，您可以使用 AWS WAF 基于速率的黑名单。使用基于速率的黑名单，您可以对 Web 应用程序可以处理的请求数量设置阈值。如果自动程序或爬虫程序超过此限制，可以使用 AWS WAF 自动阻止任何额外请求。

AWS 提供包含一组 AWS WAF 规则的预配置模板，您可以对这些规则进行自定义，以满足您的需求。这些模板旨在阻止基于 Web 的常见攻击，如恶意机器人、[SQL 注入](#)、[跨站点脚本 \(XSS\)](#)、[HTTP 泛洪](#)和已知攻击者的攻击。本教程使用这些模板来为您的网站提供防火墙保护。以下过程演示如何使用 AWS CloudFormation 部署模板。有关更多信息，包括模板的解决方案图表，请参阅 [AWS WAF 安全自动化](#)。

模板使用本教程中未包含的一些 AWS 功能，如 AWS Lambda 和 Amazon API Gateway。模板执行所有必要的配置，因此您无需为这些服务执行任何其他操作。但是，如果您希望了解有关 Lambda 和 Amazon API Gateway 的更多信息，请参阅 [AWS Lambda 开发人员指南](#)和 [Amazon API Gateway 开发人员指南](#)。

### Important

您负责承担作为此模板的一部分部署的所有 AWS 服务 (包括 Amazon S3、AWS Lambda、Amazon API Gateway、AWS WAF 等) 的费用。有关完整详细信息，请参阅每个 AWS 服务的定价页面。

### 主题

- [启动堆栈 \(模板\) \(p. 43\)](#)
- [将 Web ACL 与您的 Web 应用程序相关联 \(p. 44\)](#)
- [配置 Web 访问日志记录 \(p. 45\)](#)

## 启动堆栈 (模板)

此自动化 AWS CloudFormation 模板在 AWS 云中部署 AWS WAF 安全自动化解决方案。

### 启动 AWS CloudFormation 堆栈 (模板)

1. 登录 AWS CloudFormation [控制台](#)。
2. 如果这是您首次使用 AWS CloudFormation，请在 Select Template 页面上，选择 Specify an Amazon S3 template URL，然后输入 <https://s3.amazonaws.com/solutions-reference/aws-waf-security-automations/latest/aws-waf-security-automations.template>。如果您过去使用过 AWS CloudFormation，请选择 Create stack，然后选择 Specify an Amazon S3 template URL 并输入 <https://s3.amazonaws.com/solutions-reference/aws-waf-security-automations/latest/aws-waf-security-automations.template>。
3. 选择 Next。
4. 在 Specify Details 页面上，指定下列值：

Stack Name

为 AWS WAF 配置键入名称。这也是模板创建的 Web ACL 的名称，例如 MyWebsiteACL。

Activate SQL Injection Protection

选择 yes 以启用旨在阻止常见 SQL 注入攻击的组件。

Activate Cross-site Scripting Protection

选择 yes 以启用旨在阻止常见 XSS 攻击的组件。

Activate HTTP Flood Protection

选择 yes。此组件配置基于速率的规则，以防止来自特定 IP 地址的大量请求的攻击（例如 Web 层 DDoS 攻击或暴力登录尝试）。当来自客户端的 Web 请求超过可配置阈值时，将自动触发基于速率的规则，该阈值定义了五分钟内允许从单个 IP 地址传入的最大请求数。一旦超出此阈值，来自该 IP 地址的额外请求就会被阻止，直至请求速率降至阈值之下。有关基于速率的规则的信息，请参阅 [AWS WAF 工作原理](#)。

#### Activate Scanner & Probe Protection

选择 yes 以启用旨在阻止扫描程序和探测器的组件。

#### Activate Reputation List Protection

选择 yes 以阻止来自第三方声誉列表 (受支持列表：spamhaus、torproject 和 emergingthreats) 上的 IP 地址的请求。

#### Activate Bad Bot Protection

选择 yes。模板需要启用此保护。但是，要充分利用此保护，您必须完成不在本教程的讨论范围内的额外步骤，如创建蜜罐链接。“AWS WAF 安全自动化”中的“步骤 3.在 Web 应用程序中嵌入蜜罐链接”介绍了这些步骤。这些额外步骤是可选的，不是完成本教程所必需的。如果您选择执行这些额外步骤，请首先完成本教程，然后可以设置蜜罐链接。

#### CloudFront Access Log Bucket Name

为要在其中存储 CloudFront 分配的访问日志的 Amazon S3 存储桶键入名称。这是模板在堆栈启动过程中创建的新存储桶的名称。请勿使用现有的名称。

#### Request Threshold

这用于 HTTP 泛洪防护，因此不适用于本教程。您可以保留默认值 2000。

#### Error Threshold

这是每个 IP 地址每分钟的错误请求的最大可接受数。这由扫描程序和探测器防护使用。使用默认值 50。

#### WAF Block Period

这是一个时间段 (以分钟为单位)，在此期间，将阻止扫描程序和探测器防护所标识的适用 IP 地址。使用默认值 240。

#### Send Anonymous Usage Data

选择 yes 以向 AWS 发送匿名数据来帮助我们了解解决方案在整个客户群中的使用情况。要选择不使用此功能，请选择 no。

5. 选择 Next。
6. 不要在 Options 页面上进行任何更改。
7. 选择 Next。
8. 在 Review 页面上，审核并确认设置。请确保选中确认模板将创建 AWS Identity and Access Management (IAM) 资源的复选框。
9. 选择 Create 以部署堆栈。

您可以在 AWS CloudFormation 控制台的 Status 列中查看堆栈的状态。您应该在大约十五 (15) 分钟内看到 CREATE\_COMPLETE 状态。

## 将 Web ACL 与您的 Web 应用程序相关联

现在，将您的 Amazon CloudFront Web 分配与 Web ACL 相关联。

#### 将 Web ACL 与您的 Web 应用程序相关联

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择您新建的 WebACL。此 ACL 的名称是您在上一步中指定的名称，例如 MyWebsiteACL。
4. 选择 Rules 选项卡。
5. 选择 Add association。

6. 对于 AWS resources using this web ACL，选择您在本教程的前面创建的 CloudFront 分配。
7. 选择 Add 以保存您的更改。

## 配置 Web 访问日志记录

作为本教程的最后一个步骤，您将 Amazon CloudFront 配置为将 Web 访问日志发送到相应的 Amazon S3 存储桶，以使这些数据可供 Log Parser AWS Lambda 函数使用。

存储 CloudFront 分配的 Web 访问日志

1. 打开 Amazon CloudFront 控制台 (<https://console.aws.amazon.com/cloudfront/>)。
2. 选中您的分配旁边的复选框，然后选择 Distribution Settings。
3. 在 General 选项卡上，选择 Edit。
4. 确认对于 AWS WAF Web ACL，已输入了解决方案创建的 Web ACL (您在初始配置过程中分配给堆栈的相同名称)。
5. 对于 Logging，选择 On。
6. 对于 Bucket for Logs，选择要用于存储 Web 访问日志的 Amazon S3 存储桶 (您在[启动堆栈 \(模板\)](#) (p. 43) 中定义)。
7. 选择 Yes, edit 以保存所做更改。

下一步: [其他最佳实践](#) (p. 45).

## 其他最佳实践

您现在有多个组件来帮助保护您的网站免受 DDoS 攻击。但是，您仍可以执行其他操作。以下是您应考虑的几个最佳实践。本教程没有包含最佳实践的实施详细信息，但提供了相关文档的链接。

主题

- [隐藏 AWS 资源](#) (p. 45)
- [使用安全组](#) (p. 45)
- [网络访问控制列表 \(ACL\)](#) (p. 46)
- [保护您的源](#) (p. 46)
- [结论](#) (p. 46)

## 隐藏 AWS 资源

对于许多网站应用程序而言，您的 AWS 资源不需要完全暴露于 Internet。例如，Elastic Load Balancer (ELB) 后面的 Amazon EC2 实例可能不必可公开访问。在这种情况下，您可能决定允许用户在某些 TCP 端口上访问 ELB，并仅允许 ELB 与 Amazon EC2 实例通信。您可以通过在 Amazon Virtual Private Cloud (VPC) 中配置安全组和网络访问控制列表 (ACL) 来实现此目的。Amazon VPC 允许您预置 AWS 云的逻辑隔离部分，让您可以在自己定义的虚拟网络中启动 AWS 资源。

安全组和网络 ACL 的类似之处在于，它们都允许您控制对 Amazon VPC 内 AWS 资源的访问。使用安全组，可以在实例级别上控制入站和出站流量。网络 ACL 提供了类似的功能，不过是在 VPC 子网级别上提供。此外，Amazon EC2 安全组规则或网络 ACL 的入站数据传输不会产生费用。这可确保您不需要为安全组或网络 ACL 丢弃的流量支付任何额外费用。

## 使用安全组

您可以在启动 Amazon EC2 实例时指定安全组，或稍后将实例与安全组相关联。除非创建 allow 规则以允许流量，否则从 Internet 到安全组的所有流量都会被隐式拒绝。例如，在本教程中，您创建了一个解决方案，其中包括一个 ELB 和两个 Amazon EC2 实例。您应该考虑为 ELB 创建一个安全组 (“ELB 安全组”)，并为实例创建一个安全组 (“Web 应用程序服务器安全组”)。然后，您可以创建 Allow 规则，允许从 Internet 到

ELB 安全组的流量，并允许从 ELB 安全组到 Web 应用程序服务器安全组的流量。因此，来自 Internet 的流量无法直接与 Amazon EC2 实例通信，这使得攻击者更难了解您的网站的设计和结构。

## 网络访问控制列表 (ACL)

使用网络 ACL，您可以同时指定 Allow 和 Deny 规则。如果您希望明确拒绝发往网站的某些类型的流量，这非常有用。例如，您可以定义应该对整个子网拒绝的 IP 地址 (作为 CIDR 范围)、协议和目标端口。如果您的网站仅用于 TCP 流量，您可以创建规则来拒绝所有 UDP 流量，反之亦然。此工具在响应 DDoS 攻击时很有用，因为如果您知道源 IP 地址或其他特征，就可以创建自己的规则来缓解攻击。您可以将网络 ACL 与 AWS WAF ACL 结合使用。

## 保护您的源

您应该考虑配置 CloudFront 以禁止用户绕过 CloudFront 直接从源中请求内容。这可以提高您的源的安全性。要了解更多信息，请参阅[使用自定义标头来限制对自定义源上的内容的访问](#)。

## 结论

本教程中概述的最佳实践可帮助您构建一个能够抵御 DDoS 的架构，以保护网站免受许多常见基础设施层和应用层 DDoS 攻击的影响，从而确保可用性。您能够根据这些最佳实践构建应用程序的程度将影响您可以缓解的 DDoS 攻击的类型和数量。

有关更多信息，请参阅下列内容：

- [实现 DDoS 弹性的 AWS 最佳实践](#)
- [AWS 文档](#)

## 博客教程

博客教程

以下教程主题链接至 [AWS 安全博客](#)。

- [如何导入 IP 地址声誉列表以自动更新 AWS WAF IP 黑名单](#)
- [如何使用 AWS WAF 和 Amazon CloudFront 降低安全威胁和运营成本](#)
- [如何使用 AWS WAF、Amazon CloudFront 和 Referer Checking 防止盗链](#)
- [如何使用 AWS CloudFormation 用示例规则和匹配条件自动配置 AWS WAF](#)

# 创建和配置 Web 访问控制列表 (Web ACL)

Web 访问控制列表 (Web ACL) 使您可以精细地控制您的 Amazon CloudFront 分配或 应用程序负载均衡器 所响应的 Web 请求。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 \(p. 78\)](#)。
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 \(p. 48\)](#)。
  - 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 \(p. 52\)](#)。
  - 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 \(p. 54\)](#)。
  - 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 \(p. 55\)](#)。
  - 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 \(p. 60\)](#)。
  - 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 \(p. 63\)](#)。
  - 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 \(p. 68\)](#)。
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 请求必须匹配所有条件，AWS WAF 才会基于该规则允许或阻止请求。有关更多信息，请参阅 [使用规则 \(p. 73\)](#)。(可选) 还向规则添加速率限制，该限制指定允许来自一个特定 IP 地址的最大请求数。
4. 将规则添加到 Web ACL。对于每个规则，指定 AWS WAF 应基于添加到规则的条件允许还是阻止请求。如果将多个规则添加到一个 Web ACL，则 AWS WAF 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 \(p. 77\)](#)。

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 \(p. 47\)](#)
- [使用规则 \(p. 73\)](#)
- [使用 Web ACL \(p. 77\)](#)

## 使用条件

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 \(p. 48\)](#)。
- 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 \(p. 52\)](#)。
- 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 \(p. 54\)](#)。
- 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 \(p. 55\)](#)。
- 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 \(p. 60\)](#)。
- 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 \(p. 63\)](#)。
- 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 \(p. 68\)](#)。



#### 主题

- [使用跨站点脚本匹配条件 \(p. 48\)](#)
- [使用 IP 匹配条件 \(p. 52\)](#)
- [使用地理匹配条件 \(p. 54\)](#)
- [使用大小约束条件 \(p. 55\)](#)
- [使用 SQL 注入匹配条件 \(p. 60\)](#)
- [使用字符串匹配条件 \(p. 63\)](#)
- [使用正则表达式匹配条件 \(p. 68\)](#)

## 使用跨站点脚本匹配条件

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 AWS WAF 应对 Web 请求检查是否有恶意脚本的部分，如 URI 或查询字符串。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 \(p. 48\)](#)
- [创建或编辑跨站点脚本匹配条件时指定的值 \(p. 49\)](#)
- [在跨站点脚本匹配条件中添加和删除筛选条件 \(p. 51\)](#)
- [删除跨站点脚本匹配条件 \(p. 51\)](#)

## 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。筛选条件指示 Web 请求中您希望 AWS WAF 检查是否存在恶意脚本的部分，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 AWS WAF 行为的方式：

- 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 请求只需与跨站点脚本匹配条件中的一个筛选条件匹配，AWS WAF 即可基于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。一个筛选条件指示 AWS WAF 在 URI 中检查是否有恶意脚本，另一个筛选条件指示 AWS WAF 检查查询字符串。如果请求表现为在 URI 或查询字符串中包含恶意脚本，则 AWS WAF 允许或阻止请求。

- 每个跨站点脚本匹配条件一个筛选条件 – 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，AWS WAF 才会基于条件允许或阻止请求。

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。如果将这两个条件添加到同一个规则并将该规则添加到一个 Web ACL，则仅当 URI 和查询字符串都表现为包含恶意脚本时，AWS WAF 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 AWS WAF 配置为允许或阻止未表现为包含恶意脚本的 Web 请求。

#### 创建跨站点脚本匹配条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Cross-site scripting。

3. 选择 Create condition。
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 \(p. 49\)](#)。
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 以及特殊字符：\_!@#%^&\*,./。条件的名称在创建后不可更改。

### Part of the request to filter on

选择 AWS WAF 应对每个 Web 请求检查是否有恶意脚本的部分：

#### 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

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。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 AWS 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 的值，则 AWS WAF 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。(AWS WAF 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 \(p. 55\)](#)。

#### 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 Single query parameter (value only) (单一查询参数 (仅限值)) 类似，但此处不是检查单一参数的值，而是 AWS WAF 检查查询字符串中的所有参数值，以确定是否存在可能的恶意脚本。例如，如果 URL 是“www.xyz.com?UserName=abc&SalesRegion=seattle”，并且您选择 All query parameters (values only) (所有查询参数 (仅限值))，则当 UserName 或 SalesRegion 的值包含可能的恶意脚本时，AWS WAF 将触发匹配。

标头

如果选择 Header 作为 Part of the request to filter on 的值，则从常见标头列表中选择标头，或键入您希望 AWS WAF 检查是否有恶意脚本的标头的名称。

Transformation

转换可在 AWS WAF 检查 Web 请求之前重新格式化请求。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 AWS WAF。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

无

AWS WAF 在针对 Value to match 中的字符串检查 Web 请求之前，不会对它执行任何文本转换。

Convert to lowercase

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 &quot; 替换为 &
- 将 &nbsp; 替换为不间断空格
- 将 &lt; 替换为 <
- 将 &gt; 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

Normalize whitespace

AWS WAF 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 49\)](#)。
  - c. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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。
  - 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

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 \(p. 52\)](#)
- [编辑 IP 匹配条件 \(p. 53\)](#)
- [删除 IP 匹配条件 \(p. 53\)](#)

## 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，还可以将 AWS WAF 配置为允许或阻止不是 源自条件中指定的 IP 地址的 Web 请求。

### 创建 IP 匹配条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 IP addresses。
3. 选择 Create condition。
4. 在 Name 字段中键入名称。

该名称只能包含字母数字字符 (A-Z、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，请键入 2620:0:2d0:200::/64。

AWS WAF 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。AWS WAF 支持 IPv6 地址范围：/16、/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 [Classless Inter-Domain Routing](#)。

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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
  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 表示法键入 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，请键入 2620:0:2d0:200::/64。
- AWS WAF 支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。AWS WAF 支持 IPv6 地址范围：/16、/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 [Classless Inter-Domain Routing](#)。
- c. 要添加更多 IP 地址，请选择 Add another IP address 并键入值。
  - d. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
  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。
    - 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

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。

您可以使用地理匹配条件以及其他 AWS WAF 条件或规则来构建复杂的筛选。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

如果您使用 CloudFront 地理限制功能来阻止某个国家/地区访问您的内容，则会阻止来自该国家/地区的任何请求，并且不会将这些请求转发到 AWS WAF。因此，如果您想要根据地理位置以及其他 AWS WAF 条件允许或阻止请求，您不应使用 CloudFront 地理限制功能。而是应使用 AWS WAF 地理匹配条件。

### 主题

- [创建地理匹配条件 \(p. 54\)](#)
- [编辑地理匹配条件 \(p. 55\)](#)
- [删除地理匹配条件 \(p. 55\)](#)

## 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，还可以将 AWS WAF 配置为允许或阻止不是源自条件中指定的国家/地区的 Web 请求。

### 创建地理匹配条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Geo match。
3. 选择 Create condition。
4. 在 Name 字段中键入名称。

该名称只能包含字母数字字符 (A-Z、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 目前只能选择 Country。
7. 选择 Add location。
8. 选择 Create。

## 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 目前只能选择 Country。
  - c. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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。
  - 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。
  - 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

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 AWS WAF 应对 Web 请求检查的部分、AWS WAF 应查找的字节数以及运算符（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，如果将 AWS WAF 配置为检查请求正文（例如，通过在正文中搜索指定字符串），则 AWS WAF 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 \(p. 56\)](#)
- [创建或编辑大小约束条件时指定的值 \(p. 56\)](#)
- [在大小约束条件中添加和删除筛选条件 \(p. 59\)](#)
- [删除大小约束条件 \(p. 59\)](#)

## 创建大小约束条件

创建大小约束条件时，请指定筛选条件以确定 AWS WAF 应评估其长度的 Web 请求部分。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 AWS WAF 行为的方式：

- 每个大小约束条件一个筛选条件 – 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，AWS WAF 才会基于条件允许或阻止请求。

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。如果这两个条件添加到同一个规则并将该规则添加到一个 Web ACL，则仅当同时满足这两个条件时，AWS WAF 才会允许或阻止请求。

- 每个大小约束条件多个筛选条件 – 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，AWS WAF 即可基于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。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 AWS WAF 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 AWS WAF 配置为允许或阻止不与条件中的值匹配的 Web 请求。

#### 创建大小约束条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Size constraints。
3. 选择 Create condition。
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 \(p. 56\)](#)。
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

为大小约束条件键入名称。

该名称只能包含字母数字字符 (A-Z、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 AWS WAF 应对每个 Web 请求评估其长度的部分：

### 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

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。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 AWS 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 Single query parameter (value only) (单一查询参数 (仅限值)) 类似，但此处不是检查单一参数的值，而是 AWS WAF 检查查询字符串中所有参数的值，以确定是否存在大小约束条件。例如，如果 URL 是“www.xyz.com?UserName=abc&SalesRegion=seattle”，并且您选择 All query parameters (values only) (所有查询参数 (仅限值))，则当 UserName 或 SalesRegion 的值超出指定的大小时，AWS WAF 将触发匹配。

## Header (仅当“Part of the request to filter on”是“Header”时)

如果选择 Header 作为 Part of the request to filter on 的值，则从常见标头列表中选择标头，或键入您希望 AWS WAF 评估其长度的标头的名称。

## 比较运算符

选择您希望 AWS WAF 如何按照为 Size 指定的值评估 Web 请求中查询字符串的长度。

例如，如果为 Comparison operator 选择 Is greater than 并为 Size 键入 100，则 AWS WAF 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

键入 AWS WAF 应在查询字符串中监视的长度 (以字节为单位)。

### 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。

## Transformation

转换会在 AWS WAF 评估 Web 请求指定部分的长度之前转换请求。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 AWS WAF。

### Note

如果选择 Body 作为 Part of the request to filter on 的值，则无法将 AWS WAF 配置为执行转换，因为只转发前 8192 个字节进行检查。但是，您仍然可以基于 HTTP 请求正文的大小筛选流量，并将转换指定为 None。(AWS WAF 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：

无

AWS WAF 在检查长度之前不对 Web 请求执行任何文本转换。

## Convert to lowercase

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

## HTML decode

AWS WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 &quot; 替换为 &
- 将 &nbsp; 替换为不间断空格
- 将 &lt; 替换为 <
- 将 &gt; 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

## Normalize whitespace

AWS WAF 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 56\)](#)。
  - c. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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。
  - 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

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 AWS WAF 应检查的 Web 请求部分（如 URI 或查询字符串）。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 \(p. 60\)](#)
- [创建或编辑 SQL 注入匹配条件时指定的值 \(p. 60\)](#)
- [在 SQL 注入匹配条件中添加和删除筛选条件 \(p. 62\)](#)
- [删除 SQL 注入匹配条件 \(p. 63\)](#)

## 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 AWS WAF 应检查是否有恶意 SQL 代码的 Web 请求部分，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 AWS WAF 行为的方式：

- 每个 SQL 注入匹配条件多个筛选条件（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，AWS WAF 即可基于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。一个筛选条件指示 AWS WAF 在 URI 中检查是否有恶意 SQL 代码，另一个筛选条件指示 AWS WAF 检查查询字符串。如果请求表现为在 URI 或查询字符串中包含恶意 SQL 代码，则 AWS WAF 会允许或阻止请求。

- 每个 SQL 注入匹配条件一个筛选条件 – 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，AWS WAF 才会基于条件允许或阻止请求。

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。如果将这两个条件添加到同一个规则并将该规则添加到一个 Web ACL，则仅当 URI 和查询字符串都表现为包含恶意 SQL 代码时，AWS WAF 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 AWS WAF 配置为允许或阻止未表现为包含恶意 SQL 代码的 Web 请求。

### 创建 SQL 注入匹配条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 SQL injection。
3. 选择 Create condition。
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 \(p. 60\)](#)。
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符 (A-Z、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 AWS WAF 应对每个 Web 请求检查是否有恶意 SQL 代码的部分：

### 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

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。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 AWS 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 的值，则 AWS WAF 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。(AWS WAF 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 \(p. 55\)](#)。

### 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 Single query parameter (value only) (单一查询参数 (仅限值)) 类似，但此处不是检查单一参数的值，而是 AWS WAF 检查查询字符串中所有参数的值，以确定是否存在可能的恶意 SQL 代码。例如，如果 URL 是“www.xyz.com?UserName=abc&SalesRegion=seattle”，并且您选择 All query parameters (values only) (所有查询参数 (仅限值))，则当 UserName 或 SalesRegion 的值包含可能的恶意 SQL 代码时，AWS WAF 将触发匹配。

## 标头

如果选择 Header 作为 Part of the request to filter on 的值，则从常见标头列表中选择标头，或键入您希望 AWS WAF 检查是否有恶意 SQL 代码的标头的名称。

## Transformation

转换可在 AWS WAF 检查 Web 请求之前重新格式化请求。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 AWS WAF。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

无

AWS WAF 在针对 Value to match 中的字符串检查 Web 请求之前，不会对它执行任何文本转换。

### Convert to lowercase

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

### HTML decode

AWS WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 &quot; 替换为 &
- 将 &nbsp; 替换为不间断空格
- 将 &lt; 替换为 <
- 将 &gt; 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

### Normalize whitespace

AWS WAF 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 60\)](#)。
  - c. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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。
  - 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

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 AWS WAF 应对 Web 请求检查该字符串的部分 (如指定标头或查询字符串)。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 \(p. 64\)](#)
- [创建或编辑字符串匹配条件时指定的值 \(p. 64\)](#)



- [在字符串匹配条件中添加和删除筛选条件 \(p. 67\)](#)
- [删除字符串匹配条件 \(p. 67\)](#)

## 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 AWS WAF 应对 Web 请求检查该字符串的部分 (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 AWS WAF 行为的方式：

- 每个字符串匹配条件一个筛选条件 – 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，AWS WAF 才会基于条件允许或阻止请求。

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。如果这两个条件添加到同一个规则并将该规则添加到一个 Web ACL，则仅当请求同时包含这两个值时，AWS WAF 才会允许或阻止请求。

- 每个字符串匹配条件多个筛选条件 – 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，AWS WAF 即可基于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。如果请求在 User-Agent 标头中包含 BadBot，或在查询字符串中包含 BadParameter，则 AWS WAF 会允许或阻止请求。

### Note

将字符串匹配条件添加到规则时，您还可以将 AWS WAF 配置为允许或阻止不与条件中的值匹配的 Web 请求。

## 创建字符串匹配条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 String and regex matching。
3. 选择 Create condition。
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 \(p. 64\)](#)。
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

为字符串匹配条件键入名称。该名称只能包含字母数字字符 (A-Z、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

选择您希望 AWS WAF 检查其中是否有 Value to match 中所指定字符串的每个 Web 请求部分：

## 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

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。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 AWS 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 的值，则 AWS WAF 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。(AWS WAF 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 \(p. 55\)](#)。

## 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 Single query parameter (value only) (单一查询参数 (仅限值)) 类似，但此处不是检查单一参数的值，而是 AWS WAF 检查查询字符串中所有参数的值，以确定是否存在 Value to match (要匹配的值)。例如，如果 URL 是“www.xyz.com?UserName=abc&SalesRegion=seattle”，并且您选择 All query parameters (values only) (所有查询参数 (仅限值))，则当将 UserName 或 SalesRegion 指定为 Value to match (要匹配的值) 时，AWS WAF 将触发匹配。

Header (仅当“Part of the request to filter on”是“Header”时)

如果您从 Part of the request to filter on 选择 Header，则从常见标头列表中选择标头，或键入您希望 AWS WAF 检查是否有恶意脚本的标头的名称。

## Match type

在 AWS WAF 应检查的请求部分中，选择 Value to match 中的字符串必须在哪个位置出现才与此筛选条件匹配：

### 包含

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

转换可在 AWS WAF 检查 Web 请求之前重新格式化请求。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 AWS WAF。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

无

AWS WAF 在针对 Value to match 中的字符串检查 Web 请求之前，不会对它执行任何文本转换。

#### Convert to lowercase

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

#### HTML decode

AWS WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 `&quot;` 替换为 `&`
- 将 `&nbsp;` 替换为不间断空格
- 将 `&lt;` 替换为 `<`
- 将 `&gt;` 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

#### Normalize whitespace

AWS WAF 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不寻常的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 AWS WAF 应在 Web 请求中搜索的值。最大长度为 50 个字节。如果要对值进行 base64 编码，则 50 字节限制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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 64\)](#)。
  - c. 选择 Add。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。

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。
  - 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。
  - 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

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，它标识要搜索的模式，以及 Web 请求中您希望 AWS WAF 在其中检查模式的部分 (如指定的标头或查询字符串)。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 \(p. 68\)](#)
- [创建或编辑正则表达式匹配条件时指定的值 \(p. 69\)](#)
- [编辑正则表达式匹配条件 \(p. 71\)](#)

## 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 Web 请求中您希望 AWS WAF 在其中检查该模式集的部分 (如 URI 或查询字符串) 的筛选条件中。

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，您还可以将 AWS WAF 配置为允许或阻止不与条件中的值匹配的 Web 请求。

AWS WAF 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 String and regex matching。
3. 选择 Create condition。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 [创建或编辑正则表达式匹配条件时指定的值 \(p. 69\)](#)。
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。

## 创建或编辑正则表达式匹配条件时指定的值

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键入名称。该名称只能包含字母数字字符 (A-Z、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

选择您希望 AWS WAF 检查其中是否有 Value to match 中所指定模式的每个 Web 请求部分：

### 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

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。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 AWS 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 的值，则 AWS WAF 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。(AWS WAF 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 \(p. 55\)](#)。

#### 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 Single query parameter (value only) (单一查询参数 (仅限值)) 类似，但此处不是检查单一参数的值，而是 AWS WAF 检查查询字符串中所有参数的值，以确定是否存在 Value to match (要匹配的值) 中指定的模式。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)

如果您从 Part of the request to filter on 选择 Header，则从常见标头列表中选择标头，或键入您希望 AWS WAF 检查是否有恶意脚本的标头的名称。

#### Transformation

转换可在 AWS WAF 检查 Web 请求之前重新格式化请求。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 AWS WAF。

您只能指定一个类型的文本转换。

转换可以执行以下操作：

无

AWS WAF 在针对 Value to match 中的字符串检查 Web 请求之前，不会对它执行任何文本转换。

#### Convert to lowercase

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

#### HTML decode

AWS WAF 将 HTML 编码的字符替换为未编码的字符：

- 将 &quot; 替换为 &
- 将 &nbsp; 替换为不间断空格
- 将 &lt; 替换为 <
- 将 &gt; 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

#### Normalize whitespace

AWS WAF 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不寻常的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

键入名称, 然后指定您希望 AWS WAF 搜索的正则表达式模式。

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。如果您要指定 base64 编码值, 则最大长度是 70 个字符 (编码前)。

## 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 AWS 管理控制台, 并通过以下网址打开 AWS WAF 控制台: <https://console.aws.amazon.com/waf/>。
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。
6. 选择要删除的模式旁边的 X。

7. 选择 Save。

#### 向现有模式集中添加模式

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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。
6. 键入新的正则表达式模式。
7. 选择新模式旁边的 +。
8. 选择 Save。

#### 从现有的正则表达式匹配条件中删除筛选条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 72\)](#)。
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。
  - 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。
  - f. 对使用要删除的正则表达式匹配条件的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. 选择 Delete。

#### 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 72\)](#)。

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

通过在规则中准确指定 AWS WAF 的检查条件，您可以精确地限定 AWS WAF 应允许或阻止的 Web 请求。例如，AWS WAF 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

- [创建规则和添加条件 \(p. 73\)](#)
- [在规则中添加和删除条件 \(p. 74\)](#)
- [删除规则 \(p. 75\)](#)
- [AWS Marketplace Rule Groups \(p. 75\)](#)

## 创建规则和添加条件

如果您将多个条件添加到一个规则，则 Web 请求必须匹配所有条件，AWS WAF 才会基于该规则允许或阻止请求。

### 创建规则并添加条件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Rules。
3. 选择 Create rule。
4. 键入以下值：

名称

键入名称。

CloudWatch metric name

为 AWS WAF 将创建并与规则关联的 CloudWatch 指标键入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_!@#\*},./。且不能包含空格。

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，但还考虑到每五分钟来自指定 IP 地址的请求数。有关这些规则类型的详细信息，请参阅 [AWS WAF 如何工作 \(p. 6\)](#)。

Rate limit

如果您在创建基于速率的规则，请输入 5 分钟周期内允许的来自单个 IP 地址的最大请求数。速率限制必须等于或大于 2000。

5. 要将条件添加到规则，请指定以下值：

When a request does/does not

如果您希望 AWS WAF 基于条件中的筛选器允许或阻止请求，例如源自 IP 地址范围 192.0.2.0/24 的 Web 请求，请选择 does。

如果您希望 AWS WAF 基于条件中的筛选器的反向条件允许或阻止请求，则选择 **does not**。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且希望 AWS WAF 允许或阻止不是来自这些 IP 地址的请求，请选择 **does not**。

match/originate from

选择要添加到规则的条件类型：

- Cross-site scripting match conditions – 选择 match at least one of the filters in the cross-site scripting match condition
- IP match conditions – 选择 originate from an IP address in
- Geo match conditions – 选择 originate from a geographic location in
- Size constraint conditions – 选择 match at least one of the filters in the size constraint condition
- SQL injection match conditions – 选择 match at least one of the filters in the SQL injection match condition
- String match conditions – 选择 match at least one of the filters in the string match condition
- Regular expression match conditions – 选择 match at least one of the filters in the regex match condition

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，AWS WAF 才会基于该规则允许或阻止请求
  - 如果您将两个 IP 匹配条件添加到同一个规则，则 AWS WAF 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

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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 **Rules**。
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

如果您希望 AWS WAF 基于条件中的筛选器允许或阻止请求，例如源自 IP 地址范围 192.0.2.0/24 的 Web 请求，请选择 **does**。

如果您希望 AWS WAF 基于条件中的筛选器的反向条件允许或阻止请求，则选择 **does not**。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且希望 AWS WAF 允许或阻止不是来自这些 IP 地址的请求，请选择 **does not**。

match/originate from

选择要添加到规则的条件类型：

- Cross-site scripting match conditions – 选择 match at least one of the filters in the cross-site scripting match condition
- IP match conditions – 选择 originate from an IP address in
- Geo match conditions – 选择 originate from a geographic location in
- Size constraint conditions – 选择 match at least one of the filters in the size constraint condition
- SQL injection match conditions – 选择 match at least one of the filters in the SQL injection match condition
- String match conditions – 选择 match at least one of the filters in the string match condition
- Regular expression match conditions – 选择 match at least one of the filters in the regex match condition

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. 要删除条件，请选择条件名称右侧的 X
7. 选择 Update。

## 删除规则

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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 要从使用某个规则的 Web ACL 中将其删除，请执行以下步骤：
  - 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 Edit web ACL。
  - d. 选择要从 Web ACL 中删除的规则右侧的 X，然后选择 Update。
  - e. 对使用要删除的规则的所有其余 Web ACL 重复这些步骤。
3. 在导航窗格中，选择 Rules。
4. 选择要删除的规则的名称。
5. 选择 Delete。

## AWS Marketplace Rule Groups

AWS WAF 可提供 AWS Marketplace rule groups 帮助您保护您的资源。AWS Marketplace rule groups 是预定义、即用型规则集合，由 AWS 和 AWS 合作伙伴公司编写和更新。

某些 AWS Marketplace rule groups 旨在帮助保护特定类型的 Web 应用程序，如 WordPress、Joomla 或 PHP。其他 AWS Marketplace rule groups 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 Top 10](#) 中列出的漏洞。

您可以安装来自您的首选 AWS 合作伙伴的单个 AWS Marketplace rule group，您还可以添加您自定义的 AWS WAF 规则以增强保护。如果您需要符合监管合规性（如 PCI 或 HIPAA），或许可以使用 AWS Marketplace rule groups 来满足 Web 应用程序防火墙要求。

AWS Marketplace rule groups 不需要签订长期合同即可使用，也没有最低费用限制。订阅规则组后会向您收取月度费用（按小时比例）以及持续请求基于卷的费用。有关更多信息，请参阅 [AWS WAF 定价](#) 以及 AWS Marketplace 上每个 AWS Marketplace rule group 的描述。

## 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。当您实施并使用 AWS WAF 时，AWS Marketplace rule groups 可以帮助您节省时间。另一个好处是当出现在新的漏洞和威胁时 AWS 和我们的 AWS 合作伙伴会自动更新 AWS Marketplace rule groups。

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。

## 对 AWS Marketplace Rule Group 中规则的访问权限

每个 AWS Marketplace rule group 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 AWS Marketplace rule group 中的单个规则，所以您也无法编辑这些规则组中的任何规则。但是，您可以启用或禁用整个规则组，并且可以选择要执行的规则组操作。参阅 [使用 AWS Marketplace Rule Groups \(p. 76\)](#) 了解更多信息。

## 限制

您可以只启用一个 AWS Marketplace rule group。此规则组包含在每个 Web ACL 的 10 条规则限制内。因此，您可以在单个 Web ACL 中设置一个 AWS Marketplace rule group 和最多 9 条自定义规则。

## 定价

有关 AWS Marketplace rule group 定价的信息，请参阅 [AWS WAF 定价](#) 以及 AWS Marketplace 上每个 AWS Marketplace rule group 的描述

## 使用 AWS Marketplace Rule Groups

您可以从 AWS WAF 控制台订阅和取消订阅 AWS Marketplace rule groups。

若要订阅和使用 AWS Marketplace rule group

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 \(p. 78\)](#) 或 [编辑 Web ACL \(p. 81\)](#)。

### 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 \(p. 77\)](#)。

若要取消订阅 AWS Marketplace rule group

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。



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 \(p. 81\)](#)。
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。

## 规则组覆盖

AWS Marketplace rule groups 有两个可能的操作：无覆盖和覆盖以计数。如果您要测试规则组，请将操作设置为覆盖以计数。此规则组操作随后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。

## AWS Marketplace Rule Groups 问题排查

如果您发现有 AWS Marketplace rule group 正阻止合法流量，请执行以下步骤。

若要对 AWS Marketplace rule group 进行问题排查

1. 将 AWS Marketplace rule group 的操作从无覆盖更改为覆盖以计数。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。这还为您提供了规则组的 Amazon CloudWatch 指标。
2. 在将 AWS Marketplace rule group 的操作设置为覆盖以计数之后，请联系规则组提供商的客户支持团队来进一步进行问题排查。有关联系信息，请参阅 AWS Marketplace 产品列表页面上的规则组列表。

## 联系客户支持

有关 AWS 管理的 AWS WAF 或规则组的问题，请联系 AWS Support。有关 AWS 合作伙伴管理的规则组的问题，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 AWS Marketplace 上的合作伙伴列表。

## 创建并销售 AWS Marketplace Rule Groups

如果您要在 AWS Marketplace 上销售 AWS Marketplace rule groups，请参阅[如何在 AWS Marketplace 上销售软件](#)。

# 使用 Web ACL

将规则添加到 Web ACL 时，需要指定 AWS WAF 应基于规则中的条件允许还是阻止请求。如果您将多个规则添加到 Web ACL，则 AWS WAF 按照在 Web ACL 中列出规则的顺序，对规则评估每个请求。当 Web 请求与规则中的所有条件匹配时，AWS WAF 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，则 AWS WAF 会执行您为 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 \(p. 78\)](#)。

如果要在开始使用规则允许或阻止请求之前测试它，可以将 AWS WAF 配置为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 \(p. 82\)](#)。

### 主题

- [确定 Web ACL 的默认操作 \(p. 78\)](#)
- [创建 Web ACL \(p. 78\)](#)
- [将 Web ACL 与 CloudFront 分配或 应用程序负载均衡器 关联或取消关联 \(p. 80\)](#)
- [编辑 Web ACL \(p. 81\)](#)
- [删除 Web ACL \(p. 81\)](#)



- [测试 Web ACL \(p. 82\)](#)

## 确定 Web ACL 的默认操作

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 AWS WAF 的默认操作应该是允许 Web 请求还是阻止 Web 请求。默认操作指示在 AWS WAF 按照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，您希望 AWS WAF 执行的操作：

- Allow – 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 地址或其请求似乎包含恶意 SQL 代码或指定值的攻击者进行访问，请选择 Allow 作为默认操作。
- Block – 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 作为默认操作。

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

### 创建 Web ACL

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 如果这是您首次使用 AWS WAF，请选择 Go to AWS WAF，然后选择 Configure Web ACL。如果您以前使用过 AWS WAF，请在导航窗格中选择 Web ACLs，然后选择 Create web ACL。
3. 对于 Web ACL name，键入一个名称。

#### Note

Web ACL 在创建之后无法更改名称。

4. 对于 CloudWatch metric name，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）以及以下特殊字符：\_!"#'+\*},./。且不能包含空格。

#### Note

Web ACL 在创建之后无法更改名称。

5. 对于 Region，选择一个区域。
6. 对于 AWS resource，选择要与此 Web ACL 关联的资源，然后选择 Next。
7. 如果您已创建了希望 AWS WAF 用于检查 Web 请求的条件，请选择 Next，然后继续下一个步骤。

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 \(p. 48\)](#)
- [使用 IP 匹配条件 \(p. 52\)](#)
- [使用地理匹配条件 \(p. 54\)](#)
- [使用大小约束条件 \(p. 55\)](#)
- [使用 SQL 注入匹配条件 \(p. 60\)](#)
- [使用字符串匹配条件 \(p. 63\)](#)

- [使用正则表达式匹配条件 \(p. 68\)](#)

8. 如果您已创建了要添加到此 Web ACL 的规则 (或订阅了 AWS Marketplace rule group)，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. 选择 Create rule。
  - b. 键入以下值：

名称

键入名称。

CloudWatch metric name

为 AWS WAF 将创建并与规则关联的 CloudWatch 指标键入名称。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

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

如果您希望 AWS WAF 基于条件中的筛选器允许或阻止请求，例如源自 IP 地址范围 192.0.2.0/24 的 Web 请求，请选择 does。

如果您希望 AWS WAF 基于条件中的筛选器的反向条件允许或阻止请求，则选择 does not。例如，如果 IP 匹配条件包含 IP 地址范围 192.0.2.0/24 并且希望 AWS WAF 允许或阻止不是来自这些 IP 地址的请求，请选择 does not。

match/originate from

选择要添加到规则的条件的类型：

- Cross-site scripting match conditions – 选择 match at least one of the filters in the cross-site scripting match condition
- IP match conditions – 选择 originate from an IP address in
- Geo match conditions – 选择 originate from a geographic location in
- Size constraint conditions – 选择 match at least one of the filters in the size constraint condition
- SQL injection match conditions – 选择 match at least one of the filters in the SQL injection match condition
- String match conditions – 选择 match at least one of the filters in the string match condition
- Regex match conditions – 选择 match at least one of the filters in the regex match condition

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的类型的条件。

- d. 要将另一个条件添加到规则，请选择 Add another condition，然后重复步骤 b 和 c。请注意以下事项：
  - 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，AWS WAF 才会基于该规则允许或阻止请求

- 如果您将两个 IP 匹配条件添加到同一个规则，则 AWS WAF 只允许或阻止源自两个 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。
  - g. 继续执行步骤 10。
10. 对于已添加到 Web ACL 的每个规则，选择 AWS WAF 应基于规则中的条件对 Web 请求进行允许、阻止还是计数：
- Allow – CloudFront 或 应用程序负载均衡器 使用请求的对象进行响应。对于 CloudFront，如果对象不在边缘缓存中，则 CloudFront 将请求转发到源。
  - Block – CloudFront 或 应用程序负载均衡器 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 [结合使用 AWS WAF 与 CloudFront 自定义错误页面 \(p. 85\)](#)。
  - Count – AWS WAF 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 测试 Web ACL 的信息，请参阅 [与 Web ACL 中的规则匹配的 Web 请求计数 \(p. 82\)](#)。

#### Note

往 Web ACL 中添加 AWS Marketplace rule group 时 (与单个规则组相对)，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 \(p. 77\)](#)。

11. 如果需要更改 Web ACL 中的规则顺序，请使用 Order 列中的箭头。AWS WAF 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。这是 AWS WAF 在 Web 请求不与此 Web ACL 中的任何规则中的条件匹配时执行的操作。有关更多信息，请参阅 [确定 Web ACL 的默认操作 \(p. 78\)](#)。
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 CloudFront 分配或 应用程序负载均衡器 关联或取消关联

要关联或取消关联 Web ACL，请执行适用的过程。请注意，您还可以在创建或更新 CloudFront 分配时将 Web ACL 与分配关联。有关更多信息，请参阅 Amazon CloudFront 开发人员指南 中的 [使用 AWS WAF 控制对您的内容的访问权限](#)。

当关联 Web ACL 时，以下限制将适用：

- 与 应用程序负载均衡器 关联的 Web ACL 只能与同一区域中的其他 应用程序负载均衡器 相关联。
- 与 CloudFront 分配关联的 Web ACL 不能与 应用程序负载均衡器 关联。但是，Web ACL 可以与其他 CloudFront 分配相关联。
- 每个 应用程序负载均衡器 和 CloudFront 分配只能与一个 Web ACL 相关联。

将一个 Web ACL 与一个 CloudFront 分配或 应用程序负载均衡器 相关联

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。

2. 在导航窗格中，选择 Web ACL。
3. 选择要与 CloudFront 分配或 应用程序负载均衡器 关联的 Web ACL。
4. 在规则选项卡中，在 使用此 Web ACL 的 AWS 资源下，选择添加关联。
5. 出现提示时，使用 Resource 列表选择要将此 Web ACL 与之关联的 CloudFront 分配或 应用程序负载均衡器。如果选择 应用程序负载均衡器，还必须指定区域。
6. 选择 Add。
7. 要将此 Web ACL 与其他 CloudFront 分配或 应用程序负载均衡器 关联，请重复步骤 4 到步骤 6。

#### 从 CloudFront 分配或 应用程序负载均衡器 取消关联 Web ACL

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要从 CloudFront 分配或 应用程序负载均衡器 取消关联的 Web ACL。
4. 在 Rules 选项卡上的 AWS resources using this web ACL 下，为要取消与此 Web ACL 关联的每个 CloudFront 分配或 应用程序负载均衡器 选择 x。

## 编辑 Web ACL

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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL。
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 Order 列中的箭头。AWS WAF 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 AWS WAF 中删除规则，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

当为 AWS Marketplace rule group 设置操作时 (与单个规则组相对)，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 \(p. 77\)](#)。

9. 选择 Save changes。

## 删除 Web ACL

要删除 Web ACL，必须先删除 Web ACL 中包含的规则，然后从 Web ACL 取消关联所有 CloudFront 分配和 Application Load Balancer。请执行以下步骤。

## 删除 Web ACL

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，选择 Web ACL。
3. 选择要删除的 Web ACL。
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 AWS WAF 中删除规则，只是从此 Web ACL 删除规则。
6. 选择 Update。
7. 取消 Web ACL 与所有 CloudFront 分配和 Application Load Balancer 的关联。在 Rules (规则) 选项卡上的 AWS resources using this web ACL (使用此 Web ACL 的 AWS 资源) 下，选择每个 CloudFront 分配或应用程序负载均衡器的 x。
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

为了确保您不会在无意中将 AWS WAF 配置为阻止要允许的请求或允许要阻止的请求，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 \(p. 82\)](#)
- [查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求采样 \(p. 83\)](#)

## 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 AWS WAF 对与该规则中所有条件匹配的 Web 请求进行允许、阻止还是计数。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，AWS WAF 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匹配，AWS WAF 将使该规则的计数器递增。然后，AWS WAF 将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，AWS WAF 将使该规则的计数器递增。此操作将一直继续，直到 AWS WAF 已根据所有规则中的条件检查完请求为止。

在将 Web ACL 中的所有规则配置为对请求计数并将 Web ACL 与 CloudFront 分配或应用程序负载均衡器关联后，便可在 Amazon CloudWatch 图表中查看生成的计数。对于 Web ACL 中的每个规则以及 CloudFront 或应用程序负载均衡器为 Web ACL 转发给 AWS WAF 的所有请求，CloudWatch 允许您：

- 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 CloudWatch 对数据执行的计算，如最大值、最小值、平均值或求和

### Note

AWS WAF with CloudFront 是一个全局性服务和指标，仅当您在 AWS 控制台中选择 US East (N. Virginia) 区域时才可用。如果您选择其他区域，CloudWatch 控制台中将不显示任何 AWS WAF 指标。

## 查看 Web ACL 中规则的数据

1. 登录 AWS 管理控制台并通过以下网址打开 CloudWatch 控制台 <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 CloudWatch 对数据执行的计算。

### 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。


### Period

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 CloudFront 分配或应用程序负载均衡器 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 CloudFront 分配或应用程序负载均衡器 与一个 Web ACL 关联，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 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的各个请求的详细信息。有关更多信息，请参阅 [查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求采样 \(p. 83\)](#)。
  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 \(Web ACL\) \(p. 46\)](#)。

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 \(p. 81\)](#)。

## 查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求采样

在 AWS WAF 控制台中，您可以查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 进行检查的请求的采样。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。采样中的请求来自已在前 15 分钟内收到内容请求的所有 CloudFront 边缘站点或 Application Load Balancer。

### 查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求的采样

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
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 应用程序负载均衡器 发送请求) 代理或 应用程序负载均衡器 的 IP 地址。

URI

URL 中标识资源的部分 (例如 /images/daily-ad.jpg)。

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 请求匹配一个规则中的所有条件并且该规则的操作是 Count 时，AWS WAF 继续基于 Web ACL 中的后续规则检查该 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

AWS WAF 接收来自 CloudFront 或 应用程序负载均衡器 的请求的时间。

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。AWS WAF 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 应用程序负载均衡器 发送请求，则为 HTTP 代理或 应用程序负载均衡器 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。

## 列出根据基于速率的规则而阻止的 IP 地址

AWS WAF 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 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。



2. 在导航窗格中，选择 Rules。
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。

## AWS WAF 如何使用 Amazon CloudFront 功能

在创建 Web ACL 时，您可以指定希望 AWS WAF 检查的一个或多个 CloudFront 分配。AWS WAF 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 AWS WAF 功能。本章介绍了几种用于配置 CloudFront 以便于 CloudFront 和 AWS WAF 配合工作的方法。

### 主题

- [结合使用 AWS WAF 与 CloudFront 自定义错误页面 \(p. 85\)](#)
- [结合使用 AWS WAF 与 CloudFront 地理限制 \(p. 85\)](#)
- [选择 CloudFront 响应的 HTTP 方法 \(p. 86\)](#)

## 结合使用 AWS WAF 与 CloudFront 自定义错误页面

当 AWS WAF 根据您指定的条件阻止 Web 请求时，它会将 HTTP 状态代码 403 (Forbidden) 返回给 CloudFront。接下来，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.
```

如果您希望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 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 无法区分由您的源返回的 HTTP 状态代码 403 与请求被阻止时由 AWS WAF 返回的 HTTP 状态代码 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 Amazon CloudFront 开发人员指南 中的 [自定义错误响应](#)。

## 结合使用 AWS WAF 与 CloudFront 地理限制

您可以使用 Amazon CloudFront 的地理限制 功能 (也称为 geoblocking) 防止特定地理位置的用户访问您通过 CloudFront Web 分配分发的内容。如果希望阻止来自特定国家/地区的 Web 请求，同时还要根据其他条件阻止请求，您可以将 CloudFront 地理限制与 AWS WAF 结合使用。无论用户是从 CloudFront 地理限制黑名单上的国家/地区访问您的内容，还是请求被 AWS WAF 阻止，CloudFront 都将向查看器返回相同的 HTTP 状态代码—HTTP 403 (Forbidden)。

### Note

您可以在 Web ACL 的 Web 请求示例中看到请求来自的国家/地区的双字母国家/地区代码。有关更多信息，请参阅 [查看 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求采样 \(p. 83\)](#)。

有关 CloudFront 地理限制的更多信息，请参阅 Amazon CloudFront 开发人员指南 中的 [限制内容的地理分配](#)。

## 选择 CloudFront 响应的 HTTP 方法

您在创建 Amazon CloudFront Web 分配时，会选择希望 CloudFront 处理并转发给源的 HTTP 方法。可从以下选项中进行选择：

- GET, HEAD – 您只能使用 CloudFront 从源获取对象或获取对象标头。
- GET, HEAD, OPTIONS – 您只能使用 CloudFront 从源获取对象、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 CloudFront 获取、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。

还可以使用 AWS WAF 字符串匹配条件基于 HTTP 方法来允许或阻止请求，如[使用字符串匹配条件 \(p. 63\)](#)中所述。如果要使用 CloudFront 支持的方法组合 (如 GET 和 HEAD)，则不必将 AWS WAF 配置为阻止使用其他方法的请求。如果希望允许 CloudFront 不支持的方法组合 (例如 GET、HEAD 和 POST)，则可将 CloudFront 配置为响应所有方法，然后使用 AWS WAF 阻止使用其他方法的请求。

有关选择 CloudFront 响应的方法的更多信息，请参阅 Amazon CloudFront 开发人员指南 中主题[您在创建或更新 Web 分配时指定的值下的允许的 HTTP 方法](#)。

## AWS WAF 的身份验证和访问控制

访问 AWS WAF 需要凭证。这些凭证必须有权访问 AWS 资源，如 AWS WAF 资源或 Amazon S3 存储桶。下面几节详细说明如何使用 [AWS Identity and Access Management \(IAM\)](#) 和 AWS WAF 帮助保护对您的资源的访问。

- [身份验证 \(p. 86\)](#)
- [访问控制 \(p. 87\)](#)

### 身份验证

您可以以下面任一类型的身份访问 AWS：

- AWS 账户根用户 – 当您首次创建 AWS 账户时，最初使用的是一个对账户中所有 AWS 服务和资源有完全访问权限的单点登录身份。此身份称为 AWS 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。强烈建议您不使用根用户执行日常任务，即使是管理任务。请遵守[使用根用户的最佳实践](#)，仅将其用于创建您的首个 IAM 用户。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。
- IAM 用户 – [IAM 用户](#)是您的 AWS 账户中的一种身份，它具有特定的自定义权限 (例如，用于在 AWS WAF 中创建 a rule 的权限)。您可以使用 IAM 用户名和密码来登录以保护 AWS 网页，如 [AWS 管理控制台](#)、[AWS 开发论坛](#)或 [AWS Support Center](#)。

除了用户名和密码之外，您还可以为每个用户生成[访问密钥](#)。在通过[多个软件开发工具包](#)之一或使用 [AWS Command Line Interface \(CLI\)](#) 以编程方式访问 AWS 服务时，可以使用这些密钥。SDK 和 CLI 工具使用访问密钥对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。AWS WAF supports 签名版本 4，后者是一种用于对入站 API 请求进行身份验证的协议。有关验证请求的更多信息，请参阅 AWS General Reference 中的[签名版本 4 签名流程](#)。

- IAM 角色 – [IAM 角色](#)是可在账户中创建的一种具有特定权限的 IAM 身份。它类似于 IAM 用户，但未与特定人员关联。利用 IAM 角色，您可以获得可用于访问 AWS 服务和资源的临时访问密钥。具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合身份用户访问 – 您也可以不创建 IAM 用户，而是使用来自 AWS Directory Service、您的企业用户目录或 Web 身份提供商的既有用户身份。他们被称为联合身份用户。在通过[身份提供商](#)请求访问权限时，AWS 将为联合用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南 中的[联合身份用户和角色](#)。
- AWS 服务访问 – 您可以使用您的账户中的 IAM 角色向 AWS 服务授予对您账户中资源的访问权限。例如，您可以创建一个角色，此角色允许 Amazon Redshift 代表您访问 Amazon S3 存储桶，然后将该存储桶提供的数据加载到 Amazon Redshift 群集中。有关更多信息，请参阅 IAM 用户指南 中的[创建向 AWS 服务委派权限的角色](#)。
- 运行在 Amazon EC2 上的应用程序 – 对于在 EC2 实例上运行、并发出 AWS API 请求的应用程序，您可以使用 IAM 角色管理它们的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 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 角色向在 Amazon EC2 实例上运行的应用程序授予权限](#)。

## 访问控制

您可以使用有效的凭证对自己的请求进行身份验证，但您必须拥有权限才能创建或访问 AWS WAF 资源。例如，您必须拥有权限才能创建 AWS WAF Web ACL 或规则。

以下几节介绍如何管理 AWS WAF 的权限。我们建议您先阅读概述。

- [AWS WAF 资源访问权限管理概述](#) (p. 88)
- [为 AWS WAF 使用基于身份的策略 \(IAM 策略\)](#) (p. 91)
- [AWS WAF API 权限：操作、资源和条件参考](#) (p. 95)

## AWS Identity and Access Management

AWS WAF 与 AWS Identity and Access Management (IAM) 集成，后者是让您的企业或组织可以执行以下操作的服务：

- 在您的企业或组织的 AWS 账户下创建用户和组
- 与账户中的用户共享 AWS 账户资源
- 为每个用户分配具有唯一性的安全证书
- 控制用户对服务和资源的访问

例如，您可以将 IAM 与 AWS WAF 结合使用，以控制 AWS 账户中的哪些用户可以创建新的 Web ACL。

有关 IAM 的一般信息，请参阅以下文档：

- [AWS Identity and Access Management \(IAM\)](#)
- [IAM 入门指南](#)
- [IAM 用户指南](#)

## AWS WAF 资源访问权限管理概述

每个 AWS 资源都归某个 AWS 账户所有，创建和访问资源的权限由权限策略进行管理。账户管理员可以向 IAM 身份 (即：用户、组和角色) 附加权限策略，某些服务也支持向资源附加权限策略。

### Note

账户管理员 (或管理员用户) 是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南 中的 [IAM 最佳实践](#)。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

## 主题

- [AWS WAF 资源和操作](#) (p. 88)
- [了解资源所有权](#) (p. 89)
- [管理对资源的访问](#) (p. 89)
- [指定策略元素：操作、效果、资源和委托人](#) (p. 90)
- [在策略中指定条件](#) (p. 91)

## AWS WAF 资源和操作

在 AWS WAF 中，资源是 Web ACL 和规则。AWS WAF 还支持条件，如字节匹配、IP 匹配 和大小约束。

这些资源和条件关联有唯一 Amazon 资源名称 (ARN)，如下表所示。

WAF 控制台中的名称	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>	

要允许或拒绝对 AWS WAF 资源子集的访问，请在策略的 `resource` 元素中包含资源的 ARN。AWS WAF 的 ARN 具有以下格式：

```
arn:aws:waf::account:resource/ID
```

将 *account*、*resource* 和 *ID* 变量替换为有效值。有效值如下：

- **account** : 您的 AWS 账户的 ID。您必须指定值。
- **resource** : AWS WAF 资源的类型。
- **ID** : AWS WAF 资源的 ID，或用于指示与指定 AWS 账户关联的具有指定类型的所有资源的通配符 (\*)。

例如，以下 ARN 指定账户 111122223333 的所有 Web ACL：

```
arn:aws:waf::111122223333:webacl/*
```

有关更多信息，请参阅 IAM 用户指南 中的[资源](#)。

AWS WAF 提供一组操作来处理 AWS WAF 资源。有关可用操作的列表，请参阅[操作](#)。

## 了解资源所有权

资源所有者是创建资源的 AWS 账户。也就是说，资源所有者是委托人实体 (根账户、IAM 用户或 IAM 角色) 的 AWS 账户。以下示例说明了它的工作原理：

- 如果您使用 AWS 账户的根账户凭证创建 AWS WAF 资源，则您的 AWS 账户即为该资源的所有者。
- 如果您在 AWS 账户中创建 IAM 用户并对该用户授予创建 AWS WAF 资源的权限，则该用户可以创建 AWS WAF 资源。但是，这些 AWS WAF 资源由该用户所属的 AWS 账户所有。
- 如果您在 AWS 账户中创建具有 AWS WAF 资源创建权限的 IAM 角色，则能够担任该角色的任何人都可以创建 AWS WAF 资源。这些 AWS WAF 资源由该角色所属的 AWS 账户所有。

## 管理对资源的访问

权限策略 规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

### Note

本节讨论如何在 AWS WAF 上下文中使用 IAM。它不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅[什么是 IAM？](#) (在 IAM 用户指南 中)。有关 IAM 策略语法和介绍的信息，请参阅 IAM 用户指南 中的[AWS IAM 策略参考](#)。

附加到 IAM 身份的策略称为基于身份的策略，附加到资源的策略称为基于资源的策略。AWS WAF 只支持基于身份的策略。

### 主题

- [基于身份的策略 \(IAM 策略\) \(p. 89\)](#)
- [基于资源的策略 \(p. 90\)](#)

## 基于身份的策略 (IAM 策略)

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

- 向您账户中的用户或组附加权限策略 - 账户管理员可以使用与特定用户关联的权限策略授予该用户创建 AWS WAF 资源的权限。
- 向角色附加权限策略 (授予跨账户权限) - 您可以向 IAM 角色附加基于身份的权限策略，以授予跨账户的权限。例如，账户 A 中的管理员可以创建一个角色，以向其他 AWS 账户 (如账户 B) 或某项 AWS 服务授予跨账户权限，如下所述：
  1. 账户 A 管理员可以创建一个 IAM 角色，然后向该角色附加授予其访问账户 A 中资源的权限策略。

2. 账户 A 管理员可以向将账户 B 标识为能够担任该角色的委托人的角色附加信任策略。
3. 之后，账户 B 管理员可以委派权限，指派账户 B 中的任何用户担任该角色。这样，账户 B 中的用户就可以创建或访问账户 A 中的资源了。如果您需要授予 AWS 服务权限来担任该角色，则信任策略中的委托人也可以是 AWS 服务委托人。

有关使用 IAM 委派权限的更多信息，请参阅 IAM 用户指南 中的[访问权限管理](#)。

以下示例策略授予对所有资源执行 `waf:ListRules` 操作的权限。在当前实现中，AWS WAF 对某些 API 操作不支持使用资源 ARN (也称为资源级权限) 标识特定资源，因此必须指定通配符 (\*)：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListRules",
      "Effect": "Allow",
      "Action": [
        "waf:ListRules"
      ],
      "Resource": "*"
    }
  ]
}
```

有关将基于身份的策略用于 AWS WAF 的更多信息，请参阅[为 AWS WAF 使用基于身份的策略 \(IAM 策略\) \(p. 91\)](#)。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南 中的[身份 \(用户、组和角色\)](#)。

## 基于资源的策略

其他服务 (如 Amazon S3) 还支持基于资源的权限策略。例如，您可以将策略附加到 S3 存储桶以管理对该存储桶的访问权限。AWS WAF 不支持基于资源的策略。

## 指定策略元素：操作、效果、资源和委托人

对于每个 AWS WAF 资源 (请参阅[AWS WAF 资源和操作 \(p. 88\)](#))，该服务都定义了一组 API 操作 (请参阅[AWS WAF API 权限：操作、资源和条件参考 \(p. 95\)](#))。为授予这些 API 操作的权限，AWS WAF 定义了一组您可以在策略中指定的操作。请注意，执行某项 API 操作可能需要执行多个操作的权限。在授予特定操作的权限时，您也可以标识允许或拒绝对其执行操作的资源。

以下是最基本的策略元素：

- Resource - 在策略中，您可以使用 Amazon 资源名称 (ARN) 标识策略应用到的资源。有关更多信息，请参阅[AWS WAF 资源和操作 \(p. 88\)](#)。
- Action - 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，`waf:CreateRule` 权限允许执行 AWS WAF `CreateRule` 操作的用户权限。
- Effect - 用于指定当用户请求特定操作时的效果。可以是允许或拒绝。如果没有显式授予允许资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- Principal - 在基于身份的策略 (IAM 策略) 中，附加了策略的用户是隐式委托人。AWS WAF 不支持基于资源的策略。

有关 IAM 策略语法和介绍的更多信息，请参阅 IAM 用户指南 中的[AWS IAM 策略参考](#)。

有关显示所有 AWS WAF API 操作及其适用的资源的表，请参阅[AWS WAF API 权限：操作、资源和条件参考 \(p. 95\)](#)。



## 在策略中指定条件

当您授予权限时，可使用 IAM 策略语言来指定规定策略何时生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅 IAM 用户指南 中的 [条件](#)。

要表示条件，您可以使用预定义的条件键。没有特定于 AWS WAF 的条件键。但有 AWS 范围内的条件密钥，您可以根据需要使用。有关 AWS 范围内的键的完整列表，请参阅 IAM 用户指南 中的 [条件的可用键](#)。

## 为 AWS WAF 使用基于身份的策略 (IAM 策略)

本主题提供了基于身份的策略的示例，这些示例展示了账户管理员如何将权限策略附加到 IAM 身份 (即用户、组和角色)，从而授予对 AWS WAF 资源执行操作的权限。

### Important

我们建议您首先阅读以下介绍性主题，这些主题讲解了管理 AWS WAF 资源访问的基本概念和选项。有关更多信息，请参阅 [AWS WAF 资源访问权限管理概述](#) (p. 88)。

下面显示了一个示例权限策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateFunctionPermissions",
      "Effect": "Allow",
      "Action": [
        "waf:ListWebACLs",
        "waf:ListRules",
        "waf:GetWebACL",
        "waf:GetRule",
        "cloudwatch:ListMetrics",
        "waf:GetSampledRequests"
      ],
      "Resource": "*"
    },
    {
      "Sid": "PermissionToPassAnyRole",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::account-id:role/*"
    }
  ]
}
```

该策略包含两条语句：

- 第一条语句使用 `waf:ListWebACLs`、`waf:ListRules`、`waf:GetWebACL`、`waf:GetRule`、`cloudwatch:ListMetrics` 和 `waf:GetSampledRequests` 操作授予查看 AWS WAF Web ACL 的统计数据的权限。对于这些操作中的某些操作，AWS WAF 不支持资源级别的权限。因此，该策略指定通配符 (\*) 作为 Resource 值。
- 第二条语句授予对 IAM 角色的 IAM 操作 `iam:PassRole` 权限。Resource 值末尾的通配符 (\*) 表示该语句允许对任何 IAM 角色的 `iam:PassRole` 操作权限。要将这些权限限制到特定角色，请使用特定角色名称替换资源 ARN 中的通配符 (\*)。

该策略没有指定 Principal 元素，因为在基于身份的策略中，您不会指定获取权限的委托人。附加了策略的用户是隐式委托人。向 IAM 角色附加权限策略后，该角色的信任策略中标识的委托人将获取权限。



有关显示所有 AWS WAF API 操作及其适用的资源的表，请参阅 [AWS WAF API 权限：操作、资源和条件参考 \(p. 95\)](#)。

## 主题

- [使用 AWS WAF 控制台所需的权限 \(p. 92\)](#)
- [适用于 AWS WAF 的 AWS 托管 \(预定义\) 策略 \(p. 92\)](#)
- [客户托管策略示例 \(p. 92\)](#)

## 使用 AWS WAF 控制台所需的权限

AWS WAF 控制台为您提供了一个创建和管理 AWS WAF 资源的集成环境。此控制台提供了许多功能和工作流，通常需要创建 AWS WAF 资源的权限以及 [AWS WAF API 权限：操作、资源和条件参考 \(p. 95\)](#) 中所述特定于 API 的权限。有关这些附加控制台权限的更多信息，请参阅 [客户托管策略示例 \(p. 92\)](#)。

## 适用于 AWS WAF 的 AWS 托管 (预定义) 策略

AWS 通过提供由 AWS 创建和管理的独立 IAM 策略来解决很多常用案例。托管策略可授予常用案例的必要权限，因此，您可以免去调查都需要哪些权限的工作。有关更多信息，请参阅 IAM 用户指南 中的 [AWS 托管策略](#)。

下面的 AWS 托管策略可附加到您账户中的用户，这些托管策略特定于 AWS WAF 并按使用案例场景进行分组：

- [AWSWAFReadOnlyAccess](#) - 授予对 AWS WAF 资源的只读访问权限。
- [AWSWAFFullAccess](#) - 授予对 AWS WAF 资源的完全访问权限。

### Note

您可以通过登录到 IAM 控制台并在该控制台中搜索特定策略来查看这些权限策略。

您也可以创建自己的自定义 IAM 策略，以允许用于 AWS WAF API 操作和资源的相关权限。您可以将这些自定义策略附加到需要上述权限的 IAM 用户和组或您为 AWS WAF 资源创建的自定义执行角色 (IAM 角色)。

## 客户托管策略示例

此部分中的示例提供了一组可附加到用户的示例策略。如果您是首次创建策略，建议您先在账户中创建 IAM 用户，并按本节操作步骤所述顺序将策略附加到该用户。

在将每个策略附加到用户时，可使用控制台验证该策略的效果。最初，用户没有权限并且无法在控制台中执行任何操作。在将策略附加到用户时，可以验证用户是否能在控制台中执行各种操作。

建议您使用两个浏览器窗口：一个浏览器窗口用于创建用户和授予权限，另一个浏览器窗口用于使用用户凭证登录 AWS 管理控制台，并在向用户授予权限时验证这些权限。

有关说明如何创建可用作 AWS WAF 资源执行角色的 IAM 角色的示例，请参阅 IAM 用户指南 中的 [创建 IAM 角色](#)。

## 示例主题

- [示例 1：向用户授予对 AWS WAF、CloudFront 和 CloudWatch 的只读访问权限 \(p. 93\)](#)
- [示例 2：向用户授予对 AWS WAF、CloudFront 和 CloudWatch 的完全访问权限 \(p. 93\)](#)
- [示例 3：向指定 AWS 账户授予访问权限 \(p. 94\)](#)

- [示例 4：向指定 Web ACL 授予访问权限 \(p. 94\)](#)

## 创建 IAM 用户

首先，您需要创建一个 IAM 用户，将该用户添加到具有管理权限的 IAM 组，然后向您创建的 IAM 用户授予管理权限。随后，您可以使用专用 URL 和该用户的凭证访问 AWS。

有关说明，请参阅 IAM 用户指南 中的 [创建您的第一个 IAM 用户和管理员组](#)。

## 示例 1：向用户授予对 AWS WAF、CloudFront 和 CloudWatch 的只读访问权限

以下策略向用户授予对 AWS WAF 资源、对 Amazon CloudFront Web 分配以及对 Amazon CloudWatch 指标的只读访问权限。对于需要权限查看 AWS WAF 条件、规则和 Web ACL 中的设置、了解与 Web ACL 关联的分配以及在 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 AWS WAF 资源：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "waf:Get*",
        "waf:List*",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

## 示例 2：向用户授予对 AWS WAF、CloudFront 和 CloudWatch 的完全访问权限

以下策略使用户可以执行任何 AWS WAF 操作、对 CloudFront Web 分配执行任何操作以及在 CloudWatch 中监控指标和请求示例。它对作为 AWS WAF 管理员的用户十分有用：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "waf:*",
        "cloudfront:CreateDistribution",
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:UpdateDistribution",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront>DeleteDistribution",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "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 中的 [在 AWS 上使用 Multi-Factor Authentication \(MFA\) 设备](#)。

### 示例 3：向指定 AWS 账户授予访问权限

此策略向账户 444455556666 授予以下权限：

- 对所有 AWS WAF 操作和资源的完全访问权限。
- 对所有 CloudFront 分配的读取和更新访问权限，这使您可以关联 Web ACL 和 CloudFront 分配。
- 对所有 CloudWatch 指标和指标统计数据的读取访问权限，以便您可以在 AWS WAF 控制台中查看 CloudWatch 数据和请求示例。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:*"
      ],
      "Resource": [
        "arn:aws:waf::444455556666:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudfront:GetDistribution",
        "cloudfront:GetDistributionConfig",
        "cloudfront:ListDistributions",
        "cloudfront:ListDistributionsByWebACLId",
        "cloudfront:UpdateDistributions",
        "cloudwatch:ListMetrics",
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

### 示例 4：向指定 Web ACL 授予访问权限

此策略向账户 444455556666 中的 webacl ID 112233d7c-86b2-458b-af83-51c51example 授予以下权限：

- 对 AWS WAF Get、Update 和 Delete 操作和资源的完全访问权限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "waf:*"
      ],
      "Resource": [
```

```
        "arn:aws:waf::444455556666:webacl/112233d7c-86b2-458b-af83-51c51example"  
      ]  
    }  
  ]  
}
```

## AWS WAF API 权限：操作、资源和条件参考

在设置 [访问控制](#) (p. 87) 和编写您可挂载到 IAM 身份的权限策略 (基于身份的策略) 时，可以使用下表作为参考。该表列出了每个 AWS WAF API 操作、您可授予执行权限的对应操作以及您可为之授予权限的 AWS 资源。您可以在策略的 Action 字段中指定这些操作，并在策略的 Resource 字段中指定资源值。

您可以在 AWS WAF 策略中使用 AWS 范围的条件键来表达条件。有关 AWS 范围内的键的完整列表，请参阅 IAM 用户指南 中的 [条件的可用键](#)。

### Note

要指定操作，请在 API 操作名称之前使用 waf: 前缀 (例如，waf:CreateIPSet)。

### AWS WAF API 和必需的操作权限

#### CreateByteMatchSet

操作：waf:CreateByteMatchSet

资源：

全局性 (适用于 Amazon CloudFront)：arn:aws:waf::*account-id*:*bytematchset/entity-ID*

区域性 (适用于 应用程序负载均衡器)：arn:aws:waf-regional:region:*account-id*:*bytematchset/entity-ID*

#### CreateIPSet

操作：waf:CreateIPSet

资源：

全局性 (适用于 Amazon CloudFront)：arn:aws:waf::*account-id*:*ipset/entity-ID*

区域性 (适用于 应用程序负载均衡器)：arn:aws:waf-regional:region:*account-id*:*ipset/entity-ID*

#### CreateRule

操作：waf:CreateRule

资源：

全局性 (适用于 Amazon CloudFront)：arn:aws:waf::*account-id*:*rule/entity-ID*

区域性 (适用于 应用程序负载均衡器)：arn:aws:waf-regional:region:*account-id*:*rule/entity-ID*

#### CreateRateBasedRule

操作：waf:CreateRateBasedRule

资源：

全局性 (适用于 Amazon CloudFront)：arn:aws:waf::*account-id*:*rule/entity-ID*

区域性 (适用于 应用程序负载均衡器)：arn:aws:waf-regional:region:*account-id*:*rule/entity-ID*

### CreateSizeConstraintSet

操作 : waf:CreateSizeConstraintSet

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sizeconstraintset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sizeconstraintset/entity-ID`

### CreateSqlInjectionMatchSet

操作 : waf:CreateSqlInjectionMatchSet

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sqlinjectionmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sqlinjectionmatchset/entity-ID`

### CreateWebACL

操作 : waf:CreateWebACL

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:webacl/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:webacl/entity-ID`

### CreateXssMatchSet

操作 : waf:CreateXssMatchSet

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:xssmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:xssmatchset/entity-ID`

### DeleteByteMatchSet

操作 : waf>DeleteByteMatchSet

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:bytematchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:bytematchset/entity-ID`

### DeleteIPSet

操作 : waf>DeleteIPSet

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:ipset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:ipset/entity-ID`

#### DeleteRule

操作 : `waf:DeleteRule`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### DeleteRateBasedRule

操作 : `waf:DeleteRateBasedRule`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### DeleteSizeConstraintSet

操作 : `waf:DeleteSizeConstraintSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sizeconstraintset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sizeconstraintset/entity-ID`

#### DeleteSqlInjectionMatchSet

操作 : `waf:DeleteSqlInjectionMatchSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sqlinjectionmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sqlinjectionmatchset/entity-ID`

#### DeleteWebACL

操作 : `waf:DeleteWebACL`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:webacl/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:webacl/entity-ID`

#### DeleteXssMatchSet

操作 : `waf:DeleteXssMatchSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:xssmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:xssmatchset/entity-ID`

#### GetByteMatchSet

操作 : `waf:GetByteMatchSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:bytematchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:bytematchset/entity-ID`

#### GetChangeToken

操作 : `waf:GetChangeToken`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:changetoken/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:changetoken/entity-ID`

#### GetChangeTokenStatus

操作 : `waf:GetChangeTokenStatus`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:changetoken/token-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:changetoken/token-ID`

#### GetIPSet

操作 : `waf:GetIPSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:ipset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:ipset/entity-ID`

#### GetRule

操作 : `waf:GetRule`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### GetRateBasedRule

操作 : `waf:GetRateBasedRule`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`



区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### GetRateBasedRuleManagedKeys

操作 : `waf:GetRateBasedRuleManagedKeys`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### GetSampledRequests

操作 : `waf:GetSampledRequests`

资源 : 资源取决于 API 调用中指定的参数。您必须有权访问与针对示例的请求对应的规则或 webacl。例如 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/example1` or  
`arn:aws:waf::account-id:webacl/example2`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/example1` or  
`arn:aws:waf-regional:region:account-id:webacl/example2`

#### GetSizeConstraintSet

操作 : `waf:GetSizeConstraintSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sizeconstraintset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sizeconstraintset/entity-ID`

#### GetSqlInjectionMatchSet

操作 : `waf:GetSqlInjectionMatchSet`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sqlinjectionmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sqlinjectionmatchset/entity-ID`

#### GetWebACL

操作 : `waf:GetWebACL`

资源 :

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:webacl/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:webacl/entity-ID`

#### GetXssMatchSet

操作 : `waf:GetXssMatchSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:xssmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:xssmatchset/entity-ID`

#### ListByteMatchSets

操作 : `waf:ListByteMatchSets`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:bytematchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:bytematchset/entity-ID`

#### ListIPSets

操作 : `waf:ListIPSets`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:ipset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:ipset/entity-ID`

#### ListRules

操作 : `waf:ListRules`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### ListRateBasedRules

操作 : `waf:ListRateBasedRules`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### ListSizeConstraintSets

操作 : `waf:ListSizeConstraintSets`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sizeconstraintset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sizeconstraintset/entity-ID`

#### ListSqlInjectionMatchSets

操作 : `waf:ListSqlInjectionMatchSets`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sqlinjectionmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sqlinjectionmatchset/entity-ID`

#### ListWebACLs

操作 : `waf:ListWebACLs`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:webacl/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:webacl/entity-ID`

#### ListXssMatchSets

操作 : `waf:ListXssMatchSets`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:xssmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:xssmatchset/entity-ID`

#### UpdateByteMatchSet

操作 : `waf:UpdateByteMatchSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:bytematchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:bytematchset/entity-ID`

#### UpdateIPSet

操作 : `waf:UpdateIPSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:ipset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:ipset/entity-ID`

#### UpdateRule

操作 : `waf:UpdateRule`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### UpdateRateBasedRule

操作 : `waf:UpdateRateBasedRule`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:rule/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:rule/entity-ID`

#### UpdateSizeConstraintSet

操作 : `waf:UpdateSizeConstraintSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sizeconstraintset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sizeconstraintset/entity-ID`

#### UpdateSqlInjectionMatchSet

操作 : `waf:UpdateSqlInjectionMatchSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:sqlinjectionmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:sqlinjectionmatchset/entity-ID`

#### UpdateWebACL

操作 : `waf:UpdateWebACL`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:webacl/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:webacl/entity-ID`

#### UpdateXssMatchSet

操作 : `waf:UpdateXssMatchSet`

资源：

全局性 (适用于 Amazon CloudFront) : `arn:aws:waf::account-id:xssmatchset/entity-ID`

区域性 (适用于 应用程序负载均衡器) : `arn:aws:waf-regional:region:account-id:xssmatchset/entity-ID`

## AWS WAF 限制

AWS WAF 对每个账户的实体数施加了默认限制。您可以[请求提高](#)这些限制。

资源	默认限制
每个 AWS 账户的 Web ACL 数	50
每个 AWS 账户的规则数	100

资源	默认限制
每个 AWS 账户的基于速率的规则	5
每个 AWS 账户的条件数	每种条件类型 100 个 (例如：100 个大小约束条件、100 个 IP 匹配条件等。例外情况是正则表达式匹配条件。每个账户最多可以具有 10 个正则表达式匹配条件。不能提高此限制。)
每秒请求数	每个 web ACL 10,000 个*

\*此限制仅适用于 应用程序负载均衡器 上的 AWS WAF。CloudFront 上的 AWS WAF 的每秒请求数 (RPS) 限制与 [CloudFront 开发人员指南](#) 中描述的 CloudFront 支持的 RPS 限制相同。

无法更改 AWS WAF 实体的以下限制。

资源	限制
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
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	2000
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
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 AWS WAF 配置为在 Web 请求标头中检查指定值)	40
在字符串匹配条件中，您需要 AWS WAF 搜索的值中的字符数	50
在正则表达式匹配条件中，您需要 AWS WAF 搜索的模式中的字符数	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
每个账户的模式集数	5
每个账户的 GeoMatchSets	50
每个 GeoMatchSet 的位置	50

# AWS Firewall Manager

AWS Firewall Manager 可简化跨多个账户和多种资源的 AWS WAF 管理和维护任务。利用 Firewall Manager，您只需设置您的防火墙规则一次。该服务会跨您的账户和资源自动应用规则，即使您添加了新资源。

Firewall Manager 提供了以下优势：

- 有助于跨账户保护资源
- 有助于保护某个特定类型的所有资源，如所有 Amazon CloudFront 分配
- 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
- 让您可以使用自己的自定义规则或从 AWS Marketplace 购买托管规则

当您有大量要通过 AWS WAF 保护的资源时，或者如果您经常添加要保护的新资源，Firewall Manager 会非常有用。

要使用 Firewall Manager，请将规则添加到规则组，然后将规则组添加到某个策略。Firewall Manager 在 AWS Organizations 中将策略应用于您在组织内的所有账户中指定的资源类型（如 CloudFront 分配或 Application Load Balancer）。如果您将新账户添加到您的组织，Firewall Manager 会将该策略自动应用于该账户中的指定资源。

主题

- [AWS Firewall Manager 定价 \(p. 104\)](#)
- [AWS Firewall Manager 先决条件 \(p. 104\)](#)
- [AWS Firewall Manager 入门 \(p. 106\)](#)
- [AWS Firewall Manager 限制 \(p. 108\)](#)
- [使用规则组 \(p. 108\)](#)
- [使用 AWS Firewall Manager 策略 \(p. 110\)](#)
- [查看资源的策略合规性 \(p. 111\)](#)
- [指定另一个账户作为 AWS Firewall Manager 管理员账户 \(p. 112\)](#)

## AWS Firewall Manager 定价

AWS Firewall Manager 会对您创建的 AWS WAF Web ACL 和规则以及一些相关服务计费。有关更多信息，请参阅 [AWS Firewall Manager 定价](#)。

## AWS Firewall Manager 先决条件

本主题介绍如何为您的账户做好使用 AWS Firewall Manager 的准备。在首次使用 Firewall Manager 之前，请按顺序执行以下所有步骤。

主题

- [步骤 1：加入 AWS Organizations \(p. 105\)](#)

- [步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)
- [步骤 3：启用 AWS Config \(p. 105\)](#)

## 步骤 1：加入 AWS Organizations

要使用 AWS Firewall Manager，您的账户必须是 AWS Organizations 服务中的组织的成员。如果您的账户已经是成员，则可以跳过此步骤并转到[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

### Note

AWS 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，您所属的组织必须启用[所有功能](#)。如果仅针对整合账单配置了您的组织，请参阅[启用组织中的所有功能](#)。

如果您的账户不是组织的一部分，请按照[创建和管理 AWS Organizations](#) 中所述创建或加入组织。

在您的账户成为组织的成员后，请转到[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

## 步骤 2：设置 AWS Firewall Manager 管理员账户

AWS Firewall Manager 必须与您的 AWS 组织的主账户或与具有适当权限的成员账户关联。与 Firewall Manager 关联的账户称为“Firewall Manager 管理员账户”。

有关 AWS Organizations 和主账户的更多信息，请参阅[管理您组织中的 AWS 账户](#)。

设置 Firewall Manager 管理员账户 (控制台)

1. 使用现有的 AWS Organizations 主账户登录 AWS 管理控制台。您可以使用该账户的根用户 (不推荐) 或该账户内具有同等权限的其他 IAM 用户或 IAM 角色登录。
2. 通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。
3. 选择 Get started。
4. 键入要与 Firewall Manager 关联的账户 ID。这将是 Firewall Manager 管理员账户。账户 ID 可以是您用来登录的账户，也可以是其他账户。如果您键入的账户 ID 不是 AWS Organizations 主账户，Firewall Manager 会为您指定的成员账户设置适当的权限。

### Note

您在此步骤中输入的账户获得了跨您组织内的所有账户创建和管理 AWS WAF 规则的权限。

5. 选择 Set administrator (设置管理员)。

在设置 AWS Firewall Manager 管理员账户后，请转到[步骤 3：启用 AWS Config \(p. 105\)](#)。

## 步骤 3：启用 AWS Config

为您的 AWS 组织中的每个成员账户启用 AWS Config。有关更多信息，请参阅[AWS Config 入门](#)。

您必须为包含要保护的资源的每个 AWS 区域启用 AWS Config。您可以手动启用 AWS Config，也可以使用[AWS CloudFormation StackSets 示例模板](#)中的 AWS CloudFormation 模板“启用 AWS Config”。

您必须至少指定以下要通过 AWS Firewall Manager 保护的资源类型：应用程序负载均衡器 和/或 CloudFront 分配。

当启用 AWS Config 来保护 应用程序负载均衡器 时，所提供的资源类型列表中选择 ElasticLoadBalancingV2。



当启用 AWS Config 来保护 CloudFront 分配时，您必须在 美国东部（弗吉尼亚北部）区域中。其他区域将不会有 CloudFront 作为选项。

您现在可以将 AWS Firewall Manager 配置为开始保护您的资源。有关更多信息，请参阅[AWS Firewall Manager 入门 \(p. 106\)](#)。

## AWS Firewall Manager 入门

本主题介绍如何开始使用 AWS Firewall Manager。请按顺序执行以下步骤。

### 主题

- [步骤 1：完成前提条件 \(p. 106\)](#)
- [步骤 2：创建规则 \(p. 106\)](#)
- [步骤 3：创建规则组 \(p. 106\)](#)
- [步骤 4：创建并应用 AWS Firewall Manager 策略 \(p. 107\)](#)

## 步骤 1：完成前提条件

为 AWS Firewall Manager 准备您的账户有几个必要步骤。[AWS Firewall Manager 先决条件 \(p. 104\)](#)中介绍了这些步骤。在继续执行[步骤 2：创建规则 \(p. 106\)](#)之前，请满足所有先决条件后。

## 步骤 2：创建规则

在本步骤中，您将使用 AWS WAF 创建规则。如果您已经有要用于 AWS Firewall Manager 的 AWS WAF 规则，请跳过本步骤并转到[步骤 3：创建规则组 \(p. 106\)](#)。

### 创建 AWS WAF 规则 (控制台)

1. 创建您的条件。有关更多信息，请参阅[使用条件 \(p. 47\)](#)。
2. 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[创建规则和添加条件 \(p. 73\)](#)。

您现在已准备好转到[步骤 3：创建规则组 \(p. 106\)](#)。

## 步骤 3：创建规则组

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。您可以从 AWS Marketplace 购买托管规则组，也可以创建自己的规则组。

要从 AWS Marketplace 购买托管规则组，请参阅[AWS Marketplace Rule Groups \(p. 75\)](#)。

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)

1. 使用您在先决条件中设置的 AWS Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。
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。

5. 选择 Create an AWS Firewall Manager policy and add a new rule group (创建 AWS Firewall Manager 策略并添加新规则组)。
6. 选择一个 AWS 区域，然后选择 Next (下一步)。
7. 由于您已创建规则，因此无需创建条件。选择 Next。
8. 由于您已创建规则，因此无需创建规则。选择 Next。
9. 选择 Create rule group (创建规则组)。
10. 对于 Name (名称)，键入一个友好名称。
11. 为 AWS WAF 将创建并将与规则组关联的 CloudWatch 指标键入名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9) 以及以下特殊字符：\_!@#%&\*}. /。且不能包含空格。
12. 选择规则，然后选择 Add rule (添加规则)。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. 一个规则组有两个可能的操作：Block (阻止) 和 Count (计数)。如果您要测试规则组，请将操作设置为 Count (计数)。此操作会覆盖该组中包含的单个规则指定的任何阻止操作。即，如果将规则组的操作设置为 Count (计数)，则只会对请求进行计数而不会阻止它。相反，如果将规则组的操作设置为 Block (阻止)，则会使用该组中单个规则的操作。在本教程中，请选择 Count (计数)。
14. 选择 Create。

您现在已准备好转到[步骤 4：创建并应用 AWS Firewall Manager 策略 \(p. 107\)](#)。

## 步骤 4：创建并应用 AWS Firewall Manager 策略

在创建规则组后，您将创建 AWS Firewall Manager 策略。Firewall Manager 策略包含您要应用于资源的规则组。

### 创建 Firewall Manager 策略 (控制台)

1. 在创建规则组 (上述过程中的最后一步 [步骤 3：创建规则组 \(p. 106\)](#)) 后，控制台会显示 Rule group summary (规则组摘要) 页面。选择 Next。
2. 对于 Name (名称)，键入一个友好名称。
3. 对于 Region (区域)，选择一个 AWS 区域。
4. 选择要添加的规则组，然后选择 Add rule group (添加规则组)。
5. 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)。
6. 选择 Next。
7. 选择要保护的资源的类型。
8. 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)，键入标签，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](#)。

9. 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 AWS Organizations 中为组织内的每个账户创建一个 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，如果您选择了 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)，Firewall Manager 会在组织内的每个账户中创建一个 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。

10. 选择 Next。
11. 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)。

#### Note

Firewall Manager 在 AWS Organizations 中将策略应用于您组织中的所有账户。您无法包含或排除单个账户。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。

## AWS Firewall Manager 限制

AWS Firewall Manager 对每个账户的实体数施加了默认限制。您可以[请求提高](#)这些限制。

资源	默认限制
AWS Organizations 中每个组织的账户数	可变。发送到账户的邀请将计入此限制。如果受邀账户拒绝邀请、主账户取消邀请或邀请过期，则撤销此计数。
AWS Organizations 中每个组织的 Firewall Manager 策略数	20
每个 Firewall Manager 策略的包含或排除资源的标签数	8

与 AWS Firewall Manager 相关的以下限制无法更改。

资源	限制
每个 Firewall Manager 管理员账户的规则组数	3
每个 Firewall Manager 策略的规则组数	1
每个规则组的规则数	10

## 使用规则组

规则组 是您添加到 Web ACL 或 AWS Firewall Manager 策略的一组规则。您可以创建自己的规则组，也可以从 AWS Marketplace 购买托管规则组。有关更多信息，请参阅 [AWS Marketplace Rule Groups \(p. 75\)](#)。

#### Important

如果您要将一个 AWS Marketplace 规则组添加到您的策略，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 [AWS Marketplace Rule Groups \(p. 75\)](#)。

#### 主题

- [创建规则组 \(p. 109\)](#)
- [在规则组中添加和删除规则 \(p. 109\)](#)

## 创建规则组

当您创建要与 AWS Firewall Manager 结合使用的规则组时，请指定要添加到组的规则。

### 创建规则组 (控制台)

1. 使用您在先决条件中设置的 AWS Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。

#### Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

2. 在导航窗格中，选择 Rule groups (规则组)。
3. 选择 Create rule group (创建规则组)。
4. 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)。

#### Note

您不能将基于速率的规则添加到规则组。

5. 选择 Next。
6. 如果要创建新规则，请按照这些步骤操作以先后创建条件和规则。有关更多信息，请参阅[使用条件 \(p. 47\)](#)和[使用规则 \(p. 73\)](#)。如果您使用的是现有规则，请转到下一步。
7. 键入规则组名称。
8. 选择规则，然后选择 Add rule (添加规则)。重复操作以将更多规则添加到规则组。
9. 一个规则组有两个可能的操作：Block (阻止) 和 Count (计数)。如果您要测试规则组，请将操作设置为 Count (计数)。此操作会覆盖该组中包含的单个规则指定的任何阻止操作。即，如果将规则组的操作设置为 Count (计数)，则只会对请求进行计数而不会阻止它。相反，如果将规则组的操作设置为 Block (阻止)，则会使用该组中单个规则的操作。对于每个规则，请选择合适的选项。
10. 选择 Create。

## 在规则组中添加和删除规则

您可以在规则组中添加或删除规则。

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. 使用您在先决条件中设置的 Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。

#### Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

2. 在导航窗格中，选择 Rule groups (规则组)。
3. 选择要编辑的规则组。
4. 选择 Edit rule group (编辑规则组)。
5. 要添加规则，请执行以下步骤：
  - a. 选择规则，然后选择 Add another rule (再添加一条规则)。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。
6. 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。

## 使用 AWS Firewall Manager 策略

AWS Firewall Manager 策略包含您要应用于资源的规则组。规则组是一系列规则，并且每个规则包含您指定的条件。您只能对一个策略应用一个规则组，但可以对多个策略应用相同的规则组。

Firewall Manager 在 AWS Organizations 中将策略应用于您在组织内的所有账户中指定的资源类型（如 CloudFront 分配或 Application Load Balancer）。您无法从策略中排除单个账户。

如果您将新账户添加到您的组织，Firewall Manager 会将该策略自动应用于该账户中的指定资源。

#### 主题

- [创建 AWS Firewall Manager 策略 \(p. 110\)](#)
- [删除 AWS Firewall Manager 策略 \(p. 111\)](#)

## 创建 AWS Firewall Manager 策略

当您创建 AWS Firewall Manager 策略时，可指定要添加到策略的规则组。

#### 创建 Firewall Manager 策略 (控制台)

1. 使用您在先决条件中设置的 Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。

#### Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择 Create policy。
4. 如果您已创建要添加到策略的规则组，请选择 Create an AWS Firewall Manager policy and add existing rule groups (创建 AWS Firewall Manager 策略并添加现有规则组)。如果要创建新规则组，请选择 Create an AWS Firewall Manager policy and add a new rule group (创建 AWS Firewall Manager 策略并添加新规则组)。
5. 如果您使用的是现有规则组，请跳过本步骤并转到下一步。如果您要创建规则组，请按照[创建规则组 \(p. 109\)](#)中的说明操作。在创建规则组后，请继续执行以下步骤。
6. 键入策略名称。
7. 对于 Region (区域)，选择一个 AWS 区域。
8. 选择要添加的规则组，然后选择 Add rule group (添加规则组)。
9. 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。选择适当的操作。

10. 选择 Next。

11. 选择要保护的资源的类型。

您只能为每个策略选择一种资源类型。

12. 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)，键入标签，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](#)。

13. 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 AWS Organizations 中为组织内的每个账户创建一个 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，如果您选择了 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)，Firewall Manager 会在组织内的每个账户中创建一个 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。

14. 选择 Next。

15. 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)。

#### Note

Firewall Manager 在 AWS Organizations 中将策略应用于您组织中的所有账户。您无法包含或排除单个账户。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。

## 删除 AWS 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的圆圈。
3. 选择 Delete。

## 查看资源的策略合规性

您可以检查以了解正在将 AWS Firewall Manager 策略应用于的资源。

### 检查要将 Firewall Manager 策略应用于的资源 (控制台)

1. 使用您在先决条件中设置的 AWS Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。

#### Note

有关设置 Firewall Manager 管理员账户的信息，请参阅[步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。



2. 在导航窗格中，选择 Security policies (安全策略)。
3. 选择一个策略。Firewall Manager 将列出组织中的每个账户并显示相应状态。Compliant (合规) 状态表示该策略已应用于账户中的所有适用资源。Noncompliant (不合规) 状态表示该策略未应用于账户中的所有资源。
4. 选择一个账户。Firewall Manager 将列出账户中的每个资源并显示相应状态。Compliant (合规) 状态表示该策略已应用于资源。Noncompliant (不合规) 状态表示该策略未应用于资源。Firewall Manager 最多会列出 100 个不合规资源。

## 指定另一个账户作为 AWS Firewall Manager 管理员账户

要使用 AWS Firewall Manager，您必须使用 Firewall Manager 管理员账户登录控制台。您只能指定组织中的一个账户作为 Firewall Manager 管理员账户。该账户可以是 AWS Organizations 主账户或成员账户。要首次设置管理员账户，请参阅 [步骤 2：设置 AWS Firewall Manager 管理员账户 \(p. 105\)](#)。

如果您指定一个账户作为管理员账户，并且稍后希望指定另一个账户作为管理员账户，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。您随后必须使用 AWS Organizations 主账户登录 Firewall Manager 以指定新的管理员账户。

### 指定另一个账户作为 Firewall Manager 管理员账户 (控制台)

1. 使用当前 Firewall Manager 管理员账户登录 AWS 管理控制台，然后通过以下网址打开 Firewall Manager 控制台：<https://console.aws.amazon.com/waf/fms>。
2. 在导航窗格中，选择 Settings。
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. 从 AWS 管理控制台注销。
5. 使用您的 AWS Organizations 主账户登录 AWS 管理控制台。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.aws.amazon.com/waf/fms>。
7. 选择 Get started。
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。它可以是您用来登录的主账户，也可以是您组织中的成员账户。如果您键入的账户 ID 是成员账户而不是主账户，Firewall Manager 将为成员账户设置适当的权限。

### Note

该账户获得了跨组织内的所有账户创建和管理 AWS WAF 规则的权限。

9. 选择 Set administrator (设置管理员)。

## 关闭 AWS Firewall Manager 管理员账户

如果您在未事先撤销 AWS Firewall Manager 管理员账户 (如上面第 3 步所述) 的情况下关闭该账户，则：



- AWS 将从 Firewall Manager 撤消账户的管理员访问权限。在 AWS 从 Firewall Manager 撤消账户的管理员访问权限后，应用于以前由该管理员账户管理的任何账户的所有 Firewall Manager 策略都将被停用，并且此类策略保护将不再应用于任何这些账户。
- AWS 将在管理员账户关闭生效之日起 90 天内保留该账户的 Firewall Manager 策略数据。如果您在这 90 天窗口期内选择重新打开先前关闭的账户，AWS 将重新分配该账户作为 Firewall Manager 管理员并恢复该账户以前的 Firewall Manager 策略数据。
- 在 90 天窗口期结束后，如果未重新打开已关闭的账户，AWS 将永久删除该账户的所有 Firewall Manager 策略数据。

# AWS Shield

为防范 DDoS 攻击，AWS 提供了 AWS Shield Standard 和 AWS Shield Advanced。AWS Shield Standard 是自动包含的，除了已为 AWS WAF 和其他 AWS 服务支付的费用外，无任何附加成本。为了针对 DDoS 攻击获得附加保护，AWS 提供了 AWS Shield Advanced。AWS Shield Advanced 可为您的 Amazon EC2 实例、Elastic Load Balancing 负载均衡器、CloudFront 分配和 Route 53 托管区域提供扩展的 DDoS 攻击保护。

## 主题

- [AWS Shield 的工作原理 \(p. 114\)](#)
- [AWS Shield Advanced 使用案例示例 \(p. 118\)](#)
- [AWS Shield Advanced 定价 \(p. 118\)](#)
- [AWS Shield Advanced 入门 \(p. 119\)](#)
- [向更多 AWS 资源添加 AWS Shield Advanced 防护 \(p. 122\)](#)
- [从 AWS 资源中删除 AWS Shield Advanced \(p. 123\)](#)
- [编辑 AWS Shield Advanced 设置 \(p. 123\)](#)
- [AWS Shield Advanced：请求服务抵扣金额 \(p. 123\)](#)
- [AWS Shield Advanced 限制 \(p. 124\)](#)

## AWS Shield 的工作原理

分布式拒绝服务 (DDoS) 攻击是指多个被入侵系统尝试用流量来“淹没”目标 (如网络或 Web 应用程序) 的攻击。DDoS 攻击会阻止合法用户访问服务，并且可能导致系统因流量过大而崩溃。

AWS 针对 DDoS 攻击提供两种级别的防护：AWS Shield Standard 和 AWS Shield Advanced。

## AWS Shield Standard

所有 AWS 客户都可从 AWS Shield Standard 的自动防护功能中获益，不需要额外支付费用。AWS Shield Standard 可以抵御以您的网站或应用程序为目标的最为常见、经常发生的网络和传输层 DDoS 攻击。虽然 AWS Shield Standard 有助于为所有 AWS 客户提供保护，但如果您使用 Amazon CloudFront 和 Amazon Route 53，则可以获得特殊的优势。这些服务获得全面的可用性保护，可以防范所有已知的基础设施 (第 3 层和第 4 层) 攻击。

## AWS Shield Advanced

要针对运行在 Amazon EC2、Elastic Load Balancing (ELB)、CloudFront 和 Route 53 资源上的 Web 应用程序提高抵御攻击的防范级别，您可以订阅 AWS Shield Advanced。AWS Shield Advanced 针对这些资源提供扩展的 DDoS 攻击保护。

作为此添加保护的示例，如果您使用 Shield Advanced 保护弹性 IP 地址，在攻击期间，Shield Advanced 将自动将您的网络 ACL 部署到 AWS 网络边界，可以允许 Shield Advanced 提供保护应对更严重的 DDoS 事件。通常情况下，网络 ACL 会应用到您 Amazon VPC 中的 Amazon EC2 实例附近。网络 ACL 只可缓解您的 Amazon VPC 和实例可以处理的攻击。例如，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 的卷将会减速并可能阻止通往此实例的流量。在攻击期间，Shield Advanced 会将您的网络 ACL 提升至 AWS 边界以处理多个 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](#)。

作为 AWS Shield Advanced 客户，您可以在 DDoS 攻击期间联系 24x7 全天候 DDoS 响应团队 (DRT)，以寻求帮助。您还可以独占访问高级、实时的指标和报告，以深入了解您的 AWS 资源遭受的攻击。借助 DRT 的帮助，AWS Shield Advanced 可提供智能 DDoS 攻击检测和缓解功能，这些功能不仅适用于网络层 (第 3 层) 和传输层 (第 4 层) 攻击，还适用于应用程序层 (第 7 层) 攻击。

AWS Shield Advanced 还针对您的 AWS 账单中可能由 DDoS 攻击导致的高峰提供一些成本保护。此成本保护针对您的 Elastic Load Balancing 负载均衡器、CloudFront 分配、Route 53 托管区域和 Amazon EC2 实例提供。

AWS WAF 随 AWS Shield Advanced 提供，没有任何额外成本。有关 AWS Shield Advanced 定价的更多信息，请参阅 [AWS Shield Advanced 定价](#)。

## DDoS 攻击的类型

AWS Shield Advanced 针对多种类型的攻击提供大范围的保护。例如：

### 用户数据报协议 (UDP) 反射攻击

攻击者能够仿冒请求来源，并使用 UDP 从服务器引出高流量的响应。转向被仿冒和攻击的 IP 地址的额外网络流量会拖慢目标服务器，并阻止合法用户访问所需资源。

### SYN 泛洪

SYN 泛洪攻击的目的是通过将连接保持在半开放状态来耗尽系统的可用资源。当用户连接到 TCP 服务 (如 Web 服务器) 时，客户端将发送 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 SYN 泛洪中，永远不会返回第三个确认，服务器将一直等待响应。这会使其他用户无法连接到服务器。

### DNS 查询泛洪

在 DNS 查询泛洪中，攻击者使用多个 DNS 查询来耗尽 DNS 服务器的资源。AWS Shield Advanced 可以帮助抵御针对 Route 53 DNS 服务器上 DNS 查询泛洪攻击。

### HTTP 泛洪/缓存清除 (第 7 层) 攻击

借助 HTTP 泛洪 (包括 GET 和 POST 泛洪)，攻击者可以发送看似来自 Web 应用程序的真实用户的多个 HTTP 请求。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。

## 关于 AWS DDoS 响应团队 (DRT)

使用 AWS Shield Advanced 时，复杂的 DDoS 事件可上报至 AWS DDoS 响应团队 (DRT)，DRT 在保护 AWS、Amazon.com 及其子公司方面拥有丰富经验。

对于第 3 层和第 4 层攻击，AWS 会提供自动攻击检测并代表您主动应用缓解措施。对于第 7 层 DDoS 攻击，AWS 会尝试检测并通过 CloudWatch 警报通知 AWS Shield Advanced 客户，但不主动应用缓解措施。这是为了避免意外丢掉有效的用户流量。

您也可以在可能的攻击前或在攻击期间联系 DRT，以便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 DRT 一起预先配置一个 ACL，只“允许”打开端口 80 和 443。

AWS Shield Advanced 客户有两个选项可用于缓解第 7 层攻击：

- 提供您自己的缓解措施：AWS WAF 随 AWS Shield Advanced 提供，没有任何额外成本。您可以创建自己的 AWS WAF 规则以缓解 DDoS 攻击。AWS 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 AWS WAF 规则，设计用于阻止基于 Web 的常见攻击。您可以通过自定义这些模板来满足自己的业务需求。有关更多信息，请参阅 [AWS WAF 安全自动化](#)。

在这种情况下，不涉及 DRT。但是，您可以咨询 DRT，以便在实施最佳实践 (如 AWS WAF 常见防护) 方面获得指导。

- 咨询 DRT：如果您需要在应对攻击时获得更多支持，可以联系 [AWS Support Center](#)。重大和紧急案例将直接转给 DDoS 专家。使用 AWS Shield Advanced 时，复杂案例可上报至 DRT，DRT 在保护

AWS、Amazon.com 及其子公司方面拥有丰富的经验。如果您是 AWS Shield Advanced 客户，您还可以征求对高严重性案例的特殊处理指导。

对您的案例的响应时间取决于您选择的严重性以及 [AWS Support 计划](#) 页面中记录的响应时间。

DRT 可帮助您筛选 DDoS 攻击，以识别攻击签名和模式。经您同意后，DRT 将创建并部署用于缓解攻击的 AWS WAF 规则。

当 AWS Shield Advanced 检测到针对您的应用程序发起的大型第 7 层攻击时，DRT 可能会主动与您联系。DRT 会筛选 DDoS 事件并创建 AWS WAF 缓解操作。然后 DRT 会联系您，请求您同意应用 AWS WAF 规则。

#### Important

DRT 可帮助您分析可疑活动，并帮助您缓解问题。这种缓解通常需要 DRT 在您的账户中创建或更新 Web 访问控制列表 (Web ACL)。但是，他们需要您的授权才能执行此操作。建议您在启用 AWS Shield Advanced 的过程中，按照 [步骤 3：\(可选\) 向 DDoS 响应团队授权 \(p. 120\)](#) 中的步骤主动向 DRT 提供所需权限。提前提供权限有助于防止在实际发生攻击时耽误问题的解决。

## 帮我选择一个防护计划

在许多情况下，AWS Shield Standard 防护足以满足您的需求。AWS 服务和技术的构建方式能够在抵抗多数常见 DDoS 攻击时提供恢复弹性能力。用 AWS WAF 及其他 AWS 服务的组合作为深度防御策略来补充此内置防护可提供足够的攻击防护和缓解能力。此外，如果您拥有专业技术知识，并希望完全控制第 7 层攻击的监控和缓解，AWS Shield Standard 可能是合适的选择。有关可帮助您设计自己的 DDoS 防护的其他资源，请参阅我们的 [教程 \(p. 18\)](#)。

如果您的企业或行业是 DDoS 攻击的潜在目标，或者您希望让 AWS 负责第 3 层、第 4 层和第 7 层攻击的大多数 DDoS 防护和缓解职责，AWS Shield Advanced 可能是最佳选择。AWS Shield Advanced 不仅提供第 3 层和第 4 层防护和缓解，还包括无任何附加费用的 AWS WAF 以及面向第 7 层攻击的 DRT 帮助。如果您使用 AWS WAF 和 AWS Shield Standard，则必须设计自己的第 7 层防护和缓解流程。

AWS Shield Advanced 客户还能查看针对其 AWS 资源的 DDoS 攻击的详细信息，这很有好处。虽然 AWS Shield Standard 会针对最常见的第 3 层和第 4 层攻击提供自动防护，但查看这些攻击的详细信息时会受到限制。AWS Shield Advanced 为您提供关于第 3 层、第 4 层和第 7 层 DDoS 攻击的详细数据。

AWS Shield Advanced 还可针对以 AWS 资源为目标的 DDoS 攻击提供成本保护。这项重要功能有助于防止在您的账单中出现由 DDoS 攻击引起的意外高峰。如果成本可预测性对您而言很重要，AWS Shield Advanced 可提供该稳定性。

下表显示 AWS Shield Standard 与 AWS Shield Advanced 的比较。

功能	AWS Shield Standard	AWS Shield Advanced
活动监控		
网络流量监控	是	是
自动始终开启检测	是	是
自动化应用程序 (第 7 层) 流量监控		是
DDoS 缓解		
有助于防范常见的 DDoS 攻击，如	是	是

AWS WAF、AWS Firewall Manager 和  
AWS Shield Advanced 开发人员指南  
帮我选择一个防护计划

功能	AWS Shield Standard	AWS Shield Advanced
SYN 泛洪和 UDP 反射攻击		
对其它 DDoS 缓解容量的访问权限，包括在攻击期间网络 ACL 到 AWS 边界的自动部署。		是
自定义应用程序层 (第 7 层) 缓解	是，通过用户创建的 AWS WAF ACL。产生标准 AWS WAF 费用。	是，通过用户创建或 DRT 创建的 AWS WAF ACL。作为 AWS Shield Advanced 订阅的一部分提供。
即时规则更新	是，通过用户创建的 AWS WAF ACL。产生标准 AWS WAF 费用。	是
用于应用程序漏洞保护的 AWS WAF	是，通过用户创建的 AWS WAF ACL。产生标准 AWS WAF 费用。	是
可见性和报告		
第 3/4 层攻击通知		是
第 3/4 层攻击取证报告 (源 IP、攻击媒介等)		是
第 7 层攻击通知	是，通过 AWS WAF。产生标准 AWS WAF 费用。	是
第 7 层攻击取证报告 (Top talker 报告、采样请求等)	是，通过 AWS WAF。产生标准 AWS WAF 费用。	是
第 3/4/7 层攻击历史报告		是
DDoS 响应团队支持		
高严重性事件期间的事故管理		是
攻击期间的自定义缓解		是
攻击后分析		是
成本保护 (用于 DDoS 缩放费用的服务积分)		
Route 53		是
CloudFront		是

功能	AWS Shield Standard	AWS Shield Advanced
Elastic Load Balancing (ELB)		是
Amazon EC2		是

AWS Shield Advanced 权益 (包括 DDoS 成本保护) 受您履行 1 年订阅承诺的约束。

#### Note

虽然 AWS Shield Standard 和 AWS Shield Advanced 都提供针对 DDoS 攻击的强大保护功能，我们建议您还要使用 Amazon CloudWatch 和 AWS CloudTrail 来监控您的所有 AWS 服务。有关使用 CloudWatch 和 CloudTrail 监控 AWS WAF 的信息，请参阅[监控 AWS WAF](#)、[AWS Firewall Manager](#) 和 [AWS Shield Advanced \(p. 125\)](#)和[使用 AWS CloudTrail 记录 API 调用 \(p. 130\)](#)。

## AWS Shield Advanced 使用案例示例

您可以在许多类型的场景中使用 Shield Advanced 保护您的资源。但是，在某些情况下，您应使用其他服务或组合使用其他服务和 Shield Advanced 以提供最佳保护。以下是一些介绍如何使用 Shield Advanced 或其他 AWS 服务来帮助保护您的资源的示例。

目标	推荐的服务	相关服务文档
保护 Web 应用程序和 RESTful API 免受 DDoS 攻击	Shield Advanced 可保护 Amazon CloudFront 分配和 应用程序负载均衡器	<a href="#">Amazon Elastic Load Balancing 文档</a> 、 <a href="#">Amazon CloudFront 文档</a>
保护基于 TCP 的应用程序免受 DDoS 攻击	Shield Advanced 可保护附加到弹性 IP 地址的 网络负载均衡器	<a href="#">Amazon Elastic Load Balancing 文档</a>
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	<a href="#">Amazon Elastic Compute Cloud 文档</a>

## AWS Shield Advanced 定价

### AWS Shield Advanced 和 AWS Shield Standard 定价

AWS Shield Standard 随 AWS 服务提供，没有任何额外费用。

[AWS Shield Advanced 定价](#)页面中详述了 AWS Shield Advanced 定价。AWS Shield Advanced 具有额外成本，但 AWS Shield Advanced 客户不针对他们使用 AWS Shield Advanced 保护的资源单独为 AWS WAF 付款。这些资源的保护作为 AWS Shield Advanced 服务的一部分包括在内。而且，AWS Shield Advanced 费用不会随攻击量而增加。这样便可为扩展防护提供可预测的成本。

AWS Shield Advanced 费用适用于订阅 AWS Shield Advanced 的每个企业。如果您的企业有多个 AWS 账户，那么只要所有 AWS 账户都在同一个[整合账单账户系列](#)中，您就只需支付一个 Shield Advanced 的月费。此外，您必须是该账户中所有 AWS 账户和资源的所有者。



# AWS Shield Advanced 入门

本教程介绍如何开始使用 AWS Shield Advanced。为了获得最佳结果，请按顺序执行以下步骤。

## 主题

- [步骤 1：激活 AWS Shield Advanced \(p. 119\)](#)
- [步骤 2：指定要保护的资源 \(p. 120\)](#)
- [步骤 3：\(可选\) 向 DDoS 响应团队授权 \(p. 120\)](#)
- [步骤 4：在 CloudWatch 中创建 DDoS 控制面板并设置 CloudWatch 警报 \(p. 121\)](#)
- [步骤 5：部署 AWS WAF 规则 \(p. 121\)](#)
- [步骤 6：监控全球威胁环境控制面板 \(p. 122\)](#)

## 步骤 1：激活 AWS Shield Advanced

AWS Shield Advanced 可针对网络层 (第 3 层)、传输层 (第 4 层) 和应用程序层 (第 7 层) 攻击提供高级 DDoS 检测和缓解防护。

### Important

必须为您要保护的每个 AWS 账户激活 Shield Advanced。要为多个账户激活 Shield Advanced，请参阅[为多个账户激活和设置 AWS Shield Advanced \(p. 119\)](#)。

### 激活 AWS Shield Advanced

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 如果这是您首次登录 AWS WAF 控制台，请选择 Go to AWS Shield Advanced (转到 AWS Shield Advanced)。否则，在导航窗格中的 AWS Shield 下，选择 Protected resources (受保护的资源)。
3. 阅读每个协议条款，然后选中每个复选框，以表明您接受这些条款。继续操作之前，您必须选中所有复选框。
4. 选择 Next。

### Important

选择下一步，您就可以订阅 Shield Advanced 并激活此服务。要取消订阅，必须[联系 AWS Support](#)。

现在可转至[步骤 2：指定要保护的资源 \(p. 120\)](#)。

## 为多个账户激活和设置 AWS Shield Advanced

必须为您要保护的每个 AWS 账户激活 Shield Advanced。为此，请为每个账户执行[步骤 1：激活 AWS Shield Advanced \(p. 119\)](#)中的过程，每次要用不同的账户登录。

如果您为都在同一个[整合账单账户系列](#)中的多个账户激活 Shield Advanced，则月度订阅费用将涵盖所有这些账户。您无需为各个账户支付额外的订阅费用。您必须是该账户中所有 AWS 账户和资源的所有者。

首次从账户中激活 Shield Advanced 时，会向您显示定价协议。每次从不同的账户激活 Shield Advanced 时，定价协议都会显示在控制台中。定价协议在一个整合账单系列中涵盖所有激活的账户，但您每次激活一个账户时都必须同意条款。

现在可转至[步骤 2：指定要保护的资源 \(p. 120\)](#)。



## 步骤 2：指定要保护的资源

在如 [步骤 1：激活 AWS Shield Advanced \(p. 119\)](#) 中所述激活您的 AWS Shield Advanced 订阅后，您可以指定要保护的资源。

选择要通过 Shield Advanced 保护的资源

1. 选择要保护的资源。对于负载均衡器或弹性 IP 地址，还必须选择一个区域。

您可以从下拉列表中选择，也可以键入要保护的特定资源的 Amazon 资源名称 (ARN)。您可以选择或键入资源类型和资源的任意组合。如果您输入 ARN，该 ARN 必须位于您使用的同一个账户中。

Shield Advanced 一次最多可列出 100 个资源。如果您的资源超过 100 个，请选择 Next (下一步) 以查看下一步设置。

如果您要保护 Amazon EC2 实例，必须先将弹性 IP 地址关联到实例，然后选择弹性 IP 地址作为要保护的资源。

如果您选择弹性 IP 地址作为要保护的资源，Shield Advanced 会保护与该弹性 IP 地址关联的任何资源，无论是 Amazon EC2 实例或 Elastic Load Balancing 负载均衡器。Shield Advanced 会自动识别与弹性 IP 地址关联的资源类型并对其应用适当的缓解功能，包括配置特定于该弹性 IP 地址的网络 ACL。有关使用弹性 IP 地址与 AWS 资源的更多信息，请参阅适当的指南：[Amazon Elastic Compute Cloud 文档](#) 或 [Elastic Load Balancing 文档](#)。

Shield Advanced 不支持 EC2-Classic。

### Important

您可以从该步骤继续操作，而不选择任何资源。但是，如果您这样做，则稍后必须如[向更多 AWS 资源添加 AWS Shield Advanced 防护 \(p. 122\)](#) 中所述添加资源。Shield Advanced 不会自动保护资源；您必须指定要保护的资源。

2. 选择 Next。

现在可转至 [步骤 3：\(可选\) 向 DDoS 响应团队授权 \(p. 120\)](#)

## 步骤 3：(可选) 向 DDoS 响应团队授权

AWS Shield Advanced 的优势之一是来自 DDoS 响应团队 (DRT) 的支持。当您遇到潜在 DDoS 攻击时，您可以联系 [AWS Support Center](#)。如有必要，支持中心会将您的问题上报至 DRT。DRT 可帮助您分析可疑的活动，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 AWS WAF 规则和 Web 访问控制列表 (Web ACL)。DRT 可以检查您的 AWS WAF 配置并为您创建或更新 AWS WAF 规则和 Web ACL，但该团队需要您的授权才可以执行此操作。建议您在设置 AWS Shield Advanced 时主动向 DRT 提供所需授权。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。

如果您不希望向 DRT 授权以代表您缓解潜在攻击，请选择 Do not grant the DRT access to my account (不授权 DRT 访问我的账户)，然后选择 Finish (完成)。否则，继续执行以下步骤。

### Note

要使用 DRT 的服务，您必须订阅 [Business Support 计划](#) 或 [企业支持计划](#)。

授权 DRT 代表您缓解潜在攻击

1. 完成 [步骤 1：激活 AWS Shield Advanced \(p. 119\)](#) 后，将显示 Authorize DRT support (授权 DRT 支持) 页面。选择 Create new role for the DRT to access my account (为 DRT 创建新角色以访问我的账户) 或 Choose an existing role for the DRT to access my account (为 DRT 选择现有角色以访问我的账户)。

如果您选择使用现有角色，必须将 `AWSShieldDRTAccessPolicy` 托管策略附加到角色。有关更多信息，请参阅[附加和分离 IAM 策略](#)。如果您选择 `Create new role for the DRT to access my account` (为 DRT 创建新角色以访问我的账户)，此策略会自动附加到该角色。

如果您选择使用现有角色，该角色还必须信任服务委托人 `drt.shield.amazonaws.com`。有关更多信息，请参阅[IAM JSON 策略元素：委托人](#)。

`AWSShieldDRTAccessPolicy` 托管策略仅向 DRT 授予对 AWS WAF 和 Shield 资源的完全访问权限。该策略允许 DRT 代表您检查您的 AWS WAF 配置并创建或更新 AWS WAF 规则和 Web ACL。仅当经过您明确授权后，DRT 才能执行这些操作。

2. 填写所需信息（即新的角色名称或现有角色名称）。
3. （可选）选择 `Authorize the DRT to access your flow logs stored in Amazon S3 buckets` (授权 DRT 访问您存储在 Amazon S3 存储桶中的流日志)，然后键入要在其中存储这些日志的 Amazon S3 存储桶的名称。选择 `Add bucket` (添加存储桶)。根据需要重复，添加更多存储桶，最多 10 个。
4. 我们会向与您的账户相关联的电子邮件地址发送可能的 DDoS 活动的通知。如果您希望我们将通知发送到其他电子邮件地址，请在框中键入每个地址，然后选择添加电子邮件地址。根据需要重复此过程以添加更多电子邮件地址，最多 10 个。
5. 选择 `Finish`。

您可以随时按照[编辑 AWS Shield Advanced 设置 \(p. 123\)](#)中的说明，更改 DRT 访问方式和权限。

在授权 DRT 代表您执行操作后，我们建议您按照[步骤 4：在 CloudWatch 中创建 DDoS 控制面板并设置 CloudWatch 警报 \(p. 121\)](#)中的说明进行操作。

## 步骤 4：在 CloudWatch 中创建 DDoS 控制面板并设置 CloudWatch 警报

您可以使用 CloudWatch 监控潜在 DDoS 活动，此工具可从 Shield Advanced 收集原始数据，并将原始数据处理为便于读取的近乎实时的指标。这些统计数据会保存两周，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的[什么是 CloudWatch](#)。

有关创建 CloudWatch 控制面板的说明，请参阅[使用 Amazon CloudWatch 进行监控 \(p. 126\)](#)。有关您可以添加到控制面板的 Shield Advanced 指标的信息，请参阅[Shield Advanced 指标 \(p. 128\)](#)。

创建 CloudWatch 控制面板后，请使用[步骤 5：部署 AWS WAF 规则 \(p. 121\)](#)中所述的一个或多个资源部署 AWS WAF 规则。

## 步骤 5：部署 AWS WAF 规则

多种资源可用于帮助您快速部署 AWS WAF 资源。在创建第一组规则时，请考虑利用以下一个或多个产品：

### 安全自动化模板

AWS 提供包含一组 AWS WAF 规则的预配置模板，您可以对这些规则进行自定义，以满足您的需求。这些模板旨在阻止基于 Web 的常见攻击，如恶意机器人、SQL 注入、跨站点脚本 (XSS)、HTTP 泛洪和已知攻击者的攻击。除了激活 Shield Advanced 并为 Shield Advanced 防护指定资源外，还应使用这些预配置的模板。

有关更多信息，请参阅[AWS WAF 安全自动化](#)。AWS WAF 随 Shield Advanced 提供，没有任何额外费用。

## AWS Marketplace Rule Groups

AWS WAF 可提供 AWS Marketplace rule groups 帮助您保护您的资源。AWS Marketplace rule groups 是预定义、即用型规则集合，由 AWS 和 AWS 合作伙伴公司编写和更新。有关更多信息，请参阅 [AWS Marketplace Rule Groups \(p. 75\)](#)。

## 适用于 OWASP 十大 Web 应用程序漏洞的 AWS WAF

本文档概述如何使用 AWS WAF 缓解在开源 Web 应用程序安全计划 (OWASP) 十大缺陷列表中定义的应用程序漏洞。此列表显示了最常见的应用程序安全缺陷类别。有关更多信息，请参阅 [AWS WAF 安全自动化](#)。

作为 Shield Advanced 入门的最后一个步骤，请查看全球威胁环境控制面板，如 [步骤 6：监控全球威胁环境控制面板 \(p. 122\)](#) 中所述。

## 步骤 6：监控全球威胁环境控制面板

全局威胁环境控制面板提供了近乎实时的全球 AWS 威胁情形摘要。威胁情形包括最大规模的攻击、重要攻击载体以及重大攻击的相对数量。要查看重大 DDoS 攻击的历史记录，可以自定义不同时长的控制面板视图。有关更多信息，请参阅 [跨 AWS 监控威胁 \(p. 137\)](#)。

## 向更多 AWS 资源添加 AWS Shield Advanced 防护

在为账户启用 Shield Advanced 的过程中，需选择要保护的初始资源。您可能要为更多资源添加防护。Shield Advanced 可为多达 100 个资源提供高级监控和防护，这些资源包括弹性 IP 地址、CloudFront 分配、Amazon Route 53 托管区域或 Elastic Load Balancing 资源的任意组合。如果要增加这些限制，请联系 [AWS Support Center](#)。

### Important

在执行此过程之前，必须先完成 [步骤 1：激活 AWS Shield Advanced \(p. 119\)](#)。

### 为 AWS 资源添加防护

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 选择 Protected resources。
3. 选择 Add DDoS protection。
4. 选择或输入要保护的资源类型和资源。对于 Classic Load Balancer 和 应用程序负载均衡器 资源，还必须选择一个区域。

您可以从提供的列表中选择，也可以输入要保护的特定资源的 Amazon 资源名称 (ARN)。您可以选择或输入资源类型和资源的任意组合。

Shield Advanced 一次最多可列出 100 个资源。如果您的资源超过 100 个，请选择 Next (下一步) 以查看下一步设置。

如果您要保护 Amazon EC2 实例，必须先将弹性 IP 地址关联到实例，然后选择弹性 IP 地址作为要保护的资源。

### Note

Shield Advanced 不支持 EC2-Classic。

5. 对于 Name，键入一个友好名称，以帮助您标识受保护的 AWS 资源。例如，**My CloudFront AWS Shield Advanced distributions**。
6. (可选) 对于 Web DDoS attack，选择 Enable。系统会提示您将现有的 Web ACL 与这些资源关联，如果还没有 Web ACL，系统会提示您创建一个。

以后可通过执行[从 AWS 资源中删除 AWS Shield Advanced \(p. 123\)](#)中所述的步骤来禁用此防护。

7. 选择 Add DDoS protection。

#### Note

如果您选择弹性 IP 地址作为要保护的资源，Shield Advanced 将保护该弹性 IP 地址关联的任何资源，无论是 Amazon EC2 实例或 Elastic Load Balancing 负载均衡器。Shield Advanced 会自动识别与弹性 IP 地址关联的资源类型并对其应用适当的缓解功能，包括配置特定于该弹性 IP 地址的网络 ACL。有关使用弹性 IP 地址与 AWS 资源的更多信息，请参阅适当的指南：[Amazon Elastic Compute Cloud 文档](#)或[Elastic Load Balancing 文档](#)。Shield Advanced 不支持 EC2-Classic。

## 从 AWS 资源中删除 AWS Shield Advanced

您可以随时从您的任何资源中删除 AWS Shield Advanced 保护。

#### Important

删除某个资源将不会从 AWS Shield Advanced 删除该资源。您还必须从 AWS Shield Advanced 中删除该资源，如该过程所述。

从 AWS 资源中删除 AWS Shield Advanced 保护

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 选择 Protected resources。
3. 选择资源旁的单选按钮。
4. 选择 Delete protection。

这些步骤可从特定资源中删除 AWS Shield Advanced 保护。它们不取消您的 AWS Shield Advanced 订阅。您将继续为该服务付费。有关您的 AWS Shield Advanced 订阅的更多信息，请联系 [AWS Support Center](#)。

## 编辑 AWS Shield Advanced 设置

您可以更改 AWS Shield Advanced 设置，如添加或删除 DDoS 响应团队 (DRT) 对您账户的访问权限，或者添加或删除紧急联系人信息。

编辑 AWS Shield Advanced 设置

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 在导航窗格中，在 AWS Shield 下选择 Summary (摘要)。
3. 在 DDoS response team (DRT) support (DDoS 响应团队 (DRT) 支持) 或 Emergency contacts (紧急联系人) 下，选择 Edit (编辑)。
4. 进行必要的更改，然后选择保存。

## AWS Shield Advanced：请求服务抵扣金额

如果您已订阅 AWS Shield Advanced 并且 DDoS 攻击导致对您的 Amazon CloudFront、Elastic Load Balancing、Route 53 或 Amazon EC2 服务产生额外费用，则您可以通过 [AWS Support Center](#) 提交账单案例，申请服务抵扣金额。

如果 AWS Shield Advanced 团队确定事件是有效的 DDoS 攻击并且基础服务通过扩展吸收了该攻击，则 AWS 会为由于攻击而产生的费用提供账户服务抵扣金额。例如，如果您在攻击期间的合法 CloudFront 数据传输使用量是 20 GB，但是攻击导致您多产生了 200 GB 的数据传输费用，则 AWS 会提供服务抵扣金额以抵消增加的数据传输费用。AWS 会自动对您未来的每月账单应用所有服务抵扣金额。服务抵扣金额可应用于 AWS Shield，且不能用于支付其他 AWS 服务。服务抵扣金额有效期为 12 个月。

#### Important

要获取服务抵扣金额，AWS 必须在事件发生之后的第二个账单周期结束之前收到您的服务抵扣金额申请。

要申请服务抵扣金额，请向 [AWS Support Center](#) 提交包含以下信息的账单查询：

- 主题行中的“DDoS Concession”
- 您提出申请的每个事件中中断的日期和时间
- 受 DDoS 活动影响的 AWS 服务 (Amazon CloudFront、Elastic Load Balancing、Route 53、Amazon EC2) 和特定资源

## AWS Shield Advanced 限制

AWS Shield Advanced 为弹性 IP 地址、CloudFront 分配、Route 53 托管区域或 Elastic Load Balancing 负载均衡器提供高级监控和保护。针对每个账户，您可以监控和保护最多 100 个这样的资源类型。如果要增加这些限制，请联系 [AWS Support Center](#)。



# 监控 AWS WAF、AWS Firewall Manager 和 AWS Shield Advanced

监控功能对于保持 AWS WAF 的可靠性、可用性和性能以及使用 AWS Shield 识别可能的 DDoS 攻击非常重要。着手监控 AWS WAF 和 AWS Shield 的时候，您应当制定一个能够回答下列问题的监控计划：

- 您的监控目标是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

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。监控 AWS WAF 和相关服务时，应将历史监控数据存储下来以便与当前性能数据比较，确定正常性能模式和异常性能表现，并设计出解决问题的方法。

对于 AWS 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 \(p. 125\)](#)
- [使用 Amazon CloudWatch 进行监控 \(p. 126\)](#)
- [使用 AWS CloudTrail 记录 API 调用 \(p. 130\)](#)

## 监控工具

AWS 为您提供了多种用于监控 AWS WAF 和 AWS Shield 的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。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监控工具来监控 AWS WAF 和 AWS Shield Advanced 并在出现错误时进行报告：

- Amazon CloudWatch 警报 – 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。该操作是向 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略发送通知。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 Amazon CloudWatch 进行监控 \(p. 126\)](#)。

您不仅可以使 CloudWatch 监控 AWS WAF 和 Shield Advanced 指标 (如[使用 Amazon CloudWatch 进行监控 \(p. 126\)](#)中所述)，还应使用 CloudWatch 监控 Elastic Load Balancing 资源和 Amazon CloudFront 分配的活动。有关更多信息，请参阅[用于应用程序负载均衡器的 CloudWatch 指标](#)和[使用 CloudWatch 监控 CloudFront 活动](#)。

- Amazon CloudWatch Logs – 监控、存储和访问来自 AWS CloudTrail 或其他来源的日志文件。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的[监视日志文件](#)。

- Amazon CloudWatch Events – 匹配事件并将事件传送到一个或多个目标函数或流来进行更改、捕获状态信息和采取纠正措施。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [什么是 Amazon CloudWatch 事件](#)。
- AWS 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 CloudWatch Logs 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被 CloudTrail 交付后未发生更改。有关更多信息，请参阅 AWS CloudTrail User Guide 中的 [使用 AWS CloudTrail 记录 API 调用 \(p. 130\)](#) 和 [使用 CloudTrail 日志文件](#)。

## 手动监控工具

监控 AWS WAF 和 AWS Shield 的另一个重要环节是手动监控 CloudWatch 警报未涵盖的各项。您可以查看 AWS WAF、AWS Shield Advanced、CloudWatch 和其他 AWS 控制台控制面板，来了解 AWS 环境的状态。建议您还要查看 web ACLs and rules 的日志文件。

- 查看 AWS WAF 控制面板：
  - 在 AWS WAF Web ACLs 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 CloudFront 或 应用程序负载均衡器 已转发给 AWS WAF 的 Web 请求采样 \(p. 83\)](#)。
- 查看 CloudWatch 主页中的以下内容：
  - 当前警报和状态
  - 警报和资源的图表
  - 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
- 搜索并浏览您所有的 AWS 资源指标
- 创建和编辑警报以接收有关问题的通知

## 使用 Amazon CloudWatch 进行监控

您可以使用 CloudWatch 监控 Web 请求和 web ACLs and rules，此工具可从 AWS WAF 收集原始数据，并将数据处理为便于读取的近乎实时的指标。这些统计数据会保存两周，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的 [什么是 CloudWatch](#)。

## 创建 CloudWatch 警报

您可以创建 CloudWatch 警报，以在警报改变状态时发送 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。操作是向 Amazon SNS 主题或 Auto Scaling 策略发送的通知。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。

## AWS WAF 和 AWS Shield Advanced 指标与维度

您可以按照以下步骤查看 AWS WAF 和 Shield Advanced 的指标。

使用 CloudWatch 控制台查看指标

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。



1. 通过以下网址打开 CloudWatch 控制台：<https://console.aws.amazon.com/cloudwatch/>。
2. 如果需要，可以更改区域。从导航栏中，选择您的 AWS 资源所在的区域。有关更多信息，请参阅 [AWS 区域和终端节点](#)。

如果您要查看 CloudFront 的 AWS WAF 指标，则必须选择 美国东部（弗吉尼亚北部）区域。

3. 在导航窗格中，选择 Metrics。
4. 在 All metrics 选项卡上，选择相应的服务。

### 使用 AWS CLI 查看指标

- 对于 AWS WAF，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "WAF"
```

对于 Shield Advanced，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "DDoSProtection"
```

## AWS WAF 指标

WAF 命名空间包括以下指标。

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  计数的 Web 请求是一个符合某个特定规则中的所有条件的请求。计数的 Web 请求通常用于测试。  有效统计数据：Sum
PassedRequests	已为规则组传递的请求数。  报告标准：有非零值  传递的请求是与规则组中包含的任何规则不匹配的请求。  有效统计数据：Sum

## AWS WAF 维度

用于 CloudFront 的 AWS WAF 可以使用以下维度组合：

- 规则、WebACL
- RuleGroup、WebACL
- 规则、RuleGroup

用于 应用程序负载均衡器 的 AWS WAF 可以使用以下维度组合：

- 区域、规则、WebACL
- 区域、RuleGroup、WebACL
- 区域、规则、RuleGroup

维度	描述
Rule	下列情况之一： <ul style="list-style-type: none"><li>• 规则的指标名称。</li><li>• ALL，表示 WebACL 或 RuleGroup 中的所有规则。</li><li>• Default_Action (仅当与 WebACL 维度组合时)，表示分配给不符合与允许或阻止操作相关的任何规则的任何请求的操作。</li></ul>
RuleGroup	RuleGroup 的指标名称。
WebACL	WebACL 的指标名称。
Region	应用程序负载均衡器的区域。

## Shield Advanced 指标

### AWS Shield Advanced 指标

AWS Shield Advanced 包含以下指标。

指标	描述
DDoSDetected	指示特定 Amazon 资源名称 (ARN) 的 DDoS 事件。  报告标准：非零值指示具有 DDoS 事件。没有检测到 DDoS 事件为零。
DDoSAttackBitsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的字节数。该指标仅适用于 3/4 层 DDoS 事件。  报告标准：攻击期间的非零值。没有攻击时为零。  单位：位

指标	描述
DDoSAttackPacketsPerSecond	<p>特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的数据包数。该指标仅适用于 3/4 层 DDoS 事件。</p> <p>报告标准：攻击期间的非零值。没有攻击时为零。</p> <p>单位：数据包</p>
DDoSAttackRequestsPerSecond	<p>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。</p> <p>报告标准：攻击期间的非零值。没有攻击时为零。</p> <p>单位：请求</p>

仅当检测到对 AWS 资源的攻击时，AWS Shield Advanced 才会向 CloudWatch 报告指标。如果在指定期间没有攻击，AWS Shield Advanced 将报告零。

全局资源的指标 (CloudFront 和 Route 53) 在美国东部 (弗吉尼亚北部) 地区中报告。

Shield Advanced 发布的 DDoSDetected 指标不具有其他维度。其他指标包含相应的 AttackVector 维度：

- UDPTraffic
- UDPFragment
- GenericUDPReflection
- DNSReflection
- NTPReflection
- ChargenReflection
- SSDPReflection
- PortMapper
- RIPReflection
- SNMPReflection
- MSSQLReflection
- NetBIOSReflection
- MemcachedReflection
- SYNflood
- ACKFlood
- RequestFlood

## 创建 AWS Shield Advanced 警报

您可以将这些 Shield Advanced 指标用于 CloudWatch 警报。CloudWatch 警报可根据您定义的规则发送通知或者对您所监控的资源自动进行更改。

有关创建 CloudWatch 警报的详细说明，请参阅 [Amazon CloudWatch 用户指南](#)。在 CloudWatch 控制台中创建警报时，在选择 Create an alarm 后，选择 AWSDDOSProtectionMetrics 以使用这些 Shield Advanced 指标。然后，您可以基于特定流量创建一个警报，或者每当任一上述指标大于零时触发该警报。因为仅在检测到攻击时才报告 Shield Advanced 指标，所以第二个选项会因 Shield Advanced 观察到的任何潜在攻击而触发一个警报。

## Note

AWSDDOSProtectionMetrics 仅适用于 Shield Advanced 客户。

有关更多信息，请参阅 Amazon CloudWatch 用户指南 中的[什么是 CloudWatch](#)。

# 使用 AWS CloudTrail 记录 API 调用

AWS WAF、AWS Shield Advanced 和 AWS Firewall Manager 与 AWS CloudTrail 集成，后者是一个提供用户、角色或 AWS 服务所采取操作的记录的服务。如果您创建跟踪，可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶、Amazon CloudWatch Logs 和 Amazon CloudWatch Events。通过使用 CloudTrail 收集的信息，您可以确定向这些服务发出了什么请求、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。

每个事件或日志条目都包含有关生成请求的人员的信息。身份信息帮助您确定以下内容：

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 [CloudTrail userIdentity 元素](#)。

CloudTrail 日志文件可以包含一个或多个日志条目。每个条目列出了多个 JSON 格式的事件。一个日志条目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。日志条目不是公用 API 调用的有序堆栈跟踪，因此它们不会以任何特定顺序显示。

您可以创建跟踪并根据需要将日志文件存储在 Amazon S3 存储桶中任意长时间，也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。

您还可以将多个 AWS 区域和多个 AWS 账户中的日志文件聚合到单个 Amazon S3 存储桶中。

要在传送日志文件时获得通知，请将 CloudTrail 配置为在传送新日志文件时发布 Amazon SNS 通知。有关更多信息，请参阅[CloudTrail 配置 Amazon SNS 通知](#)。

有关更多信息，请参阅[接收多个区域中的 CloudTrail 日志文件](#)和[从多个账户中接收 CloudTrail 日志文件](#)。

要了解有关 CloudTrail 的更多信息，包括如何对其进行配置和启用，请参阅 [AWS CloudTrail User Guide](#)

## CloudTrail 中的 AWS WAF 信息

CloudTrail 记录所有 AWS WAF 操作，[AWS WAF API 参考](#)中介绍了这些操作。例如，调用 ListWebACL、UpdateWebACL 和 DeleteWebACL 会在 CloudTrail 日志文件中生成条目。

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了以下操作 (见 eventName 元素)：

- CreateRule
- GetRule
- UpdateRule
- DeleteRule

```
{  
  "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": "AWS 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": "AWS 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": "AWS 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": "AWS 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"
}
```

```
]
}
```

## CloudTrail 中的 AWS Shield Advanced 信息

AWS 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](#)
- [DeleteSubscription](#)

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 DeleteProtection 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-west-2",
    "sourceIPAddress": "AWS 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-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6acca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```

## CloudTrail 中的 AWS Firewall Manager 信息

AWS 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](#)

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 `GetAdminAccount` 操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890987654321231",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
        "accountId": "123456789012",
        "accessKeyId": "1AFGDT647FHU83JHFI81H",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated":
                "creationDate":
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId":
                "1234567890987654321231",
```

```
"arn:aws:iam::123456789012:role/Admin",  
"123456789012",  
  
    },  
    "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"  
}  
  
    "arn":  
    "accountId":  
    "userName": "Admin"  
    }
```

# 响应 DDoS 攻击

第 3 层和第 4 层攻击由 AWS 自动应对。如果您使用 Shield Advanced 保护您的 Amazon EC2 实例，在攻击期间，Shield Advanced 将自动将您的 Amazon VPC 网络 ACL 部署到 AWS 网络边界，可以允许 Shield Advanced 提供保护应对更严重的 DDoS 事件。有关网络 ACL 的更多信息，请参阅[网络 ACL](#)。

如果 CloudWatch 中的 DDoS 警报 指示可能存在第 7 层攻击，您有两个选择：

- 自己调查和缓解攻击：如果您确定该活动属于 DDoS 攻击，您可以创建自己的 AWS WAF 规则来缓解攻击。AWS WAF 随 AWS Shield Advanced 提供，没有任何额外费用。AWS 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 AWS WAF 规则，设计用于阻止基于 Web 的常见攻击。您可以通过自定义规则来满足自己的业务需求。有关更多信息，请参阅[AWS WAF 安全自动化](#)和[创建 Web ACL \(p. 78\)](#)。
- 如果您是 AWS Shield Advanced 客户，您还可以选择联系 [AWS Support Center](#)：如果您希望应用缓解措施方面获得帮助，您可以联系 [AWS Support Center](#)。重大和紧急案例将直接转给 DDoS 专家。使用 AWS Shield Advanced 时，复杂案例可上报至 DRT，DRT 在保护 AWS、Amazon.com 及其子公司方面拥有丰富的经验。

要获得 DRT 支持，请联系 [AWS Support Center](#) 并说明您是 AWS Shield Advanced 客户，可能正遭到攻击。我们的代表会将您的电话转给适当的 DDoS 专家。如果您使用 Distributed Denial of Service (DDoS) 服务类型通过 [AWS Support Center](#) 开立案例，则可以通过聊天或电话直接与 DDoS 专家交流。DDoS 攻击工程师可以帮助您识别攻击、建议对 AWS 架构的改进，并提供关于使用 AWS 服务缓解 DDoS 攻击的指导。

## Important

对于第 7 层攻击，DRT 可帮助您分析可疑活动，然后协助您缓解问题。这种缓解措施通常需要 DRT 在您的账户中创建或更新 AWS WAF Web 访问控制列表 (Web ACL)。但是，他们需要您的授权才能执行此操作。建议您在启用 AWS Shield Advanced 的过程中，按照[步骤 3：\(可选\) 向 DDoS 响应团队授权 \(p. 120\)](#) 中的步骤主动向 DRT 提供所需权限。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。

您也可以在可能的攻击前或在攻击期间联系 DRT，以便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 DRT 一起预先配置一个 ACL，只“允许”打开端口 80 和 443。

# 审查 DDoS 事件

AWS Shield Advanced 提供实时指标和报告，以便全面了解您的 AWS 资源所遭受的攻击。

这些指标和报告仅适用于 AWS Shield Advanced 客户。要激活 AWS Shield Advanced，请参阅[激活 AWS Shield Advanced \(p. 119\)](#)。

您可以查看有关攻击的近乎实时的指标，包括：

- 攻击类型
- 开始时间
- Duration
- 每秒阻止的数据包
- HTTP 请求示例

可供查看有关活跃事件和最近 12 个月内发生的事件的详细信息。

## Shield Advanced 详细信息报告

此外，AWS Shield Advanced 可让您了解在发生攻击时您的整体流量。您可以查看以下前几项的详细信息：

- IP
- URL
- 引用站点
- ASN
- 国家/地区
- 用户代理

使用此信息来创建 AWS WAF 规则，以帮助防止未来的攻击。例如，如果您发现您有大量的请求来自一个您通常不开展业务的国家/地区，则可以创建一个 AWS WAF 规则来阻止来自该国家/地区的请求。

### Note

您应该始终首先使用 Count 而不是 Block 来测试规则。一旦您认为新规则能确定正确的请求，就可以修改规则以阻止这些请求。

### 查看 DDoS 事件

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 选择 Incidents。
3. 选择要调查的攻击的 Incident type。

如果您确定可能正在遭受攻击，可以通过 [AWS Support Center](#) 与 DRT 联系，或通过创建新的 Web 访问控制列表 (Web ACL) 自行缓解攻击。

### 缓解潜在的 DDoS 攻击

1. 在 AWS WAF 中创建与异常行为匹配的条件。
2. 将这些条件添加到一个或多个 AWS WAF 规则中。
3. 将这些规则添加到 Web ACL 并将该 Web ACL 配置为对与规则匹配的请求计数。
4. 监控这些计数，以确定是否应阻止请求的来源。如果请求量仍然异常高，请更改您的 Web ACL 以阻止这些请求。

有关更多信息，请参阅 [创建 Web ACL \(p. 78\)](#)。

AWS 提供了预配置的模板，旨在帮助您快速入门。这些模板中包含一组 AWS WAF 规则，可对其进行自定义以最适合您的需要，这些规则设计用于阻止基于 Web 的常见攻击。有关更多信息，请参阅 [AWS WAF 安全自动化](#)。

## 跨 AWS 监控威胁

如果您是 Shield Advanced 客户，除事故页面上提供的有关您的资源遭受的攻击的信息外，您还可以使用全局威胁环境控制面板跨 Amazon CloudFront、Elastic Load Balancing 和 Route 53 查看有关 DDoS 威胁情形的趋势和指标。

全球威胁环境控制面板可提供近乎实时的全球 AWS 威胁情形摘要，其中包括最大规模的攻击、重要攻击载体以及重大攻击的相对数量。您可以自定义不同时长的控制面板视图，以便查看重大 DDoS 攻击的历史记录。

#### 若要查看全球威胁环境控制面板

1. 登录 AWS 管理控制台，并通过以下网址打开 AWS WAF 控制台：<https://console.aws.amazon.com/waf/>。
2. 选择全球威胁环境。
3. 选择一个时间段。

您可以使用全球威胁环境控制面板上的信息，更好地了解威胁情形并帮助您做出决策，以更好地保护您的 AWS 资源。

# 使用 AWS WAF 和 AWS Shield Advanced API

本部分介绍如何向 AWS WAF 和 Shield Advanced API 发出请求，以在 AWS WAF 中创建和管理匹配集、规则和 Web ACL 以及在 Shield Advanced 中创建和管理订阅及防护。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 AWS SDKs \(p. 139\)](#)
- [向 AWS WAF 或 Shield Advanced 发出 HTTPS 请求 \(p. 139\)](#)
- [HTTP 响应 \(p. 141\)](#)
- [对请求进行身份验证 \(p. 142\)](#)

## 使用 AWS SDKs

如果 AWS 为您使用的语言提供了 SDK，请使用该 SDK 而不是尝试使用 API 自行操作。SDK 可简化身份验证、轻松与您的开发环境集成，并可让您轻松访问 AWS WAF 和 Shield Advanced 命令。有关 AWS SDK 的更多信息，请参阅主题[设置 \(p. 3\)](#)中的[步骤 3：下载工具 \(p. 4\)](#)。

## 向 AWS WAF 或 Shield Advanced 发出 HTTPS 请求

AWS WAF 和 Shield Advanced 请求是 HTTPS 请求，如 [RFC 2616](#) 所定义。与所有 HTTP 请求相似，发往 AWS 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

AWS WAF 和 Shield Advanced 要求 HTTP 请求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。在 [AWS 区域和终端节点](#) 中可以找到各个终端节点。例如，用于 CloudFront 分配的 AWS WAF 的 Host 标头的值为 `waf.amazonaws.com:443`。

### x-amz-date 或 Date (必需)

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, AWS 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 AWS 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 \(p. 142\)](#)。

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, 如以下示例所示:

```
Content-Type: application/x-amz-json-1.1
```

条件: 对 POST 请求是必需的。

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 AWS 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 AWS WAF 和 Shield Advanced API 操作都要求您在请求正文中包含 JSON 格式的数据。

以下示例请求使用一个简单的 JSON 语句来更新 IPSet (在控制台中称为 IP 匹配条件), 以包含 IP 地址 192.0.2.44 (用 CIDR 表示法记为 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

所有 AWS WAF 和 Shield Advanced API 操作的响应中都包含 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

AWS WAF 或 Shield Advanced 创建的用于唯一标识您的请求的值，例如，K2QH8DN0U907N97FNA2GDLL8OBVV4KQNSO5AEMVJF66Q9ASUAAJG。如果您在使用 AWS WAF 时遇到问题，AWS 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

AWS WAF 或 Shield Advanced 作出响应的日期和时间，例如，Wed, 07 Oct 2015 12:00:00 GMT。

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 AWS 为您使用的语言提供了 SDK，建议您使用该 SDK。与使用 AWS WAF 或 Shield Advanced API 相比，所有 AWS SDK 都会大大简化签名请求的流程，从而为您节省大量时间。此外，SDK 还可轻松与您的开发环境集成，并可让您轻松访问相关命令。

AWS WAF 和 Shield Advanced 要求您通过对请求签名来验证您发送的每个请求的身份。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，AWS WAF 或 Shield Advanced 将使用与您用于对该请求进行签名的相同哈希函数和输入重新计算签名。如果所得签名与该请求中的签名相匹配，则 AWS WAF 或 Shield Advanced 处理该请求。如果不匹配，则拒绝请求。

AWS WAF 和 Shield Advanced 支持使用 [AWS 签名版本 4](#) 进行的身份验证。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：

- 您要将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)。

# AWS WAF 和 AWS Shield Advanced PCI DSS 合规性

AWS WAF 和 AWS Shield Advanced 是符合支付卡行业 (PCI) 数据安全标准 (DSS) 3.2 的服务。PCI 标准委员会于 2016 年 4 月发布了 PCI DSS 3.2 版，作为现行最新要求集。PCI DSS 3.2 修订并阐明了在线信用卡交易在加密、访问控制、变更管理、应用程序安全性和风险管理计划方面的要求。

有关 AWS 和 PCI DSS 3.2 合规性的更多信息，请参阅 AWS 安全博客上的 [AWS Becomes First Cloud Service Provider to Adopt New PCI DSS 3.2](#)。有关 PCI DSS 3.2 版的更多信息，请参阅 [PCI DSS 3.2：新增功能](#)。

# 资源

下列相关资源在您使用此服务的过程中会有所帮助。

## AWS 资源

Amazon Web Services 中提供一些有用的指南、论坛和其他资源。

- [AWS WAF 开发论坛](#) – 基于社区的论坛，供开发人员讨论与 AWS WAF 有关的技术问题。
- [Shield Advanced 开发论坛](#) – 基于社区的论坛，供开发人员讨论与 Shield Advanced 有关的技术问题。
- [AWS WAF 产品信息](#) – 提供 AWS WAF 相关信息 (包括功能、定价等信息) 的主要网页。
- [Shield Advanced 产品信息](#) – 提供 Shield Advanced 相关信息 (包括功能、定价等信息) 的主要网页。
- [课程和研讨会](#) – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强 AWS 技能并获得实践经验。
- [AWS 开发人员工具](#) – 指向开发人员工具、软件开发工具包、IDE 工具包和命令行工具的链接，这些资源用于开发和管理 AWS 应用程序。
- [AWS 白皮书](#) – 指向 AWS 技术白皮书的完整列表的链接，这些资料涵盖了架构、安全性、经济性等主题，由 AWS 解决方案架构师或其他技术专家编写。
- [AWS Support 中心](#) - 用于创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 AWS Trusted Advisor。
- [AWS Support](#) - 提供有关 AWS Support 信息的主要网页，是一种一对一的快速响应支持渠道，可帮助您在云中构建和运行应用程序。
- [联系我们](#) - 查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。
- [AWS 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

update-history-change	update-history-description	update-history-date
<a href="#">扩展了允许的 CIDR 范围</a>	在创建 IP 匹配条件时，AWS WAF 现在支持 IPv4 地址范围：/8 和任何介于 /16 到 /32 之间的范围。	June 5, 2018
<a href="#">在条件中支持查询参数</a>	创建条件时，您现在可以在请求中搜索特定的参数。	June 5, 2018
<a href="#">Shield Advanced 入门向导</a>	引入一个新的简化流程来订阅 AWS Shield Advanced。	June 5, 2018

## 早期更新

下表描述此 AWS WAF 开发人员指南 每次发布时进行的重要修改。

变更	API 版本	描述	发布日期
更新	2016-08-24	Marketplace rule groups	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	全球威胁环境控制面板	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
更新	2016-08-24	基于速率的规则	2017 年 6 月
更新	2016-08-24	重新组织	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
更新	2015-08-24	添加了有关 AWS WAF 的 <a href="#">AWS WAF 和 AWS Shield Advanced PCI DSS 合规性 (p. 144)</a> 的信息。	2016 年 7 月 25 日
新功能	2015-08-24	您现在可以通过 AWS CloudTrail 记录您对 AWS WAF 进行的所有 API 调用，AWS CloudTrail 是一种 AWS 服务，可记录您账户的 API 调用并将日志文件传输到您的 S3 存储桶。CloudTrail 日志可以用于执行安全分析、跟踪 AWS 资源的更改以及帮助进行合规性审核。通过将 AWS WAF 与 CloudTrail 集成，您可以确定向 AWS WAF API 发出的请	2016 年 4 月 28 日

变更	API 版本	描述	发布日期
		<p>求、发出每个请求的源 IP 地址、发出请求的人员以及时间等。</p> <p>如果您已在使用 AWS CloudTrail，则会开始在 AWS CloudTrail 日志中看到 AWS WAF API 调用。如果您还没有为您的账户打开 AWS CloudTrail，则可以从 <a href="#">AWS 管理控制台</a> 打开 CloudTrail。除对 Amazon S3 和 Amazon SNS 的使用按照标准收费外，打开 CloudTrail 不另外收费。</p>	
新功能	2015-08-24	<p>您现在可以使用 AWS 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 <a href="#">使用跨站点脚本匹配条件 (p. 48)</a>。</p>	2016 年 29 月 3 日
新功能	2015-08-24	<p>在此版本中，AWS WAF 添加了以下功能：</p> <ul style="list-style-type: none"><li>• 您可以将 AWS 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 <a href="#">使用大小约束条件 (p. 55)</a>。</li><li>• 您可以将 AWS 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，请参阅以下文档：<ul style="list-style-type: none"><li>• <a href="#">创建或编辑字符串匹配条件时指定的值 (p. 64)</a></li><li>• <a href="#">创建或编辑 SQL 注入匹配条件时指定的值 (p. 60)</a></li><li>• <a href="#">创建或编辑大小约束条件时指定的值 (p. 56)</a></li></ul></li></ul>	2016 年 1 月 27 日
新功能	2015-08-24	<p>您现在可以使用 AWS WAF 控制台选择您要关联到 Web ACL 的 CloudFront 分配。有关更多信息，请参阅<a href="#">关联或取消关联 Web ACL 与 CloudFront 分配</a>。</p>	2015 年 11 月 16 日
首次发布	2015-08-24	<p>这是 AWS WAF 开发人员指南的首次发布。</p>	2015 年 10 月 6 日



# AWS 词汇表

有关最新 AWS 术语，请参阅 AWS General Reference 中的 [AWS 词汇表](#)。