aws

开发人员指南

AWS WAFAWS Firewall Manager、和 AWS Shield Advanced

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

Table of Contents

AWS WAF、、 AWS Shield Advanced、和 AWS Firewall Manager？

您可以AWS Firewall Manager结合使用AWS WAFAWS Shield、和来创建全面的安全解决方案。 AWS WAF 是一种 Web 应用程序防火墙，可用于监控最终用户向您的应用程序发送的 Web 请求并控制对您的内容的访问。Shield Advanced 可在网络和传输层（第 3 层和第 4 层）以及应用层（第 7 层）提供针对 AWS 资源的分布式拒绝服务 (DDoS) 攻击的保护。 AWS Firewall Manager 即使添加了新资源，也可跨账户 AWS WAF 和资源管理和 Shield Advanced 等保护。

主题

什么是 AWS WAF？

AWS WAF 是一个 Web 应用程序防火墙，允许您监控转发到受保护的 Web 应用程序资源的 HTTP 和 HTTPS 请求。您可以保护以下资源类型：

- 亚马逊 CloudFront 配送
- Amazon API Gateway REST API
- 应用程序负载均衡器
- AWS AppSync GraphQL API
- Amazon Cognito 用户池
- AWS App Runner 服务
- AWS 已验证访问实例

AWS WAF 允许您控制对内容的访问权限。根据指定的条件（如请求源自的 IP 地址或查询字符串的值），受保护资源会使用所请求的内容或者使用 HTTP 状态代码 403（禁止）或自定义响应来响应请求。

在最简单的层面上， AWS WAF 允许您选择以下行为之一：

- 允许除您指定的请求之外的所有请求 — 如果您想让 Amazon CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync AWS App Runner、Amazon Cognito 或 AWS 已验证访问权限为公共网站提供内容，但又想阻止攻击者的请求时，这很有用。
- 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。
- 统计符合您条件的请求 – 您可以使用 Count 操作来跟踪您的 Web 流量，而无需修改处理方式。您可以用它来进行常规监控，也可以用来测试您的新 Web 请求处理规则。当你想根据 Web 请求中的新属性允许或阻止请求时，可以先配置 AWS WAF 为计算与这些属性匹配的请求。这样，您就可以在将规则切换为允许或阻止匹配请求之前确认新的配置设置。
- 对符合您条件的请求运行验证码或质询检查：您可以对请求实施验证码和静默质询控制，以帮助减少机器人流向受保护资源的流量。

使用 AWS WAF 有几个好处：

- 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，规则可以阻止或计算不仅满足指定条件，而且在一分钟或五分钟内超过指定数量的请求的 Web 请求。
- 可以重复用于多个 Web 应用程序的规则。
- 来自 AWS 和 AWS Marketplace 卖家的托管规则组。
- 实时指标和采样的 Web 请求。
- 使用 AWS WAF API 进行自动管理。

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 可能是正确的选择。有关的更多信息 AWS WAF，请参阅AWS WAF。

什么是 AWS Shield Advanced？

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

Shield Advanced 为您的 Amazon EC2 实例、Elastic Load Balancing 负载均衡器、 CloudFront 分配、Route 53 托管区域和 AWS Global Accelerator 标准加速器提供扩展的 DDoS 攻击保护。Shield Advanced 会产生额外冲锋。Shield Advanced 选项和功能包括应用程序层 DDoS 自动缓解、高级事件可见性以及 Shield Response Team (SRT) 的专门支持。如果您拥有高可见性网站或容易遭受频繁的 DDoS 攻击，请考虑购买 Shield Advanced 提供的额外保护。有关其他信息，请参阅AWS Shield Advanced 功能和选项和决定是否订阅 AWS Shield Advanced 和应用其他保护。

什么是 AWS Firewall Manager？

AWS Firewall Manager 简化您跨多个账户和资源的管理和维护任务，以实现各种保护，包括 AWS WAF Amazon VPC 安全组和网络 ACL 以及 Amazon Route 53 Resolver DNS 防火墙。 AWS Shield Advanced AWS Network Firewall使用 Firewall Manager 一次设置好保护措施，该服务就会自动将其应用于您的账户和资源，即使添加新资源和账户时也是如此。

有关 Firewall Manager 的更多信息，请参阅 AWS Firewall Manager。

设置您的账户以使用服务

本主题介绍一些初步步骤，例如创建账户，以便您做好使用 AWS WAF AWS Firewall Manager、和的准备 AWS Shield Advanced。您无需为这些预备项目付费。您只需为所使用的 AWS 服务付费。

主题

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

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

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

下载工具

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

- API 指南记录了该服务支持的操作，并提供了指向相关软件开发工具包和 CLI 文档的链接：
  - AWS WAF API 引用
  - AWS Shield Advanced API 引用
  - AWS Firewall Manager API 引用
- 要调用 API 而不必处理诸如组装原始 HTTP 请求之类的低级细节，可以使用 S AWS DK。 AWS 软件开发工具包提供封装服务功能的函数和数据类型。 AWS 要下载 S AWS DK 并访问安装说明，请参阅相应页面：
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  有关软件开发工具 AWS 包的完整列表，请参阅 Amazon Web Services 工具。
- 您可以使用 AWS Command Line Interface (AWS CLI) 通过命令行控制多个 AWS 服务。您还可以使用脚本自动执行命令。有关更多信息，请参阅 AWS Command Line Interface。
- AWS Tools for Windows PowerShell 支持这些 AWS 服务。有关更多信息，请参阅 AWS Tools for PowerShell Cmdlet 参考。

AWS WAF

AWS WAF 是一个 Web 应用程序防火墙，允许您监控转发到受保护的 Web 应用程序资源的 HTTP (S) 请求。您可以保护以下资源类型：

- 亚马逊 CloudFront 配送
- Amazon API Gateway REST API
- 应用程序负载均衡器
- AWS AppSync GraphQL API
- Amazon Cognito 用户池
- AWS App Runner 服务
- AWS 已验证访问实例

AWS WAF 允许您控制对内容的访问权限。根据指定的规则（如请求源自的 IP 地址或查询字符串的值），与受保护资源相关的服务会使用所请求的内容或者使用 HTTP 状态代码 403（禁止）或自定义响应来响应请求。

> **Note**
>
> 您还可以使用 AWS WAF 保护托管在亚马逊弹性容器服务 (Amazon ECS) 容器中的应用程序。Amazon ECS 是一项高度可扩展的快速容器管理服务，它可轻松运行、停止和管理集群上的 Docker 容器。要使用此选项，您需要将 Amazon ECS 配置为使用启用的 Application Load Balancer AWS WAF 来路由和保护服务中任务的 HTTP (S) 第 7 层流量。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的服务负载均衡。

主题

- 中的 IP 集和正则表达式模式集 AWS WAF
- AWS WAF中的自定义 Web 请求和响应
- AWS WAF 网络请求上的标签
- AWS WAF 智能威胁缓解
- 记录 AWS WAF Web ACL 流量
- 测试和调整您的 AWS WAF 保护措施
- 如何 AWS WAF 使用 Amazon CloudFront 功能
- 您使用 AWS WAF 服务的安全性
- AWS WAF 配额
- 将您的 AWS WAF 经典资源迁移到 AWS WAF

如何 AWS WAF 运作

您可以使用 AWS WAF 控制受保护的资源如何响应 HTTP (S) Web 请求。为此，您可以定义 Web 访问控制列表（ACL），然后将其与要保护的一个或多个 Web 应用程序资源相关联。关联的资源会将传入的请求转发给，以便 Web ACL AWS WAF 进行检查。

在 Web ACL 中，您可以创建规则以定义要在请求中查找的流量模式，并指定要对匹配的请求执行哪些操作。操作选择包括以下内容：

- 允许请求转到受保护的资源以进行处理和响应。
- 阻止请求。
- 计算请求数量。
- 运行验证码或对请求进行质询检查，以验证人类用户和标准浏览器的使用情况。

AWS WAF 组件

以下是以下内容的核心组成部分 AWS WAF：

- Web ACL — 您可以使用 Web 访问控制列表 (ACL) 来保护一组 AWS 资源。您可以创建 Web ACL 并通过添加规则来定义其保护策略。规则可定义检查 Web 请求的条件，并指定对符合条件的请求采取的行动。您还可以为 Web ACL 设置默认操作，指示是阻止还是允许通过规则尚未阻止或允许的任何请求。有关 Web ACL 的更多信息，请参阅AWS WAF Web 访问控制列表 (Web ACL)。

  Web ACL 是一种 AWS WAF 资源。

- 规则：每条规则都包含定义检查条件的语句，还包含在 Web 请求满足条件时要执行的操作。当 Web 请求满足条件时，这是一个匹配。您可以配置规则来阻止匹配请求、允许请求通过、对请求进行计数，或者对使用验证码拼图或静默客户端浏览器质询的请求运行机器人控制功能。有关规则的更多信息，请参阅AWS WAF 规则。

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

- 规则组-您可以直接在 Web ACL 中定义规则，也可以在可重复使用的规则组中定义规则。 AWS 托管规则和 AWS Marketplace 卖家提供托管规则组供您使用。您还可以定义自己的规则组。有关规则组的更多信息，请参阅AWS WAF 规则组。

  规则组是一种 AWS WAF 资源。

主题

AWS WAF 网络 ACL 容量单位 (WCU)

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

AWS WAF 管理规则、规则组和 Web ACL 的容量。

规则 WCU

AWS WAF 在创建或更新规则时计算规则容量。 AWS WAF 以不同的方式计算每种规则类型的容量，以反映每条规则的相对成本。与使用更多处理能力的更复杂规则相比，运行成本很低的简单规则使用更少的 WCU。例如，与使用正则表达式模式集来检查请求的语句相比，大小限制规则语句使用的 WCU 更少。

规则容量要求通常从规则类型的基本成本开始，并随着复杂性而增加，例如，当您在检查之前添加文本转换或检查 JSON 正文时。有关规则容量要求的信息，请参阅 规则语句基础知识 上的规则语句列表。

规则组 WCU

规则组的 WCU 要求由您在规则组中定义的规则决定。一个规则组的最大容量为 5,000 个 WCU。

每个规则组都有一个不可变的容量设置，由所有者在创建时分配。对于您通过创建的托管规则组和规则组，情况确实如此 AWS WAF。修改规则组时，所做更改必须使规则组的 WCU 保持在其容量范围内。这可确保使用该规则组的 Web ACL 保持在其容量要求内。

规则组中使用的 WCU 等于规则的 WCU 的总和，减去通过组合规则行为可以获得的任何处理优化。AWS WAF 例如，如果您定义了两个规则来检查同一 Web 请求组件，并且每条规则在检查组件之前都对其应用了特定的转换，则 AWS WAF 可能只能向您收取一次应用转换的费用。在 Web ACL 中使用规则组的 WCU 成本始终是您在创建规则组时定义的固定 WCU 设置。

创建规则组时，请注意将容量设置得足够高，以适应您要在规则组的整个生命周期中使用的规则。

Web ACL WCU

Web ACL 的 WCU 要求由您在 Web ACL 中使用的规则和规则组决定。

- 在 Web ACL 中使用规则组的成本是规则组的容量设置。
- 使用规则的成本是规则计算出的 WCU 减去可以从 Web ACL 的规则组合中获得的任何处理优化。AWS WAF 例如，如果您定义了两个规则来检查同一 Web 请求组件，并且每条规则在检查组件之前都对其应用了特定的转换，则 AWS WAF 可能只能向您收取一次应用转换的费用。

Web ACL 的基本价格包括最多 1,500 个 WCU。根据分层定价模型，使用超过 1,500 个 WCU 会产生额外费用。 AWS WAF 随着您的网络 ACL WCU 使用量的变化，会自动调整您的 Web ACL 定价。有关定价的详细信息，请参阅 AWS WAF 定价。

Web ACL 的最大容量为 5,000 个 WCU。

确定规则组或 Web ACL 的 WCU

如前几节所述，规则组或 Web ACL 中使用的 WCU 总数将等于或小于规则组或 Web ACL 中定义的所有规则的 WCU 之和。

在 AWS WAF 控制台中，您可以看到向 Web ACL 或规则组添加规则时消耗的容量。控制台显示您添加规则时使用的容量单位。

通过 API，您可以检查要在 Web ACL 或规则组中使用的规则的最大容量要求。为此，请向检查容量调用提供规则的 JSON 列表。有关更多信息，请参阅 AWS WAF V2 API 参考CheckCapacity中的。

你可以用来保护的资源 AWS WAF

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

亚马逊配 CloudFront 送

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

AWS WAF 可在全球范围内 CloudFront 分发，但您必须使用美国东部区域（弗吉尼亚北部）来创建 Web ACL 和 Web ACL 中使用的任何资源，例如规则组、IP 集和正则表达式模式集。有些接口提供了 “全局 (CloudFront)” 的区域选择。选择此选项等同于选择美国东部（弗吉尼亚州北部）地区或“us-east-1”。

区域性资源

您可以保护所有可用区域的 AWS WAF 区域资源。您可以参阅 Amazon Web Services 一般参考 中的 AWS WAF 端点和限额。

您可以使用 AWS WAF 保护以下区域资源类型：

- Amazon API Gateway REST API
- 应用程序负载均衡器
- AWS AppSync GraphQL API
- Amazon Cognito 用户池
- AWS App Runner 服务
- AWS 已验证访问实例

您只能将 Web ACL 关联到 AWS 区域中的应用程序负载均衡器。例如，您无法将 Web ACL 关联到 AWS Outposts上的应用程序负载均衡器。

Web ACL 及其使用的任何其他 AWS WAF 资源必须与受保护资源位于同一区域。在监控和管理受保护区域资源的 Web 请求时，请 AWS WAF 将所有数据与受保护资源保存在同一个区域。

对多重资源关联的限制

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

- 每个 AWS 资源只能与一个 Web ACL 关联。Web ACL 和 AWS 资源之间的关系是 one-to-many。
- 您可以将 Web ACL 与一个或多个 CloudFront 分配相关联。您不能将已与 CloudFront 分配关联的 Web ACL 与任何其他 AWS 资源类型相关联。

入门 AWS WAF

本教程介绍如何使用 AWS WAF 来执行以下任务：

- 设置 AWS WAF。
- 使用控制 AWS WAF 台中的向导创建 Web 访问控制列表 (Web ACL)。
- 选择 AWS WAF 要检查的 Web 请求的 AWS 资源。本教程介绍了 Amazon 的操作步骤 CloudFront。Amazon API Gateway REST API、应用程序负载均衡器、 AWS AppSync GraphQL API、Amazon Cognito 用户池、服务或 AWS 已验证访问 AWS App Runner 实例的过程基本相同。
- 添加要用于筛选 Web 请求的规则和规则组。例如，您可以指定请求的来源 IP 地址以及请求中仅由攻击者使用的值。对于每个规则，您可以指定如何处理匹配的 Web 请求。您可以采取阻止或计算等操作，也可以运行像验证码这样的机器人质询。您可以为在 Web ACL 中定义的每条规则以及您在规则组中定义的每条规则定义操作。
- 请为 Web ACL 指定默认操作（Block 或 Allow）。当 Web ACL 中的规则未明确允许或阻止请求时，这是对请求采取的操作。 AWS WAF

> **Note**
>
> AWS 对于您在本教程中创建的资源，每天向您收取的费用通常少于 0.25 美元。当您完成本教程时，建议您删除资源以避免产生不必要的费用。

主题

第 1 步：设置 AWS WAF

如果您尚未按照 设置您的账户以使用服务 中的常规设置步骤操作，请立即执行操作。

步骤 2：创建 Web ACL

AWS WAF 控制台将指导您完成配置过程， AWS WAF 以根据您指定的标准（例如请求来源的 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。有关 AWS WAF Web ACL 的更多信息，请参阅AWS WAF Web 访问控制列表 (Web ACL)。

创建 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS WAF 主页上，选择创建 Web ACL。
3. 对于 名称，输入要用于标识此 Web ACL 的名称。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

4. （可选）对于 描述 - 可选，如果需要，请输入 Web ACL 的较长描述。
5. 对于CloudWatch 指标名称，如果适用，请更改默认名称。按照控制台上的指导进行有效字符操作。该名称不能包含为 AWS WAF保留的特殊字符、空格或指标名称，包括“All”和“Default_Action”。

   > **Note**
   >
   > 创建 Web ACL 后，您无法更改 CloudWatch 指标名称。

6. 对于资源类型，选择CloudFront分配。区域会自动填充到 Gl obal (CloudFront) 以进行 CloudFront 分配。
7. （可选）对于关联 AWS 资源-可选，选择添加 AWS 资源。在对话框中，选择要关联的资源，然后选择添加。 AWS WAF 返回到描述 Web ACL 和关联的 AWS 资源页面。
8. 选择下一步。

步骤 3：添加字符串匹配规则

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

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

  > **Warning**
  >
  > 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制在中处理超大请求组件 AWS WAF。

  有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。
- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

有关 AWS WAF 规则的更多信息，请参阅AWS WAF 规则。

创建字符串匹配规则语句

1. 在 添加规则和规则组 页面上，选择 添加规则、添加我自己的规则和规则组、规则生成器，然后选择 规则可视化编辑器。

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

2. 对于 名称，输入要用于标识此规则的名称。
3. 对于 类型，选择 常规规则。

4. 对于 如果请求，选择 与语句匹配。

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

5. 在 St at ement 中，对于 Inspect，打开下拉列表并选择 AWS WAF 要检查的 Web 请求组件。对于此示例，选择 标头。

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

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

   在此示例中，选择 完全匹配字符串。这表示 AWS WAF 会检查每个 Web 请求中的用户代理标头，寻找与您指定的字符串相同的字符串。

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

   对于此示例，请输入MyAgent。 AWS WAF 将检查 Web 请求中的`User-Agent`标头以获取值`MyAgent`。

8. 将 文本转换 保留设置为 无。

9. 对于操作，选择您希望规则在与 Web 请求匹配时执行的操作。在此示例中，选择计数，其他选项保持不变。计数操作会为与规则匹配的 Web 请求创建指标，但不会影响请求是允许还是阻止。有关操作选择的更多信息，请参阅 规则操作 和 Web ACL 规则和规则组评估。

10. 选择 添加规则。

步骤 4：添加 AWS 托管规则规则组

AWS 托管规则提供了一组托管规则组供您使用，其中大部分对 AWS WAF 客户免费。有关规则组的更多信息，请参阅AWS WAF 规则组。我们将向此 Web ACL 添加 AWS 托管规则组。

添加 AWS 托管规则规则组

1. 在 添加规则和规则组 页面上，选择 添加规则，然后选择 添加托管规则组。

2. 在添加托管规则组页面上，展开 AWS 托管规则组。（您还将看到为 AWS Marketplace 卖家提供的商品。 您可以订阅他们的产品，然后按照与 AWS 托管规则组相同的方式使用它们。）

3. 对要添加的每个规则组执行以下操作：

   a. 在操作列中，打开添加到 Web ACL切换选项。

b. 选择编辑，然后在规则组的规则列表中打开覆盖所有规则操作下拉列表并选择 Count。这会将规则组中所有规则的操作设置为仅计数。这样，您就可以在使用规则组中的所有规则之前，查看其中的任何规则其对 Web 请求的行为。

c. 选择保存规则。

4. 选择添加规则，然后选择 添加托管规则组。这样，您将返回到添加规则和规则组页面。

步骤 5：完成 Web ACL 配置

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

完成 Web ACL 配置

1. 在 添加规则和规则组 页面上，选择 下一步。
2. 在设置规则优先级页面上，您可以看到 Web ACL 中规则和规则组的处理顺序。 AWS WAF 从列表顶部开始处理它们。您可以通过上下移动规则来更改处理顺序。要执行此操作，请在列表中选择一个，然后选择 上移 或 下移。有关规则优先级的更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。
3. 选择下一步。
4. 在配置指标页面上，对于亚马逊 CloudWatch指标，您可以查看规则和规则组的计划指标，也可以查看网络请求采样选项。有关查看采样请求的信息，请参阅 查看 Web 请求示例。有关 Amazon CloudWatch 指标的信息，请参阅使用 Amazon 进行监控 CloudWatch。

   您可以在 AWS WAF 控制台的 Web ACL 页面的 “流量概述” 选项卡下访问 Web 流量指标摘要。控制台控制面板提供网络 ACL 的 Amazon CloudWatch 指标的近乎实时的摘要。有关更多信息，请参阅 Web ACL 流量概述控制面板。
5. 选择 下一步。
6. 在 审核和创建 Web ACL 页面上，查看您的设置，然后选择 创建 Web ACL。

该向导将返回到 Web ACL 页面，其中列出了您的新 Web ACL。

步骤 6：清除资源

现在您已成功完成了教程。为防止您的账户产生额外 AWS WAF 费用，请清理您创建的 AWS WAF 对象。或者，您可以更改配置以匹配您真正想要管理的 Web 请求 AWS WAF。

> **Note**
>
> AWS 对于您在本教程中创建的资源，每天向您收取的费用通常少于 0.25 美元。完成后，建议您删除资源以防止产生不必要的费用。

删除 AWS WAF 收取费用的对象

1. 在 Web ACL 页面中，从列表中选择您的 Web ACL，然后选择 编辑。
2. 在关联 AWS 资源选项卡上，对于每个关联的资源，选择资源名称旁边的单选按钮，然后选择取消关联。这会断开 Web ACL 与您的 AWS 资源的关联。
3. 在以下每个屏幕中，选择 下一步，直到您返回到 Web ACL 页面。

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

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

AWS WAF Web 访问控制列表 (Web ACL)

Web 访问控制列表 (Web ACL) 可让您对受保护资源响应的所有 HTTP(S) Web 请求进行精细控制。您可以保护亚马逊 CloudFront、亚马逊 API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已验证访问资源。 AWS App Runner

您可以使用如下条件来允许或阻止请求：

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

您还可以针对这些条件的任何组合进行测试。您可以屏蔽或统计不仅满足指定条件，而且在一分钟内超过指定请求数的 Web 请求。您可以使用逻辑运算符组合条件。您还可以根据请求运行验证码拼图和静默客户端会话质询。

您在 AWS WAF 规则语句中提供匹配条件和对匹配项采取的操作。您可以直接在 Web ACL 中定义规则语句，也可以在可重复使用的规则组（您在 Web ACL 中使用的）中进行定义。有关选项的完整列表，请参阅 规则语句基础知识 和 规则操作。

要指定您的 Web 请求检查和处理条件，请执行以下任务：

1. 为与您指定的任何规则都不匹配的 Web 请求选择 Web ACL 默认操作（Allow 或 Block）。有关更多信息，请参阅 Web ACL 默认操作。
2. 添加要在 Web ACL 中使用的任何规则组。托管规则组通常包含阻止 Web 请求的规则。有关规则组的信息，请参阅AWS WAF 规则组。
3. 在一条或多条规则中指定其他匹配条件和处理说明。要添加多个规则，请从 AND 或 OR 规则语句开始，并将要组合的规则嵌套在这些语句下。如果要否定某个规则选项，请将该规则嵌套在 NOT 语句中。您可以选择性地使用基于速率的规则（而不是常规规则）来限制来自满足条件的任何单个 IP 地址的请求数。有关规则的信息，请参阅 AWS WAF 规则。

如果您向 Web ACL 添加多个规则，则 AWS WAF 会按照 Web ACL 中列出的顺序对这些规则进行评估。有关更多信息，请参阅 Web ACL 规则和规则组评估。

创建 Web ACL 时，您可以指定要使用它的资源类型。有关信息，请参阅 创建 Web ACL。定义 Web ACL 后，您可以将其与资源相关联，以开始为资源提供保护。有关更多信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

AWS 资源如何处理来自的响应延迟 AWS WAF

在某些情况下， AWS WAF 可能会遇到内部错误，从而延迟对相关 AWS 资源的响应，以决定是允许还是阻止请求。在这些情况下， CloudFront 通常会允许请求或提供内容，而区域服务通常会拒绝请求并且不提供内容。

主题

- Web ACL 规则和规则组评估
- Web ACL 默认操作
- 管理车身检查的大小限制
- 验证码、挑战和代币的配置
- 使用 Web ACL

Web ACL 规则和规则组评估

Web ACL 对 Web 请求的处理方式取决于以下几点：

- Web ACL 和内部规则组中规则的数字优先级设置
- 规则和 Web ACL 上的操作设置
- 您对添加的规则组中的规则的任何覆盖

有关规则操作设置的列表，请参阅 规则操作。

您可以在规则操作设置和默认 Web ACL 操作设置中自定义请求和响应处理。有关信息，请参阅AWS WAF中的自定义 Web 请求和响应。

主题

- Web ACL 中规则和规则组的处理顺序
- 如何 AWS WAF 处理 Web ACL 中的规则和规则组操作
- 规则组的操作覆盖选项

Web ACL 中规则和规则组的处理顺序

在 Web ACL 和任何规则组中，您可以使用数字优先级设置来确定规则的评估顺序。您必须为 Web ACL 中的每条规则指定该 Web ACL 中唯一的优先级设置，也必须为规则组中的每条规则指定该规则组中唯一的优先级设置。

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

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

例如，假设您的 Web ACL 中有以下规则和规则组，其优先级如下所示：

- Rule1 – 优先级 0
- RuleGroupA — 优先级 100

  - RuleA1 – 优先级 10,000
  - RuleA2 – 优先级 20,000
- Rule2 – 优先级 200
- RuleGroupB — 优先级 300
  - RuleB1 – 优先级 0
  - RuleB2 – 优先级 1

AWS WAF 将按以下顺序评估此 Web ACL 的规则：

- Rule1
- RuleGroupA rulea1
- RuleGroupA rulea2
- Rule2
- RuleGroupB ruleB1
- RuleGroupB ruleB2

如何 AWS WAF 处理 Web ACL 中的规则和规则组操作

配置规则和规则组时，您可以选择 AWS WAF 如何处理匹配的 Web 请求：

- Allow 和 Block 正在终止操作 – Allow 操作 Block 会停止对匹配的 Web 请求进行 Web ACL 的所有其他处理。如果 Web ACL 中的规则找到了与请求的匹配项，并且规则操作为Allow或Block，则该匹配将确定 Web ACL 的 Web 请求的最终处置。 AWS WAF 不处理 Web ACL 中匹配规则之后的任何其他规则。对于直接添加到 Web ACL 的规则和添加的规则组中的规则，此原理同样适用。通过 Block 操作，受保护的资源将无法接收或处理 Web 请求。
- Count 是非终止操作 – 当具有 Count 操作的规则与请求匹配时， AWS WAF 会对请求进行计数，然后继续处理 Web ACL 规则集中的后续规则。
- CAPTCHA并且Challenge可以是非终止或终止操作 — 当具有其中一个操作的规则与请求匹配时，AWS WAF 会检查其令牌状态。如果请求具有有效的令牌，则将匹配项 AWS WAF 视为Count匹配项，然后继续处理 Web ACL 规则集中遵循的规则。如果请求没有有效的令牌，则 AWS WAF 终止评估并向客户端发送验证码拼图或静默的后台客户端会话挑战来解决。

如果规则评估未导致任何终止操作，则将 Web ACL 默认操作 AWS WAF 应用于请求。有关信息，请参阅 Web ACL 默认操作。

在 Web ACL 中，您可以覆盖规则组内规则的操作设置，也可以覆盖规则组返回的操作。有关信息，请参阅 规则组的操作覆盖选项。

操作和优先级设置之间的交互

AWS WAF 适用于 Web 请求的操作受到 Web ACL 中规则的数字优先级设置的影响。例如，假设您的 Web ACL 有一条规则具有 Allow 操作且数字优先级为 50，另一条规则具有 Count 操作且数字优先级为 100。 AWS WAF 按优先级顺序评估 Web ACL 中的规则，从最低设置开始，因此在评估计数规则之前，它将先评估允许规则。同时匹配两个规则的 Web 请求将首先匹配允许规则。因为Allow是终止操作， AWS WAF 将停止对这场比赛的评估，并且不会根据计数规则评估请求。

- 如果您只想在计数规则指标中包含与允许规则不匹配的请求，则可以采用规则的优先级设置。
- 另一方面，如果您想要计数规则中的计数指标，即使请求与允许规则匹配也是如此，则需要为计数规则指定比允许规则更低的数字优先级设置，以便首先运行计数规则。

有关优先级设置的更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

规则组的操作覆盖选项

将规则组添加到 Web ACL 时，您可以覆盖它对匹配的 Web 请求所执行的操作。覆盖 Web ACL 配置中的规则组的操作不会改变规则组本身。它只会改变在 Web ACL 上下文中 AWS WAF 使用规则组的方式。

规则组规则操作优先于规则

您可以将规则组内规则的操作覆盖为任何有效的规则操作。执行此操作时，将完全按照配置规则的操作为覆盖设置处理匹配的请求。

> **Note**
>
> 规则操作可以是终止，也可以是非终止。终止操作会停止对请求的 Web ACL 评估，要么允许请求继续访问受保护的应用程序，要么将其阻止。

以下是规则操作选项：

- Allow— AWS WAF 允许将请求转发到受保护的 AWS 资源进行处理和响应。这是终止操作。在您定义的规则中，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。

- Block— AWS WAF 阻止请求。这是终止操作。默认情况下，您的受保护 AWS 资源以 HTTP 403 (Forbidden) 状态代码进行响应。在您定义的规则中，您可以自定义响应。当 AWS WAF 阻止请求时，Block操作设置将决定受保护资源发送回客户端的响应。
- Count— 对请求进行 AWS WAF 计数，但不确定是允许还是阻止请求。这是一个非终止操作。 AWS WAF 继续处理 Web ACL 中的其余规则。在您定义的规则中，您可以将自定义标头插入请求中，也可以添加其他规则可以匹配的标签。
- CAPTCHA并且 Challenge — AWS WAF 使用 CAPTCHA 谜题和静默挑战来验证请求不是来自机器人，并 AWS WAF 使用代币来跟踪最近成功的客户响应。

  只有当浏览器访问 HTTPS 端点时，才能运行验证码谜题和静默挑战。浏览器客户端必须在安全的环境中运行才能获取令牌。

  > **Note**
  >
  > 当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中将其作为规则操作覆盖时，您需要支付额外费用。有关更多信息，请参阅AWS WAF 定价。

  这些规则操作可以是终止操作，也可以是非终止操作，具体取决于请求中令牌的状态：

  - 未过期的有效令牌不终止 — 如果根据配置的验证码或质疑免疫时间，令牌有效且未过期，则 AWS WAF 处理与操作类似的请求。Count AWS WAF 继续根据 Web ACL 中的其余规则检查 Web 请求。与 Count 配置类似，在您定义的规则中，您可以选择使用自定义标头配置这些操作以插入到请求中，也可以添加其他规则可以匹配的标签。
  - 以对无效或过期令牌的请求被阻止而终止 — 如果令牌无效或指定的时间戳已过期，则 AWS WAF 终止对 Web 请求的检查并阻止请求，类似于操作。Block AWS WAF 然后使用自定义响应代码响应客户端。因为CAPTCHA，如果请求内容表明客户端浏览器可以处理它，则会在 JavaScript 插页式广告中 AWS WAF 发送一个验证码拼图，该拼图旨在区分人类客户端和机器人。对于Challenge操作， AWS WAF 会发送带有静默挑战的 JavaScript 插页式广告，该挑战旨在将普通浏览器与机器人运行的会话区分开来。

  有关更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

有关如何使用此选项的信息，请参阅 覆盖规则组的规则操作。

将规则操作覆盖为 Count

规则操作覆盖的最常见用例是将部分或全部规则操作覆盖到 Count，以测试和监控规则组的行为，然后再将其投入生产。

您也可以使用它对生成误报的规则组进行故障排除。当规则组阻止了您不希望阻止的流量时，就会出现误报。如果您在规则组中发现某条规则将阻止您希望允许通过的请求，则您可以保留该规则的计数操作覆盖，使其无法对您的请求采取行动。

有关在测试中使用规则操作覆盖的更多信息，请参阅 测试和调整您的 AWS WAF 保护措施。

JSON 列表 – **RuleActionOverrides** 取代 **ExcludedRules**

如果您在 2022 年 10 月 27 日之前Count在 Web ACL 配置中将规则组规则操作设置为，请在 Web ACL JSON 中将覆盖内容 AWS WAF 保存为ExcludedRules。现在，用于将规则替换为 Count 的 JSON 设置位于 RuleActionOverrides 设置中。

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

- 当前设置示例：

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

- 旧设置示例：

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

```
          ]
OLD SETTING
```

我们建议您将您的 JSON 列表中的所有 `ExcludedRules` 设置更新为 `RuleActionOverrides` 设置，并将操作设置为 Count。API 接受任一设置，但如果您只使用新 `RuleActionOverrides` 设置，则您的控制台工作和 API 工作之间的 JSON 列表都将保持一致。

规则组将操作重写返回到 Count

您可以覆盖规则组返回的操作，将其设置为 Count。

> **Note**
>
> 这不是测试规则组中规则的好选择，因为它不会改变 AWS WAF 评估规则组本身的方式。它只会影响如何 AWS WAF 处理规则组评估返回到 Web ACL 的结果。如果要测试规则组中的规则，请使用上一节中描述的方式 规则组规则操作优先于规则。

当您将规则组操作改写为时Count，将正常 AWS WAF 处理规则组评估。

如果规则组中没有匹配的规则，或者所有匹配的规则都有 Count 操作，则此覆盖对规则组或 Web ACL 的处理没有影响。

规则组中第一个与 Web 请求匹配且具有终止规则操作的规则会导致 AWS WAF 停止评估该规则组，并将终止操作结果返回到 Web ACL 评估级别。此时，在 Web ACL 评估中，此替代生效。 AWS WAF 覆盖终止操作，因此规则组评估的结果只是一个Count操作。 AWS WAF 然后继续处理 Web ACL 中的其余规则。

有关如何使用此选项的信息，请参阅 将规则组的评估结果覆盖为 Count。

Web ACL 默认操作

当您创建和配置 Web ACL 时，必须设置 Web ACL 的默认操作。 AWS WAF 将此操作应用于通过所有 Web ACL 规则评估但未应用终止操作的任何 Web 请求。终止操作会停止对请求的 Web ACL 评估，要么允许请求继续访问受保护的应用程序，要么将其阻止。有关规则操作的信息，请参阅 规则操作。

Web ACL 默认操作必须确定 Web 请求的最终处置，因此这是一个终止操作：

- 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 地址或其请求表现为包含恶意 SQL 代码或指定值的攻击者进行访问，请选择 Allow 作为默认操作。然后，向 Web ACL 添加

规则时，请添加标识并阻止要阻止的特定请求的规则。在此操作中，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。

- Block – 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。然后，向 Web ACL 添加规则时，请添加标识并允许要允许的特定请求的规则。默认情况下，对于Block操作， AWS 资源以 HTTP `403 (Forbidden)` 状态代码进行响应，但您可以自定义响应。

有关自定义请求和响应的信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

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

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

托管规则组规则通常使用 Block 操作，但并非所有规则都使用该操作。例如，某些用于机器人控制功能的规则使用 CAPTCHA 和 Challenge 操作设置。有关托管规则组的信息，请参阅托管规则组。

管理车身检查的大小限制

车身检查大小限制是 AWS WAF 可以检查的最大请求主体尺寸。当 Web 请求正文大于限制时，底层主机服务仅将限制范围内的内容转发给以 AWS WAF 供检查。

- 对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB（8,192 字节）。
- 对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB（16,384 字节），您可以将任何资源类型的限制以 16 KB 为增量增加，最多 64 KB。设置选项为 16 KB、32 KB、48 KB 和 64 KB。

超大正文处理

如果您的 Web 流量包括大于限制的正文，则将应用您配置的超大处理方式。有关超大尺寸处理选项的信息，请参阅在中处理超大请求组件 AWS WAF。

提高限额设置的定价注意事项

AWS WAF 对检查处于资源类型默认限制范围内的流量收取基本费率。

对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access 资源，如果您提高限制设置，则 AWS WAF 可以检查的流量将包括身体大小不超过您的新限制。只有检查正文大小大于默认 16 KB 的请求时，您才需要支付额外费用。有关定价的更多信息，请参阅AWS WAF 定价。

修改车身检查尺寸限制的选项

您可以为 API Gateway CloudFront、Amazon Cognito、App Runner 或已验证访问资源配置身体检查大小限制。

创建或编辑 Web ACL 时，可以在资源关联配置中修改正文检查大小限制。有关 API，请参阅 Web ACL 的关联配置，网址为AssociationConfig。有关控制台，请参阅指定 Web ACL 关联资源的页面上的配置。有关控制台配置的指导，请参阅 使用 Web ACL。

验证码、挑战和代币的配置

您可以在 Web ACL 中为使用CAPTCHA或规则操作的Challenge规则以及用于管理 AWS WAF 托管保护的静默客户端挑战的应用程序集成 SDK 配置选项。

这些功能通过验证码拼图对最终用户进行质询，以及为客户端会话提供静默质询，从而减少机器人活动。当客户端成功响应时， AWS WAF 会提供一个令牌供其在 Web 请求中使用，并以上次成功的拼图和质询回复加时间戳。有关更多信息，请参阅 AWS WAF 智能威胁缓解。

在您的 Web ACL 配置中，您可以配置如何 AWS WAF 管理这些令牌：

- 验证码和质询免疫时间 – 它们指定了验证码或质询时间戳的有效期。Web ACL 设置由所有未配置自己的免疫时间设置的规则继承，也由应用程序集成软件开发工具包继承。有关更多信息，请参阅 时间戳过期： AWS WAF 代币免疫时间。
- 令牌域-默认情况下，仅 AWS WAF 接受与 Web ACL 关联的资源域的令牌。如果您配置了令牌域列表，则 AWS WAF 接受列表中所有域的令牌以及关联资源的域的令牌。有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

使用 Web ACL

本节介绍通过 AWS 控制台创建、管理和使用 Web ACL 的过程。

对于您正在使用的任何 Web ACL，您可以在 AWS WAF 控制台的 Web ACL 页面的流量概述选项卡下访问网络流量指标的摘要。控制台控制面板提供了在评估您的应用程序网络流量时 AWS WAF 收集的

Amazon CloudWatch 指标的近乎实时的摘要。有关控制面板的更多信息，请参阅 Web ACL 流量概述控制面板。有关监控 Web ACL 流量的更多信息，请参阅 监控和调整。

> **⚠ 生产流量风险**
>
> 在 Web ACL 中为生产流量部署更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

> **Note**
>
> 在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

主题

- 创建 Web ACL
- 编辑 Web ACL
- 管理 Web ACL 中的规则组行为
- 将 Web ACL 与资源关联或取消关联 AWS
- 删除 Web ACL

创建 Web ACL

要创建新的 Web ACL，请按照本页上的步骤使用 Web ACL 创建向导。

> **⚠ 生产流量风险**
>
> 在 Web ACL 中为生产流量部署更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

> **Note**
>
> 在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

创建 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 请在导航窗格中选择 Web ACL，然后选择 创建 Web ACL。
3. 对于 名称，输入要用于标识此 Web ACL 的名称。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

4. （可选）对于 描述 - 可选，如果需要，请输入 Web ACL 的较长描述。
5. 对于CloudWatch 指标名称，如果适用，请更改默认名称。按照控制台上的指导进行有效字符操作。名称不能包含为其保留的特殊字符、空格或指标名称 AWS WAF，包括 “全部” 和 “Default_Action”。

   > **Note**
   >
   > 创建 Web ACL 后，您无法更改 CloudWatch 指标名称。

6. 在 “资源类型” 下，选择要与此 Web ACL 关联的 AWS 资源类别，即 Amazon CloudFront 分配或区域资源。有关更多信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。
7. 对于区域，如果您选择了区域资源类型，请选择 AWS WAF 要存储 Web ACL 的区域。

   您只需要为区域资源类型选择此选项。对于 CloudFront 分发，对于全球 () 应用程序，区域被硬编码为美国东部（弗吉尼亚北部CloudFront）区域。`us-east-1`
8. （CloudFront、API Gateway、Amazon Cognito、App Runner 和已验证访问权限）对于 Web 请求检查大小限制-可选，如果您想指定不同的身体检查大小限制，请选择该限制。检查机身大小超过默认值 16 KB 可能会产生额外费用。有关此选项的更多信息，请参阅管理车身检查的大小限制。
9. （可选）对于关联 AWS 资源-可选，如果您想立即指定资源，请选择添加 AWS 资源。在对话框中，选择要关联的资源，然后选择添加。 AWS WAF 返回到描述 Web ACL 和关联 AWS 资源页面。
10. 选择下一步。
11. （可选）如果要添加托管规则组，请在 添加规则和规则组 页面上，选择 添加规则，然后选择 添加托管规则组。对要添加的每个托管规则组执行以下操作：

    a. 在添加托管规则组页面上，展开 AWS 托管规则组或您选择的 AWS Marketplace 卖家的列表。

    b. 对于要添加的规则组，在操作列中，打开添加到 Web ACL切换选项。

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

       - 覆盖部分或全部规则的规则操作。如果您没有为规则定义覆盖操作，则评估将使用规则组中定义的规则操作。有关此选项的更多信息，请参阅规则组的操作覆盖选项。
       - 通过添加范围缩小语句，缩小规则组检查的 Web 请求的范围。有关此选项的更多信息，请参阅范围缩小语句。
       - 某些托管规则组要求您提供其他配置。请参阅您的托管规则组提供程序所提供的文档。有关 AWS 托管规则组的特定信息，请参阅AWS 的托管规则 AWS WAF。

       完成设置后，选择保存规则。

    选择 添加规则 以完成托管规则的添加，然后返回 添加规则和规则组 页面。
12. （可选）如果要添加您自己的托管规则组，请在 添加规则和规则组 页面上，选择 添加规则，然后选择 添加我自己的规则和规则组。对要添加的每个规则组执行以下操作：

a. 在 添加我自己的规则和规则组 页面上，选择 规则组。

b. 在名称中，输入要用于此 Web ACL 中的规则组规则的名称。不要使用以 AWS、Shield、PreFM 或 PostFM 开头的名称。这些字符串要么是保留字符串，要么可能与其他服务所管理的规则组混淆。请参阅 其他服务提供的规则组。

c. 从列表中选择您的规则组。

> **Note**
>
> 如果要覆盖自己的规则组的规则操作，请先将其保存到 Web ACL 中，然后在 Web ACL 的规则列表中编辑 Web ACL 和规则组参考语句。您可以将规则操作改写为任何有效的操作设置，就像对托管规则组所做的那样。

d. 选择 添加规则。

13. （可选）如果要添加您自己的规则，请在 添加规则和规则组 页面上，依次选择 添加规则、添加我自己的规则和规则组、规则生成器，然后选择 规则可视化编辑器。

> **Note**
>
> 控制台 规则可视化编辑器 支持一个嵌套级别。例如，您可以使用单个逻辑 AND 或 OR 语句，并在其中嵌套一个级别的其他语句，但不能在逻辑语句中嵌套逻辑语句。要管理更复杂的规则语句，请使用 规则 JSON 编辑器。有关规则的所有选项的信息，请参阅 AWS WAF 规则。
> 此过程涵盖 规则可视化编辑器。

a. 对于 名称，输入要用于标识此规则的名称。不要使用以 AWS、Shield、PreFM 或 PostFM 开头的名称。这些字符串要么是保留字符串，要么可能与其他服务所管理的规则组混淆。

b. 根据您的需求输入您的规则定义。您可以在逻辑 AND 和 OR 规则语句中组合规则。该向导将根据上下文指导您学习每个规则的选项。有关规则选项的信息，请参阅 AWS WAF 规则。

c. 对于 操作，选择您希望规则在与 Web 请求匹配时执行的操作。有关您的选择的信息，请参阅规则操作和 Web ACL 规则和规则组评估。

如果您使用的是 CAPTCHA 或 Challenge 操作，请根据规则的需要调整免疫时间配置。如果您未指定设置，则规则将从 Web ACL 继承设置。要修改 Web ACL 免疫时间设置，请在创建 Web ACL 后对其进行编辑。有关免疫时间的更多信息，请参阅 时间戳过期： AWS WAF 代币免疫时间。

> **Note**
>
> 当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中将其作为规则操作覆盖时，您需要支付额外费用。有关更多信息，请参阅AWS WAF 定价。

如果您想自定义请求或响应，请选择相应选项并填写自定义的详细信息。有关更多信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

如果您想让您的规则为匹配的 Web 请求添加标签，请选择相应选项并填写标签详细信息。有关更多信息，请参阅 AWS WAF 网络请求上的标签。

d. 选择 添加规则。

14. 选择 Web ACL 的默认操作（Block 或 Allow）。当 Web ACL 中的规则未明确允许或阻止请求时，这是对请求采取的操作。 AWS WAF 有关更多信息，请参阅 Web ACL 默认操作。

    如果您想自定义默认操作，请选择相应选项并填写自定义的详细信息。有关更多信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

15. 您可以定义令牌域列表，以便在受保护的应用程序之间实现令牌共享。当您使用 AWS 托管规则组进行 AWS WAF 欺诈控制账户创建、防欺诈 (ACFP)、防欺诈控制账户接管 (ATP) 和机器人控制时， AWS WAF 令牌由和Challenge AWS WAF 操作以及应用程序集成 SDK 使用。CAPTCHA

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

    默认情况下，仅 AWS WAF 接受受保护资源域的令牌。如果您在此列表中添加令牌域，则 AWS WAF 接受列表中所有域和关联资源域的令牌。有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

16. 选择 下一步。

17. 在 “设置规则优先级” 页面中，选择您的规则和规则组，然后按照您想要的顺序 AWS WAF 进行处理。 AWS WAF 从列表顶部开始处理规则。保存 Web ACL 时， AWS WAF 会按照规则的列出顺序为规则分配数字优先级设置。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

18. 选择 下一步。

19. 在配置指标页面中，查看选项并应用所需的任何更新。您可以通过为多个来源提供相同的CloudWatch 指标名称来合并这些指标。

20. 选择下一步。

21. 在 审核和创建 Web ACL 页面中，检查您的定义。如果要更改任何区域，请为该区域选择 Edit (编辑)。这将使您返回到 Web ACL 向导中的页面。进行任何更改，然后在后续页面中选择 下一步，直到您返回 审核和创建 Web ACL 页面。
22. 选择 创建 Web ACL。您的新 Web ACL 将在 Web ACL 页面中列出。

编辑 Web ACL

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

生产流量风险

在 Web ACL 中为生产流量部署更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

Note

在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

编辑 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述。

Note

由管理的 Web ACL AWS Firewall Manager 的名称以开头`FMManagedWebACLV2-`。Firewall Manager 管理员通过防火墙管理器 AWS WAF 策略对其进行管理。这些 Web ACL 可能包含指定为在 Web ACL 中最先运行和最后运行的规则组集，这两个规则组集分别位于由您添加和管理的任何规则或规则组的两端。您无法更改任何第一个和最后一个规则组规范。第一个和最后一个规则组的名称分别以

PREFMManaged- 和 POSTFMManaged- 开头。有关这些策略的更多信息，请参阅 AWS WAF 政策。

4. 根据需要编辑 Web ACL。选择您感兴趣的配置区域的选项卡，然后编辑可变设置。对于您编辑的每个设置，当您选择保存并返回 Web ACL 的描述页面时，控制台会保存您对 Web ACL 所做的更改。

   下面列出了包含 Web ACL 配置组件的选项卡。

   - 规则选项卡
     - 在 Web ACL 中定义的规则 – 您可以编辑和管理在 Web ACL 中定义的规则，正如您创建 Web ACL 时的操作一样。

       > **Note**
       >
       > 请勿更改任何未手动添加到 Web ACL 的规则的名称。如果您使用其他服务为您管理规则，则更改其名称可能会取消或削弱他们提供预期保护的能力。 AWS Shield Advanced 并且 AWS Firewall Manager 两者都在您的 Web ACL 中创建规则。有关信息，请参阅 其他服务提供的规则组。

       > **Note**
       >
       > 如果您更改了规则的名称，并且希望该规则的指标名称反映更改，则还必须更新该指标名称。 AWS WAF 当您更改规则名称时，不会自动更新规则的指标名称。在控制台中编辑规则时，您可以使用规则 JSON 编辑器更改指标名称。您也可以通过 API 以及在用于定义 Web ACL 或规则组的任何 JSON 列表中更改这两个名称。

       有关规则和规则组设置的信息，请参阅 AWS WAF 规则 和 AWS WAF 规则组。
     - Web ACL 规则使用的容量单位 – Web ACL 的当前容量使用情况。这一项仅供查看。
     - 与任何规则都不匹配的请求的默认 Web ACL 操作 – 有关此设置的信息，请参阅 Web ACL 默认操作。
     - Web ACL 验证码和质询配置 – 这些免疫时间决定了验证码或质询令牌在被获取后的有效时间。只有在创建 Web ACL 之后，才能在此处修改此设置。有关这些设置的信息，请参阅时间戳过期： AWS WAF 代币免疫时间。

    - 令牌域名列表 — AWS WAF 接受列表中所有域名和关联资源域的令牌。有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。
- “关联 AWS 资源” 选项卡
    - Web 请求检查大小限制 — 仅适用于保护 CloudFront 分发的 Web ACL。车身检查的大小限制决定了车身部件的多少被转 AWS WAF 送到接受检查。有关该设置的更多信息，请参阅 管理车身检查的大小限制。
    - 关联 AWS 资源-Web ACL 当前关联并保护的资源列表。您可以找到与 Web ACL 位于同一区域的资源，并将它们与 Web ACL 关联起来。有关更多信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。
- 自定义响应正文选项卡
    - 自定义响应正文可供将操作设置为 Block 的 Web ACL 规则使用。有关更多信息，请参阅 Block 操作的自定义响应。
- 日志和指标选项卡
    - 日志记录 – 记录 Web ACL 评估的流量。有关信息，请参阅 记录 AWS WAF Web ACL 流量。
    - 采样的请求 – 有关与 Web 请求匹配的规则的信息。有关查看采样请求的信息，请参阅 查看 Web 请求示例。
    - CloudWatch 指标 — Web ACL 中规则的指标。有关 Amazon CloudWatch 指标的信息，请参阅使用 Amazon 进行监控 CloudWatch。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

管理 Web ACL 中的规则组行为

本节介绍修改在 Web ACL 中使用规则组的方式的选项。此信息适用于所有规则组类型。将规则组添加到 Web ACL 后，您可以将规则组中各个规则的操作覆盖为 Count 或任何其他有效的规则操作设置。您也可以将规则组生成的操作覆盖为 Count，这不会影响规则组内规则的评估方式。

有关这些选项的信息，请参阅 规则组的操作覆盖选项。

覆盖规则组的规则操作

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

最常见的用例是将规则操作覆盖为 Count 以测试新的或更新的规则。如果您启用了指标，则会收到您覆盖的每条规则的指标。有关测试的更多信息，请参阅 测试和调整您的 AWS WAF 保护措施。

覆盖规则组的规则操作

您可以在向 Web ACL 添加托管规则组时进行这些更改，也可以在编辑 Web ACL 时对任何类型的规则组进行更改。这些说明适用于已添加到 Web ACL 的规则组。有关此选项的更多信息，请访问规则组规则操作优先于规则。

1. 编辑 Web ACL。
2. 在 Web ACL 页面的规则选项卡中，选择规则组，然后选择编辑。
3. 在规则组的规则部分，根据需要管理操作设置。
   - 所有规则 – 要为规则组中的所有规则设置覆盖操作，请打开覆盖所有规则操作下拉列表并选择覆盖操作。要移除所有规则的覆盖，请选择移除所有覆盖。
   - 单一规则 – 要为单个规则设置覆盖操作，请打开该规则的下拉列表并选择覆盖操作。要移除规则的覆盖，请打开该规则的下拉列表并选择移除覆盖。
4. 完成更改后，选择保存规则。规则操作和覆盖操作设置列于规则组页面中。

以下 JSON 列表示例显示了 Web ACL 中的规则组语句，该语句将规则操作覆盖为适用 `CategoryVerifiedSearchEngine` 和 `CategoryVerifiedSocialMedia` 规则的 Count。在 JSON 中，您可以通过为每条规则提供一个 `RuleActionOverrides` 条目来覆盖所有规则操作。

```
{
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
```

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

将规则组的评估结果覆盖为 Count

您可以覆盖规则组评估产生的操作，而无需更改规则组中规则的配置或评估方式。此选项并不是常用选项。如果规则组中的任何规则产生了匹配，则此覆盖会将规则组产生的操作设置为 Count。

> **Note**
>
> 这是一个不常见的用例。大多数操作覆盖都是在规则级别的规则组内完成的，如中所覆盖规则组的规则操作述。

添加或编辑规则组时，可以在 Web ACL 中覆盖规则组生成的操作。在控制台中，打开规则组的覆盖规则组操作（可选）窗格并启用覆盖。在 JSON 集 `OverrideAction` 中的规则组语句中，如以下示例列表中所示：

```
{
```

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

将 Web ACL 与资源关联或取消关联 AWS

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

- 将区域 Web ACL 与下面列出的任何区域资源相关联。对于此选项，Web ACL 必须与您的资源位于同一区域。
  - Amazon API Gateway REST API
  - 应用程序负载均衡器
  - AWS AppSync GraphQL API
  - Amazon Cognito 用户池
  - AWS App Runner 服务
  - AWS 已验证访问实例
- 将全球网络 ACL 与 Amazon CloudFront 分配关联。全局 Web ACL 将具有美国东部（弗吉尼亚州北部）区域的硬编码区域。

在创建或更新 CloudFront 分配本身时，也可以将 Web ACL 与分配相关联。有关信息，请参阅《Amazon CloudFront 开发者指南》中的使用 AWS WAF 来控制对您的内容的访问权限。

对多重关联的限制

根据以下限制，您可以将单个 Web ACL 与一个或多个 AWS 资源相关联：

- 每个 AWS 资源只能与一个 Web ACL 关联。Web ACL 和 AWS 资源之间的关系是 one-to-many。
- 您可以将 Web ACL 与一个或多个 CloudFront 分配相关联。您不能将已与 CloudFront 分配关联的 Web ACL 与任何其他 AWS 资源类型相关联。

其他限制。

当关联 Web ACL 时，以下限制也将适用：

- 您只能将 Web ACL 关联到 AWS 区域中的应用程序负载均衡器。例如，您无法将 Web ACL 关联到 AWS Outposts上的应用程序负载均衡器。
- 您无法将 Amazon Cognito 用户池与使用 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 托管规则组`AWSManagedRulesACFPRuleSet`或欺 AWS WAF 诈控制账户接管预防 (ATP) 托管规则组的网络 ACL 关联。`AWSManagedRulesATPRuleSet`有关账户创建欺诈预防的信息，请参阅 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP)。有关账户盗用防护的信息，请参阅 AWS WAF 防欺诈控制账户接管 (ATP)。

> **⚠ 生产流量风险**
>
> 在为生产流量部署 Web ACL 之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对您的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

将 Web ACL 与 AWS 资源关联

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

解除 Web ACL 与资源的关联 AWS

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 Web ACL。
3. 选择要从资源取消关联的 Web ACL 名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在关联 AWS 资源选项卡上，选择要取消与此 Web ACL 关联的资源。

   > **Note**
   >
   > 一次必须取消关联一个资源。请勿选择多个资源。

5. 选择取消关联。控制台打开确认对话框。确认您选择解除 Web ACL 与 AWS 资源的关联。

删除 Web ACL

要删除 Web ACL，首先要取消所有 AWS 资源与 Web ACL 的关联。请执行以下过程。

删除 Web ACL

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

AWS WAF 规则组

规则组是您添加到 Web ACL 的一组可重复使用的规则。有关 Web ACL 的更多信息，请参阅AWS WAF Web 访问控制列表 (Web ACL)。

规则组主要分为以下类别：

- 您自己的规则组，由您自己创建和维护
- 托 AWS 管规则团队为您创建和维护的托管规则组。
- AWS Marketplace 卖家为您创建和维护的托管规则组。
- 由其他服务（例如 AWS Firewall Manager 和 Shield Advanced）拥有和管理的规则组。

规则组和 Web ACL 之间的区别

规则组和 Web ACL 都包含规则，其定义方式相同。规则组与 Web ACL 的区别如下：

- 规则组不能包含规则组引用语句。
- 通过向每个 Web ACL 添加规则组引用语句，可以在多个 Web ACL 中重复使用单个规则组。您不能重复使用 Web ACL。
- 规则组没有默认操作。在 Web ACL 中，您可以为包含的每个规则或规则组设置默认操作。规则组或 Web ACL 中的每个规则都定义了一个操作。
- 您不能直接将规则组与 AWS 资源相关联。要使用规则组保护资源，请在 Web ACL 中使用规则组。
- Web ACL 具有系统定义的最大容量，即为 5,000 Web ACL 容量单位 (WCU)。每个规则组的 WCU 设置必须在创建时设置。您可以使用此设置来计算使用规则组会给您的 Web ACL 增加多少额外容量需求。有关 WCU 的更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU)。

有关规则的信息，请参阅 AWS WAF 规则。

本部分提供有关创建和管理规则组的指导，介绍可供您使用的托管规则组，并提供托管规则组的使用指导。

主题

托管规则组

托管规则组是 AWS Marketplace 卖家为您编写 AWS 和维护的预定义 ready-to-use 规则的集合。基本 AWS WAF 定价适用于您对任何托管规则组的使用。有关 AWS WAF 定价信息，请参阅AWS WAF 定价。

- 除基本 AWS WAF 费用外， AWS WAF 机器人控制、 AWS WAF 欺诈控制账户接 AWS 管预防 (ATP) 和 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 的托管规则组需支付额外费用。有关定价的详细信息，请参阅 AWS WAF 定价。
- 所有其他 AWS 托管规则组均可供 AWS WAF 客户使用，无需支付额外费用。
- AWS Marketplace 托管规则组可通过订阅获得 AWS Marketplace。这些规则组中的每一个都由 AWS Marketplace 卖家拥有和管理。有关使用 AWS Marketplace 托管规则组的定价信息，请联系 AWS Marketplace 卖家。

一些托管规则组旨在帮助保护特定类型的 Web 应用程序WordPress，例如 Joomla 或 PHP。其他托管规则组可提供广泛的保护功能以应对已知威胁或常见的 Web 应用程序漏洞，包括 OWASP 十大漏洞中列出的一些漏洞。如果您需要符合监管合规性（如 PCI 或 HIPAA），您可以使用托管规则组来满足 Web 应用程序防火墙要求。

自动更新

随时了解不断变化的威胁情形会非常耗时且成本高昂。当您实施并使用 AWS WAF时，托管规则组可以帮助您节省时间。当出现新的漏洞 AWS 和威胁时，许多 AWS Marketplace 卖家会自动更新托管规则组并提供新版本的规则组。

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

限制访问托管规则组中的规则

每个托管规则组都提供了旨在防护的攻击和漏洞类型的全面描述。为了保护规则组提供程序的知识产权，您将无法查看规则组中的单个规则的所有详细信息。此限制还有助于避免恶意用户设计专门避开已发布规则的威胁。

主题

- 受版本控制的托管规则组
- 使用托管规则组
- AWS 的托管规则 AWS WAF
- AWS Marketplace 托管规则组

受版本控制的托管规则组

许多托管规则组提供者使用版本控制来更新规则组的选项和功能。通常，托管规则组的特定版本是静态的。有时，提供商可能需要更新托管规则组的部分或全部静态版本，以应对新出现的安全威胁。

在 Web ACL 中使用版本化托管规则组时，您可以选择默认版本并让提供商管理您使用的静态版本，也可以选择特定的静态版本。

找不到您想要的版本？

如果您在规则组的版本列表中看不到任何版本，则该版本可能已计划到期或已经过期。在某个版本计划到期后， AWS WAF 不再允许您为规则组选择该版本。

AWS 托管规则规则组的 SNS 通知

除 IP 信誉规则组外， AWS 托管规则组都提供版本控制和 SNS 更新通知。提供通知的 AWS 托管规则组都使用相同的 SNS 主题 Amazon 资源名称 (ARN)。要注册 SNS 通知，请参阅收到有关新版本和更新的通知。

主题

- 托管规则组的版本生命周期
- 托管规则组的版本过期
- 处理托管规则组版本的最佳实践

托管规则组的版本生命周期

提供程序会处理托管规则组静态版本的以下生命周期阶段：

- 发布和更新 – 托管规则组提供程序通过向 Amazon Simple Notification Service (Amazon SNS)主题发出通知，宣布其托管规则组即将推出以及其托管规则组的新静态版本。提供程序还可以使用该主题来传达有关其规则组的其他重要信息，例如紧急更新。

  您可以订阅规则组的主题并配置接收通知的方式。有关更多信息，请参阅 收到有关新版本和更新的通知。
- 过期计划 – 托管规则组提供程序制定旧版本规则组的过期计划。已计划过期的版本将无法添加到您的 Web ACL 规则中。在某个版本计划到期后，在 Amazon 中使用倒计时指标 AWS WAF 跟踪到期时间 CloudWatch。

- 版本过期-如果您将 Web ACL 配置为使用托管规则组的过期版本，则在 Web ACL 评估期间，将 AWS WAF 使用该规则组的默认版本。此外，还会 AWS WAF 阻止对 Web ACL 的任何更新，这些更新既不会移除规则组，也不会将其版本更改为未过期的规则。

如果您使用 AWS Marketplace 托管规则组，请向提供商询问有关版本生命周期的任何其他信息。

托管规则组的版本过期

如果您使用规则组的特定版本，请确保不要继续使用已过期的版本。您可以通过规则组的 SNS 通知和 Amazon CloudWatch 指标来监控版本过期。

如果您在 Web ACL 中使用的版本已过期，则会 AWS WAF 阻止对 Web ACL 的任何更新，其中不包括将规则组移至未过期的版本。您可以将规则组更新到可用版本或将其从 Web ACL 中删除。

托管规则组的过期处理取决于规则组提供程序。对于 AWS 托管规则组，过期的版本会自动更改为规则组的默认版本。对于 AWS Marketplace 规则组，请向提供者询问他们如何处理过期问题。

当提供程序创建新版本的规则组时，它会设置该版本的预测生命周期。虽然版本未计划到期，但 Amazon CloudWatch 指标值将设置为预测的生命周期设置，在中 CloudWatch，您将看到该指标的固定值。在提供程序计划指标到期后，指标值每天都会递减，直到到期当天达到 0。有关监控过期的信息，请参阅追踪版本过期。

处理托管规则组版本的最佳实践

使用版本控制托管规则组时，请遵循这项处理版本控制的最佳实践指南。

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

- 默认版本- AWS WAF 始终将默认版本设置为提供商当前推荐的静态版本。当提供程序更新其推荐的静态版本时， AWS WAF 会自动更新 Web ACL 中规则组的默认版本设置。

  当您使用托管规则组的默认版本时，最佳做法是执行以下操作：

  - 订阅通知 – 订阅规则组变更通知并密切关注这些变更。大多数提供程序会发送有关新静态版本和默认版本变更的高级通知。它们允许您在将默认版本 AWS 切换到新静态版本之前检查其效果。有关更多信息，请参阅 收到有关新版本和更新的通知。
  - 查看静态版本设置的影响，并在将默认版本设置为静态版本之前根据需要进行调整 – 在将默认版本设置为新的静态版本之前，请查看静态版本对监控和管理 Web 请求的影响。新的静态版本可能有新的规则需要审查。如果您需要修改规则组的使用方式，请查找误报或其他意外行为。例如，您可以将规则设置为计数，以明确如何处理新行为，同时阻止它们阻塞流量。有关更多信息，请参阅测试和调整您的 AWS WAF 保护措施。

- 静态版本 – 如果您选择使用静态版本，则在准备采用新版本的规则组时，必须手动更新版本设置。

  当您使用托管规则组的静态版本时，最佳做法是执行以下操作：

  - 始终保持最新版本 – 您的托管规则组应尽可能接近最新版本。发布新版本时，请对其进行测试，根据需要调整设置，并及时实施新版本。有关测试的信息，请参阅 测试和调整您的 AWS WAF 保护措施。
  - 订阅通知 – 订阅规则组变更通知，以了解提供程序何时发布新的静态版本。大多数提供程序会提前通知版本更改。此外，为了修复安全漏洞或出于其他紧急原因，提供程序有时可能需要更新您正在使用的静态版本。如果您订阅了提供程序通知，您便能够及时获知最新情况。有关更多信息，请参阅 收到有关新版本和更新的通知。
  - 避免版本过期 – 避免让静态版本在您使用期间过期。提供程序对过期版本的处理可能有所不同，可能包括强制升级到可用版本或其他可能产生意想不到的后果的更改。跟踪到 AWS WAF 期指标并设置警报，让您在足够的时间内成功升级到支持的版本。有关更多信息，请参阅 追踪版本过期。

使用托管规则组

本节提供有关访问和管理托管规则组的指导。

将托管规则组添加到 Web ACL 时，您可以根据您自己的规则组选择相同的配置选项，也可以选择其他设置。

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

在 Web ACL 中使用托管规则组时，可以编辑以下设置：

- 版本 – 仅当规则组已进行版本控制时才可用。有关更多信息，请参阅 受版本控制的托管规则组。
- 覆盖规则操作 – 您可以将规则组中规则的操作覆盖为任何操作。将其设置为 Count 有助于在使用规则组管理 Web 请求之前对其进行测试。有关更多信息，请参阅 规则组规则操作优先于规则。
- 缩小范围语句 – 您可以添加范围缩小语句，以筛选出您不想使用规则组进行评估的 Web 请求。有关更多信息，请参阅 范围缩小语句。
- 覆盖规则组操作 – 您可以覆盖规则组评估所产生的操作，并将其设置为“仅限 Count”。该选项不是常用选项。它不会改变 AWS WAF 评估规则组中规则的方式。有关更多信息，请参阅 规则组将操作重写返回到 Count。

编辑 Web ACL 中的托管规则组设置

- 控制台
  - （可选）将托管规则组添加到 Web ACL 时，可以选择编辑来查看和编辑设置。
  - （可选）将托管规则组添加到 Web ACL 后，从 Web ACL 页面中选择您刚刚创建的 Web ACL。这会使您转至 Web ACL 编辑页面。
    - 选择 规则。
    - 选择规则组，然后选择编辑以查看和编辑设置。
- API 和 CLI – 在控制台之外，您可以在创建和更新 Web ACL 时管理托管规则组设置。

检索托管规则组列表

您可以检索可供您在 Web ACL 中使用的托管规则组列表。列表包含以下内容：

- 所有 AWS 托管规则规则组。
- 您已订阅的 AWS Marketplace 规则组。

> **Note**
>
> 有关订阅 AWS Marketplace 规则组的信息，请参阅AWS Marketplace 托管规则组。

检索托管规则组列表时，返回的列表取决于您使用的接口：

- 控制台-通过控制台，您可以查看所有托管规则组，包括您尚未订阅的 AWS Marketplace 规则组。对于您尚未订阅的内容，该界面提供了可供您订阅的链接。
- API 和 CLI – 在控制台之外，您的请求仅返回可供您使用的规则组。

检索托管规则组列表

- 控制台 – 在创建 Web ACL 的过程中，在添加规则和规则组页面上，选择添加托管规则组。此时将在顶层列出提供程序名称。展开每个提供程序列表以查看托管规则组的列表。对于受版本控制规则组，此级别显示的信息是默认版本的信息。当您将托管规则组添加到 Web ACL 时，控制台会根据命名方案 `<Vendor Name>-<Managed Rule Group Name>` 列出规则组。
- API –
  - `ListAvailableManagedRuleGroups`

- CLI –
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

检索托管规则组中的规则

您可以检索托管规则组中的规则列表。API 和 CLI 调用会返回规则规范，您可以在 JSON 模型中或通过这些规则进行引用 AWS CloudFormation。

检索托管规则组中的规则列表

- 控制台
  - （可选）将托管规则组添加到 Web ACL 时，可以选择编辑来查看规则。
  - （可选）将托管规则组添加到 Web ACL 后，从 Web ACL 页面中选择您刚刚创建的 Web ACL。这会使您转至 Web ACL 编辑页面。
    - 选择 规则。
    - 选择要查看其规则列表的规则组，然后选择编辑。 AWS WAF 显示了规则组中的规则列表。
- API – `DescribeManagedRuleGroup`
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

检索托管规则组的可用版本

托管规则组的可用版本是尚未计划到期的版本。该列表显示哪个版本是规则组的当前默认版本。

检索托管规则组的可用版本列表

- 控制台
  - （可选）将托管规则组添加到 Web ACL 时，选择编辑以查看该规则组的信息。展开版本下拉列表以查看可用版本列表。
  - （可选）将托管规则组添加到 Web ACL 后，在 Web ACL 上选择 编辑，然后选择并编辑该规则组规则。展开版本下拉列表以查看可用版本列表。
- API –
  - `ListAvailableManagedRuleGroupVersions`
- CLI –

- `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

通过控制台向 Web ACL 添加托管规则组

本指南适用于所有 AWS 托管规则规则组以及您订阅的 AWS Marketplace 规则组。

> **生产流量风险**
>
> 在 Web ACL 中为生产流量部署更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

> **Note**
>
> 在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

通过控制台向 Web ACL 添加托管规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 Web ACL。
3. 在 Web ACL 页面中，从 Web ACL 列表中选择规则组要加入的 Web ACL。然后，您将进入单个 Web ACL 的页面。
4. 在 Web ACL 页面中，选择规则选项卡。
5. 在规则窗格中，选择添加规则，然后选择添加托管规则组。
6. 在添加托管规则组页面中，展开规则组供应商的选择范围，以查看可用规则组列表。
7. 对于每个要添加的规则组，请选择添加到 Web ACL。如果要更改规则组的 Web ACL 配置，请选择编辑，进行更改，然后选择保存规则。有关这些选项的信息，请在 受版本控制的托管规则组 中参阅版本控制指南，并在 托管规则组语句 中参阅在 Web ACL 中使用托管规则组的指南。
8. 在添加托管规则组页面的底部，选择添加规则。

9. 在设置规则优先级页面中，根据需要调整规则的运行顺序，然后选择保存。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

在您的 Web ACL 页面中，您添加的托管规则组列在规则选项卡下。

在将 AWS WAF 保护措施用于生产流量之前，请先对其进行测试和调整。有关信息，请参阅 测试和调整您的 AWS WAF 保护措施。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

收到有关托管规则组新版本和更新的通知

托管规则组提供程序使用 SNS 通知来宣布规则组的更改，例如即将推出的新版本和紧急安全更新。

如何订阅 SNS 通知

要订阅规则组的通知，您需要在美国东部（弗吉尼亚州北部）区域 us-east-1 为规则组的 Amazon SNS 主题 ARN 创建 Amazon SNS 订阅。

有关如何订阅的信息，请参阅 Amazon Simple Notification Service 开发人员指南。

> **Note**
>
> 仅在 us-east-1 区域创建 SNS 主题订阅。

版本控制的 AWS 托管规则组都使用相同的 SNS 主题 Amazon 资源名称 (ARN)。有关 AWS 托管规则组通知的更多信息，请参阅部署通知。

从哪里找到托管规则组的 Amazon SNS 主题 ARN

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

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

有关 Amazon SNS 通知格式以及如何筛选收到的通知的一般信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的解析消息格式和 Amazon SNS 订阅筛选策略。

追踪规则组的版本过期时间

如果您使用规则组的特定版本，请确保不要继续使用已过期的版本。

> **Tip**
>
> 注册接收托管规则组的 Amazon SNS 通知，并及时了解托管规则组的版本。您将受益于规则组 up-to-date 提供的最多保护，并在到期之前保持领先地位。有关信息，请参阅 收到有关新版本和更新的通知。

通过 Amazon 监控托管规则组的到期日程安排 CloudWatch

1. 在中 CloudWatch，找到您的托管规则组 AWS WAF 的到期指标。这些指标具有以下指标名称和维度：
   - 指标名称：DaysToExpiry
   - 指标维度：Region、ManagedRuleGroup、Vendor 和 Version

   如果 Web ACL 中有一个用于评估流量的托管规则组，则您将获得相应的指标。该指标不适用于您不使用的规则组。

2. 对您感兴趣的指标设置警报，以便及时通知您切换到更高版本的规则组。

有关使用亚马逊 CloudWatch 指标和配置警报的信息，请参阅亚马逊 CloudWatch 用户指南。

JSON 和 YAML 中的托管规则组配置示例

API 和 CLI 调用会返回托管规则组中所有规则的列表，您可以在 JSON 模型中或通过这些规则进行引用 AWS CloudFormation。

JSON

您可以使用 JSON 在规则语句中引用和修改托管规则组。下表显示了 JSON 格式的 AWS 托管规则组。`AWSManagedRulesCommonRuleSet`在 RuleActionOverrides 规范列出的规则中，其操作已被覆盖为 Count。

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

          {

            "ActionToUse": {

              "Count": {}

            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
```

```
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

您可以使用 AWS CloudFormation YAML 模板在规则语句中引用和修改托管规则组。下表显示了 AWS CloudFormation 模板中的 “ AWS 托管规则” 规则组。AWSManagedRulesCommonRuleSet在 RuleActionOverrides 规范列出的规则中，其操作已被覆盖为 Count。

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS 的托管规则 AWS WAF

AWS 的托管规则 AWS WAF 是一项托管服务，可针对常见的应用程序漏洞或其他有害流量提供保护。您可以选择从 AWS 托管规则中为每个 Web ACL 选择一个或多个规则组，最高不超过 Web ACL 容量单位 (WCU) 的最大限制。

减少误报并测试规则组的更改

在生产环境中使用任何托管规则组之前，请根据 测试和调整您的 AWS WAF 保护措施 中的指导在非生产环境中对其进行测试。在向 Web ACL 添加规则组以测试规则组的新版本时，以及在规则组无法按需要处理 Web 流量时，请遵循测试和调整指南。

共同分担安全责任

AWS 托管规则旨在保护您免受常见 Web 威胁的侵害。根据文档使用 AWS 托管规则组时，可以为您的应用程序增加另一层安全保护。但是， AWS 托管规则规则组并不是用来取代您的安全职责，后者由您选择的 AWS 资源决定。请参阅分担责任模型，确保您的资源 AWS 得到适当保护。

AWS 托管规则规则组列表

我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

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

> **Note**
>
> 有关检索 AWS 托管规则组版本的信息，请参阅检索托管规则组的可用版本。

所有 AWS 托管规则组都支持标签，本节中的规则列表包括标签规范。您可以通过调用 `DescribeManagedRuleGroup` 从 API 检索托管规则组的标签。标签列在响应的 AvailableLabels 属性中。有关标签的信息，请参阅 AWS WAF 网络请求上的标签。

在将 AWS WAF 保护措施用于生产流量之前，请先对其进行测试和调整。有关信息，请参阅 测试和调整您的 AWS WAF 保护措施。

AWS 托管规则规则组

- 基准规则组
  - 核心规则集 (CRS) 托管规则组
  - 管理员保护托管规则组
  - 已知错误输入托管规则组
- 使用案例特定规则组
  - SQL 数据库托管规则组
  - Linux 操作系统托管规则组
  - POSIX 操作系统托管规则组
  - Windows 操作系统托管规则组

基准规则组

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

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

核心规则集 (CRS) 托管规则组

VendorName:AWS，名称：AWSManagedRulesCommonRuleSet，WCU：700

核心规则集 (CRS) 规则组包含通常适用于 Web 应用程序的规则。该规则组有助于防止利用各种漏洞，包括 OWASP 出版物（如 OWASP Top 10）中描述的一些高风险和经常发生的漏洞。考虑将此规则组用于任何 AWS WAF 用例。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
NoUserAgent_HEADER	检查是否存在缺少 HTTP User-Agent 标头的请求。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:NoUserAgent_Header
UserAgent_BadBots_HEADER	检查是否存在表明请求是恶意机器人的常见 User-Agent 标头值。示例模式包括 nessus

Rule name（规则名称）	描述和标签
	和 nmap。有关机器人管理的信息，另请参阅 AWS WAF 机器人控制规则组。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:BadBots_Header
SizeRestrictions_QUERYSTRING	检查是否存在超过 2,048 字节的 URI 查询字符串。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString
SizeRestrictions_Cookie_HEADER	检查是否存在超过 10,240 字节的 Cookie 标头。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header
SizeRestrictions_BODY	检查是否存在超过 8 KB（8,192 字节）的请求正文。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:SizeRestrictions_Body

Rule name（规则名称）	描述和标签
`SizeRestrictions_URIPATH`	检查 URI 路径是否超过 1024 字节。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`
`EC2MetaDataSSRF_BODY`	检查是否存在恶意方试图从请求正文中泄漏 Amazon EC2 元数据。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Rule name（规则名称）	描述和标签
EC2MetaDataSSRF_COOKIE	检查是否存在恶意方试图从请求 Cookie 中泄漏 Amazon EC2 元数据。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie
EC2MetaDataSSRF_URIPATH	检查是否存在恶意方试图从请求 URI 路径中泄漏 Amazon EC2 元数据。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath
EC2MetaDataSSRF_QUERYARGUMENTS	检查是否存在恶意方试图从请求查询参数中泄漏 Amazon EC2 元数据。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments
GenericLFI_QUERYARGUMENTS	检查查询参数中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 `../../` 的技术尝试遍历路径。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments

Rule name（规则名称）	描述和标签
`GenericLFI_URIPATH`	检查 URI 路径中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 `../../` 的技术尝试遍历路径。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`
`GenericLFI_BODY`	检查请求正文中是否存在本地文件包含 (LFI) 攻击。示例包括使用类似于 `../../` 的技术尝试遍历路径。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Rule name（规则名称）	描述和标签
RestrictedExtensions_URIPATH	检查是否存在 URI 路径中包含无法安全读取或运行的系统文件扩展名的请求。示例模式包括类似于 .log 和 .ini 的扩展名。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath
RestrictedExtensions_QUERYARGUMENTS	检查是否存在查询参数中包含无法安全读取或运行的系统文件扩展名的请求。示例模式包括类似于 .log 和 .ini 的扩展名。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	检查所有查询参数的值，以防有人试图通过嵌入包含 IPv4 地址的 URL 在 Web 应用程序中利用 RFI（远程文件包含）。例如，在利用尝试中包含 IPv4 主机标头的 http://、https://、ftp://、ftps:// 和 file:// 等模式。 规则操作：Block 标签：awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments

Rule name（规则名称）	描述和标签
`GenericRFI_BODY`	检查请求正文中是否有人试图通过嵌入包含 IPv4 地址的 URL 来利用 Web 应用程序中的 RFI（远程文件包含）。例如，在利用尝试中包含 IPv4 主机标头的 `http://`、`https://`、`ftp://`、`ftps://` 和 `file://` 等模式。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:GenericRFI_Body`

Rule name（规则名称）	描述和标签
`GenericRFI_URIPATH`	检查 URI 路径中是否有人试图通过嵌入包含 IPv4 地址的 URL 来利用 Web 应用程序中的 RFI（远程文件包含）。例如，在利用尝试中包含 IPv4 主机标头的 `http://`、`https://`、`ftp://`、`ftps://` 和 `file://` 等模式。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`
`CrossSiteScripting_COOKIE`	使用内置功能检查 Cookie 标头的值以了解常见的跨站点脚本 (XSS) 模式。 AWS WAF 跨站点脚本攻击规则语句示例模式包括类似于 `<script>alert("hello")</script>` 的脚本。 **Note** 该规则组的 2.0 版本未填充 AWS WAF 日志中的规则匹配详细信息。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

Rule name（规则名称）	描述和标签
`CrossSiteScripting_QUERYARGUMENTS`	使用内置检查常见跨站点脚本 (XSS) 模式的查询参数值。 AWS WAF 跨站点脚本攻击规则语句示例模式包括类似于 `<script>alert("hello")</script>` 的脚本。 **Note** 该规则组的 2.0 版本未填充 AWS WAF 日志中的规则匹配详细信息。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Rule name（规则名称）	描述和标签
`CrossSiteScripting_BODY`	使用内置检查请求正文中常见的跨站脚本 (XSS) 模式。 AWS WAF 跨站点脚本攻击规则语句示例模式包括类似于 `<script>alert("hello")</script>` 的脚本。 **Note** 该规则组的 2.0 版本未填充 AWS WAF 日志中的规则匹配详细信息。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`

Rule name（规则名称）	描述和标签
`CrossSiteScripting_URIPATH`	使用内置检查常见跨站脚本 (XSS) 模式的 URI 路径值。 AWS WAF 跨站点脚本攻击规则语句示例模式包括类似于 `<script>alert("hello")</script>` 的脚本。 **Note** 该规则组的 2.0 版本未填充 AWS WAF 日志中的规则匹配详细信息。 规则操作：Block 标签：`awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

管理员保护托管规则组

VendorName:`AWS`，名称：`AWSManagedRulesAdminProtectionRuleSet`，WCU：100

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

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

Note

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

Rule name（规则名称）	描述和标签
`AdminProtection_URIPATH`	检查针对通常为管理 Web 服务器或应用程序而保留的 URI 路径。示例模式包括 `sqlmanager` 。 规则操作：Block 标签：`awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

已知错误输入托管规则组

VendorName:`AWS`，名称：`AWSManagedRulesKnownBadInputsRuleSet`，WCU：200

已知错误输入规则组包含用于阻止请求模式的规则，这些模式确认无效且与漏洞攻击或发现相关联。这有助于降低恶意人员发现易受攻击的应用程序的风险。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

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

Rule name（规则名称）	描述和标签
	示例模式包括（`java.lang.Runtime).getRuntime().exec("whoami")` 。 **Warning** 此规则仅检查请求标头的前 8 KB 或前 200 个标头（以先达到的限制为准），并且它使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

Rule name（规则名称）	描述和标签
`JavaDeserializationRCE_BODY`	检查请求正文中是否存在指示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞（CVE-2022-22963、CVE-2022-22965）。示例模式包括 `(java.lang.Runtime).getRuntime().exec("whoami")` 。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`

Rule name（规则名称）	描述和标签
JavaDeserializationRCE_URIPATH	检查请求 URI 中是否存在指示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞（CVE-2022-22963、CVE-2022-22965）。示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami") 。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath
JavaDeserializationRCE_QUERYSTRING	检查请求查询字符串中是否存在指示 Java 反序列化远程命令执行 (RCE) 尝试的模式，例如 Spring Core 和 Cloud Function RCE 漏洞（CVE-2022-22963、CVE-2022-22965）。示例模式包括 (java.lang.Runtime).getRuntime().exec("whoami") 。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString
Host_localhost_HEADER	检查请求中的主机标头是否有指示本地主机的模式。示例模式包括 localhost 。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header

Rule name（规则名称）	描述和标签
PROPFIND_METHOD	检查请求中用于 PROPFIND 的 HTTP 方法，这是一种类似于 HEAD 的方法，但具有泄漏 XML 对象的额外意图。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:Propfind_Method
ExploitablePaths_URIPATH	检查 URI 路径中是否有恶意方试图访问可利用的 Web 应用程序路径。示例模式包括类似于 web-inf 的路径。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath

Rule name（规则名称）	描述和标签
Log4JRCE_HEADER	检查请求标头的键和值是否存在 Log4j 漏洞（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105），并防止远程代码执行 (RCE) 尝试。示例模式包括 ${jndi:ldap://example.com/} 。 **Warning** 此规则仅检查请求标头的前 8 KB 或前 200 个标头（以先达到的限制为准），并且它使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header
Log4JRCE_QUERYSTRING	检查查询字符串中是否存在 Log4j 漏洞（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105），并防止远程代码执行 (RCE) 尝试。示例模式包括 ${jndi:ldap://example.com/} 。 规则操作：Block 标签：awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString

Rule name（规则名称）	描述和标签
`Log4JRCE_BODY`	检查正文中是否存在 Log4j 漏洞（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105），并防止远程代码执行 (RCE) 尝试。示例模式包括 `${jndi:ldap://example.com/}` 。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和已验证访问权限，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Rule name（规则名称）	描述和标签
`Log4JRCE_URIPATH`	检查 URI 路径中是否存在 Log4j 漏洞（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105），并防止远程代码执行 (RCE) 尝试。示例模式包括 `${jndi:ldap://example.com/}` 。 规则操作：Block 标签：`awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

使用案例特定规则组

特定于用例的规则组为许多不同的 AWS WAF 用例提供增量保护。选择适用于您的应用程序的规则组。

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

SQL 数据库托管规则组

VendorName:`AWS`，名称：`AWSManagedRulesSQLiRuleSet`，WCU：200

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

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
SQLi_QUERYARGUMENTS	使用内置 AWS WAF SQL 注入攻击规则语句的（敏感度级别设置为Low）检查所有查询参数的值中是否存在与恶意 SQL 代码匹配的模式。 规则操作：Block 标签：awswaf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	检查所有查询参数的值，以查找与恶意 SQL 代码匹配的模式。该规则检查的模式不在规则 SQLi_QUERYARGUMENTS 的范围内。 规则操作：Block 标签：awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
SQLi_BODY	使用内置 AWS WAF SQL 注入攻击规则语句的（敏感度级别设置为Low）检查请求正文中是否存在与恶意 SQL 代码匹配的模式。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对

Rule name（规则名称）	描述和标签
	于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:sql-database:SQLi_Body`

Rule name（规则名称）	描述和标签
SQLiExtendedPatterns_BODY	检查请求正文中是否存在与恶意 SQL 代码匹配的模式。该规则检查的模式不在规则 SQLi_BODY 的范围内。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body
SQLi_COOKIE	使用内置 AWS WAF SQL 注入攻击规则语句的（敏感度级别设置为 Low）检查请求 Cookie 标头中是否存在与恶意 SQL 代码匹配的模式。 规则操作：Block 标签：awswaf:managed:aws:sql-database:SQLi_Cookie

Linux 操作系统托管规则组

VendorName:AWS，名称：AWSManagedRulesLinuxRuleSet，WCU：200

Linux 操作系统规则组包含阻止请求模式的规则，这些请求模式与利用 Linux 特定漏洞（包括 Linux 特定的本地文件包含 (LFI) 攻击）相关。该规则组有助于防止暴露攻击者不应当访问的文件内容或执行代码的攻击。如果应用程序的任何部分在 Linux 上运行，则应评估此规则组。您应将此规则组与 POSIX 操作系统 规则组结合使用。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
LFI_URIPATH	检查请求路径，以查找是否有恶意方试图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 规则操作：Block 标签：awswaf:managed:aws:linux-os:LFI_URIPath
LFI_QUERYSTRING	检查查询字符串的值，以查找是否有恶意方试图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 规则操作：Block

Rule name（规则名称）	描述和标签
	标签：awswaf:managed:aws:linux-os:LFI_QueryString
LFI_HEADER	检查请求标头，以查找是否有恶意方试图利用 Web 应用程序中的本地文件包含 (LFI) 漏洞。示例模式包括类似于 /proc/version 的文件，它们可能向攻击者提供操作系统信息。 **Warning** 此规则仅检查请求标头的前 8 KB 或前 200 个标头（以先达到的限制为准），并且它使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:linux-os:LFI_Header

POSIX 操作系统托管规则组

VendorName:AWS，名称：AWSManagedRulesUnixRuleSet，WCU：100

POSIX 操作系统规则组包含的规则可阻止与利用 POSIX 和类似 POSIX 的操作系统特定漏洞（包括 Linux 特定的本地文件包含 (LFI) 攻击）相关的请求模式。该规则组有助于防止暴露攻击者不应当访问的文件内容或执行代码的攻击。如果应用程序的任何部分在 POSIX 或类似 POSIX 的操作系统（包括 Linux、AIX、HP-UX、macOS、Solaris、FreeBSD 和 OpenBSD）上运行，则应评估此规则组。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
`UNIXShellCommandsVariables_QUERYSTRING`	检查查询字符串的值是否有人企图利用在 Unix 系统上运行的 Web 应用程序中的命令注入、LFI 和路径遍历漏洞。示例包括类似于 `echo $HOME` 和 `echo $PATH` 的模式。 规则操作：Block 标签：`awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	检查请求正文，以查找是否有恶意方试图利用在 Unix 系统上运行的 Web 应用程序中的命令注入、LFI 和路径遍历漏洞。示例包括类似于 `echo $HOME` 和 `echo $PATH` 的模式。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大

Rule name（规则名称）	描述和标签
	内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body
UNIXShellCommandsVariables_HEADER	检查所有请求标头是否有人企图利用在 Unix 系统上运行的 Web 应用程序中的命令注入、LFI 和路径遍历漏洞。示例包括类似于 echo $HOME 和 echo $PATH 的模式。 **Warning** 此规则仅检查请求标头的前 8 KB 或前 200 个标头（以先达到的限制为准），并且它使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header

Windows 操作系统托管规则组

VendorName:AWS，名称：AWSManagedRulesWindowsRuleSet，WCU：200

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

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
`WindowsShellCommands_COOKIE`	检查 Web 应用程序中是否有 WindowsShell 命令注入尝试的请求 cookie 标头。匹配模式代表WindowsShell 命令。示例模式包括 `||nslookup` 和 `;cmd`。 规则操作：Block 标签：`awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie`
`WindowsShellCommands_QUERYARGUMENTS`	检查 Web 应用程序中WindowsShell 命令注入尝试的所有查询参数的值。匹配模式代表WindowsShell 命令。示例模式包括 `||nslookup` 和 `;cmd`。 规则操作：Block 标签：`awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`
`WindowsShellCommands_BODY`	

Rule name（规则名称）	描述和标签
	检查请求正文中是否有 Web 应用程序中的 WindowsShell 命令注入尝试。匹配模式代表 WindowsShell 命令。示例模式包括 `|| nslookup` 和 `;cmd`。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 `Continue` 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：`awswaf:managed:aws:windows-os:WindowsShellCommands_Body`
`PowerShellCommands_COOKIE`	检查 Web 应用程序中是否有 PowerShell 命令注入尝试的请求 cookie 标头。匹配模式代表PowerShell 命令。例如，`Invoke-Expression` 。 规则操作：Block 标签：`awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`

Rule name（规则名称）	描述和标签
PowerShellCommands_QUERYARGUMENTS	检查 Web 应用程序中PowerShell 命令注入尝试的所有查询参数的值。匹配模式代表PowerShell 命令。例如，Invoke-Expression 。 规则操作：Block 标签：awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments
PowerShellCommands_BODY	检查请求正文中是否有 Web 应用程序中的 PowerShell 命令注入尝试。匹配模式代表 PowerShell 命令。例如，Invoke-Expression 。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:windows-os:PowerShellCommands_Body

PHP 应用程序托管规则组

VendorName:AWS，名称：AWSManagedRulesPHPRuleSet，WCU：100

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

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
PHPHighRiskMethodsVariables_HEADER	检查所有标头，以发现 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 $_GET 超全局变量的函数。 **Warning** 此规则仅检查请求标头的前 8 KB 或前 200 个标头（以先达到的限制为准），并且它使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header

Rule name（规则名称）	描述和标签
PHPHighRiskMethodsVariables_QUERYSTRING	检查请求 URL 中第一个？之后的所有内容，查找 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 $_GET 超全局变量的函数。 规则操作：Block 标签：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString
PHPHighRiskMethodsVariables_BODY	检查请求主体的值以查找 PHP 脚本代码注入尝试。示例模式包括类似 fsockopen 和 $_GET 超全局变量的函数。 **Warning** 此规则仅检查请求正文，但不得超过 Web ACL 和资源类型的正文大小限制。对于 Application Load Balancer 和 AWS AppSync，限制固定为 8 KB。对于 CloudFront API Gateway、Amazon Cognito、App Runner 和 Verified Access，默认限制为 16 KB，您可以在网页 ACL 配置中将限制提高到 64 KB。此规则使用 Continue 选项来处理超大内容。有关更多信息，请参阅 在中处理超大请求组件 AWS WAF。 规则操作：Block 标签：awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

WordPress 应用程序托管规则组

VendorName:AWS，名称：AWSManagedRulesWordPressRuleSet，WCU：100

WordPress 应用程序规则组包含的规则用于阻止与利用特定于WordPress 网站的漏洞相关的请求模式。如果您正在运行，则应评估此规则组WordPress。此规则组应与 SQL 数据库 和 PHP 应用程序 规则组一起使用。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

> **Note**
>
> 下表描述了该规则组的最新静态版本。对于其他版本，请使用 API 命令DescribeManagedRuleGroup。

Rule name（规则名称）	描述和标签
WordPressExploitableCommands_QUERYSTRING	检查请求查询字符串中是否存在可能在易受攻击的安装或插件中被利用的高风险WordPress命令。示例模式包括类似于 do-reset-wordpress 的命令。 规则操作：Block 标签：awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING
WordPressExploitablePaths_URIPATH	检查请求 URI 路径中是否有已知存在容易被利用的漏洞的 WordPress 文件。xmlrpc.php 规则操作：Block

Rule name（规则名称）	描述和标签
	标签：awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH

IP 声誉规则组

IP 声誉规则组请求源 IP 地址阻止请求。

> **Note**
>
> 这些规则使用 Web 请求源中的源 IP 地址。如果您的流量通过了一个或多个代理或负载均衡器，则 Web 请求源将包含最后一个代理的地址，而不是客户端的源地址。

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

此类别中的规则组不提供版本控制或 SNS 更新通知。

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

Amazon IP 声誉列表托管规则组

VendorName:AWS，名称：AWSManagedRulesAmazonIpReputationList，WCU：25

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

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

Rule name（规则名称）	描述和标签
`AWSManagedIPReputationList`	检查是否存在被确定为积极参与恶意活动的 IP 地址。 AWS WAF 从各种来源收集 IP 地址列表 MadPot，包括 Amazon 用来保护客户免受网络犯罪侵害的威胁情报工具。有关的更多信息 MadPot，请参阅https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime。 规则操作：Block 标签：`awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	检查来自正在对 AWS 资源进行侦察的 IP 地址的连接。 规则操作：Block 标签：`awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	检查是否存在被确定为积极参与 DDoS 活动的 IP 地址。 规则操作：Count 标签：`awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

匿名 IP 列表托管规则组

VendorName:`AWS`，名称：`AWSManagedRulesAnonymousIpList`，WCU：50

此匿名 IP 列表包含用于阻止来自以下服务的请求的规则：这些服务允许对查看者身份进行模糊处理。其中包括来自 VPN、代理、Tor 节点和 Web 托管提供程序的请求。如果要筛选出可能试图从应用程序中隐藏其身份的查看者，则此规则组非常有用。阻止这些服务的 IP 地址有助于减少机器人和规避地域限制。

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

Rule name（规则名称）	描述和标签
`AnonymousIPList`	检查已知用于匿名处理客户端信息的源的 IP 地址列表，例如 TOR 节点、临时代理和其他遮蔽服务。 规则操作：Block 标签：`awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`
`HostingProviderIPList`	检查来自 Web 托管和云提供程序的 IP 地址列表，这些提供程序不太可能产生最终用户流量。IP 列表不包括 AWS IP 地址。 规则操作：Block 标签：`awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList`

AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组

VendorName:`AWS`，名称：`AWSManagedRulesACFPRuleSet`，WCU：50

F AWS WAF raud Control 账户创建防欺诈 (ACFP) 管理的规则组可以标记和管理可能属于欺诈性账户创建尝试的请求。规则组通过检查客户端发送到应用程序的注册和账户创建端点的账户创建请求来实现此目的。

ACFP 规则组以各种方式检查账户创建尝试，让您可以查看和控制潜在的恶意交互。规则组使用请求令牌来收集有关客户端浏览器的信息以及有关创建账户创建请求时的人机交互级别的信息。该规则组按

IP 地址和客户端会话汇总请求，并按提供的账户信息（例如实际地址和电话号码）进行聚合，以检测和管理批量创建账户的尝试。此外，该规则组会检测并阻止使用已泄露的凭证创建新账户，从而保护应用程序和新用户的安全状况。

使用此规则组的注意事项

此规则组需要自定义配置，其中包括应用程序的账户注册和账户创建路径的规范。除非另有说明，否则此规则组中的规则会检查您的客户端发送到这两个端点的所有请求。如需配置和实施此规则组，请参阅 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP) 中的指导。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

此规则组是 AWS WAF中智能威胁缓解保护的一部分。有关信息，请参阅 AWS WAF 智能威胁缓解。

为了降低成本并确保您可以根据需要管理 Web 流量，请按照 智能威胁缓解的最佳实践 中的指导使用此规则组。

此规则组不可与 Amazon Cognito 用户群体一起使用。您无法将使用此规则组的 Web ACL 与用户群体相关联，也无法将此规则组添加到已与用户群体关联的 Web ACL 中。

此规则组添加的标签

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

令牌标签

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

有关令牌和令牌管理的信息，请参阅 AWS WAF 网络请求令牌。

有关此处描述的标签组件的信息，请参阅 AWS WAF 标签语法和命名要求。

客户端会话标签

该标签`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 令牌管理用于识别客户端会话的唯一标识符。如果客户端获取了新令牌，例如在丢弃其正在使用的令牌之后，标识符可能会更改。

> **Note**
>
> AWS WAF 不报告该标签的 Amazon CloudWatch 指标。

令牌状态标签：标签命名空间前缀

令牌状态标签报告令牌的状态、质询以及其中包含的 CAPTCHA 信息。

每个令牌状态标签都以下列命名空间前缀之一开头：

- `awswaf:managed:token:` – 用于报告令牌的一般状态以及令牌的质询信息的状态。
- `awswaf:managed:captcha:` – 用于报告令牌的 CAPTCHA 信息的状态。

令牌状态标签：标签名称

在前缀之后，标签的其余部分提供详细的令牌状态信息：

- `accepted` – 请求令牌存在且包含以下内容：
  - 有效的质询或 CAPTCHA 解决方案。
  - 未过期的质询或 CAPTCHA 时间戳。
  - 对 Web ACL 有效的域规范。

  示例：标签 `awswaf:managed:token:accepted` 表明 Web 请求的令牌具有有效的质询解决方案、未过期的质询时间戳以及有效的域。
- `rejected` – 请求令牌存在但不符合接受标准。

  除了被拒绝的标签外，令牌管理还添加了一个自定义标签命名空间和名称来指示原因。
  - `rejected:not_solved` – 令牌缺少质询或 CAPTCHA 解决方案。
  - `rejected:expired` – 根据您的 Web ACL 配置的令牌免疫时间，令牌的质询或 CAPTCHA 时间戳已过期。
  - `rejected:domain_mismatch` – 令牌的域与您的 Web ACL 的令牌域配置不匹配。
  - `rejected:invalid`— AWS WAF 无法读取指示的标记。

  示例：标签 `awswaf:managed:captcha:rejected` 和 `awswaf:managed:captcha:rejected:expired` 表示请求被拒绝，因为令牌中的 CAPTCHA 时间戳已超过 Web ACL 中配置的 CAPTCHA 令牌免疫时间。

- absent – 请求没有令牌，或者令牌管理器无法读取它。

  示例：标签 awswaf:managed:captcha:absent 表示请求没有令牌。

ACFP 标签

该规则组生成带有命名空间前缀 awswaf:managed:aws:acfp: 的标签，后接自定义命名空间和标签名称。规则组可能会向一个请求添加多个标签。

您可以通过调用 DescribeManagedRuleGroup 从 API 检索一个规则组的所有标签。标签列在响应的 AvailableLabels 属性中。

账户创建欺诈预防规则列表

此部分列出了 AWSManagedRulesACFPRuleSet 中的 ACFP 规则以及规则组的规则添加到 Web 请求的标签。

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

该规则组中的所有规则都需要 Web 请求令牌，但前两个 UnsupportedCognitoIDP 和 AllRequests 除外。有关令牌提供的信息的描述，请参阅 AWS WAF 代币特征。

除非另有说明，否则此规则组中的规则会检查您的客户端发送到您在规则组配置中提供的账户注册和账户创建页面路径的所有请求。有关配置此规则组的信息，请参阅 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP)。

Rule name（规则名称）	描述和标签
UnsupportedCognitoIDP	检查流向 Amazon Cognito 用户群体的 Web 流量。ACFP 不可用于 Amazon Cognito 用户群体，此规则有助于确保不使用其他 ACFP 规则组规则来评估用户群体流量。 规则操作：Block

Rule name（规则名称）	描述和标签
	标签：`awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	将规则操作应用于访问注册页面路径的请求。在配置规则组时可以配置注册页面路径。 默认情况下，此规则会将 Challenge 应用于请求。通过应用此操作，该规则可确保在规则组中的其余规则评估任何请求之前，客户端获得质询令牌。 确保您的最终用户在提交账户创建请求之前加载注册页面路径。 令牌由客户端应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。为了获得最有效的令牌获取，我们强烈建议使用应用程序集成软件开发工具包。有关更多信息，请参阅 AWS WAF 客户端应用程序集成。 规则操作：Challenge 标签：无

Rule name（规则名称）	描述和标签
RiskScoreHigh	检查是否存在 IP 地址或其他被认为高度可疑因素的账户创建请求。这种评估通常基于多个影响因素，您可以在规则组添加到请求的 risk_score 标签中看到这些因素。 规则操作：Block 标签：awswaf:managed:aws:acfp:risk_score:high 该规则也可能适用于该请求 medium 或 low 风险评分标签。 如果 AWS WAF 无法成功评估 Web 请求的风险评分，则该规则会添加标签 awswaf:managed:aws:acfp:risk_score:evaluation_failed 此外，该规则还添加了带有命名空间的标签 awswaf:managed:aws:acfp:risk_score:contributor: ，其中包括风险评分评估状态和特定风险评分贡献者的结果，例如 IP 声誉和被盗凭证评估。

Rule name（规则名称）	描述和标签
`SignalCredentialCompromised`	在被盗凭证数据库中搜索在账户创建请求中提交的凭证。 此规则可确保新客户以积极的安全态势初始化其账户。 **Note** 您可以添加自定义阻止响应，向最终用户描述问题并告诉他们如何继续操作。有关信息，请参阅 ACFP 示例：针对被泄漏凭证的自定义响应。 规则操作：Block 标签：`awswaf:managed:aws:acfp:signal:credential_compromised` 规则组应用以下相关标签，但不对其采取任何操作，因为并非所有账户创建中的请求都具有凭证：`awswaf:managed:aws:acfp:signal:missing_credential`

Rule name（规则名称）	描述和标签

`SignalClientHumanInteractivityAbsentLow`	检查账户创建请求的令牌中是否有数据表明人机应用程序交互出现异常。人机交互通过鼠标移动、按键等交互来检测。如果页面有 HTML 表单，则人机交互包括与表单的交互。
	
	Note
	此规则仅检查对账户创建路径的请求，并且仅在您实施了应用程序集成软件开发工具包后才会进行评估。软件开发工具包实施以被动方式捕获人机交互并将信息存储在请求令牌中。有关更多信息，请参阅 AWS WAF 代币特征 和 AWS WAF 客户端应用程序集成。
	
	规则操作：CAPTCHA
	
	标签：无。该规则根据不同的因素确定匹配项，因此没有适用于所有可能的匹配场景的单独标签。
	
	规则组可以将下列一个或多个标签应用于请求：
	
	`awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high`
	
	`awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data`
	
	`awswaf:managed:aws:acfp:signal:form_detected` .

Rule name（规则名称）	描述和标签
`SignalAutomatedBrowser`	检查请求中是否显示客户端浏览器可能已自动运行。 规则操作：Block 标签：`awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	检查请求的令牌是否存在不一致的浏览器询问数据。有关更多信息，请参阅 AWS WAF 代币特征。 规则操作：CAPTCHA 标签：`awswaf:managed:aws:acfp:signal:browser_inconsistency`

Rule name（规则名称）	描述和标签
`VolumetricIpHigh`	检查从各个 IP 地址发送的高流量账户创建请求。高流量是指在 10 分钟的窗口内超过 20 个请求。 **Note** 由于延迟，此规则适用的阈值可能略有不同。对于高流量，在应用规则操作之前，一些请求可能会超出限制。 规则操作：CAPTCHA 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` 该规则将以下标签应用于中流量（每 10 分钟窗口内 16-20 个请求）和低流量（每 10 分钟窗口内 11-15 个请求）的请求，但不对它们采取任何操作：`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` 和 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` 。

Rule name（规则名称）	描述和标签
`VolumetricSessionHigh`	检查来自各个客户端会话的高流量账户创建请求。高流量是指在 30 分钟的窗口内超过 10 个请求。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` 该规则将以下标签应用于中流量（每 30 分钟窗口内 6-10 个请求）和低流量（每 30 分钟窗口内 2-5 个请求）的请求，但不对它们采取任何操作：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium` 和 `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low`。

Rule name（规则名称）	描述和标签
`AttributeUsernameTraversalHigh`	检查单个客户端会话中是否存在使用不同用户名的高流量账户创建请求。高流量的阈值为 30 分钟内超过 10 个请求。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` 该规则将以下标签应用于中流量（每 30 分钟窗口内 6-10 个请求）和低流量（每 30 分钟窗口内 2-5 个请求）的用户名遍历请求，但不对它们采取任何操作：`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` 和 `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low` 。

Rule name（规则名称）	描述和标签
`VolumetricPhoneNumberHigh`	检查是否存在使用相同电话号码的高流量账户创建请求。高流量的阈值为 30 分钟内超过 10 个请求。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` 该规则将以下标签应用于中流量（每 30 分钟窗口内 6-10 个请求）和低流量（每 30 分钟窗口内 2-5 个请求）的请求，但不对它们采取任何操作：`awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium` 和 `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low` 。

Rule name（规则名称）	描述和标签
`VolumetricAddressHigh`	检查是否存在使用相同物理地址的高流量账户创建请求。高流量的阈值为每 30 分钟窗口内超过 100 个请求。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

Rule name（规则名称）	描述和标签
`VolumetricAddressLow`	检查是否存在使用相同物理地址的中流量和低流量账户创建请求。中流量的阈值为每 30 分钟窗口超过 51-100 个请求，而低流量的阈值为每 30 分钟窗口 11-50 个请求。 该规则适用于中流量或低流量。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：CAPTCHA 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:address:low` 或 `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Rule name（规则名称）	描述和标签
`VolumetricIPSuccessfulResponse`	检查是否存在针对单个 IP 地址的高流量创建账户成功请求。此规则汇总了受保护资源对账户创建请求的成功响应。高流量的阈值为每 10 分钟窗口内超过 10 个请求。 此规则有助于防止批量创建账户的尝试。它的阈值低于仅计算请求的规则 `VolumetricIpHigh` 。 如果您已将规则组配置为检查响应正文或 JSON 组件，则 AWS WAF 可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指示器。 此规则根据受保护资源对最近来自相同 IP 地址的登录尝试的成功和失败响应，将规则操作和标签应用于来自某个 IP 地址的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败。 **Note** AWS WAF 仅在保护 Ama CloudFront zon 分销的 Web ACL 中评估此规则。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在规则开始匹配后续尝试之前，客户端发送账户创建成功尝试的次数可能会超过允许的次数。 规则操作：Block

Rule name（规则名称）	描述和标签
	标签：awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high 该规则组还将以下相关标签应用于请求，但没有任何关联操作。所有计数均适用 10 分钟窗口。awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium 对应超过 5 个成功请求，awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low 对应超过 1 个成功请求，awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high 对应超过 10 个失败请求，awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium 对应超过 5 个失败请求，awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low 对应超过 1 个失败请求。

Rule name（规则名称）	描述和标签
`VolumetricSessionSuccessful Response`	检查受保护资源对从单个客户端会话发送的账户创建请求是否有低流量成功响应。这有助于防止批量创建账户的尝试。低流量的阈值为每 30 分钟窗口内超过 1 个请求。 这有助于防止批量创建账户的尝试。此规则使用的阈值低于仅跟踪请求的规则 `VolumetricSessionHigh` 。 如果您已将规则组配置为检查响应正文或 JSON 组件，则 AWS WAF 可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指示器。 此规则根据受保护资源对最近来自相同客户端会话的登录尝试的成功和失败响应，将规则操作和标签应用于来自某个客户端会话的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败。 **Note** AWS WAF 仅在保护 Ama CloudFront zon 分销的 Web ACL 中评估此规则。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在规则开始匹配后续尝试之前，客户端发送账户创建失败尝试的次数可能会超过允许的次数。

Rule name（规则名称）	描述和标签
	规则操作：Block 标签：awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low 该规则组还将以下相关标签应用于请求。所有计数均适用 30 分钟窗口。awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high 对应超过 10 个成功请求，awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:medium 对应超过 5个成功请求，awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high 对应超过 10 个失败请求，awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium 对应超过 5 个失败请求，awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low 对应超过 1 个失败请求。

Rule name（规则名称）	描述和标签
`VolumetricSessionTokenReuseIp`	检查是否存在账户创建请求在 5 个以上不同 IP 地址中使用同一令牌。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF 防欺诈控制账户盗用 (ATP) 规则组

VendorName:`AWS`，名称：`AWSManagedRulesATPRuleSet`，WCU：50

F AWS WAF raud Control 账户盗用预防 (ATP) 管理的规则组标记并管理可能属于恶意账户接管尝试的请求。规则组通过检查客户端发送到应用程序登录端点的登录尝试来实现此目的。

- 请求检查 – ATP 允许您查看和控制异常登录尝试和使用被盗凭证的登录尝试，以防止可能导致欺诈活动的账户盗用。ATP 根据被盗凭证数据库检查电子邮件和密码组合，当在暗网上发现新的泄露凭证时，会定期更新。ATP 按 IP 地址和客户端会话汇总数据，以检测和阻止发送过多可疑请求的客户端。
- 响应检查-对于 CloudFront 分配，除了检查传入的登录请求外，ATP 规则组还会检查您的应用程序对登录尝试的响应，以跟踪成功率和失败率。利用这些信息，ATP 可以暂时阻止登录失败次数过多的客户端会话或 IP 地址。 AWS WAF 会异步执行响应检查，因此不会增加 Web流量的延迟。

使用此规则组的注意事项

此规则组需要特定配置。如需配置和实施此规则组，请参阅 AWS WAF 防欺诈控制账户接管 (ATP) 中的指导。

此规则组是 AWS WAF中智能威胁缓解保护的一部分。有关信息，请参阅 AWS WAF 智能威胁缓解。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

为了降低成本并确保您可以根据需要管理 Web 流量，请按照 智能威胁缓解的最佳实践 中的指导使用此规则组。

此规则组不可与 Amazon Cognito 用户群体一起使用。您无法将使用此规则组的 Web ACL 与用户群体相关联，也无法将此规则组添加到已与用户群体关联的 Web ACL 中。

此规则组添加的标签

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

令牌标签

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

有关令牌和令牌管理的信息，请参阅 AWS WAF 网络请求令牌。

有关此处描述的标签组件的信息，请参阅 AWS WAF 标签语法和命名要求。

客户端会话标签

该标签`awswaf:managed:token:id:`*`identifier`*包含 AWS WAF 令牌管理用于识别客户端会话的唯一标识符。如果客户端获取了新令牌，例如在丢弃其正在使用的令牌之后，标识符可能会更改。

> **Note**
>
> AWS WAF 不报告该标签的 Amazon CloudWatch 指标。

令牌状态标签：标签命名空间前缀

令牌状态标签报告令牌的状态、质询以及其中包含的 CAPTCHA 信息。

每个令牌状态标签都以下列命名空间前缀之一开头：

- awswaf:managed:token: – 用于报告令牌的一般状态以及令牌的质询信息的状态。
- awswaf:managed:captcha: – 用于报告令牌的 CAPTCHA 信息的状态。

令牌状态标签：标签名称

在前缀之后，标签的其余部分提供详细的令牌状态信息：

- accepted – 请求令牌存在且包含以下内容：
  - 有效的质询或 CAPTCHA 解决方案。
  - 未过期的质询或 CAPTCHA 时间戳。
  - 对 Web ACL 有效的域规范。

  示例：标签 awswaf:managed:token:accepted 表明 Web 请求的令牌具有有效的质询解决方案、未过期的质询时间戳以及有效的域。
- rejected – 请求令牌存在但不符合接受标准。

  除了被拒绝的标签外，令牌管理还添加了一个自定义标签命名空间和名称来指示原因。
  - rejected:not_solved – 令牌缺少质询或 CAPTCHA 解决方案。
  - rejected:expired – 根据您的 Web ACL 配置的令牌免疫时间，令牌的质询或 CAPTCHA 时间戳已过期。
  - rejected:domain_mismatch – 令牌的域与您的 Web ACL 的令牌域配置不匹配。
  - rejected:invalid— AWS WAF 无法读取指定的标记。

  示例：标签 awswaf:managed:captcha:rejected 和 awswaf:managed:captcha:rejected:expired 表示请求被拒绝，因为令牌中的 CAPTCHA 时间戳已超过 Web ACL 中配置的 CAPTCHA 令牌免疫时间。
- absent – 请求没有令牌，或者令牌管理器无法读取它。

  示例：标签 awswaf:managed:captcha:absent 表示请求没有令牌。

ATP 标签

ATP 托管规则组生成带有命名空间前缀 awswaf:managed:aws:atp: 的标签，后接自定义命名空间和标签名称。

除了规则列表中注明的标签外，规则组还可以添加以下任何标签：

- awswaf:managed:aws:atp:signal:credential_compromised – 表示在请求中提交的凭证位于被盗凭证数据库中。
- awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint— 仅适用于受保护的 Amazon CloudFront 分配。表示客户端会话发送了多个使用可疑 TLS 指纹的请求。
- awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip – 表示有 5 个以上不同的 IP 地址使用同一令牌。由于延迟，此规则适用的阈值可能略有不同。在应用标签之前，一些请求可能会超出限制。

您可以通过调用 DescribeManagedRuleGroup 从 API 检索一个规则组的所有标签。标签列在响应的 AvailableLabels 属性中。

账户盗用防护规则列表

此部分列出了 AWSManagedRulesATPRuleSet 中的 ATP 规则以及规则组的规则添加到 Web 请求的标签。

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

Rule name（规则名称）	描述和标签
UnsupportedCognitoIDP	检查流向 Amazon Cognito 用户群体的 Web 流量。ATP 不可用于 Amazon Cognito 用户群体，此规则有助于确保不使用其他 ATP 规则组规则来评估用户群体流量。 规则操作：Block 标签：awswaf:managed:aws:atp:unsupported:cognito_idp
VolumetricIpHigh	检查从各个 IP 地址发送的高流量请求。高流量是指在 10 分钟的窗口内超过 20 个请求。

Rule name（规则名称）	描述和标签
	Note 由于延迟，此规则适用的阈值可能略有不同。对于高流量，在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:volumetric:ip:high` 该规则将以下标签应用于中流量（每 10 分钟窗口内 16-20 个请求）和低流量（每 10 分钟窗口内 11-15 个请求）的请求，但不对它们采取任何操作：`awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` 和 `awswaf:managed:aws:atp:aggregate:volumetric:ip:low` 。

Rule name（规则名称）	描述和标签
`VolumetricSession`	检查来自各个客户端会话的高流量请求。其阈值为每 30 分钟窗口内超过 20 个请求。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:volumetric:session`
`AttributeCompromisedCredentials`	检查来自同一个客户端会话的多个使用被盗凭证的请求。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`

Rule name（规则名称）	描述和标签
`AttributeUsernameTraversal`	检查来自同一个客户端会话的多个使用用户名遍历的请求。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	检查使用相同用户名且使用密码遍历的多个请求。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:attribute:password_traversal`
`AttributeLongSession`	检查来自同一个客户端会话的多个使用长时间对话的请求。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:attribute:long_session`

Rule name（规则名称）	描述和标签
`TokenRejected`	检查是否有令牌管理部门拒绝的带有令 AWS WAF 牌的请求。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 规则操作：Block 标签：无。要检查令牌是否被拒绝，请使用标签匹配规则在标签上进行匹配：`awswaf:managed:token:rejected`
`SignalMissingCredential`	检查是否存在缺少用户名或密码的凭证的请求。 规则操作：Block 标签：`awswaf:managed:aws:atp:signal:missing_credential`

Rule name（规则名称）	描述和标签
`VolumetricIpFailedLoginResponseHigh`	检查最近是否存在导致登录尝试失败率过高的 IP 地址。高流量是指在 10 分钟窗口内来自某个 IP 地址的登录请求失败超过 10 个。 如果您已将规则组配置为检查响应正文或 JSON 组件，则 AWS WAF 可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指示器。 此规则根据受保护资源对最近来自相同 IP 地址的登录尝试的成功和失败响应，将规则操作和标签应用于来自某个 IP 地址的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败。 **Note** AWS WAF 仅在保护 Ama CloudFront zon 分销的 Web ACL 中评估此规则。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在规则开始匹配后续尝试之前，客户端发送登录失败尝试的次数可能会超过允许的次数。 规则操作：Block 标签：`awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high`

Rule name（规则名称）	描述和标签
	该规则组还将以下相关标签应用于请求，但没有任何关联操作。所有计数均适用 10 分钟窗口。awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium 对应超过 5 个失败请求，awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low 对应超过 1 个失败请求，awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high 对应超过 10 个成功请求，awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium 对应超过 5 个成功请求，awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low 对应超过 1 个成功请求。

Rule name（规则名称）	描述和标签
`VolumetricSessionFailedLogi nResponseHigh`	检查最近是否存在导致登录尝试失败率过高的客户端会话。高流量是指在 30 分钟窗口内来自某个客户端会话的登录请求失败超过 10 个。 如果您已将规则组配置为检查响应正文或 JSON 组件，则 AWS WAF 可以检查这些组件类型的前 65,536 字节 (64 KB) 以查看成功或失败指示器。 此规则根据受保护资源对最近来自相同客户端会话的登录尝试的成功和失败响应，将规则操作和标签应用于来自某个客户端会话的新 Web 请求。在配置规则组时，您可以定义如何计算成功和失败。 **Note** AWS WAF 仅在保护 Ama CloudFront zon 分销的 Web ACL 中评估此规则。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在规则开始匹配后续尝试之前，客户端发送登录失败尝试的次数可能会超过允许的次数。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。

Rule name（规则名称）	描述和标签
	规则操作：Block 标签：awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high 该规则组还将以下相关标签应用于请求，但没有任何关联操作。所有计数均适用 30 分钟窗口。awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium 对应超过 5 个失败请求，awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low 对应超过 1 个失败请求，awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high 对应超过 10 个成功请求，awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium 对应超过 5 个成功请求，awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low 对应超过 1 个成功请求。

AWS WAF 机器人控制规则组

VendorName:AWS，名称：AWSManagedRulesBotControlRuleSet，WCU：50

机器人控制功能托管规则组提供管理来自机器人的请求的规则。机器人可能会消耗过多的资源，歪曲业务指标，导致停机以及执行恶意活动。

保护级别

机器人控制功能托管规则组提供两种保护级别供您选择：

- 常见 – 检测各种自我识别的机器人，例如 Web 抓取框架、搜索引擎和自动浏览器。此级别的机器人控制功能保护使用传统的机器人检测技术（例如静态请求数据分析）来识别常见的机器人。这些规则会标记来自这些机器人的流量，并阻止他们无法验证的流量。
- 定向 – 包括通用级保护，并针对无法自我识别的复杂机器人添加定向检测。目标保护结合了速率限制和验证码以及后台浏览器质询，缓解了机器人活动。
  - **TGT_** – 提供目标保护的规则的名称以 TGT_ 开头。所有目标保护都使用浏览器查询、指纹识别和行为启发式等检测技术来识别恶意机器人流量。
  - **TGT_ML_** – 使用机器学习的目标保护规则的名称以 TGT_ML_ 开头。这些规则使用对网站流量统计数据的自动机器学习分析来检测表明分布式、协调的机器人活动的异常行为。 AWS WAF 分析有关您的网站流量的统计信息，例如时间戳、浏览器特征和之前访问的 URL，以改进 Bot Control 机器学习模型。默认情况下，机器学习功能处于启用状态，但您可以在规则组配置中将其禁用。禁用机器学习时， AWS WAF 不评估这些规则。

目标保护级别和 AWS WAF 基于速率的规则声明均提供速率限制。有关两个选项的对比，请参阅 基于速率的规则和定向机器人控制功能规则中的速率限制选项。

使用此规则组的注意事项

此规则组是 AWS WAF中智能威胁缓解保护的一部分。有关信息，请参阅 AWS WAF 智能威胁缓解。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

为了降低成本并确保您可以根据需要管理 Web 流量，请按照 智能威胁缓解的最佳实践 中的指导使用此规则组。

我们会定期更新基于机器学习的目标保护级别规则的机器学习 (ML) 模型，以改善机器人预测。基于 ML 的规则的名称以开头。TGT_ML_如果您发现这些规则所做的机器人预测突然发生重大变化，请通过您的客户经理联系我们或在 Center 提起诉AWS Support 讼。

此规则组添加的标签

此托管规则组会为其评估的 Web 请求添加标签，这些标签可用于在 Web ACL 中在此规则组之后运行的规则。 AWS WAF 还会记录亚马逊 CloudWatch 指标的标签。有关标签和标签指标的一般信息，请参阅 Web 请求上的标签 和 标签指标和维度。

令牌标签

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

有关令牌和令牌管理的信息，请参阅 AWS WAF 网络请求令牌。

有关此处描述的标签组件的信息，请参阅 AWS WAF 标签语法和命名要求。

客户端会话标签

该标签`awswaf:managed:token:id:`*`identifier`*包含一个唯一标识符， AWS WAF 令牌管理使用该标识符来标识客户端会话。如果客户端获取了新令牌，例如在丢弃其正在使用的令牌之后，标识符可能会更改。

> **Note**
>
> AWS WAF 不报告该标签的 Amazon CloudWatch 指标。

令牌状态标签：标签命名空间前缀

令牌状态标签报告令牌的状态、质询以及其中包含的 CAPTCHA 信息。

每个令牌状态标签都以下列命名空间前缀之一开头：

- `awswaf:managed:token:` – 用于报告令牌的一般状态以及令牌的质询信息的状态。
- `awswaf:managed:captcha:` – 用于报告令牌的 CAPTCHA 信息的状态。

令牌状态标签：标签名称

在前缀之后，标签的其余部分提供详细的令牌状态信息：

- `accepted` – 请求令牌存在且包含以下内容：
  - 有效的质询或 CAPTCHA 解决方案。

  - 未过期的质询或 CAPTCHA 时间戳。
  - 对 Web ACL 有效的域规范。

  示例：标签 awswaf:managed:token:accepted 表明 Web 请求的令牌具有有效的质询解决方案、未过期的质询时间戳以及有效的域。
- rejected – 请求令牌存在但不符合接受标准。

  除了被拒绝的标签外，令牌管理还添加了一个自定义标签命名空间和名称来指示原因。
  - rejected:not_solved – 令牌缺少质询或 CAPTCHA 解决方案。
  - rejected:expired – 根据您的 Web ACL 配置的令牌免疫时间，令牌的质询或 CAPTCHA 时间戳已过期。
  - rejected:domain_mismatch – 令牌的域与您的 Web ACL 的令牌域配置不匹配。
  - rejected:invalid— AWS WAF 无法读取指示的标记。

  示例：标签 awswaf:managed:captcha:rejected 和 awswaf:managed:captcha:rejected:expired 表示请求被拒绝，因为令牌中的 CAPTCHA 时间戳已超过 Web ACL 中配置的 CAPTCHA 令牌免疫时间。
- absent – 请求没有令牌，或者令牌管理器无法读取它。

  示例：标签 awswaf:managed:captcha:absent 表示请求没有令牌。

机器人控制功能标签

机器人控制功能托管规则组生成带有命名空间前缀的标签，awswaf:managed:aws:bot-control:后面是自定义命名空间和标签名称。规则组可能会向一个请求添加多个标签。

每个标签都反映了机器人控制功能规则的调查发现：

- awswaf:managed:aws:bot-control:bot: – 有关与请求关联的机器人的信息。
  - awswaf:managed:aws:bot-control:bot:name:*<name>* – 机器人名称（如有），如自定义命名空间 bot:name:slurp、bot:name:googlebot 和 bot:name:pocket_parser。
  - awswaf:managed:aws:bot-control:bot:category:*<category>*— 机器人的类别，例如 AWS WAF，由bot:category:search_engine和定义bot:category:content_fetcher。
  - awswaf:managed:aws:bot-control:bot:organization:*<organization>* – 机器人的发布者，如 bot:organization:google。

- `awswaf:managed:aws:bot-control:bot:verified` – 用于表示可以识别自己并且机器人控制功能已经能够验证的机器人。这用于常见的理想机器人，与类别标签（例如 `bot:category:search_engine` 或 `bot:name:googlebot` 等名称标签）结合使用时可能很有效。

  > **Note**
  >
  > 机器人控制功能使用来自 Web 请求源的 IP 地址来帮助确定机器人是否经过验证。您无法将其配置为使用 AWS WAF 转发的 IP 配置来检查其他 IP 地址源。如果您已验证通过代理或负载均衡器进行路由的机器人，则可以添加一条在机器人控制功能规则组之前运行的规则来帮助解决此问题。将您的新规则配置为使用转发 IP 地址，并明确允许来自已验证机器人的请求。有关使用转发 IP 地址的信息，请参阅 转发的 IP 地址。

- `awswaf:managed:aws:bot-control:bot:user_triggered:verified` – 用于表示类似于已验证机器人，但最终用户可以直接调用的机器人。机器人控制功能规则将此类机器人视为未经验证的机器人。
- `awswaf:managed:aws:bot-control:bot:developer_platform:verified` – 用于表示类似于已验证机器人，但开发者平台使用它来编写脚本的机器人，例如 Google Apps 脚本。机器人控制功能规则将此类机器人视为未经验证的机器人。
- `awswaf:managed:aws:bot-control:bot:unverified` – 用于表示可以识别自己的机器人，因此可以对其进行命名和分类，但它不会发布可用于独立验证其身份的信息。这些类型的机器人签名可能会被伪造，因此被视为未经验证。

- `awswaf:managed:aws:bot-control:targeted:<additional-details>` – 用于机器人控制功能目标保护的特定标签。
- `awswaf:managed:aws:bot-control:signal:<signal-details>` 和 `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` – 用于在某些情况下提供有关请求的更多信息。

  以下是信号标签的示例。该列表并不完整：

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension` – 指示检测到有助于自动化的浏览器扩展，如 SeleniumIDE。

    只要用户安装了这种类型的扩展，即使他们没有积极使用它，也会添加此标签。如果为此实施标签匹配规则，请注意规则逻辑和操作设置中存在误报的可能性。例如，您可以使用 CAPTCHA 操作代替 Block，或者可以将此标签匹配与其他标签匹配相结合，以增强您对正在使用自动化的信心。

- awswaf:managed:aws:bot-control:signal:automated_browser – 表示请求包含表明客户端浏览器可能已自动运行的指标。
- awswaf:managed:aws:bot-control:targeted:signal:automated_browser— 表示请求的 AWS WAF 令牌包含表明客户端浏览器可能已自动运行的指标。

您可以通过调用 DescribeManagedRuleGroup 从 API 检索一个规则组的所有标签。标签列在响应的 AvailableLabels 属性中。

机器人控制功能托管规则组将标签应用于一组通常允许的可验证机器人。规则组不会阻止这些已验证机器人。如果需要，您可以编写使用机器人控制功能托管规则组所应用的标签的自定义规则，以阻止这些机器人或其中的一部分。有关此项与示例的更多信息，请参阅 AWS WAF 机器人控制。

机器人控制功能规则列表

此部分列出了机器人控制功能规则。

> **Note**
>
> 我们为 AWS 托管规则组中的规则发布的信息旨在为您提供使用规则所需的足够信息，同时不提供不良行为者可能用来规避规则的信息。如果您需要本文档以外的信息，请联系 AWS Support 中心。

Rule name（规则名称）	描述
CategoryAdvertising	检查是否存在用于广告目的的机器人。例如，您可能会使用第三方广告服务，这些服务需要以编程方式访问您的网站。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:advertising 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。

Rule name（规则名称）	描述
`CategoryArchiver`	检查是否存在用于存档目的的机器人。这些机器人会爬网并捕获内容以创建档案。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:archiver` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。
`CategoryContentFetcher`	检查是否存在代表用户访问应用程序网站、获取 RSS feed 等内容或验证您的内容的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:content_fetcher` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。

Rule name（规则名称）	描述
`CategoryEmailClient`	检查是否存在检查电子邮件中指向应用程序网站的链接的机器人。这可能包括企业和电子邮件提供程序运行的机器人，用于验证电子邮件中的链接并举报可疑电子邮件。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:email_client` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。
`CategoryHttpLibrary`	检查机器人从各种编程语言的 HTTP 库中生成的请求。其中可能包括您选择允许或监控的 API 请求。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:http_library` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。

Rule name（规则名称）	描述
`CategoryLinkChecker`	检查是否存在检查断开链接的机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:link_checker` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。
`CategoryMiscellaneous`	检查是否存在与其他类别不匹配的其他机器人。 规则操作，仅适用于未经验证的机器人：Block 标签：`awswaf:managed:aws:bot-control:bot:category:miscellaneous` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。

Rule name（规则名称）	描述
CategoryMonitoring	检查是否存在用于监控目的的机器人。例如，您可以使用机器人监控服务，这些服务会定期对应用程序网站执行 Ping 操作，以监控性能和正常运行时间等信息。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:monitoring 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。
CategoryScrapingFramework	检查来自网页抓取框架的机器人，这些框架用于自动爬取和从网站提取内容。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:scraping_framework 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。

Rule name（规则名称）	描述
CategorySearchEngine	检查是否存在搜索引擎机器人，这些机器人会抓取网站以进行内容索引并提供信息以生成搜索引擎结果。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:search_engine 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。
CategorySecurity	检查是否存在扫描 Web 应用程序漏洞或执行安全审核的机器人。例如，您可以使用第三方安全供应商来扫描、监控或审核 Web 应用程序的安全性。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:security 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。

Rule name（规则名称）	描述
CategorySeo	检查用于搜索引擎优化的机器人。例如，您可以使用搜索引擎工具来抓取您的网站，以帮助您提高搜索引擎排名。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:seo 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。
CategorySocialMedia	检查社交媒体平台是否使用机器人，以便在用户共享您的内容时提供内容摘要。 规则操作，仅适用于未经验证的机器人：Block 标签：awswaf:managed:aws:bot-control:bot:category:social_media 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。
CategoryAI	检查是否存在人工智能（AI）机器人。 规则操作：Block 标签：awswaf:managed:aws:bot-control:bot:category:ai

Rule name（规则名称）	描述
SignalAutomatedBrowser	检查请求中是否显示客户端浏览器可能已自动运行。自动浏览器可用于测试或抓取。例如，您可以使用这些类型的浏览器来监控或验证您的应用程序网站。 规则操作：Block 标签：awswaf:managed:aws:bot-control:signal:automated_browser
SignalKnownBotDataCenter	检查机器人通常使用的数据中心指标。 规则操作：Block 标签：awswaf:managed:aws:bot-control:signal:known_bot_data_center
SignalNonBrowserUserAgent	检查是否存在似乎并非来自 Web 浏览器的用户代理字符串。此类别可以包括 API 请求。 规则操作：Block 标签：awswaf:managed:aws:bot-control:signal:non_browser_user_agent

Rule name（规则名称）	描述
TGT_VolumetricIpTokenAbsent	检查过去 5 分钟内来自客户端的 5 个或更多不包含有效质询令牌的请求。有关 AWS WAF 网络请求令牌 令牌的更多信息，请参阅。 **Note** 如果来自同一客户端的请求最近缺少令牌，则此规则可能会与具有令牌的请求相匹配。 由于延迟，此规则适用的阈值可能略有不同。 此规则对缺失令牌的处理方式与令牌标签不同：awswaf:managed:token:absent 。令牌标签会标记没有令牌的单个请求。此规则会为每个客户端 IP 保留缺少令牌的请求计数，并与超过限制的客户端进行匹配。 规则操作，仅适用于未已验证机器人的客户端：Challenge 标签：awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 awswaf:managed:aws:bot-control:bot:verified 。

Rule name（规则名称）	描述
`TGT_VolumetricSession`	检查客户端会话在任意 5 分钟窗口内是否出现异常的大量请求。该评估基于与使用历史交通模式 AWS WAF 保持的标准体积基线的比较。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 **Note** 启用后，此规则可能需要 5 分钟才能生效。Bot Control 通过将当前流量与计算的流量基线进行比较来识别网络流量中的异常行为。 AWS WAF 规则操作，仅适用于未已验证机器人的客户端：CAPTCHA 标签：`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high` 规则组将以下标签应用于高于最低阈值的中流量和较低流量的请求。对于这些级别，无论客户端是否经过验证，该规则都不采取任何行动：`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` 和 `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` 。

Rule name（规则名称）	描述
	对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。
`TGT_SignalAutomatedBrowser`	检查请求的令牌，以了解是否有迹象表明客户端浏览器可能已自动运行。有关更多信息，请参阅 AWS WAF 代币特征。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 规则操作，仅适用于未已验证机器人的客户端：CAPTCHA 标签：`awswaf:managed:aws:bot-control:targeted:signal:automated_browser` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。

Rule name（规则名称）	描述
`TGT_SignalBrowserInconsistency`	检查浏览器询问数据是否不一致。有关更多信息，请参阅 AWS WAF 代币特征。 仅当 Web 请求具有令牌时，此检查才适用。令牌由应用程序集成软件开发工具包以及规则操作 CAPTCHA 和 Challenge 添加到请求中。有关更多信息，请参阅 AWS WAF 网络请求令牌。 规则操作，仅适用于未已验证机器人的客户端：CAPTCHA 标签：`awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。

Rule name（规则名称）	描述
`TGT_TokenReuseIp`	检查是否存在 5 个以上不同 IP 地址中使用同一令牌的情况。 **Note** 由于延迟，此规则适用的阈值可能略有不同。在应用规则操作之前，一些请求可能会超出限制。 规则操作：Count 标签：`awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Rule name（规则名称）	描述
`TGT_ML_CoordinatedActivityMedium` 和 `TGT_ML_CoordinatedActivityHigh`	检查是否存在与分布式、协调的机器人活动一致的异常行为。规则级别表示一组请求参与协调攻击的可信度。 **Note** 仅当规则组配置为使用机器学习 (ML) 时，这些规则才会运行。有关配置此选择的信息，请参阅 将 AWS WAF Bot Control 托管规则组添加到 Web ACL。 AWS WAF 通过机器学习分析网站流量统计数据来执行此检查。 AWS WAF 每隔几分钟分析一次网络流量，并优化分析以检测分布在许多 IP 地址上的低强度、持续时间长的机器人。 在确定未进行协调攻击之前，这些规则可能与极少数请求相匹配。因此，如果您只看到一两个匹配项，则结果可能是误报。但是，如果您看到很多符合这些规则的匹配项，那么您可能正在经历协调攻击。 **Note** 使用 ML 选项启用机器人控制功能定向规则后，这些规则可能需要长达 24 小时才能生效。Bot Control 通过将当前流量与计算出的流量基线进行比较来识别网络流量中的异常行为。 AWS WAF AWS WAF 仅在您使用带有 ML 选项的 Bot Control 目标规则时才计算基线，并

Rule name（规则名称）	描述
	且最多可能需要 24 小时才能建立有意义的基准。 我们会定期更新这些规则的机器学习模型，以改善机器人预测。如果您发现这些规则所做的机器人预测突然发生重大变化，请联系您的客户经理或在 Center 提起诉AWS Support 讼。 规则操作，仅适用于未已验证机器人的客户端： • 中等: Count • High: Count 标签：`awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` 和 `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` 对于已验证机器人，规则组不采取任何行动，但会添加规则标签和标签 `awswaf:managed:aws:bot-control:bot:verified` 。 规则组还添加标签 `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` 以指示低置信度，但它不应用任何规则或对这些请求采取任何操作。

版本化 AWS 托管规则规则组的部署

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

> **Note**
>
> 本节仅适用于版本化的 AWS 托管规则规则组。唯一未进行版本控制的规则组是 IP 信誉规则组。

主题

- AWS 托管规则规则组部署通知
- AWS 托管规则的标准部署概述
- AWS 托管规则的典型版本状态
- AWS 托管规则的发布候选部署
- AWS 托管规则的静态版本部署
- AWS 托管规则的默认版本部署
- AWS 托管规则的异常部署
- AWS 托管规则的默认部署回滚

AWS 托管规则规则组部署通知

AWS 受版本控制的托管规则组都为部署提供 SNS 更新通知，并且都使用相同的 SNS 主题 Amazon 资源名称 (ARN)。唯一未进行版本控制的规则组是 IP 信誉规则组。

对于影响保护的部署（例如对默认版本的更改），AWS 提供 SNS 通知，以通知您计划中的部署并告知您何时开始部署。对于不影响保护的部署，例如候选版本和静态版本部署，AWS 可能会在部署开始后甚至在部署完成后通知您。部署完新静态版本后，将在变更日志AWS 托管规则变更日志和文档历史记录页面中 AWS 更新本指南。文档历史记录

要接收有关 AWS 托管规则组的所有更新，AWS 请订阅本指南任何 HTML 页面上的 RSS 提要，并订阅 AWS 托管规则规则组的 SNS 主题。有关订阅 SNS 通知的信息，请参阅。收到有关托管规则组新版本和更新的通知

SNS 通知的内容

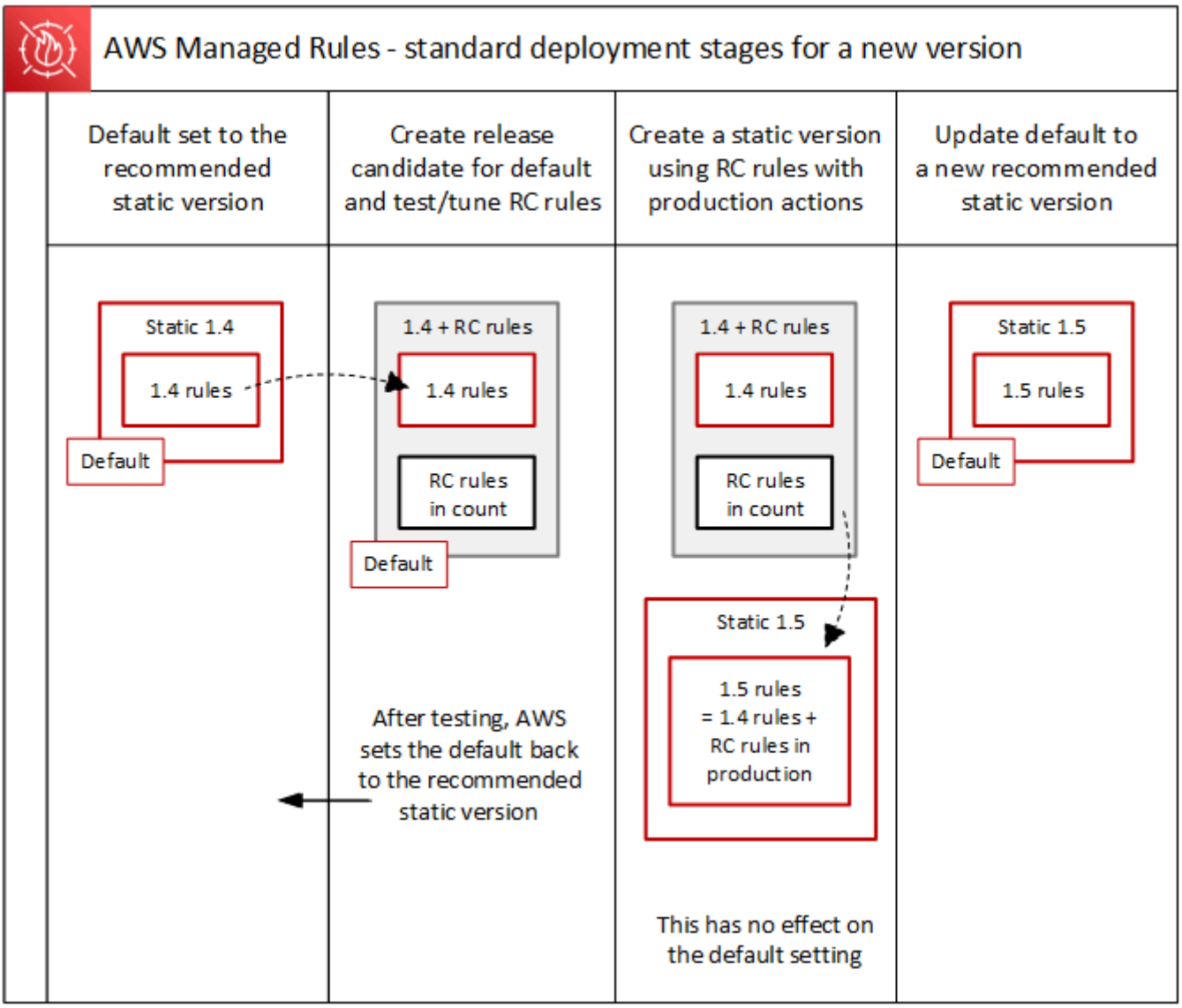
Amazon SNS 通知中的字段始终包含 “主题”、“消息” 和。 MessageAttributes其他字段取决于消息的类型以及通知所针对的托管规则组。下面是 AWSManagedRulesCommonRuleSet 的一个通知列表示例。

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

AWS 托管规则的标准部署概述

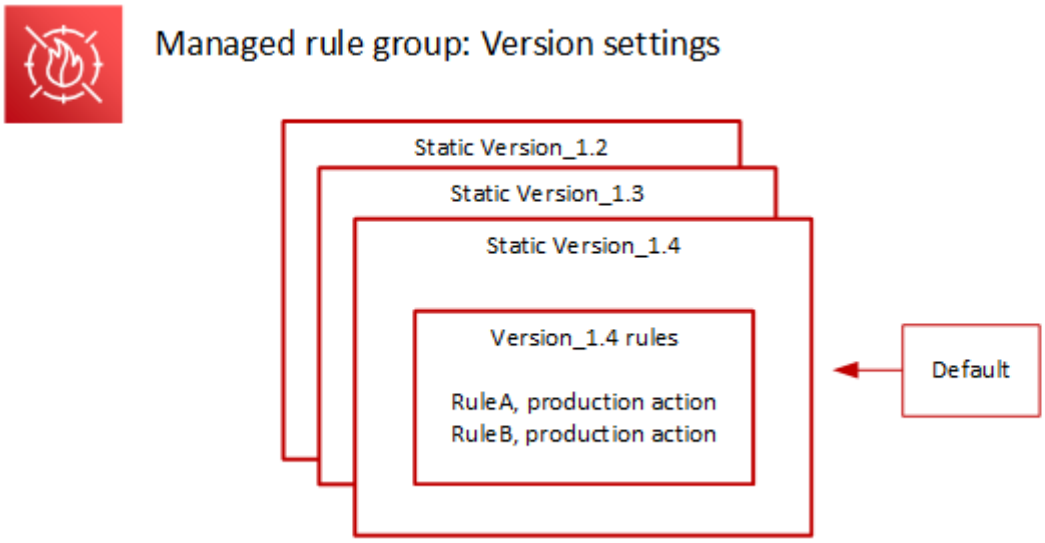
AWS 使用三个标准部署阶段推出新的 AWS 托管规则功能：候选版本、静态版本和默认版本。

下图描述了这些标准部署。以下各节详述了其中的各个部分。



AWS 托管规则的典型版本状态

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



静态版本中大多数规则的生产操作是Block，但可能设置为不同的值。有关规则操作设置的详细信息，请在 AWS 托管规则规则组列表 参阅每个规则组的规则列表。

AWS 托管规则的发布候选部署

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

如果您使用默认版本，则候选发布版本部署不会改变规则组管理 Web 流量的方式。在测试候选规则时，您可能会注意到以下几点：

- 默认版本名称从 `Default (using Version_X.Y)` 更改为 `Default (using Version_X.Y_PLUS_RC_COUNT)`。
- Amazon 中的其他计数指标 CloudWatch 名称RC_COUNT中包含其名称。它们由候选发布规则生成。

AWS 测试候选版本大约一周，然后将其删除并将默认版本重置为当前推荐的静态版本。

AWS 对候选版本部署执行以下步骤：

1. 创建候选版本 — 根据当前推荐的静态版本（即默认版本所指向的版本） AWS 添加候选版本。

   候选发布版本的名称是附加了 _PLUS_RC_COUNT 的静态版本名称。例如，如果当前推荐的静态版本是 `Version_2.1`，则候选发布版本将命名为 `Version_2.1_PLUS_RC_COUNT`。

   候选发布版本包含以下规则：

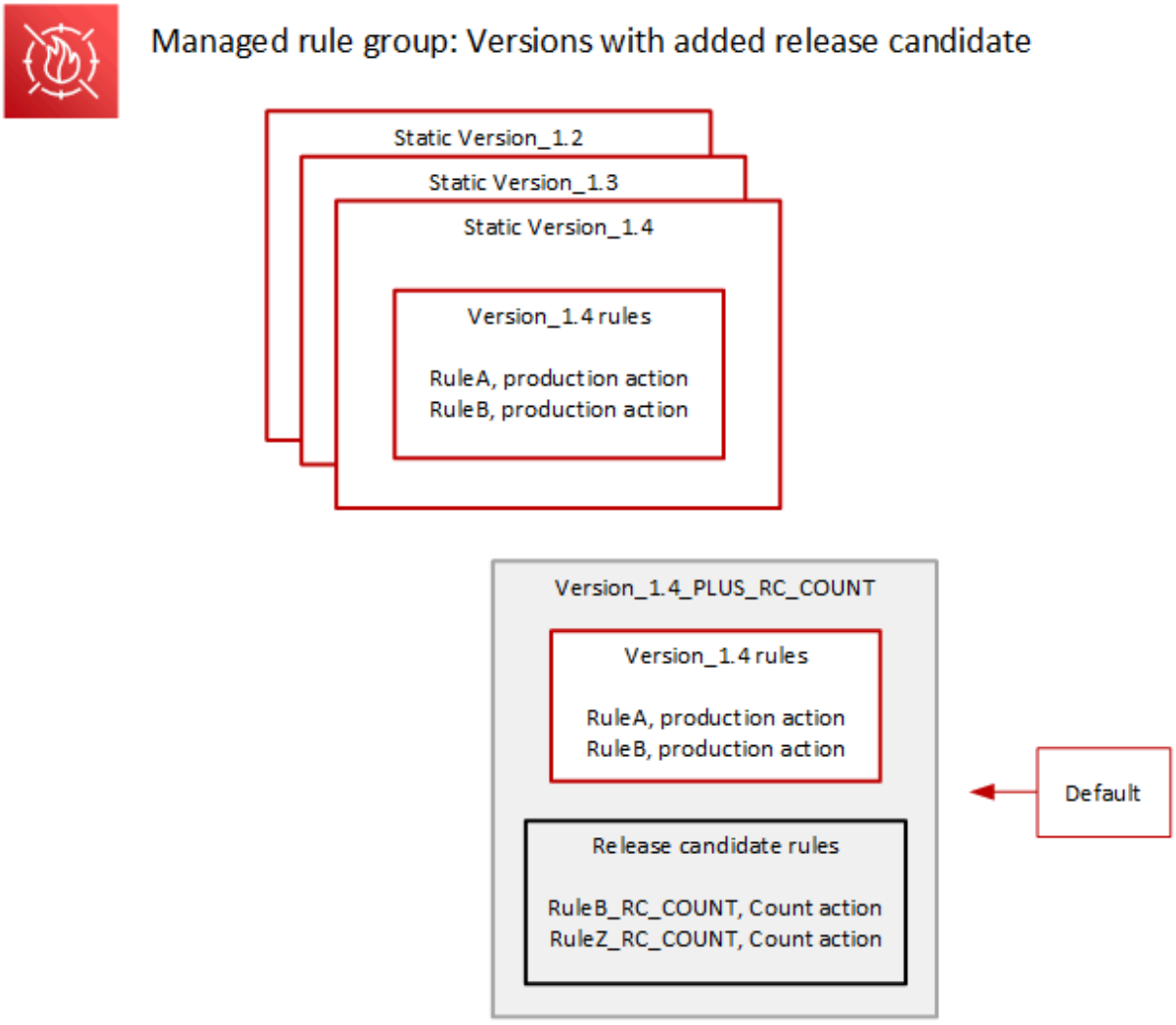
- 规则完全从当前推荐的静态版本中复制，规则配置未做任何更改。
- 候选新规则，规则操作设置为 Count，名称以 _RC_COUNT 结尾。

  大多数候选规则都对规则组中已存在的规则提供了改进建议。每条规则的名称都是在现有规则的名称后附上 _RC_COUNT。

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

   您将看到默认版本的名称从仅表示静态版本的名称（如 Default (using Version_1.4)）更改为表示静态版本加上候选发布规则（如 Default (using Version_1.4_PLUS_RC_COUNT)）。此命名方案使您能够识别管理 Web 流量的静态版本。

   下图显示了此时示例规则组版本的状态。



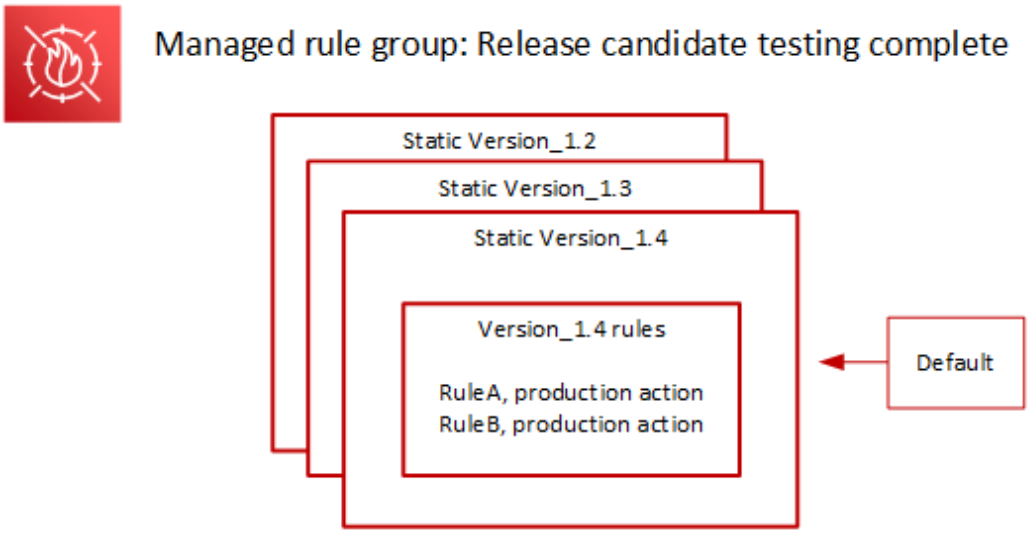
   候选版本规则始终使用 Count 操作进行配置，因此它们不会改变规则组管理 Web 流量的方式。

候选发布规则生成 Amazon CloudWatch 计数指标， AWS 用于验证行为和识别误报。 AWS 根据需要进行调整，以调整候选发布版本计数规则的行为。

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

3. 将默认版本恢复为推荐的静态版本-测试候选发布规则后， AWS 将默认版本设置回当前推荐的静态版本。默认版本名称设置会删除结_PLUS_RC_COUNT尾，并且规则组停止为候选发布规则生成 CloudWatch 计数指标。这是一个静默更改，与部署默认版本回滚不同。

下图显示了候选发布版本测试完成后示例规则组版本的状态。



定时和通知

AWS 根据需要部署候选发布版本，以测试规则组的改进。

- SNS — 在部署开始时 AWS 发送 SNS 通知。该通知指明了测试候选发布版本的预计时间。测试完成后， AWS 默默返回静态版本设置的默认值，不另行通知。
- 更改日志- AWS 不更新此类部署的变更日志或本指南的其他部分。

AWS 托管规则的静态版本部署

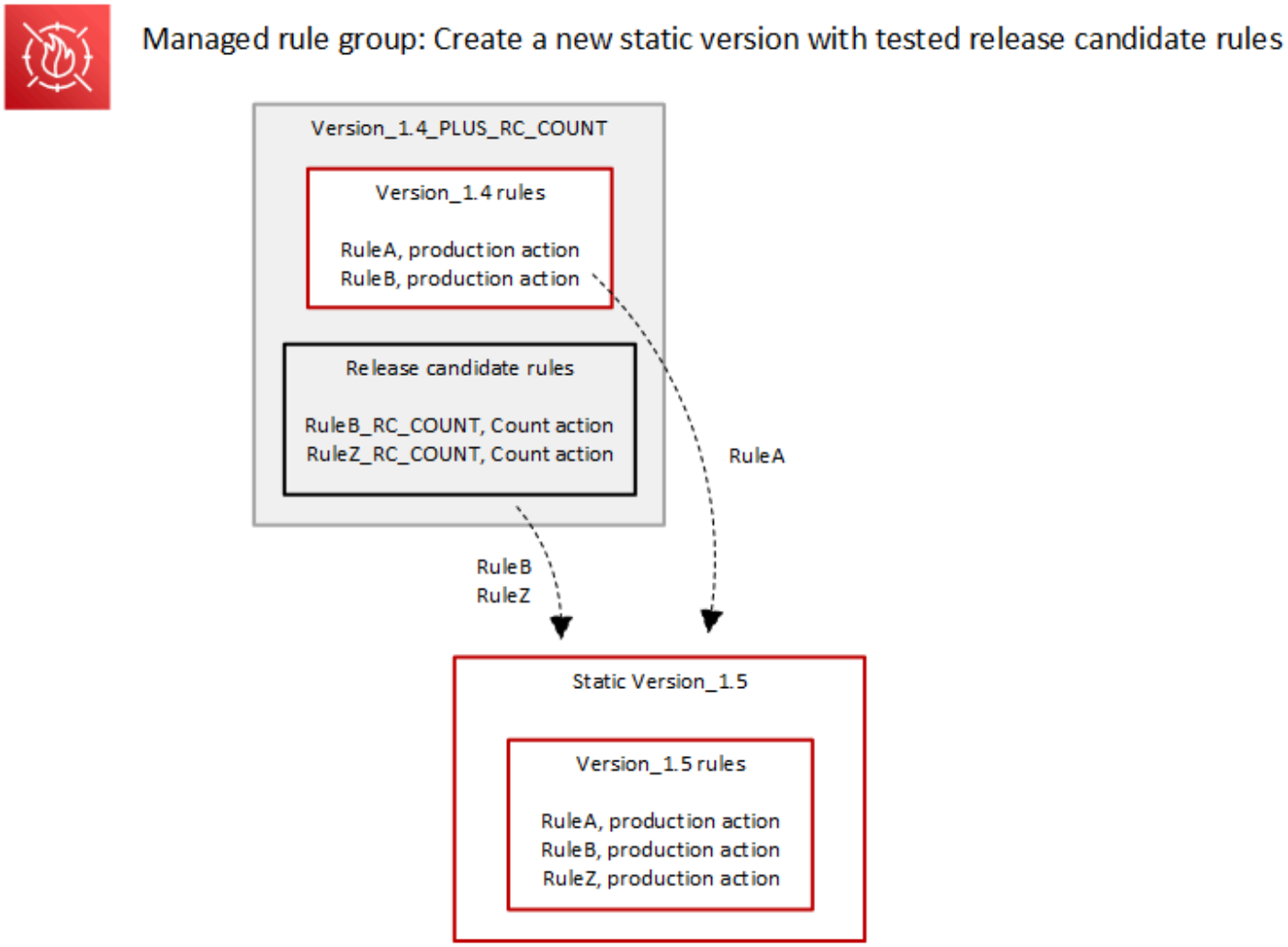
当 AWS 确定候选版本对规则组进行了有价值的更改时，会根据候选版本为该规则组 AWS 部署新的静态版本。此部署不会更改规则组的默认版本。

新的静态版本包含候选发布版本中的以下规则：

- 来自先前静态版本的规则，其在候选发布规则中没有替换候选规则。
- 候选发布规则，包含以下更改：
  - AWS 通过删除候选版本后缀_RC_COUNT来更改规则名称。
  - AWS 将规则操作从更改Count为其生产规则操作。

  对于替换先前已有规则的候选发布规则，这将取代新静态版本中先前规则的功能。

下图描述了根据候选发布版本创建新的静态版本的过程。



部署后，新的静态版本可供您测试，如果您愿意，也可以将其用于保护中。您可以访问 AWS 托管规则规则组列表，在规则组的规则列表中查看新的和更新的规则操作和描述。

静态版本在部署后是不可变的，并且只有在 AWS 过期时才会更改。有关版本生命周期的信息，请参阅受版本控制的托管规则组。

定时和通知

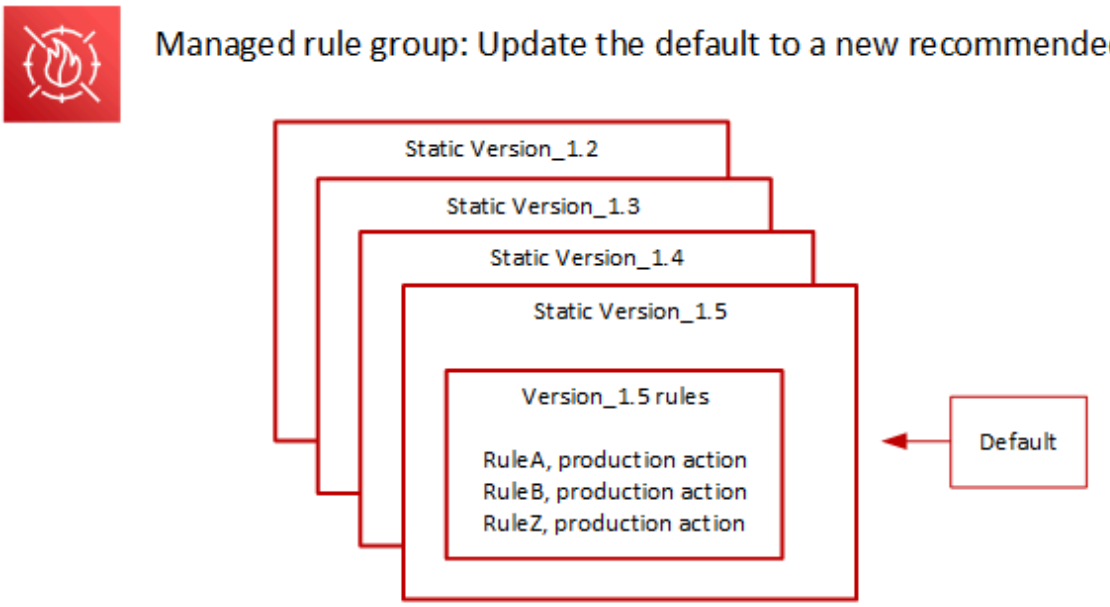
AWS 根据需要部署新的静态版本，以部署对规则组功能的改进。部署静态版本不会影响默认版本设置。

- SNS — 部署完成后 AWS 发送 SNS 通知。
- 更改日志-部署完成所有可用区域后，根据需要 AWS 更新本指南中的规则组定义，然后在 Managed Rules 规则组变更日志和文档历史记录页面中宣布发布。 AWS WAF AWS

AWS 托管规则的默认版本部署

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

下图显示了将默认版本设置 AWS 移至新的静态版本后示例规则组版本的状态。



在将此更改部署到默认版本之前，会 AWS 提供通知，以便您可以测试即将到来的更改并为之做好准备。如果您使用默认版本，则无法执行任何操作，并且可以在更新期间继续使用该版本。相反，如果您想在默认版本部署的计划开始之前延迟切换到新版本，则可以明确配置规则组，使其使用作为默认设置的静态版本。

定时和通知

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

- SNS — 至少在目标部署日前一周 AWS 发送 SNS 通知，然后在部署当天，即部署开始时再发送一次 SNS 通知。每份通知都包括规则组名称、默认版本更新到的静态版本、部署日期以及正在执行更新的每个 AWS 区域的计划部署时间。
- 更改日志- AWS 不更新此类部署的变更日志或本指南的其他部分。

AWS 托管规则的异常部署

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

AWS 为异常部署提供尽可能多的提前通知。

定时和通知

AWS 仅在需要时才执行异常部署。

- SNS — 尽可能在目标部署日之前 AWS 发送 SNS 通知，然后在部署开始时再发送一个 SNS 通知。每份通知都包括规则组名称、正在进行的更改和部署日期。
- 更改日志 — 如果部署是针对静态版本的，则在所有可用版本的部署完成后，根据需要 AWS 更新本指南中的规则组定义，然后在 Managed Rules 规则组更改日志和文档历史记录页面中宣布该版本。AWS WAF AWS

AWS 托管规则的默认部署回滚

在某些条件下， AWS 可能会将默认版本回滚到之前的设置。所有 AWS 区域的回滚时间通常不到十分钟。

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

回滚默认版本设置后，会 AWS 加快出现问题的静态版本的到期时间，并加快发布新的静态版本以解决该问题。

定时和通知

AWS 仅在需要时才执行默认版本回滚。

- SNS — 在回滚时 AWS 发送单个 SNS 通知。通知包括规则组名称、要对默认版本设置的版本和部署日期。这类部署非常快，因此通知不提供区域的时间信息。
- 更改日志- AWS 不更新此类部署的变更日志或本指南的其他部分。

AWS 托管规则免责声明

AWS 托管规则旨在保护您免受常见网络威胁的侵害。根据文档使用 AWS 托管规则组时，可以为您的应用程序增加另一层安全保护。但是， AWS 托管规则规则组并不是用来取代您的安全职责，后者由您选择的 AWS 资源决定。请参阅分担责任模型，确保您的资源 AWS 得到适当保护。

AWS 托管规则变更日志

本节列出了自 2019 年 11 月发布 AWS WAF 以来对 AWS 托管规则的更改。

> **Note**
>
> 此变更日志报告了对的 AWS 托管规则中的规则和规则组的 AWS WAF更改。
> 对于IP 声誉规则组，此变更日志报告规则和规则组的更改，并报告规则使用的 IP 地址列表来源的重大变化。由于 IP 地址列表的动态性质，它不会报告 IP 地址列表本身的更改。如果您对 IP 地址列表有疑问，请联系您的客户经理或在 Cent AWS Support er 提交案例。

规则组和规则	描述	日期
AWS WAF 机器人控制规则组 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组	机器人和欺诈规则组现已版本化。如果您使用这些规则组中的任何一个，则此更新不会改变它们处理您的网络流量的方式。 此更新将当前规则组版本设置为静态版本 1.0，并将默认版本设置为指向该版本。 有关版本化托管规则的更多信息，请参阅以下内容： • 受版本控制的托管规则组 • 版本化 AWS 托管规则规则组的部署 • 收到有关托管规则组新版本和更新的通知	2024-05-29

规则组和规则	描述	日期
POSIX 操作系统托管规则组 • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	已发布此规则组的静态版本 3.0。这不会更改默认版本设置。 已将其移除UNIXShellCommandsVariables_QUERYARGUMENTS 并替换为UNIXShellCommandsVariables_QUERYSTRING 。如果您在标签上有与之匹配的规则UNIXShellCommandsVariables_QUERYARGUMENTS ，则在使用此版本时，请将其切换为与标签上的匹配UNIXShellCommandsVariables_QUERYSTRING 。新标签是awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString 。 添加了匹配所有标题的规则UNIXShellCommandsVariables_HEADER 。 使用改进的检测逻辑更新了托管规则组中的所有规则。 更正了记录在案的标签大小写UNIXShellCommandsVariables_BODY 。	2024-05-28

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组 • CrossSiteScripting*	已发布此规则组的静态版本 1.12。 将签名添加到所有跨站点脚本规则中，以改进检测并减少误报。	2024-05-21
SQL 数据库托管规则组 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLiExtendedPatterns_QUERYARGUMENTS	已发布此规则组的静态版本 1.2。 在列出的规则中添加了JS_DECODE 文本转换。	2024-05-14
已知错误输入托管规则组 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_QUERYSTRING • Log4JRCE_QUERYSTRING • Log4JRCE_BODY • Log4JRCE_HEADER	已发布此规则组的静态版本 1.22。 在列出的规则中添加了JS_DECODE 文本转换。	2024-05-08
POSIX 操作系统托管规则组	发布了此规则组的静态版本 2.2。 在两个规则中都添加了JS_DECODE 文本转换。	2024-05-08

规则组和规则	描述	日期
Windows 操作系统托管规则组 • PowerShellCommands_BODY	发布了此规则组的静态版本 2.1。 向中添加了特征码PowerShellCommands_BODY 以改进检测。	2024-05-03
Amazon IP 声誉列表托管规则组 • AWSManagedIPReputationList	更新了 IP 信誉列表的来源，以改进对积极参与恶意活动的地址的识别并减少误报。 此更新不涉及新版本，因为此规则组未进行版本控制。	2024-03-13
已知错误输入托管规则组	发布了此规则组的静态版本 1.21。 添加了签名以改进检测并减少误报。	2023-12-16
已知错误输入托管规则组 • ExploitablePaths_URIPATH	发布了此规则组的静态版本 1.20。 更新了 ExploitablePaths_URIPATH 规则，以增加对与“Atlassian Confluence CVE-2023-22518 授权不当”漏洞相匹配的请求的检测。此漏洞会影响所有版本的 Confluence 数据中心和服务器。有关更多信息，请参阅 NIST：国家漏洞数据库：CVE-2023-22518 详细信息。	2023-12-14

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组 • CrossSiteScripting*	发布了此规则组的静态版本 1.11。 将签名添加到所有跨站点脚本规则中，以改进检测并减少误报。	2023-12-06
AWS WAF 机器人控制规则组 • 新标签：awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low	将协调活动低标签添加到规则组的目标保护级别标签中。此标签未与任何规则关联。此标签是对中高级规则和标签的补充。	2023-12-05
机器人控制功能标签 • 标签：awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension	向规则组添加了一个信号标签，指示检测到有助于自动化的浏览器扩展。此标签并非特定于单个规则。	2023-11-14
核心规则集 (CRS) 托管规则组 • EC2MetaDataSSRF_QUERYARGUMENTS	发布了此规则组的静态版本 1.10。 更新了一条规则，以改进检测并减少误报。	2023-11-02

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组 • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_URIPATH • EC2MetaDataSSRF_QUERYARGUMENTS	发布了此规则组的静态版本 1.9。 更新了规则，以改进检测并减少误报。	2023-10-30
POSIX 操作系统托管规则组 • UNIXShellCommandsVariables_QUERYARGUMENTS	发布了此规则组的静态版本 2.1。 更新了查询参数规则，以改进检测。	2023-10-12
核心规则集 (CRS) 托管规则组 • GenericLFI_QUERYARGUMENTS • GenericLFI_URIPATH • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	发布了此规则组的静态版本 1.8。 更新了规则，以改进检测。	2023-10-11

规则组和规则	描述	日期
已知错误输入托管规则组 • ExploitablePaths_URIPATH	异常部署：发布了此规则组的静态版本 1.19。更新了默认版本，以使用 1.19。 更新了 ExploitablePaths_URIPATH 规则，以增加对与 Atlassian Confluence CVE-2023-22515 权限升级漏洞相匹配的请求的检测。此漏洞会影响某些版本的 Atlassian Confluence。有关更多信息，请参阅 NIST：国家漏洞数据库：CVE-2023-22515 详细信息和 Atlassian Support：CVE-2023-22515 常见问题解答。 有关部署类型的信息，请参阅 AWS 托管规则的异常部署。	2023-10-04
已知错误输入托管规则组 • Host_localhost_HEADER • Log4J* • JavaDeserialization*	异常部署：发布了此规则组的静态版本 1.18。这是此静态版本的快速推出，以适应版本 1.19 的创建和推出。 更新了 Host_localhost_HEADER 规则以及所有 Log4J 和 Java 反序列化规则，以改进检测。 有关部署类型的信息，请参阅 AWS 托管规则的异常部署。	2023-10-04

规则组和规则	描述	日期
AWS WAF 机器人控制规则组 • TGT_TokenReuseIp • TGT_ML_CoordinatedActivityMedium • TGT_ML_CoordinatedActivityHigh	向规则组添加了带有 Count 操作的规则。 令牌重用 IP 规则可检测并计算通过 IP 地址共享的令牌。 协调活动规则使用对网站流量的自动机器学习 (ML) 分析来检测与机器人相关的活动。在规则组配置中，您可以选择退出使用 ML。在此版本中，当前使用目标保护级别的客户可以选择使用机器学习。选择退出将禁用协调活动规则。	2023-09-06
AWS WAF 机器人控制规则组 • CategoryAI	已将规则 CategoryAI 添加到规则组中。	2023-08-30

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_QUERYARGUMENTS • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_URIPATH	发布了此规则组的静态版本 1.7。 更新了受限扩展和 EC2 元数据 SSRF 规则，以改进检测并减少误报。	2023-07-26
AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组 新规则组中的所有规则	添加了规则组 AWSManagedRulesACFPRuleSet 。	2023-06-13
Linux 操作系统托管规则组 • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	发布了此规则组的静态版本 2.2。 添加了签名，以改进检测。	2023-05-22

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	发布了此规则组的静态版本 1.6。 更新了跨站脚本攻击（XSS）和受限扩展规则，以改进检测并减少误报。	2023-04-28

规则组和规则	描述	日期
PHP 应用程序托管规则组 • 更新了 PHPHighRiskMethodsVariables_BODY • 删除了 PHPHighRiskMethodsVariables_QUERYARGUMENTS • 新增了 PHPHighRiskMethodsVariables_QUERYSTRING • 新增了 PHPHighRiskMethodsVariables_HEADER	发布了此规则组的静态版本 2.0。 添加了签名，以改进所有规则中的检测。 已将规则 PHPHighRiskMethodsVariables_QUERYARGUMENTS 替换为 PHPHighRiskMethodsVariables_QUERYSTRING ，它会检查整个查询字符串，而不仅仅是查询参数。 添加了规则 PHPHighRiskMethodsVariables_HEADER ，以扩大覆盖范围，纳入所有标头。 更新了以下标签，使其与标准 AWS 托管规则标签保持一致： • 旧名称：PHPHighRiskMethodsVariables_BODY 新名称：PHPHighRiskMethodsVariables_Body • 旧名称：PHPHighRiskMethodsVariables_QUERYARGUMENTS 新名称：PHPHighRiskMethodsVariables_QueryString	2023-02-27

规则组和规则	描述	日期
AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 • VolumetricIpFailedLoginResponseHigh • VolumetricSessionFailedLoginResponseHigh	添加了登录响应检查规则，用于受保护的 Amazon CloudFront 分配。这些规则可以阻止来自 IP 地址和客户端会话的新登录尝试，这些地址和客户端会话最近导致的登录尝试失败次数过多。	2023-02-15
核心规则集 (CRS) 托管规则组 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	发布了此规则组的静态版本 1.5。 更新了跨站脚本攻击（XSS）筛选器，以改进检测。	2023-01-25

规则组和规则	描述	日期
Linux 操作系统托管规则组 • LFI_COOKIE ：已删除 • LFI_HEADER ：已添加 • LFI_URIPATH • LFI_QUERYSTRING	发布了此规则组的静态版本 2.1。 删除了规则 LFI_COOKIE 及其标签 awswaf:managed:aws:linux-os:LFI_Cookie ，并替换为新规则 LFI_HEADER 及其标签 awswaf:managed:aws:linux-os:LFI_Header 。此更改将检查范围扩展到多个标头。 已为所有规则添加文本转换和签名，以改进检测。	2022-12-15
核心规则集 (CRS) 托管规则组 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	发布了此规则组的静态版本 1.4。 已在 NoUserAgent_HEADER 中添加文本转换，以删除所有空字节。更新了跨站点脚本规则中的筛选器，以改进检测。	2022-12-05

规则组和规则	描述	日期
已知错误输入托管规则组 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER	发布了此规则组的静态版本 1.17。 更新了 Java 反序列化规则，并增加了对与 Apache CVE-2022-42889 匹配的请求的检测，它是 1.10.0 之前的 Apache Commons Text 版本中的远程代码执行 (RCE) 漏洞。有关更多信息，请参阅 NIST：国家漏洞数据库：CVE-2022-42889 详细信息和 CVE-2022-42889：由于不安全的插值默认设置，1.10.0 之前的 Apache Commons Text 在应用于不受信任的输入时允许 RCE。 改进了 Host_localhost_HEADER 中的检测。	2022-10-20
已知错误输入托管规则组 • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY	发布了此规则组的静态版本 1.16。 删除了 1.15 版本中 AWS 识别的误报。	2022-10-05

规则组和规则	描述	日期
POSIX 操作系统托管规则组 PHP 应用程序托管规则组 WordPress 应用程序托管规则组	更正了记录在案的标签名称。	2022-09-19
IP 声誉规则组 • AWSManagedIPDDoSList	此更改不会改变规则组处理 Web 流量的方式。 根据 Amazon 威胁情报，添加了一项新规则，其中包含检查积极参与 DDoS 活动的 IP 地址的 Count 行动。	2022-08-30

规则组和规则	描述	日期
已知错误输入托管规则组 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	发布了此规则组的静态版本 1.15。 删除了 Log4JRCE，并将其替换为 Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 和 Log4JRCE_BODY ，以便对误报进行更精细的监控和管理。 添加了签名，以改进对 PROPFIND_METHOD 和所有 JavaDeserializationRCE* 和 Log4JRCE* 规则的检测和阻止。 更新了标签，以更正 Host_localhost_HEADER 和所有 JavaDeserializationRCE* 规则中的大小写。 更正了的 JavaDeserializationRCE_HEADER 描述。	2022-08-22
AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 • UnsupportedCognitoIDP	添加了一条规则，禁止对 Amazon Cognito 用户群体 Web 流量使用账户防盗托管规则组。	2022-08-11

规则组和规则	描述	日期
核心规则集 (CRS) 托管规则组	AWS 已为版本Version_1.2 和规则组Version_2.0 的计划过期。这些版本将于 2022 年 9 月 9 日到期。有关版本到期的信息，请参阅 受版本控制的托管规则组。	2022-06-09
核心规则集 (CRS) 托管规则组 • GenericLFI_URIPATH GenericRFI_URIPATH	发布了此规则组的版本 1.3。此版本更新了规则 GenericLFI_URIPATH 和 GenericRFI_URIPATH 中的匹配签名，以改进检测。	2022-05-24
AWS WAF 机器人控制规则组 • CategoryEmailClient	已将规则 CategoryEmailClient 添加到规则组中。	2022-04-06
已知错误输入托管规则组 • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	发布了此规则组的版本 1.14。四条 JavaDeserializiztionRCE 规则已移至 Block 模式。	2022-03-31

规则组和规则	描述	日期
已知错误输入托管规则组 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	发布了此规则组的版本 1.13。更新了 Spring Core 和云函数 RCE 漏洞的文本转换。这些规则处于计数模式，用于收集指标并评估匹配的模式。该标签可用于阻止自定义规则中的请求。后续版本将在区块模式下使用这些规则进行部署。	2022-03-31

规则组和规则	描述	日期
已知错误输入托管规则组 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	发布了此规则组的版本 1.12。已为 Spring Core 和云函数 RCE 漏洞添加签名。这些规则处于计数模式，用于收集指标并评估匹配的模式。该标签可用于阻止自定义规则中的请求。后续版本将在区块模式下使用这些规则进行部署。 删除了规则Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 和 Log4JRCE_BODY ，并将其替换为规则 Log4JRCE。	2022-03-30
IP 声誉规则组 • AWSManagedReconnaissanceList	更新了 AWSManagedReconnaissanceList 规则，将操作从计数改为阻止。	2022-02-15
AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 新规则组中的所有规则	添加了规则组 AWSManagedRulesATPRuleSet 。	2022-02-11

规则组和规则	描述	日期
已知错误输入托管规则组 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY	发布了此规则组的版本 1.9。为了灵活使用此功能，删除了规则 Log4JRCE，并将其替换为规则 Log4JRCE_HEADER 、Log4JRCE_QUERYSTRING 、Log4JRCE_URI 和 Log4JRCE_BODY 。添加了签名，以改进检测和阻止。	2022-01-28
核心规则集 (CRS) • CrossSiteScripting_URIPATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_COOKIE	发布了此规则组的版本 2.0。对于这些规则，调整了检测签名，以减少误报。将 URL_DECODE 文本转换替换为双 URL_DECODE_UNI 文本转换。新增了 HTML_ENTITY_DECODE 文本转换。	2022-01-10
核心规则集 (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	作为该规则组版本 2.0 的一部分，新增了 URL_DECODE_UNI 文本转换。已从 URL_DECODE 文本转换中移除 RestrictedExtensions_URIPATH 。	2022-01-10

规则组和规则	描述	日期
SQL 数据库 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	发布了此规则组的版本 2.0。将 URL_DECODE 文本转换替换为双 URL_DECODE_UNI 文本转换，并新增了 COMPRESS_WHITE_SPACE 文本转换。 向 SQLiExtendedPatterns_QUERYARGUMENTS 中添加了更多检测签名。 向 SQLi_BODY 中添加了 JSON 检查。 添加了规则 SQLiExtendedPatterns_BODY 。 删除了规则 SQLi_URIPATH 。	2022-01-10
已知错误输入 • Log4JRCE	发布了规则 Log4JRCE 的 1.8 版，以改进标头检查和匹配条件。	2021-12-17
已知错误输入 • Log4JRCE	发布了规则 Log4JRCE 的 1.4 版，用于调整匹配条件并检查其他标头。发布了版本 1.5，以调整匹配条件。	2021-12-11

规则组和规则	描述	日期
已知错误输入 • Log4JRCE • BadAuthToken_COOKIE_AUTHORIZATION	为回应 Log4j 中最近披露的安全问题，添加了规则 Log4JRCE 版本 1.2。有关信息，请参阅 CVE-2021-44228 此规则用于检查常用 URI 路径、查询字符串、请求正文的前 8KB 和常用标头。该规则使用双 URL_DECODE_UNI 文本转换。发布了 Log4JRCE 的 1.3 版，以调整匹配条件并检查其他标头。 删除了规则 BadAuthToken_COOKIE_AUTHORIZATION 。	2021-12-10

下表列出了 2021 年 12 月之前的变更。

规则组和规则	描述	日期	
Amazon IP 声誉列表	AWSManagedReconnaissanceList	在监控/计数模式下添加了 AWSManagedReconnaissanceList 规则。此规则包含正在对 AWS 资源执行侦测的 IP 地址。	2021-11-23
Windows 操作系统	WindowsShellCommands PowerShellCommands	为 WindowsShell 命令添加了三条新规则：WindowsShellCommands_COOKIE WindowsSh	2021-11-23

规则组和规则	描述	日期	
		ellComman ds_QUERYA RGUMENTS 、和WindowsSh ellComman ds_BODY 。 添加了新 PowerShel l 规则:PowerShel lCommands _COOKIE . 通过删除字符串 _Set1 和 _Set2 重构了 PowerShel lComands 规则命名。 向 PowerShel lRules 中添加了更全面的检测签名。 为所有 Windows 操作系统规则添加了 URL_DECODE_UNI 文本转换。	

规则组和规则	描述	日期	
Linux 操作系统	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	将双 URL_DECODE 文本转换替换为双 URL_DECODE_UNI 。 添加了 NORMALIZE_PATH_WIN 作为第二个文本转换。 将 LFI_BODY 规则替换为 LFI_COOKIE 规则。 为所有 LFI 规则添加了更全面的检测签名。	2021-11-23
核心规则集 (CRS)	SizeRestrictions_BODY	降低了大小限制，以阻止正文有效负载大于 8 KB 的 Web 请求。以前，该限制为 10 KB。	2021-10-27
核心规则集 (CRS)	EC2MetaDataSSRF_BODY EC2MetaDataSSRF_COOKIE EC2MetaDataSSRF_URIPATH EC2MetaDataSSRF_QUERYARGUMENTS	添加了更多检测签名。添加了双 Unicode 网址解码，以改善阻止效果。	2021-10-27

规则组和规则	描述	日期	
核心规则集 (CRS)	GenericLFI_QUERYARGUMENTS GenericLFI_URIPATH RestrictedExtensions_URIPATH RestrictedExtensions_QUERYARGUMENTS	添加了双 Unicode 网址解码，以改善阻止效果。	2021-10-27
核心规则集 (CRS)	GenericRFI_QUERYARGUMENTS GenericRFI_BODY GenericRFI_URIPATH	根据客户反馈更新了规则签名以减少误报。添加了双 Unicode 网址解码，以改善阻止效果。	2021-10-27
全部	所有规则	为所有尚不支持 AWS WAF 标签的规则添加了对标签的支持。	2021-10-25
Amazon IP 声誉列表	AWSManagedIPReputationList_xxxx	重组了 IP 信誉列表，删除了规则名称中的后缀，并增加了对标签的支持。 AWS WAF	2021-05-04

规则组和规则	描述	日期	

匿名 IP 列表	`AnonymousIPList`
	
	`HostingProviderList`
		增加了对 AWS WAF 标签的支持。	2021-05-04

机器人控制功能	全部	添加了机器人控制功能规则集。	2021-04-01
核心规则集 (CRS)	`GenericRFI_QUERYARGUMENTS`	添加了双重 URL 解码。	2021-03-03
核心规则集 (CRS)	`RestrictedExtensions_URIPATH`	改进了规则的配置并添加了额外的 URL 解码。	2021-03-03
管理保护	`AdminProtection_URIPATH`	添加了双重 URL 解码。	2021-03-03
已知错误输入	`ExploitablePaths_URIPATH`	改进了规则的配置并添加了额外的 URL 解码。	2021-03-03
Linux 操作系统	`LFI_QUERYARGUMENTS`	改进了规则的配置并添加了额外的 URL 解码。	2021-03-03
Windows 操作系统	全部	改进了规则的配置。	2020-09-23

规则组和规则	描述	日期	
PHP 应用程序	PHPHighRiskMethodsVariables_QUERYARGUMENTS PHPHighRiskMethodsVariables_BODY	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-09-16
POSIX 操作系统	UNIXShellCommandsVariables_QUERYARGUMENTS UNIXShellCommandsVariables_BODY	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-09-16
核心规则集	GenericLFI_QUERYARGUMENTS GenericLFI_URIPATH GenericLFI_BODY	将文本转换从 HTML 解码更改为 URL 解码，以改善阻止。	2020-08-07
Linux 操作系统	LFI_URIPATH LFI_QUERYARGUMENTS LFI_BODY	将文本转换从 HTML 实体解码更改为 URL 解码，以改善检测和阻止。	2020-05-19

规则组和规则	描述	日期	
匿名 IP 列表	全部	IP 声誉规则组 中新的规则组可阻止来自以下这些服务的请求：这些服务允许对查看者身份进行模糊处理，以帮助缓解自动程序和规避地理限制的情况。	2020-03-06
WordPress 应用程序	`WordPressExploitableCommands_QUERYSTRING`	用于检查查询字符串中是否存在可利用的命令的新规则。	2020-03-03

核心规则集 (CRS)	`SizeRestrictions_QUERYSTRING`
	
	`SizeRestrictions_Cookie_HEADER`
	
	`SizeRestrictions_BODY`
	
	`SizeRestrictions_URIPATH`
		调整了大小值约束以提高准确性。	2020-03-03

SQL 数据库	`SQLi_URIPATH`	这些规则现在会检查消息 URI。	2020-01-23

规则组和规则	描述	日期	
SQL 数据库	SQLi_BODY SQLi_QUERYARGUMENTS SQLi_COOKIE	更新了文本转换。	2019-12-20
核心规则集 (CRS)	CrossSiteScripting_URIPATH CrossSiteScripting_BODY CrossSiteScripting_QUERYARGUMENTS CrossSiteScripting_COOKIE	更新了文本转换。	2019-12-20

AWS Marketplace 托管规则组

AWS Marketplace 托管规则组可通过 AWS Marketplace 控制台订阅获得，网址为AWS Marketplace。订阅 AWS Marketplace 托管规则组后，可以在中使用它 AWS WAF。要在 AWS Firewall Manager AWS WAF 策略中使用 AWS Marketplace 规则组，组织中的每个账户都必须订阅该规则组。

在将 AWS WAF 保护措施用于生产流量之前，请先对其进行测试和调整。有关信息，请参阅 测试和调整您的 AWS WAF 保护措施。

AWS Marketplace 规则组定价

AWS Marketplace 规则组没有长期合同，也没有最低承诺。当您订阅规则组时，将按月收取费用（按小时比例）和根据数量收取持续请求费用。有关更多信息，请参阅AWS WAF 定价和每个 AWS Marketplace 规则组的描述，网址为AWS Marketplace。

对 AWS Marketplace 规则组有疑问吗？

如果对 AWS Marketplace 卖家管理的规则组有疑问或请求更改功能，请联系提供商的客户支持团队。要查找联系信息，请访问 AWS Marketplace，参阅提供程序的列表。

AWS Marketplace 规则组提供者决定如何管理规则组，例如如何更新规则组以及规则组是否已版本控制。提供程序还会确定规则组的详细信息，包括规则、规则操作以及规则添加到匹配的 Web 请求中的任何标签。

订阅 AWS Marketplace 托管规则组

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

> **Important**
>
> 要在 AWS Firewall Manager 策略中使用 AWS Marketplace 规则组，组织中的每个账户都必须先订阅该规则组。

订阅 AWS Marketplace 托管规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，请选择 AWS 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或编辑 Web ACL。

   > **Note**
   >
   > 将规则组添加到 Web ACL 时，可以覆盖规则组中规则的操作和规则组结果的操作。有关更多信息，请参阅 规则组的操作覆盖选项。

订阅规则组后，您可以像在其他托管 AWS Marketplace 规则组中一样在 Web ACL 中使用该规则组。有关信息，请参阅 创建 Web ACL。

取消订阅 AWS Marketplace 托管规则组

您可以在 AWS WAF 控制台上取消订阅 AWS Marketplace 规则组。

> **Important**
>
> 要停止对 AWS Marketplace 托管规则组收取订阅费用，除了取消订阅该托管规则组外，还必须将其从所有 Firewall Manager AWS WAF 策略中 AWS WAF 和策略中的所有 Web ACL 中删除。如果您取消订阅 AWS Marketplace 托管规则组，但未将其从 Web ACL 中删除，则将继续向您收取订阅费用。

取消订阅 AWS Marketplace 托管规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 从所有 Web ACL 中删除规则组。有关更多信息，请参阅 编辑 Web ACL。
3. 在导航窗格中，请选择 AWS Marketplace。
4. 选择 管理您的订阅。
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。

对 AWS Marketplace 规则组进行故障排除

如果您发现某个 AWS Marketplace 规则组阻止了合法流量，则可以通过执行以下步骤来解决问题。

AWS Marketplace 规则组故障排除

1. 覆盖操作，以计入阻止合法流量的规则。您可以使用 AWS WAF 抽样请求或 AWS WAF 日志来确定哪些规则阻止了特定的请求。您可以通过查看日志中的 `ruleGroupId` 字段或采样请求中的 `RuleWithinRuleGroup` 来标识规则。您可以采用模式 `<Seller Name>#<RuleGroup Name>#<Rule Name>` 标识规则。
2. 如果将特定规则设置为仅计算请求数并不能解决问题，则可以覆盖所有规则操作，或者将 AWS Marketplace 规则组本身的操作从 “不覆盖” 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。

3. 覆盖单个规则操作或整个 AWS Marketplace 规则组操作后，请联系规则组提供商的客户支持团队以进一步解决问题。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 AWS 支持人员

有关问题 AWS WAF 或由其管理的规则组 AWS，请联系 AWS Support。如果 AWS Marketplace 卖家管理的规则组存在问题，请联系提供商的客户支持团队。要查找联系信息，请参阅提供商的列表 AWS Marketplace。

管理您自己的规则组

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

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

主题

- 创建规则组
- 编辑规则组
- 在 Web ACL 中使用规则组
- 与其他账号共享规则组
- 删除规则组

创建规则组

要创建新的规则组，请按照本页上的步骤进行操作。

创建规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 规则组，然后选择 创建规则组。
3. 为规则输入名称和描述。您将使用名称和描述来标识该规则集以便管理和使用它。

   不要使用以 `AWS`、`Shield`、`PreFM` 或 `PostFM` 开头的名称。这些字符串要么是保留字符串，要么可能与其他服务所管理的规则组混淆。请参阅 其他服务提供的规则组。

> **Note**
>
> 规则组在创建之后无法更改名称。

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

   向规则组添加规则时，添加规则和设置容量 窗格会显示所需的最小容量，该容量基于已添加的规则。您可以根据此容量和规则组的未来计划来帮助估算规则组将需要的容量。
8. 检查规则组的设置，然后选择创建。

编辑规则组

要在规则组中添加或删除规则或更改配置设置，请使用本页面上的步骤访问规则组。

> **生产流量风险**
>
> 如果您更改当前在 Web ACL 中使用的规则组，则无论在何处使用 Web ACL，这些更改都将影响您的 Web ACL 行为。请务必在暂存或测试环境中对所有更改进行测试和调整，直到您可以接受可能对流量产生的影响。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

编辑规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 规则组。
3. 选择要编辑的规则组的名称。控制台会将您引入规则组的页面。
4. 根据需要编辑规则组。您可以编辑规则组的可变属性，与创建时的操作类似。控制台会随时保存您的更改。

> **Note**
>
> 如果您更改了规则的名称，并且希望该规则的指标名称反映更改，则还必须更新该指标名称。 AWS WAF 当您更改规则名称时，不会自动更新规则的指标名称。在控制台中编辑规则时，您可以使用规则 JSON 编辑器更改指标名称。您也可以通过 API 以及在用于定义 Web ACL 或规则组的任何 JSON 列表中更改这两个名称。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

在 Web ACL 中使用规则组

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

> **⚠ 生产流量风险**
>
> 在 Web ACL 中为生产流量部署更改之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对更新后的规则进行测试和调整。有关操作指南，请参阅 测试和调整您的 AWS WAF 保护措施。

> **Note**
>
> 在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

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

在 Web ACL 中，您可以通过将单个规则操作设置为 Count 或通过任何其他操作来更改规则组及其规则的行为。这可以帮助您执行测试规则组、识别规则组中规则的误报，以及自定义托管规则组处理请求的方式等操作。有关更多信息，请参阅 规则组的操作覆盖选项。

如果您的规则组包含基于速率的语句，则您使用该规则组的每个 Web ACL 都会对基于速率的规则分别进行费率跟踪和管理，与您使用规则组的任何其他 Web ACL 无关。有关更多信息，请参阅 基于速率的规则语句。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

与其他账号共享规则组

您可以与其他 AWS 账户共享您拥有的规则组，供该账户使用。您只能通过 AWS WAF API 执行此操作。有关更多信息，请参阅 AWS WAF API 参考PutPermissionPolicy中的。

删除规则组

按照本部分中的指导删除规则组。

删除引用的集合和规则组

删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时， AWS WAF 会检查该实体当前是否正在 Web ACL 中使用。如果它发现它正在使用中，则 AWS WAF 会警告你。 AWS WAF 几乎总是能够确定 Web ACL 是否引用了某个实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在您的 Web ACL 中进行检查。如果实体是引用的集合，请确保没有规则组正在使用它。

删除规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 规则组。
3. 选择要删除的规则组，然后选择删除。

其他服务提供的规则组

如果您或您组织中的管理员使用 AWS Firewall Manager 或使用 AWS Shield Advanced 来管理资源保护 AWS WAF，则可能会看到规则组参考语句已添加到您账户的 Web ACL 中。

这些规则组的名称以以下字符串开头：

- **`ShieldMitigationRuleGroup`**— 这些规则组由受保护的应用程序层（第 7 层）资源管理， AWS Shield Advanced 并用于为受保护的应用程序层（第 7 层）资源提供自动的 DDoS 缓解。

  当您为受保护的资源启用自动应用程序层 DDoS 缓解时，Shield Advanced 会将其中一个规则组添加到您与该资源关联的 Web ACL 中。Shield Advanced 为规则组参考语句分配了 10,000,000 的优先级设置，这样它就可以在您在 Web ACL 中配置的规则之后运行。有关这些规则组的更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

  > **Warning**
  >
  > 不要尝试在 Web ACL 中手动管理此规则组。特别是，不要手动从 Web ACL 中删除 `ShieldMitigationRuleGroup` 规则组参考语句。这样可能会对与 Web ACL 关联的所有资源造成意外后果。应使用 Shield Advanced 来禁用与 Web ACL 关联的资源的自动缓解功能。当不需要自动缓解时，Shield Advanced 会为您移除规则组。

- **PREFMManaged**和 **POSTFMManaged** — 这些规则组由管理 AWS Firewall Manager。Firewall Manager 为它们提供了 Firewall Manager 创建和管理的 Web ACL。Web ACL 的名称以 FMManagedWebACLV2 开头。有关这些 Web ACL 和规则组的信息，请参阅 AWS WAF 政策。

AWS WAF 规则

AWS WAF 规则定义了如何检查 HTTP (S) Web 请求以及当请求符合检查标准时要采取的操作。规则只能在规则组或 Web ACL 的上下文中进行定义。

规则本身并不存在。 AWS WAF 它们不是 AWS 资源，也没有 Amazon 资源名称 (ARN)。您可以在规则组或定义规则的 Web ACL 中按名称访问规则。您可以使用包含规则的规则组或 Web ACL 的 JSON 视图来管理规则并将其复制到其他 Web ACL。您也可以通过 AWS WAF 控制台规则生成器对其进行管理，该生成器可用于 Web ACL 和规则组。

Rule name（规则名称）

每条规则都需要一个名称。避免使用以 AWS 开头的名称和用于其他服务为您管理的规则组或规则的名称。请参阅 其他服务提供的规则组。

> **Note**
>
> 如果您更改了规则的名称，并且希望该规则的指标名称反映更改，则还必须更新该指标名称。AWS WAF 当您更改规则名称时，不会自动更新规则的指标名称。在控制台中编辑规则时，您可以使用规则 JSON 编辑器更改指标名称。您也可以通过 API 以及在用于定义 Web ACL 或规则组的任何 JSON 列表中更改这两个名称。

规则语句

每条规则还需要一个规则语句，用于定义规则如何检查 Web 请求。规则语句可能包含任何深度的其他嵌套语句，具体取决于规则和语句类型。一些规则语句采用一组条件。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。

您可以定义用于检查条件的规则，如下所示：

- 可能是恶意的脚本。攻击者会嵌入可以利用 Web 应用程序漏洞的脚本。这称为跨站脚本攻击（XSS）。
- 请求源自的 IP 地址或地址范围。

- 请求源自的国家/地区或地理位置。
- 请求的指定部分的长度（如查询字符串）。
- 可能是恶意的 SQL 代码。攻击者会尝试通过在 Web 请求中嵌入恶意 SQL 代码从数据库提取数据。这称为 SQL 注入。
- 请求中出现的字符串，例如，在 `User-Agent` 标头中出现的值或是在查询字符串中出现的文本字符串。您还可以使用正则表达式 (regex) 指定这些字符串。
- Web ACL 中先前的规则添加了到请求中的标签。

除了具有 Web 请求检查标准的语句（如前面的列表中的语句）之外，还 AWS WAF 支持AND0R、和的逻辑语句N0T，用于合并规则中的语句。

例如，根据您最近发现的攻击者请求，您可以创建一条规则，其逻辑 AND 语句由以下嵌套语句组合而成：

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

在这种情况下，Web 请求需要匹配所有语句才能匹配顶级 AND。

主题

规则操作

当网络请求符合规则中定义的条件时，规则操作会告诉 AWS WAF 您如何处理该请求。您可以选择为每个规则操作添加自定义行为。

> **Note**
>
> 规则操作可以是终止，也可以是非终止。终止操作会停止对请求的 Web ACL 评估，要么允许请求继续访问受保护的应用程序，要么将其阻止。

以下是规则操作选项：

- Allow— AWS WAF 允许将请求转发到受保护的 AWS 资源进行处理和响应。这是终止操作。在您定义的规则中，您可以在请求中插入自定义标头，然后再将其转发到受保护的资源。
- Block— AWS WAF 阻止请求。这是终止操作。默认情况下，您的受保护 AWS 资源以 HTTP `403 (Forbidden)` 状态代码进行响应。在您定义的规则中，您可以自定义响应。当 AWS WAF 阻止请求时，Block操作设置将决定受保护的资源发送回客户端的响应。
- Count— 对请求进行 AWS WAF 计数，但不确定是允许还是阻止请求。这是一个非终止操作。 AWS WAF 继续处理 Web ACL 中的其余规则。在您定义的规则中，您可以将自定义标头插入请求中，也可以添加其他规则可以匹配的标签。
- CAPTCHA并且 Challenge — AWS WAF 使用 CAPTCHA 谜题和静默挑战来验证请求不是来自机器人，并 AWS WAF 使用代币来跟踪最近成功的客户响应。

  只有当浏览器访问 HTTPS 端点时，才能运行验证码谜题和静默挑战。浏览器客户端必须在安全的环境中运行才能获取令牌。

  > **Note**
  >
  > 当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中将其作为规则操作覆盖时，您需要支付额外费用。有关更多信息，请参阅AWS WAF 定价。

  这些规则操作可以是终止操作，也可以是非终止操作，具体取决于请求中令牌的状态：

  - 未过期的有效令牌不终止 — 如果根据配置的验证码或质疑免疫时间，令牌有效且未过期，则 AWS WAF 处理与操作类似的请求。Count AWS WAF 继续根据 Web ACL 中的其余规则检查 Web 请求。与 Count 配置类似，在您定义的规则中，您可以选择使用自定义标头配置这些操作以插入到请求中，也可以添加其他规则可以匹配的标签。
  - 以对无效或过期令牌的请求被阻止而终止 — 如果令牌无效或指定的时间戳已过期，则 AWS WAF 终止对 Web 请求的检查并阻止请求，类似于操作。Block AWS WAF 然后使用自定义响应代码响应客户端。因为CAPTCHA，如果请求内容表明客户端浏览器可以处理它，则会在 JavaScript 插页式广告中 AWS WAF 发送一个验证码拼图，该拼图旨在区分人类客户端和机器人。对于Challenge

操作， AWS WAF 会发送带有静默挑战的 JavaScript 插页式广告，该挑战旨在将普通浏览器与机器人运行的会话区分开来。

有关更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

有关自定义请求和响应的信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

有关为匹配请求添加标签的信息，请参阅 AWS WAF 网络请求上的标签。

有关 Web ACL 和规则设置如何交互的信息，请参阅 Web ACL 规则和规则组评估。

规则语句基础知识

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

中的每条规则都 AWS WAF 有一个顶级规则语句，该语句可以包含其他语句。规则语句可能非常简单。例如，您可以在 Web ACL 中设置一个规则语句，提供一组来源国来检查 Web 请求，也可以在 Web ACL 中设置一个规则语句，只引用一个规则组。规则语句也可能非常复杂。例如，您可以编写一个使用逻辑 AND、OR 和 NOT 语句组合多个其他语句的语句。

对于大多数规则，您可以为匹配的请求添加自定义 AWS WAF 标签。 AWS 托管规则组中的规则为匹配的请求添加标签。规则添加的标签提供有关规则请求的信息，这些规则稍后会在 Web ACL 以及 AWS WAF 日志和指标中进行评估。有关标签的信息，请参见AWS WAF 网络请求上的标签和标签匹配规则语句。

嵌套规则语句

AWS WAF 支持嵌套许多规则语句，但不支持所有规则语句嵌套。例如，您不能将规则组语句嵌套到其他语句中。某些场景需要使用嵌套，例如范围缩小语句和逻辑语句。下面的规则语句列表和规则详细信息描述了每个类别和规则的嵌套功能和要求。

控制台中规则的可视化编辑器仅支持规则语句的嵌套级别。例如，可以在具有逻辑性的 AND 或 OR 规则中嵌套多种类型的语句，但不能嵌套其他 AND 或 OR 规则，因为这需要第二层嵌套。要实现多级嵌套，请通过控制台中的 JSON 规则编辑器或 API 以 JSON 格式提供规则定义。

主题

- Web 请求组件规格和处理
- 范围缩小语句

- 引用集合或规则组的语句

Web 请求组件规格和处理

本节介绍可以在检查 Web 请求组成部分的规则语句中指定的设置。有关用法的信息，请参阅 匹配规则语句 中的各个规则语句。

这些 Web 请求组件的子集也可以在基于速率的规则中用作自定义请求聚合键。有关信息，请参阅 基于速率的规则聚合选项和密钥。

对于请求组件设置，您可以指定组件类型本身以及任何其他选项，具体取决于组件类型。例如，当您检查包含文本的组件类型时，可以在对其进行检查之前对其应用文本转换。

> **Note**
>
> 除非另有说明，否则，如果 Web 请求没有规则语句中指定的请求组件，则 AWS WAF 会将该请求评估为与规则条件不匹配。

目录

- 文本转换选项

请求组件选项

本部分将介绍您可以指定检查 Web 请求的哪些组件。您可以为在 Web 请求中查找模式的匹配规则语句指定请求组件。其中包括字符串匹配、正则表达式模式匹配、SQL 注入攻击和大小约束语句。有关如何使用这些请求组件设置的信息，请访问 匹配规则语句，参阅各个规则语句。

除非另有说明，否则，如果 Web 请求没有规则语句中指定的请求组件，则 AWS WAF 会将该请求评估为与规则条件不匹配。

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

AWS WAF 控制台和 API 文档为以下位置的请求组件设置提供了指导：

- 控制台上的规则生成器 – 在常规规则类型的语句设置中，在请求组件下的检查对话框中选择要检查的组件。
- API 语句内容 – `FieldToMatch`

本节的其余部分将介绍 Web 请求检查部分的选项。

主题

- HTTP method
- 单个标头
- 所有标头
- 标头顺序
- Cookie
- URI 路径
- JA3 指纹
- 查询字符串
- Single query parameter (单个查询参数)

- All query parameters (所有查询参数)
- Body
- JSON 正文

HTTP method

检查请求中的 HTTP 方法。HTTP 方法指示 Web 请求要求受保护的资源执行的操作的类型，如 POST 或 GET。

单个标头

检查请求中的单个命名标头。

对于此选项，您可以指定标头名称，例如 User-Agent 或 Referer。名称的字符串不区分大小写。

所有标头

检查所有请求标头，包括 Cookie。您可以应用筛选器来检查所有标头的子集。

对于此选项，您需要提供以下规范：

- 匹配模式-用于获取标题子集以供检查的过滤器。 AWS WAF 在标题键中查找这些模式。

  匹配模式设置可采用以下的一种设置：
  - 全部 – 匹配所有键。评估所有标头的规则检查条件。
  - 排除标头 – 仅检查其键与此处指定的任何字符串都不匹配的标头。键的字符串匹配不区分大小写。
  - 包含标头 – 仅检查键与此处指定的字符串之一匹配的标头。键的字符串匹配不区分大小写。
- 匹配范围-标题中 AWS WAF 应根据规则检查标准进行检查的部分。您可以指定键、值或全部来检查键和值是否匹配。

  全部不需要在键中找到匹配项，也无需在值中找到匹配项。它需要在键或值中找到匹配项，或者两者兼有。如需要求在键和值中进行匹配，请使用逻辑 AND 语句组合两个匹配规则，一个检查键，另一个检查值。
- 超大处理 — AWS WAF 应如何处理标头数据大于 AWS WAF 可以检查的请求。 AWS WAF 最多可以检查请求标头的前 8 KB（8,192 字节），最多可以检查前 200 个标头。在达到第一个限制之前 AWS WAF ，内容可供检查。您可以选择继续检查，也可以跳过检查并将请求标记为匹配或不匹配规则。有关处理超大处理内容的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

标头顺序

检查包含请求标头名称列表的字符串，这些标头名称按 AWS WAF 收到以供检查的 Web 请求中显示的顺序排列。 AWS WAF 生成字符串，然后将其用作字段来匹配检查中的组件。 AWS WAF 例如，用冒号分隔字符串中的标题名称，不添加空格。`host:user-agent:accept:authorization:referer`

对于此选项，您需要提供以下规范：

- 超大处理 — AWS WAF 应如何处理标头数据数量大于或大于 AWS WAF 可以检查的请求。 AWS WAF 最多可以检查请求标头的前 8 KB（8,192 字节），最多可以检查前 200 个标头。在达到第一个限制之前 AWS WAF ，内容可供检查。您可以选择继续检查可用标头，也可以跳过检查并将请求标记为匹配或不匹配规则。有关处理超大处理内容的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

Cookie

检查所有请求 Cookie。您可以应用筛选器来检查所有 Cookie 的子集。

对于此选项，您需要提供以下规范：

- 匹配模式 – 用于获取 Cookie 子集以供检查的筛选器。 AWS WAF 在 Cookie 密钥中查找这些模式。

  匹配模式设置可采用以下的一种设置：

  - 全部 – 匹配所有键。评估所有 Cookie 的规则检查条件。
  - 排除 Cookie – 仅检查其键与此处指定的任何字符串都不匹配的 Cookie。键的字符串匹配不区分大小写且必须精确。
  - 包含 Cookie – 仅检查键与此处指定的字符串之一匹配的 Cookie。键的字符串匹配不区分大小写且必须精确。
- 匹配范围 — Cookie 中 AWS WAF 应根据规则检查标准进行检查的部分。您可以为键和值指定键、值或全部。

  全部不需要在键中找到匹配项，也无需在值中找到匹配项。它需要在键或值中找到匹配项，或者两者兼有。如需要求在键和值中进行匹配，请使用逻辑 AND 语句组合两个匹配规则，一个检查键，另一个检查值。
- 超大处理 — AWS WAF 应如何处理包含大于 cookie 数据 AWS WAF 可检查范围的请求。 AWS WAF 最多可以检查请求的 cookie 的前 8 KB（8,192 字节），最多可以检查前 200 个 cookie。在达到第一个限制之前 AWS WAF ，内容可供检查。您可以选择继续检查，也可以跳过检查并将请求标

记为匹配或不匹配规则。有关处理超大处理内容的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

URI 路径

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

如果您不使用带有此选项的文本转换，则 AWS WAF 不会对 URI 进行标准化处理，并完全按照请求中从客户端收到的内容进行检查。有关文本转换的信息，请参阅 文本转换选项。

JA3 指纹

检查请求的 JA3 指纹。

> **Note**
>
> JA3 指纹检查仅适用于 Amazon CloudFront 发行版和应用程序负载均衡器。

JA3 指纹是一个 32 字符的哈希值，源自传入请求的 TLS Client Hello。此指纹用作客户端 TLS 配置的唯一标识符。 AWS WAF 计算并记录每个具有足够的 TLS Client Hello 信息用于计算的请求的此指纹。几乎所有的 Web 请求都包含此信息。

如何获取客户端的 JA3 指纹

您可以从 Web ACL 日志中获取客户端请求的 JA3 指纹。 AWS WAF 如果能够计算出指纹，它就会将其包含在日志中。有关日志记录字段的信息，请参阅 日志字段。

规则语句要求

您只能在字符串匹配语句中检查 JA3 指纹，该语句设置为与您提供的字符串完全匹配。在字符串匹配语句规范中提供日志中的 JA3 指纹字符串，以便与今后任何具有相同 TLS 配置的请求相匹配。有关字符串匹配语句的信息，请参阅 字符串匹配规则语句。

您必须为此规则语句提供回退行为。如果无法计算 JA3 指纹，则回退行为 AWS WAF 是您 AWS WAF 要分配给 Web 请求的匹配状态。如果您选择匹配， AWS WAF 会将 Web 请求视为与规则语句匹配，并将规则操作应用于请求。如果您选择不匹配，则 AWS WAF 会将请求视为与规则语句不匹配。

如需使用此匹配选项，必须记录您的 Web ACL 流量。有关信息，请参阅 记录 AWS WAF Web ACL 流量。

查询字符串

检查 URL 中在？字符之后出现的部分（如果有）。

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

Single query parameter (单个查询参数)

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

对于此选项，您还可以指定一个查询参数。例如，如果 URL 为 `www.xyz.com?UserName=abc&SalesRegion=seattle`，则可以为该查询参数指定 `UserName` 或 `SalesRegion`。参数名称的长度上限是 30 个字符。名称不区分大小写，因此如果您指定 `UserName` 作为名称， AWS WAF 匹配 `UserName` 的所有变体，包括 `username` 和 `UsERName`。

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

All query parameters (所有查询参数)

检查请求中的所有查询参数。这与单一查询参数组件选择类似，但 AWS WAF 会检查查询字符串中所有参数的值。例如，如果 URL 为 `www.xyz.com?UserName=abc&SalesRegion=seattle`，并且如果 `UserName` 或 `SalesRegion` 的值与检查条件匹配， AWS WAF 则会触发匹配。

选择此选项会在基本成本的基础上增加 10 个 WCU。

Body

以纯文本形式检查请求正文。您也可以使用 JSON 内容类型将正文评估为 JSON。

请求正文紧跟在请求标头之后的请求部分。它包含 Web 请求所需的任何其他数据，例如，表单中的数据。

- 在控制台中，您可以在请求选项选择正文下选择此选项，方法是选择内容类型选择纯文本。
- 在 API 中，您可以在规则的 `FieldToMatch` 规范中指定 `Body` 以纯文本形式检查请求正文。

对于 Applicati AWS AppSync on Load Balancer 和， AWS WAF 可以检查请求正文的前 8 KB。对于 CloudFront，默认情况下，API Gateway、Amazon Cognito、App Runner 和 Verified Access AWS WAF 可以检查前 16 KB，您可以在 Web ACL 配置中将限制提高到 64 KB。有关更多信息，请参阅 管理车身检查的大小限制。

您必须为此组件类型指定超大尺寸处理。超大处理定义了如何 AWS WAF 处理主体数据大于 AWS WAF 可以检查的请求。您可以选择继续检查，也可以跳过检查并将请求标记为匹配或不匹配规则。有关处理超大处理内容的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

您也可以将正文评估为已解析的 JSON。有关信息，请参阅下面的部分。

JSON 正文

检查以 JSON 形式评估的请求正文。您还可以以纯文本形式评估正文。

请求正文紧跟在请求标头之后的请求部分。它包含 Web 请求所需的任何其他数据，例如，表单中的数据。

- 在控制台中，您可以在请求选项选择正文下选择此选项，方法是选择内容类型选择JSON。
- 在 API 中，您可以在规则的 `FieldToMatch` 规范中指定 `JsonBody`。

对于 Applicati AWS AppSync on Load Balancer 和， AWS WAF 可以检查请求正文的前 8 KB。对于 CloudFront，默认情况下，API Gateway、Amazon Cognito、App Runner 和 Verified Access AWS WAF 可以检查前 16 KB，您可以在 Web ACL 配置中将限制提高到 64 KB。有关更多信息，请参阅 管理车身检查的大小限制。

您必须为此组件类型指定超大尺寸处理。超大处理定义了如何 AWS WAF 处理主体数据大于 AWS WAF 可以检查的请求。您可以选择继续检查，也可以跳过检查并将请求标记为匹配或不匹配规则。有关处理超大处理内容的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

当将 Web 请求正文作为已解析的 JSON 进行 AWS WAF 检查时，它会解析并从 JSON 中提取元素，并使用规则的匹配语句标准检查您指定的部分。

选择此选项会使匹配语句的基本成本 WCU 翻倍。例如，如果在没有 JSON 解析的情况下，匹配语句的基本成本为 5 个 WCU，则使用 JSON 解析会将成本加倍到 10 个 WCU。

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

1. AWS WAF 解析和提取 JSON 内容并识别要检查的元素。为此，请 AWS WAF 使用您在规则的 JSON 正文规范中提供的标准。

2. AWS WAF 对提取的元素应用任何文本转换，然后将生成的 JSON 元素集与规则语句的匹配条件进行匹配。如果有任何元素匹配，则 Web 请求与该规则匹配。

您可以为 AWS WAF 第一个模式匹配步骤指定以下标准，以识别要检查的 JSON 元素：

- 正文解析后备行为 – 如果它无法完全解析 JSON 正文， AWS WAF 应该怎么做。这些选项如下所示：
  - 无（默认行为）-仅在内容遇到解析错误之前对其进行 AWS WAF 评估。
  - 评估为字符串-以纯文本形式检查正文。 AWS WAF 将您为 JSON 检查定义的文本转换和检查标准应用于正文文本字符串。
  - 匹配-将 Web 请求视为与规则语句相匹配。 AWS WAF 将规则操作应用于请求。
  - 不匹配 – 将 Web 请求视为与规则语句不匹配。

  AWS WAF 尽最大努力解析整个 JSON 正文，但由于字符无效、密钥重复、截断以及根节点不是对象或数组的任何内容等原因，可能会被迫停止解析。

  AWS WAF 将以下示例中的 JSON 解析为两个有效的键:值对：
  - 缺少逗号：`{"key1":"value1""key2":"value2"}`
  - 缺少冒号：`{"key1":"value1","key2""value2"}`
  - 额外的冒号：`{"key1"::"value1","key2""value2"}`
- JSON 匹配范围 — JSON 中 AWS WAF 应检查的元素类型。您可以为键和值指定键、值或全部。

  全部不需要在键中找到匹配项，也无需在值中找到匹配项。它需要在键或值中找到匹配项，或者两者兼有。如需要求在键和值中进行匹配，请使用逻辑 AND 语句组合两个匹配规则，一个检查键，另一个检查值。
- 要检查的内容-已解析和提取的 JSON 中 AWS WAF 要检查的元素。

  您必须指定以下各项之一：
  - 完整的 JSON 内容 – 评估已解析的 JSON 中的所有元素。
  - 仅包含的元素 – 仅评估 JSON 中与您提供的 JSON 指针条件相匹配的元素。有关 JSON 指针语法的信息，请参阅互联网工程任务组 (IETF) 文档JavaScript 对象表示法 (JSON) 指针。

    不要使用此选项来包含 JSON 中的 所有路径。改用完整 JSON 内容。

    例如，您可以在控制台中提供以下信息：

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

在 API 或 CLI 中，您可以提供以下内容：

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

JSON 正文检查场景示例

如果包含的元素设置为 `/a/b`，则对于以下 JSON 正文：

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

以下列表描述 AWS WAF 了每个匹配范围设置的计算结果。键 b 作为所包含的元素路径的一部分，不会进行评估。

- 对于设置为“全部”的匹配范围：e、f，和 g。
- 对于设置为“键”的匹配范围：e 和 f。
- 对于设置为“值”的匹配范围：g。

转发的 IP 地址

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

使用 IP 地址的规则语句

使用 IP 地址的规则语句如下：

- IP 集匹配 – 检查 IP 地址是否与 IP 集中定义的地址相匹配。
- 地理匹配 – 使用 IP 地址确定来源国和地区，并将来源国与国家列表进行匹配。
- 基于速率的规则语句 – 可以按其 IP 地址聚合请求，以确保没有单个 IP 地址以过高速率发送请求。您可以单独使用 IP 地址聚合，也可以与其他聚合键结合使用。

您可以指示使用来自`X-Forwarded-For`标头或 AWS WAF 其他 HTTP 标头的转发 IP 地址来处理这些规则语句中的任何一个，而不是使用 Web 请求的来源。有关如何提供规范的详细信息，请参阅各个规则语句类型的指南。

> **Note**
>
> 如果您指定的标头不存在于请求中，则 AWS WAF 根本不会将该规则应用于 Web 请求。

回退行为

使用转发的 IP 地址时，如果请求的指定位置没有有效的 IP 地址，则需要指明 AWS WAF 要分配给 Web 请求的匹配状态：

- MATCH-将 Web 请求视为与规则语句相匹配。 AWS WAF 将规则操作应用于请求。
- 不匹配 – 将 Web 请求视为与规则语句不匹配。

AWS WAF 机器人控制中使用的 IP 地址

Bot Control 托管规则组使用来自 AWS WAF的 IP 地址验证机器人。如果您使用机器人控制功能，并且已经验证了通过代理或负载均衡器进行路由的机器人，则需要使用自定义规则明确允许它们。例如，您可以配置自定义 IP 集匹配规则，该规则使用转发 IP 地址来检测和允许已验证机器人。您可以使用该规则通过多种方式自定义机器人管理。有关信息以及示例，请参阅 AWS WAF 机器人控制。

使用转发 IP 地址的一般注意事项

在使用转发 IP 地址之前，请注意以下一般注意事项：

- 在此过程中，代理可以修改标头，并代理可能会以不同的方式处理标头。
- 攻击者可能会更改标头的内容以试图绕过 AWS WAF 检查。
- 标头内的 IP 地址可能格式错误或无效。

- 请求中可能根本不存在您指定的标头。

使用转发的 IP 地址的注意事项 AWS WAF

以下列表描述了在中使用转发的 IP 地址的要求和注意事项： AWS WAF

- 对于任何一条规则，您可以为转发 IP 地址指定一个标头。标头规范不区分大小写。
- 对于基于速率的规则语句，任何嵌套的范围界定语句都不会继承转发的 IP 配置。为每条使用转发 IP 地址的语句指定配置。
- 对于地理匹配和基于费率的规则， AWS WAF 使用标题中的第一个地址。例如，如果标题包含 us `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF es `10.1.1.1`
- 对于 IP 集匹配，您可以指明是与标头中的第一个地址、最后一个地址还是任何地址进行匹配。如果指定，则 AWS WAF 检查标头中的所有地址是否匹配，最多 10 个地址。如果标头包含的地址超过 10 个，则 AWS WAF 检查最后 10 个地址。
- 包含多个地址的标头必须在地址之间使用逗号分隔符。如果请求使用逗号以外的分隔符，则 AWS WAF 会认为标头中的 IP 地址格式不正确。
- 如果标头内的 IP 地址格式错误或无效，则 AWS WAF 根据您在转发的 IP 配置中指定的回退行为，将 Web 请求指定为与规则匹配或不匹配。
- 如果您指定的标头不存在于请求中，则 AWS WAF 根本不会将该规则应用于请求。这意味着这 AWS WAF 不应用规则操作，也不应用回退行为。
- 使用转发 IP 标头作为 IP 地址的规则语句不会使用 Web 请求来源报告的 IP 地址。

使用转发的 IP 地址的最佳实践 AWS WAF

使用转发 IP 地址时，请使用以下最佳实践：

- 在启用转发 IP 配置之前，请仔细考虑请求标头的所有可能状态。您可能需要使用多个规则来获得您想要的行为。
- 要检查多个转发 IP 标头或检查 Web 请求来源和转发 IP 标头，请对每个 IP 地址源使用一条规则。
- 要阻止标头无效的 Web 请求，请将规则操作设置为阻止，并将转发 IP 配置的回退行为设置为匹配。

转发 IP 地址的 JSON 示例

只有当 `X-Forwarded-For` 标头包含来源国为 US 的 IP 时，以下地理匹配语句才会匹配：

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

以下基于速率的规则根据 X-Forwarded-For 标头中的第一个 IP 来聚合请求。该规则仅计算与嵌套地理匹配语句匹配的请求，并且仅阻止与地理匹配语句匹配的请求。嵌套的地理匹配语句还使用 X-Forwarded-For 标头来确定 IP 地址是否表示 US 来源国。如果是，或者标头存在但格式不正确，则地理匹配语句将返回匹配项。

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
```

```
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

用于检查 HTTP/2 伪标头的选项

支持 HTTP/2 流量的受保护 AWS 资源不会将 HTTP/2 伪标头转发到以 AWS WAF 供检查，但它们在用于检查的 Web 请求组件中提供伪标头的内容。 AWS WAF

您可以使用 AWS WAF 仅检查下表中列出的伪标头。

映射到 Web 请求组件的 HTTP/2 伪标头内容

HTTP/2 伪标头	要检查的 Web 请求组件	文档
`:method`	HTTP method	HTTP method
`:authority`	`Host` 标头	单个标头 所有标头
`:path` URI 路径	URI 路径	URI 路径

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

文本转换选项

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

当您将其与 JSON 正文请求组件选择一起使用时， AWS WAF 会在解析并从 JSON 中提取要检查的元素之后应用您的转换。有关更多信息，请参阅 JSON 正文。

如果提供多个转换，还应当设置 AWS WAF 应用这些转换的顺序。

WCU – 每个文本转换为 10 WCU。

AWS WAF 控制台和 API 文档还在以下位置为这些设置提供了指导：

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

文本转换的选项

每个转换清单都显示了控制台和 API 规范，后面是描述。

Base64 decode – `BASE64_DECODE`

AWS WAF 解码一个 Base64 编码的字符串。

Base64 decode extension – `BASE64_DECODE_EXT`

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

Command line – CMD_LINE

此选项可以缓解攻击者可能注入操作系统命令行命令并使用不寻常的格式来掩盖部分或全部命令的情况。

使用此选项可执行以下转换：

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

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF 通过将多个空格替换为一个空格并将以下字符替换为空格字符 (ASCII 32) 来压缩空白：

- Formfeed (ASCII 12)
- Tab (ASCII 9)
- 换行符 (ASCII 10)
- 回车 (ASCII 13)
- 垂直制表符 (ASCII 11)
- 不间断空格 (ASCII 160)

CSS decode – CSS_DECODE

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

Escape sequences decode – ESCAPE_SEQ_DECODE

AWS WAF 解码以下 ANSI C 转义序列：\a、、\b、\f、、\n、\r、\t、\v、\\\?、（十六进制）\'\"、\xHH（八进制）。\0000无效的编码保留在输出中。

Hex decode – HEX_DECODE

AWS WAF 将一串十六进制字符解码为二进制。

HTML entity decode – HTML_ENTITY_DECODE

AWS WAF 用相应的字符替换以十六进制格式&#xhhhh;或十进制格式表示&#nnnn;的字符。

AWS WAF 将以下 HTML 编码的字符替换为未编码的字符。此列表使用小写的 HTML 编码，但处理方式不区分大小写，"因此处理方式相同。&QuOt;

HTML 编码字符	替换为.....
"	"
&	&
<	<
>	>
或	不间断空格，十进制 160
\n，十进制 10
	\t，十进制 9
{ 或 {	{
|、| 或		|
} 或 }	}
!	!
#	#
$	$
&percent; 或 %	%
'	\
(	(
)	)
* 或 *	*
+	+

HTML 编码字符	替换为……
,	,
.	.
/	/
:	:
;	;
=	=
?	?
˜ 或 ˜	~
−	-
[或 [	[
\	\\
] 或]	]
&hat;	^
_ 或 &underbar;	_
` 或 `	`

JS decode – JS_DECODE

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

Lowercase – LOWERCASE

AWS WAF 将大写字母 (A-Z) 转换为小写字母 (a-z)。

MD5 – MD5

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

None – NONE

AWS WAF 检查收到的 Web 请求，不进行任何文本转换。

Normalize path – NORMALIZE_PATH

AWS WAF 通过删除不在输入开头的多个斜杠、目录自引用和目录反向引用来规范化输入字符串。

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF 将反斜杠字符转换为正斜杠，然后使用转换处理生成的字符串。NORMALIZE_PATH

Remove nulls – REMOVE_NULLS

AWS WAF 从输入中移除所有NULL字节。

Replace comments – REPLACE_COMMENTS

AWS WAF 将每次出现的 C 风格注释 (/*... */) 替换为单个空格。它不会压缩连续出现的多个事件。它会将未终止的注释替换为空格 (ASCII 0x20)。它不会更改独立终止的注释 (*/)。

Replace nulls – REPLACE_NULLS

AWS WAF 用空格NULL字符 (ASCII 0x20) 替换输入中的每个字节。

SQL hex decode – SQL_HEX_DECODE

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

URL decode – URL_DECODE

AWS WAF 解码 URL 编码的值。

URL decode Unicode – URL_DECODE_UNI

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

UTF8 to Unicode – UTF8_TO_UNICODE

AWS WAF 将所有 UTF-8 字符序列转换为 Unicode。这有助于标准化输入，并最大限度地减少非英语语言的误报和假阴性。

范围缩小语句

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

- 托管规则组语句-如果您向托管规则组语句添加范围缩小语句，则 AWS WAF 会将任何与范围向下语句不匹配的请求评估为与规则组不匹配。只有符合范围缩小语句的请求才会根据规则组进行评估。对于定价基于被评估请求的数量的托管规则组，范围缩小语句可以帮助其控制成本。

  有关托管规则组语句的更多信息，请参阅 托管规则组语句。
- 基于速率的规则语句 – 没有范围缩小语句的基于速率的规则语句会限制该规则评估的所有请求。如果您只想控制特定类别的请求的速率，请在基于速率的规则中添加范围缩小语句。例如，要仅跟踪和控制来自特定地理区域的请求速率，可以在地理匹配语句中指定该地理区域，并将其作为范围缩小语句添加到基于速率的规则中。

  有关基于速率的规则语句的更多信息，请参阅 基于速率的规则语句。

您可以在范围缩小语句中使用任何可嵌套规则。有关可用语句，请参阅 匹配规则语句 和 逻辑规则语句。范围缩小语句的 WCU 是您在其中定义的规则语句所需的 WCU。使用范围缩小语句不会产生额外成本。

您可以像在常规规则中使用该语句一样配置范围缩小语句。例如，您可以对正在检查的 Web 请求组件应用文本转换，也可以指定要用作 IP 地址的被转发 IP 地址。这些配置仅适用于范围缩小语句，不由包含的托管规则组或基于速率的规则语句继承。

例如，如果您在范围缩小语句中对查询字符串应用文本转换，则在应用转换后，范围缩小语句会检查查询字符串。如果请求与范围缩小语句条件相匹配，则 AWS WAF 会将 Web 请求以其原始状态传递给包含规则，而不进行范围缩小语句的转换。包含范围缩小语句的规则可能会应用自己的文本转换，但它不会从范围缩小语句中继承任何文本转换。

您不能使用范围缩小语句为包含规则语句指定任何请求检查配置。不能将范围缩小语句用作包含规则语句的 Web 请求预处理器。范围缩小语句的唯一作用是确定哪些请求会传递到包含规则语句以进行检查。

引用集合或规则组的语句

有些规则使用可重复使用的实体，这些实体由您或 AWS Marketplace 卖家在您的 Web ACL 之外进行管理。 AWS更新可重用实体时， AWS WAF 会将更新传播到您的规则。例如，如果您在 Web ACL 中使用 AWS 托管规则组，则在 AWS 更新规则组时，会将更改 AWS 传播到您的 Web ACL，以更新其

行为。如果您在规则中使用 IP 集语句，则在更新该集合时，会将更改 AWS WAF 传播到所有引用该规则的规则，因此使用这些规则的所有 Web ACL 都将 up-to-date 与您的更改一起保存。

以下是可在规则语句中使用的可重用实体。

- IP 集 – 您创建和管理自己的 IP 集。您可以在控制台上从导航窗格访问这些内容。有关管理 IP 集的信息，请参阅 中的 IP 集和正则表达式模式集 AWS WAF。
- 正则表达式匹配集 – 您创建和管理自己的正则表达式匹配集。您可以在控制台上从导航窗格访问这些内容。有关管理正则表达式模式集的信息，请参阅 中的 IP 集和正则表达式模式集 AWS WAF。
- AWS 托管规则规则组- AWS 管理这些规则组。当您将托管规则组添加到 Web ACL 时，您可以在控制台上使用这些规则组。有关这些规则组的更多信息，请参阅 AWS 托管规则规则组列表。
- AWS Marketplace 托管规则组 — AWS Marketplace 卖家管理这些规则组，您可以订阅这些规则组以使用它们。要管理您的订阅，请在控制台的导航窗格中选择 AWS Marketplace。将 AWS Marketplace 托管规则组添加到 Web ACL 时，会列出托管规则组。对于您尚未订阅的规则组，您也可以在该页面 AWS Marketplace 上找到指向的链接。有关 AWS Marketplace 卖家管理的规则组的更多信息，请参阅AWS Marketplace 托管规则组。
- 您自己的规则组 – 当您需要某些无法通过托管规则组提供的行为时，您通常需要管理自己的规则组。您可以在控制台上从导航窗格访问这些内容。有关更多信息，请参阅 管理您自己的规则组。

删除引用的集合或规则组

删除被引用的实体时， AWS WAF 会检查该实体当前是否正在 Web ACL 中使用。如果 AWS WAF 发现它正在使用中，它会警告你。 AWS WAF 几乎总是能够确定 Web ACL 是否引用了某个实体。但是在极少数情况下，它可能无法执行此操作。如果您需要确保要删除的实体未在使用中，请在删除它之前先在 Web ACL 中进行检查。

匹配规则语句

匹配语句将 Web 请求或其来源与您提供的条件进行比较。对于许多此类语句， AWS WAF 比较请求中匹配内容的特定组成部分。

匹配语句是可嵌套的。您可以将这些语句中的任何一个嵌套在逻辑规则语句中，也可以在范围缩小语句中使用它们。有关逻辑规则语句的信息，请参阅 逻辑规则语句。有关范围缩小语句的信息，请参阅 范围缩小语句。

下表描述了可以添加到规则中的常规匹配语句，并提供计算每个 Web ACL 容量单位 (WCU) 使用量的指南。有关 WCU 的信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU)。

匹配语句	描述	WCU
地理匹配	检查请求的来源国，并贴上来源国和地区的标签。	1
IP 集匹配	根据一组 IP 地址和地址范围检查请求。	大多数情况下为 1。如果您将语句配置为使用带有被转发 IP 地址的标头，并在标头中指定位置 Any，则 WCU 将增加 4。
标签匹配规则语句	检查对由同一 Web ACL 中其他规则添加的标签的请求。	1
正则表达式匹配规则语句	将正则表达式模式与指定的请求组件进行比较。	3，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。
正则表达式模式集	将正则表达式模式与指定的请求组件进行比较。	每个模式集 25 个，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。
大小约束	根据指定的请求组件检查大小限制。	1，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。

匹配语句	描述	WCU
		如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。
SQLi 攻击	检查指定请求组件中是否存在恶意 SQL 代码。	20，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。
字符串匹配	将字符串与指定的请求组件进行比较。	基本成本取决于字符串匹配的类型，介于 1 和 10 之间。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。
XSS 脚本攻击	检查指定请求组件中是否存在跨站脚本攻击。	40，作为基本成本。 如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

地理匹配规则语句

使用地理或地理匹配语句根据来源国家和地区管理 Web 请求。地理匹配语句会为 Web 请求添加标签，标明来源国和原产地。无论语句条件是否与请求匹配，都会添加这些标签。地理匹配语句还会根据请求的来源国进行匹配。

如何使用地理匹配语句

您可以使用地理匹配语句进行国家或地区匹配，如下所示：

- 国家 – 您可以单独使用地理匹配规则来管理仅基于其来源国的请求。规则语句与国家/地区代码相匹配。您也可以使用与来源国标签相匹配的标签匹配规则来遵循地理匹配规则。
- 区域 – 使用地理匹配规则和标签匹配规则，根据请求的来源区域管理请求。您不能单独使用地理匹配规则来匹配区域代码。

有关使用标签匹配规则的信息，请参阅 标签匹配规则语句 和 AWS WAF 网络请求上的标签。

地理匹配语句的工作原理

使用地理匹配语句，按如下方式 AWS WAF 管理每个 Web 请求：

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

   AWS WAF 使用 MaxMind GeoIP 数据库确定请求的位置。MaxMind 尽管准确性因国家和知识产权类型等因素而异，但它们在国家一级的数据的准确性非常高。有关的更多信息 MaxMind，请参阅 MaxMind IP 地理定位。如果您认为任何 GeoIP 数据不正确，可以通过 “更正 GeoIP2 数据” 向 Maxmind 提交更MaxMind 正请求。

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

   - 您可以访问 ISO 网站，在 ISO 在线浏览平台 (OBP) 上搜索国家/地区代码。
   - 在维基百科上，国家/地区代码按照 ISO 3166-2 列出。

     URL `https://en.wikipedia.org/wiki/ISO_3166-2:<ISO country code>` 中列出了某个国家/地区的地区代码。例如，美国的地区代码参见 ISO 3166-2:US，乌克兰的地区代码参加 ISO 3166-2:UA。

2. 确定要添加到请求中的国家/地区标签和地区标签 – 这些标签表示地理匹配语句使用源 IP 还是转发的 IP 配置。

   - 源 ID

     国家标签为 awswaf:clientip:geo:country:*<ISO country code>*。例如，awswaf:clientip:geo:country:US 表示美国。

     区域标签为 awswaf:clientip:geo:region:*<ISO country code>*-*<ISO region code>*。例如，awswaf:clientip:geo:region:US-OR 表示美国俄勒冈。

   - 转发的 IP

     国家标签为 awswaf:forwardedip:geo:country:*<ISO country code>*。例如，awswaf:forwardedip:geo:country:US 表示美国。

     区域标签为 awswaf:forwardedip:geo:region:*<ISO country code>*-*<ISO region code>*。例如，awswaf:forwardedip:geo:region:US-OR 表示美国俄勒冈。

   如果请求的指定 IP 地址没有相应的国家或地区代码，则 AWS WAF 在标签中使用 XX 代替该值。例如，以下标签适用于国家/地区代码不可用的客户端 IP：awswaf:clientip:geo:country:XX 和以下标签适用于国家/地区为美国但其地区代码不可用的转发 IP：awswaf:forwardedip:geo:region:US-XX。

3. 根据规则条件评估请求的国家/地区代码

无论是否找到匹配，地理匹配语句都会在其检查的所有请求中添加国家和地区标签，无论是否找到匹配。

> **Note**
>
> AWS WAF 在规则的 Web 请求评估结束时添加所有标签。因此，与地理匹配语句中的标签匹配时，必须在包含地理匹配语句的规则之外的另一条规则中定义。

如果您只想检查区域值，则可以编写带有 Count 操作和单个国家/地区代码匹配的地理匹配规则，后接区域标签的标签匹配规则。即使采用这种方法，您也需要提供国家/地区代码以供地理匹配规则进行评估。您可以通过指定不太可能成为您网站流量来源的国家/地区，来减少日志记录和计数指标。

CloudFront 分布和 CloudFront 地理限制功能

对于 CloudFront 分发，如果您使用 CloudFront 地理限制功能，请注意该功能不会将被屏蔽的请求转发到 AWS WAF。它确实会将允许的请求转发到 AWS WAF。如果您想根据地理位置以及可以在中指定的其他条件来阻止请求 AWS WAF，请使用 AWS WAF 地理匹配语句，不要使用 CloudFront 地理限制功能。

地理匹配语句的特征

嵌套 – 您可以嵌套此语句类型。

WCU – 1 WCU。

设置 – 此语句使用以下设置：

- 国家/地区代码 – 用于比较地理匹配的一系列国家/地区代码。这些必须是 ISO 3166 国际标准的 alpha-2 国家/地区 ISO 代码中的双字符国家/地区代码，例如 `["US","CN"]`。
- （可选）转发 IP 配置-默认情况下， AWS WAF 使用 Web 请求来源中的 IP 地址来确定来源国。或者，您可以将规则配置为在 HTTP 标头中使用转发的 IP，如下所`X-Forwarded-For`示。 AWS WAF 使用标头中的第一个 IP 地址。使用此配置，您还可以指定一种回退行为，以应用于标头中包含格式错误的 IP 地址的 Web 请求。回退行为将请求的匹配结果设置为匹配或不匹配。有关更多信息，请参阅 转发的 IP 地址。

在何处查找规则语句

- 控制台上的规则生成器 – 在请求选项中，选择来源国家/地区。
- API — GeoMatchStatement

示例

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

- AND statement
  - 地理匹配语句，列出您要组织的国家/地区
  - NOT statement
    - IP 集语句，用于指定要允许通过的 IP 地址

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

以下伪代码描述了这种方法的示例：

1. 地理匹配语句列出了一些国家/地区，这些国家/地区有您想要阻止的区域，但操作设置为“计数”。无论匹配状态如何，这都会对每个 Web 请求进行标记，还可以为您提供感兴趣的国家/地区的计数指标。
2. 带有阻止操作的 AND 语句
   - 标签匹配语句，用于指定要阻止的国家/地区的标签
   - NOT statement
     - 标签匹配语句，用于指定您想要允许通过的国家/地区的区域的标签

以下 JSON 列表显示了前面伪代码中描述的两个规则的实施。这些规则禁止来自美国的所有流量，但来自俄勒冈州和华盛顿州的流量除外。地理匹配语句会为其检查的所有请求添加国家/地区和区域标签。标签匹配规则在地理匹配规则之后运行，因此它可以与地理匹配规则刚刚添加的国家/地区和区域标签进行匹配。地理匹配语句使用转发 IP 地址，因此标签匹配还会指定转发 IP 标签。

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
   "Action": {
     "Count": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "geoMatchForLabels"
```

```
    }
},
{
   "Name": "blockUSButNotOROrWA",
   "Priority": 11,
   "Statement": {
     "AndStatement": {
       "Statements": [
         {
           "LabelMatchStatement": {
             "Scope": "LABEL",
             "Key": "awswaf:forwardedip:geo:country:US"
           }
         },
         {
           "NotStatement": {
             "Statement": {
                "OrStatement": {
                  "Statements": [
                    {
                       "LabelMatchStatement": {
                         "Scope": "LABEL",
                         "Key": "awswaf:forwardedip:geo:region:US-OR"
                       }
                    },
                    {
                       "LabelMatchStatement": {
                         "Scope": "LABEL",
                         "Key": "awswaf:forwardedip:geo:region:US-WA"
                       }
                    }
                  ]
               }
             }
           }
         }
       ]
     }
   },
   "Action": {
     "Block": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
```

```
      "CloudWatchMetricsEnabled": true,
      "MetricName": "blockUSButNotOROrWA"
    }
}
```

再举一个例子，您可以将地理匹配与基于速率的规则相结合，为特定国家/地区或区域的用户确定资源的优先级。您可以为每个用于区分用户的地理匹配语句或标签匹配语句创建不同的基于速率的语句。为首选国家/地区中的用户设置较高的速率限制，并为其他用户设置较低的速率限制。

以下 JSON 列表显示了地理匹配规则，后面是基于速率的规则，这些规则限制来自美国的流量。这些规定允许来自俄勒冈州的流量高于来自全国其他任何地方的流量。

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

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

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

IP 集匹配规则语句

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

AWS WAF 支持除之外的所有 IPv4 和 IPv6 CIDR 范围。`/0`有关 CIDR 表示法的更多信息，请参阅维基百科条目无类别域间路由。一个 IP 集最多可以容纳 10,000 个 IP 地址或 IP 地址范围以供检查。

> **Note**
>
> 每个 IP 集匹配规则引用一个 IP 集，该集的创建和维护独立于规则。您可以在多个规则中使用单个 IP 集，并且在更新引用的集合时，AWS WAF 会自动更新引用该集合的所有规则。有关创建和管理 IP 集的信息，请参阅 创建和管理 IP 集。

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

嵌套 – 您可以嵌套此语句类型。

WCU – 大多数 1 个 WCU。如果将语句配置为使用转发 IP 地址并指定 ANY 的位置，则 WCU 使用量将增加 4。

此语句使用以下设置：

- IP 集规范 – 从列表中选择要使用的 IP 集或创建一个新的 IP 集。
- （可选）转发 IP 配置 – 用于代替请求来源的备用转发 IP 标头名称。您可以指定是与标头中的第一个地址、最后一个地址还是任何地址进行匹配。您还可以指定一种回退行为，以应用于指定标头中包含格式错误的 IP 地址的 Web 请求。回退行为将请求的匹配结果设置为匹配或不匹配。有关更多信息，请参阅 转发的 IP 地址。

在何处查找规则语句

- 控制台上的规则生成器 – 在请求选项中，选择来源 IP 地址。
- 在控制台上@@ 添加我自己的规则和规则组页面 – 选择 IP 设置选项。
- API — IP SetReferenceStatement

标签匹配规则语句

标签匹配语句根据字符串规范检查 Web 请求中的标签。可用于检查规则的标签是指在同一 Web ACL 评估中已由其他规则添加到 Web 请求中的标签。

在 Web ACL 评估之外，标签不会保留，但您可以在中访问标签指标， CloudWatch 并且可以在 AWS WAF 控制台中查看任何 Web ACL 的标签信息摘要。有关更多信息，请参阅 标签指标和维度 和 监控和调整。您还可看到日志中的标签。有关信息，请参阅 日志字段。

> **Note**
>
> 标签匹配语句只能查看之前在 Web ACL 中评估过的规则中的标签。有关如何 AWS WAF 评估 Web ACL 中的规则和规则组的信息，请参阅Web ACL 中规则和规则组的处理顺序。

有关添加和匹配标签的信息，请参阅 AWS WAF 网络请求上的标签。

嵌套 – 您可以嵌套此语句类型。

WCU – 1 WCU

此语句使用以下设置：

- 匹配范围 – 将其设置为 标签 以匹配标签名称以及前面的命名空间和前缀（可选）。将其设置为命名空间以匹配部分或全部命名空间规范，也可以匹配前面的前缀。
- Key – 要与之匹配的字符串。如果指定命名空间匹配范围，则应仅指定命名空间和前缀（可选），并带有结尾冒号。如果指定标签匹配范围，则必须包括标签名称，并且可以选择包括前述命名空间和前缀。

有关这些设置的信息，请参阅AWS WAF 与标签匹配的规则和AWS WAF 标签匹配示例。

在何处查找规则语句

- 控制台上规则生成器 – 对于请求选项，选择有标签。
- API — LabelMatchStatement

正则表达式匹配规则语句

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

对于想要使用数学逻辑组合匹配条件的情况，此语句类型是 正则表达式模式集匹配规则语句 一个不错的替代方案。例如，如果您希望请求组件与某些正则表达式模式匹配而不匹配其他正则表达式模式，则可以使用 AND 规则语句 和 NOT 规则语句 来组合正则表达式匹配语句。

AWS WAF 支持 PCRE 库使用的模式语法，但libpcre有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

嵌套 – 您可以嵌套此语句类型。

WCU – 3 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

> **Warning**
>
> 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制在中处理超大请求组件 AWS WAF。

  有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。
- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

在何处查找规则语句

- 控制台上规则生成器 – 对于匹配类型，选择匹配正则表达式。
- API — RegexMatchStatement

正则表达式模式集匹配规则语句

正则表达式模式集匹配检查您指定的 Web 请求部分中是否存在您在正则表达式模式集中指定的正则表达式模式。

AWS WAF 支持 PCRE 库使用的模式语法，但`libpcre`有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

> **Note**
>
> 每个正则表达式模式集匹配规则引用一个正则表达式模式集，该集的创建和维护独立于规则。你可以在多个规则中使用单个正则表达式模式集，当你更新被引用的集合时， AWS WAF 会自动更新所有引用它的规则。
> 有关创建和管理正则表达式模式集的信息，请参阅 创建和管理正则表达式模式集。

正则表达式模式集匹配语句指示 AWS WAF 在您选择的请求组件中搜索集合中的任何模式。如果请求组件与集合中的任何模式匹配，Web 请求将匹配模式集规则语句。

如果要使用逻辑组合正则表达式模式匹配，例如与某些正则表达式进行匹配而不匹配其他正则表达式，请考虑使用 正则表达式匹配规则语句。

嵌套 – 您可以嵌套此语句类型。

WCU – 25 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

> **Warning**
>
> 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制在中处理超大请求组件 AWS WAF。

有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。

- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

此语句需要以下设置：

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

在何处查找规则语句

- 控制台上的规则生成器 – 对于匹配类型，选择字符串匹配条件 > 从正则表达式集中匹配模式。
- API — RegexPatternSetReferenceStatement

大小约束规则语句

大小约束语句将 Web 请求组件中的字节数与您提供的数字进行比较，并根据您的比较条件进行匹配。比较条件是一个运算符，例如大于 (>) 或小于 (<)。例如，您可以匹配具有大于 100 字节的查询字符串的请求。

> **Note**
>
> 此语句仅检查 Web 请求组件的大小。不检查组件的内容。

如果您检查 URI 路径，则路径中的任何 / 都算作一个字符。例如，URI 路径 `/logo.jpg` 的长度是 9 个字符。

嵌套 – 您可以嵌套此语句类型。

WCU – 1 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。

  在应用了任何转换后，大小约束语句仅检查组件的大小。不检查组件的内容。
- 可选的文本转换-在检查请求组件的大小之前 AWS WAF 要对其执行的转换。例如，您可以压缩空白或对 HTML 实体进行解码。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

此外，此语句需要以下设置：

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

在何处查找规则语句

- 控制台上的规则生成器 – 对于匹配类型，在大小匹配条件下选择要使用的条件。
- API — SizeConstraintStatement

SQL 注入攻击规则语句

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

嵌套 – 您可以嵌套此语句类型。

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

如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

  > **Warning**
  >
  > 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制[在中处理超大请求组件 AWS WAF](#)。

  有关请求组件的更多信息，请参阅 [Web 请求组件规格和处理](#)。

- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 [文本转换选项](#)。

此外，此语句需要以下设置：

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

  HIGH 设置可检测更多 SQL 注入攻击，是一项推荐设置。由于灵敏度更高，此设置会生成更多的误报，尤其是在您的 Web 请求通常包含异常字符串的情况下。在 Web ACL 测试和调整期间，您可能需要实施更多工作以减少误报。有关信息，请参阅 [测试和调整您的 AWS WAF 保护措施](#)。

  设置越低，SQL 注入检测越不严格，误报也就越少。对于具有针对 SQL 注入攻击的其他保护或对误报具有低容忍度的资源，LOW 可能是一个更好的选择。

在何处查找规则语句

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

字符串匹配规则语句

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

嵌套 – 您可以嵌套此语句类型。

WCU – 基本费用取决于您使用的匹配类型。

- 完全匹配字符串 – 2
- 以字符串开头 – 2
- 以字符串结尾 – 2
- 包含字符串 – 10
- 包含单词 – 10

如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

  > **Warning**
  >
  > 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制在中处理超大请求组件 AWS WAF。

  有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。
- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

此外，此语句需要以下设置：

- 要匹配的字符串 — 这是您 AWS WAF 要与指定请求组件进行比较的字符串。字符串通常由可打印 ASCII 字符组成，但您可以使用从十六进制 0x00 到 0xFF (十进制 0 到 255) 的任何字符。
- 字符串匹配条件-这表示您 AWS WAF 要执行的搜索类型。
  - 完全匹配字符串 – 字符串和请求组件的值相同。
  - 以字符串开头 – 字符串出现在请求组件的开头。
  - 以字符串结尾 – 字符串出现在请求组件的末尾。

- 包含字符串 – 该字符串出现在请求组件中的任何位置。
- 包含词 – 您指定的字符串必须显示在请求组件中。

  对于此选项，指定的字符串必须仅包含字母数字字符或下划线（A-Z、a-z、0-9 或 _）。

  请求必须满足以下条件之一：

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

在何处查找规则语句

- 控制台上的规则生成器 – 对于匹配类型，请选择字符串匹配条件，然后填写匹配所依据的字符串。
- API — ByteMatchStatement

跨站点脚本攻击规则语句

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

嵌套 – 您可以嵌套此语句类型。

WCU – 40 个 WCU，作为基本成本。如果您使用请求组件所有查询参数，请添加 10 个 WCU。如果您使用请求组件 JSON 正文，则将基本成本 WCU 增加一倍。对于您应用的每个文本转换，添加 10 个 WCU。

此语句类型在 Web 请求组件上运行，需要以下请求组件设置：

- 请求组件 – Web 请求中要检查的部分，例如查询字符串或正文。

> **Warning**
>
> 如果您检查请求组件 B ody、JSON 正文、Header s 或 Cookie，请阅读有关内容 AWS WAF 可检查数量的限制在中处理超大请求组件 AWS WAF。

有关请求组件的更多信息，请参阅 Web 请求组件规格和处理。

- 可选的文本转换-在检查请求组件之前 AWS WAF 要对其执行的转换。例如，您可以将空格转换为小写或标准化空格。如果您指定了多个转换，则按列出的顺序 AWS WAF 处理这些转换。有关信息，请参阅 文本转换选项。

在何处查找规则语句

- 控制台上的规则生成器 – 对于匹配类型，请选择攻击匹配条件 > 包含 XSS 注入攻击。
- API — XssMatchStatement

逻辑规则语句

使用逻辑规则语句合并其他语句或否定其结果。每个逻辑规则语句至少需要一个嵌套语句。

要在逻辑上组合或否定规则语句的结果，可将这些语句嵌套在逻辑规则语句下。

逻辑规则语句是可嵌套的。您可以将这些语句嵌套在其他逻辑规则语句中，也可以在范围缩小语句中使用它们。有关范围缩小语句的信息，请参阅 范围缩小语句。

> **Note**
>
> 控制台上的可视化编辑器支持单层规则语句嵌套，可满足多种需求。如需嵌套更多级别，请在控制台上编辑规则的 JSON 表示形式或使用 API。

下表描述了逻辑规则语句，并提供了计算每个 Web ACL 容量单位 (WCU) 使用量的指南。有关 WCU 的信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU)。

逻辑语句	描述	WCU
AND 逻辑	将嵌套语句与 AND 逻辑相结合。	基于嵌套语句
NOT 逻辑	否定嵌套语句的结果。	基于嵌套语句
OR 逻辑	将嵌套语句与 OR 逻辑相结合。	基于嵌套语句

AND 规则语句

AND 规则语句将嵌套语句与逻辑 AND 运算相结合，因此所有嵌套语句都必须匹配 AND 语句才能进行匹配。这至少需要两个嵌套语句。

嵌套 – 您可以嵌套此语句类型。

WCU – 取决于嵌套语句。

在何处查找规则语句

- 控制台上的规则生成器 – 对于如果有请求，选择匹配所有语句 (AND)，然后填写嵌套语句。
- API — AndStatement

示例

以下列表显示了如何使用 AND 和 NOT 逻辑规则语句来消除 SQL 注入攻击语句的匹配结果误报。在这个示例中，假设我们可以编写一个单字节匹配语句来匹配导致误报的请求。

AND 语句匹配与字节匹配语句不匹配且与 SQL 注入攻击语句匹配的请求。

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
```

```
            "Statement": {
              "ByteMatchStatement": {
                "SearchString": "string identifying a false positive",
                "FieldToMatch": {
                  "Body": {
                    "OversizeHandling": "MATCH"
                  }
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "CONTAINS"
              }
            }
          }
        },
        {
          "SqliMatchStatement": {
            "FieldToMatch": {
              "Body": {
                "OversizeHandling": "MATCH"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "SQLiExcludeFalsePositives"
```

```
      }
    }
```

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

使用控制台规则可视化编辑器，您可以将大多数可嵌套语句嵌套在逻辑规则语句下，例如前面的示例中所示的语句。您不能使用可视化编辑器来嵌套 OR 或 AND 语句。要配置这种类型的嵌套，您需要以 JSON 格式提供规则语句。例如，以下 JSON 规则列表包括嵌套在 AND 语句中的 OR 语句。

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
```

```
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

NOT 规则语句

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

例如，如果您要阻止并非来自特定国家/地区的请求，请创建一个将操作设置为阻止的 NOT 语句，然后嵌套指定该国家/地区的地理匹配语句。

嵌套 – 您可以嵌套此语句类型。

WCU – 取决于嵌套语句。

在何处查找规则语句

- 控制台上的规则生成器 – 对于如果有请求，选择与语句不匹配 (NOT)，然后填写嵌套语句。
- API — NotStatement

OR 规则语句

OR 规则语句将嵌套语句与 OR 逻辑相结合，因此其中一个嵌套语句必须匹配 OR 语句才能进行匹配。这至少需要两个嵌套语句。

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

相反，如果您想阻止不是来自特定国家/地区或包含特定查询字符串的请求，则可以修改之前的 OR 语句，将地理匹配语句嵌套在 NOT 语句中更低的一个级别。此级别的嵌套要求您使用 JSON 格式，因为控制台仅支持一个级别的嵌套。

嵌套 – 您可以嵌套此语句类型。

WCU – 取决于嵌套语句。

在何处查找规则语句

- 控制台上的规则生成器 – 对于如果有请求，选择至少匹配其中一条语句 (OR)，然后填写嵌套语句。
- API — OrStatement

示例

下表显示了使用 OR 来组合另外两个语句的情况。如果其中一个嵌套语句匹配，则 OR 语句是匹配的。

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
```

```
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

使用控制台规则可视化编辑器，您可以在逻辑规则语句下嵌套大多数可嵌套语句，但不能使用可视化编辑器嵌套 OR 或 AND 语句。要配置这种类型的嵌套，您需要以 JSON 格式提供规则语句。例如，以下 JSON 规则列表包括嵌套在 AND 语句中的 OR 语句。

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

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

```
  }
}
```

基于速率的规则语句

当请求的速率过快时，基于速率的规则会计算传入的请求和速率限制请求。该规则根据您的标准聚合请求，并根据规则的评估窗口、请求限制和操作设置对聚合分组进行计数和速率限制。

> **Note**
>
> 您还可以使用 Bot Control AWS 托管规则规则组的目标保护级别对 Web 请求进行速率限制。使用此托管规则组会产生额外费用。有关更多信息，请参阅 基于速率的规则和定向机器人控制功能规则中的速率限制选项。

AWS WAF 针对您使用的基于速率的规则的每个实例，分别跟踪和管理 Web 请求。例如，如果您在两个 Web ACL 中提供相同的基于速率的规则设置，则这两个规则语句中的每一个都代表基于速率的规则的单独实例，并且每个语句都由其自己的跟踪和管理。 AWS WAF如果您在规则组中定义了基于费率的规则，然后在多个位置使用该规则组，则每次使用都会创建基于费率的规则的单独实例，该实例将通过该实例进行自己的跟踪和管理。 AWS WAF

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

scope-down 语句 — 此规则类型可以采用 scope-down 语句，以缩小规则跟踪的请求范围和速率限制。scope-down 语句可以是可选的，也可以是必需的，具体取决于您的其他规则配置设置。本节将介绍详细信息。有关范围缩小语句的一般信息，请参见。范围缩小语句

WCU – 2，作为基本成本。对于您指定的每个自定义聚合键，添加 30 个 WCU。如果您在规则中使用范围缩小语句，请计算并添加该语句的 WCU。

在何处查找规则语句

- 控制台上 Web ACL 中的规则生成器 – 对于规则下的类型，请选择基于速率的规则。
- API — RateBasedStatement

主题

- 基于速率的规则的高级设置
- 基于费率的规则注意事项

- 基于速率的规则聚合选项和密钥
- 基于速率的规则聚合实例和计数
- 基于速率的规则请求速率限制行为
- 基于速率的规则示例
- 列出基于速率的规则实施速率限制的 IP 地址

基于速率的规则的高级设置

基于速率的规则语句使用以下高级设置：

- 评估窗口-从当前时间回顾， AWS WAF 应包含在其请求计数中的时间（以秒为单位）。例如，对于设置为 120，当 AWS WAF 检查速率时，它会计算当前时间之前 2 分钟的请求数。有效设置为 60（1 分钟）、120（2 分钟）、300（5 分钟）和 600（10 分钟），默认设置为 300（5 分钟）。

  此设置并不能确定 AWS WAF 检查费率的频率，而是决定每次检查时它看起来多久以前。 AWS WAF 经常检查费率，其时间与评估窗口的设置无关。
- 速率限制-在指定的评估窗口内仅 AWS WAF 应跟踪的符合您的标准的最大请求数。允许的最低限制设置为 100。当违反此限制时，会将规则操作设置 AWS WAF 应用于符合您条件的其他请求。

  AWS WAF 在您设置的限制附近应用速率限制，但不能保证精确的限制匹配。有关更多信息，请参阅 基于费率的规则注意事项。
- 请求聚合 – 用于基于速率的规则计数和速率限制的 Web 请求的聚合条件。您设置的速率限制适用于每个聚合实例。有关详细信息，请参阅 聚合选项和键 和 聚合实例和计数。
- 操作 – 对规则速率限制的请求采取的操作。您可以使用除 Allow 以外的任何规则操作。与往常一样，这是在规则级别设置的，但有一些特定于基于费率的规则的限制和行为。有关规则操作的一般信息，请参阅 规则操作。有关速率限制的特定信息，请参阅基于速率的规则请求速率限制行为本节中的。
- 检查范围和速率限制 – 您可以通过添加范围缩小语句来缩小基于速率的语句跟踪的请求范围和速率限制。如果您指定范围缩小语句，则该规则将仅对与范围缩小语句匹配的请求进行聚合、计数和速率限制。如果您选择请求聚合选项全部计数，则需要使用范围缩小语句。有范围缩小语句的更多信息，请参阅 范围缩小语句。
- （可选）转发 IP 配置 – 仅当您在请求聚合中指定标头中的 IP 地址时才使用此配置，可以单独指定，也可以作为自定义键设置的一部分。 AWS WAF 检索指定标头中的第一个 IP 地址并将其用作聚合值。用于此目的的常用标头是 `X-Forwarded-For`，但您也可以指定任何标头。有关更多信息，请参阅 转发的 IP 地址。

基于费率的规则注意事项

AWS WAF 速率限制旨在控制高请求率，并以尽可能最高效、最有效的方式保护应用程序的可用性。它不适用于精确的请求速率限制。

- AWS WAF 使用更重视最近请求的算法来估计当前的请求速率。因此， AWS WAF 将在您设置的限制附近应用速率限制，但不能保证精确的限制匹配。
- 每次 AWS WAF 估算请求速率时，都要 AWS WAF 回顾一下在配置的评估窗口内收到的请求数。由于这个因素以及传播延迟等其他因素，请求可能会在长达几分钟的时间内以过高的速率传入，然后才 AWS WAF 会对其进行检测和速率限制。同样。请求速率可能在一段时间内低于该限制，然后才 AWS WAF 会检测到下降并停止速率限制操作。通常，此延迟低于 30 秒。
- 如果您更改正在使用的规则中的任何速率限制设置，则更改会重置该规则的速率限制计数。这最多可以将规则的速率限制活动暂停一分钟。速率限制设置包括评估窗口、速率限制、请求聚合设置、转发的 IP 配置和检查范围。

基于速率的规则聚合选项和密钥

默认情况下，基于速率的规则会根据请求 IP 地址对请求进行聚合和速率限制。您可以将规则配置为使用其他各种聚合键和键组合。例如，您可以根据转发的 IP 地址、HTTP 方法或查询参数进行聚合。您还可以指定聚合密钥组合，例如 IP 地址和 HTTP 方法，或者两个不同 Cookie 的值。

> **Note**
>
> 您在聚合键中指定的所有请求组件都必须包含在 Web 请求中，才能对请求进行评估或由规则对其进行速率限制。

您可以使用以下聚合选项配置基于速率的规则。

- 源 IP 地址 – 仅使用 Web 请求源向该 IP 地址发送的请求源进行聚合。

  源 IP 地址可能不包含原始客户端的地址。如果 Web 请求通过一个或多个代理或负载均衡器，则其中将包含最后一个代理的地址。
- 标头中的 IP 地址 – 仅使用 HTTP 标头中的客户端地址进行聚合。这也称为转发 IP 地址。

  使用此配置，您还可以指定一种回退行为，以应用于标头中包含格式错误的 IP 地址的 Web 请求。回退行为将请求的匹配结果设置为匹配或不匹配。如果没有匹配项，则基于速率的规则不计入请求或

限制请求的速率。为了匹配，基于速率的规则将该请求与指定标头中包含格式错误 IP 地址的其他请求组合在一起。

请谨慎使用此选项，因为代理可能会不一致地处理标头，也可以对其进行修改以绕过检查。有关最佳实践和其他信息，请参阅 转发的 IP 地址。

- 全部计数 – 对与规则的范围缩小语句匹配的所有请求进行计数和速率限制。此选项需要范围缩小语句。这通常用于对一组特定的请求进行速率限制，例如带有特定标签的所有请求或来自特定地理区域的所有请求。
- 自定义键 – 使用一个或多个自定义聚合键进行聚合。要将任一 IP 地址选项与其他聚合键结合使用，请在自定义键下定义它们。

  自定义聚合键是 请求组件选项 中所述的 Web 请求组件选项的子集。

  关键选项如下所示。除非另有说明，否则您可以多次使用一个选项，例如，两个标头或三个标签命名空间。

  - 标签命名空间 – 使用标签命名空间作为聚合键。每个具有指定标签命名空间的不同完全限定标签名称都构成了聚合实例。如果您只使用一个标签命名空间作为自定义键，则每个标签名称都完全定义了一个聚合实例。

    基于速率的规则仅使用通过 Web ACL 中事先评估的规则添加到请求中的标签。

    有关标签命名空间的信息，请参阅 AWS WAF 标签语法和命名要求。
  - 标头 – 使用命名的标头作为聚合键。标头中的每个不同值都构成聚合实例。

    标头采用可选的文本转换。请参阅 文本转换选项。
  - Cookie – 使用命名的 Cookie 作为聚合密钥。Cookie 中的每个不同值都构成聚合实例。

    Cookie 采用可选的文本转换。请参阅 文本转换选项。
  - 查询参数 – 在请求中使用单个查询参数作为聚合键。命名查询参数的每个不同值都构成聚合实例。

    查询参数采用可选的文本转换。请参阅 文本转换选项。
  - 查询字符串 – 使用请求中的整个查询字符串作为聚合键。每个不同的查询字符串都构成聚合实例。此类型的键只能使用一次。

    查询字符串采用可选的文本转换。请参阅 文本转换选项。
  - URI 路径 – 使用请求中的 URI 路径作为聚合键。每个不同的 URI 路径都构成聚合实例。此类型的键只能使用一次。

URI 路径采用可选的文本转换。请参阅 文本转换选项。

- HTTP 方法 – 使用请求的 HTTP 方法作为聚合密钥。每个不同的 HTTP 方法都构成聚合实例。此类型的键只能使用一次。
- IP 地址 – 使用 Web 请求源中的 IP 地址与其他密钥组合使用 Web 请求源中的 IP 地址进行聚合。

  这可能不包含原始客户端的地址。如果 Web 请求通过一个或多个代理或负载均衡器，则其中将包含最后一个代理的地址。
- 标头中的 IP 地址 – 使用 HTTP 标头中的客户端地址与其他密钥组合进行聚合。这也称为转发 IP 地址。

  请谨慎使用此选项，因为代理可能会对标头进行不一致的处理，并且可以对其进行修改以绕过检查。有关最佳实践和其他信息，请参阅 转发的 IP 地址。

基于速率的规则聚合实例和计数

当基于速率的规则使用您的聚合条件评估 Web 请求时，该规则为指定的聚合键找到的每组唯一值都将定义一个唯一的聚合实例。

- 多键 – 如果您定义了多个自定义键，则每个键的值将构成聚合实例的定义。每个唯一的值组合都定义了一个聚合实例。
- 单键 – 如果您在自定义密钥中或通过选择单例 IP 地址选项之一选择了单个密钥，则该密钥的每个唯一值都定义了一个聚合实例。
- 全部计数-无密钥 – 如果您选择了聚合选项全部计数，则该规则评估的所有请求都属于该规则的单个聚合实例。此选择需要范围缩小语句。

基于速率的规则分别计算其识别的每个聚合实例的 Web 请求。

例如，假设基于速率的规则使用以下 IP 地址和 HTTP 方法值评估 Web 请求：

- IP 地址 10.1.1.1，HTTP 方法 POST
- IP 地址 10.1.1.1，HTTP 方法 GET
- IP 地址 127.0.0.0，HTTP 方法 POST
- IP 地址 10.1.1.1，HTTP 方法 GET

该规则根据您的聚合条件创建不同的聚合实例。

- 如果聚合标准只是 IP 地址，则每个单独的 IP 地址都是一个聚合实例，并分别计算每个 IP 地址的请求 AWS WAF 数。我们示例的聚合实例和请求计数如下所示：
  - IP 地址 10.1.1.1：计数 3
  - IP 地址 127.0.0.0：计数 1
- 如果聚合条件是 HTTP 方法，则每个 HTTP 方法都是一个聚合实例。我们示例的聚合实例和请求计数如下所示：
  - HTTP 方法 POST：计数 2
  - HTTP 方法 GET：计数 2
- 如果聚合条件是 IP 地址和 HTTP 方法，则每个 IP 地址和每个 HTTP 方法都将构成组合的聚合实例。我们示例的聚合实例和请求计数如下所示：
  - IP 地址 10.1.1.1，HTTP 方法 POST：计数 1
  - IP 地址 10.1.1.1，HTTP 方法 GET：count 2
  - IP 地址 127.0.0.0，HTTP 方法 POST：计数 1

基于速率的规则请求速率限制行为

AWS WAF 用于对基于速率的规则的请求进行速率限制的标准与用于汇总该 AWS WAF 规则请求的标准相同。如果您为规则定义了范围缩小语句，则 AWS WAF 只会聚合 scope-down 语句匹配的请求、计数请求和速率限制请求。

要使基于速率的规则将其规则操作设置应用于特定 Web 请求，匹配条件如下：

- Web 请求与规则的范围缩小语句（如果已定义）相匹配。
- Web 请求属于一个聚合实例，其请求数当前已超过规则的限制。

如何 AWS WAF 应用规则操作

当基于速率的规则对请求应用速率限制时，它会应用规则操作，如果您在操作规范中定义了任何自定义处理或标签，则该规则将应用这些操作。这种请求处理方式与匹配规则将其操作设置应用于匹配的 Web 请求的方式相同。基于速率的规则仅对主动限制速率的请求应用标签或执行其他操作。

您可以使用除 Allow 以外的任何规则操作。有关规则操作的一般信息，请参阅 规则操作。

以下列表描述了每个操作的速率限制是如何起作用的。

- Block— AWS WAF 阻止请求并应用您定义的任何自定义屏蔽行为。

- Count— 对请求进行 AWS WAF 计数，应用您定义的所有自定义标头或标签，并继续对请求进行 Web ACL 评估。

  此操作不会限制请求的速率。它只计算超过限制的请求。

- CAPTCHA 或 Challenge – AWS WAF 会像 Block 或 Count 一样处理请求，具体取决于请求令牌的状态。

  此操作不会限制具有有效令牌的请求的速率。它限制了超过限制且缺少有效令牌的请求速率。

  - 如果请求没有有效的未过期令牌，则该操作会阻止该请求并将验证码拼图或浏览器质询发送回客户端。

    如果最终用户或客户端浏览器成功响应，则客户端会收到有效的令牌并自动重新发送原始请求。如果聚合实例的速率限制仍然有效，则这个带有有效的未过期令牌的新请求将按照下一个要点中所述的操作进行应用。

  - 如果请求具有有效的未过期令牌，则 CAPTCHA 或 Challenge 操作会验证令牌并且不对请求采取任何操作，与 Count 操作类似。基于速率的规则在不采取任何终止操作的情况下将请求评估返回到 Web ACL，然后 Web ACL 继续对请求进行评估。

  有关更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

如果您仅对 IP 地址或转发 IP 地址进行速率限制

当您将规则配置为仅对转发 IP 地址的 IP 地址进行速率限制时，规则实例最多可以对 10,000 个 IP 地址进行速率限制。如果规则实例识别出超过 10,000 个 IP 地址并进行限制速率，则它只会限制 10,000 个最高发件人。

使用此配置，您可以检索基于速率的规则当前限制速率的 IP 地址列表。如果您使用的是 scope-down 语句，则受速率限制的请求只是 IP 列表中与 scope-down 语句匹配的请求。有关检索 IP 地址列表的信息，请参阅 列出基于速率的规则实施速率限制的 IP 地址。

基于速率的规则示例

本节介绍各种常见的基于速率的规则用例的配置示例。

每个示例都提供了用例的描述，然后在 JSON 列表中显示了自定义配置规则的解决方案。

> **Note**
>
> 这些示例中显示的 JSON 列表是在控制台中创建的，方法是配置规则，然后使用规则 JSON 编辑器对其进行编辑。

主题

对登录页面的请求进行速率限制

如需在不影响网站其余部分流量的前提下限制对网站登录页面的请求数量，您可以创建一个基于速率的规则，该规则使用范围缩小语句来匹配登录页面的请求，并将请求聚合设置为 全部计数。

基于速率的规则将计算单个聚合实例中登录页面的所有请求，并在请求超过限制时应用规则操作。

以下 JSON 列表显示了此规则配置的示例。全部计数聚合选项在 JSON 中作为设置 CONSTANT 列出。此示例匹配以开头 /login 的登录页面。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
```

```
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

对来自任何 IP 地址、用户代理对的登录页面的请求进行速率限制

如需限制超过限制的 IP 地址、用户代理对登录网站页面的请求数量，请将请求聚合设置为自定义键，并提供聚合条件。

以下 JSON 列表显示了此规则配置的示例。在此示例中，我们将每个 IP 地址、用户代理对的请求限制设置为在任何五分钟内发出 100 个请求。

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
```

```
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

对缺少特定标头的请求进行速率限制

要限制缺少特定标头的请求数量，可以将全部计数聚合选项与范围缩小语句一起使用。使用逻辑 NOT 语句配置范围缩小语句，该语句包含一条仅当标头存在且具有值时才返回 true 的语句。

以下 JSON 列表显示了此规则配置的示例。

```
{
  "Name": "test-rbr",
```

```
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

对带有特定标签的请求进行速率限制

您可以将速率限制与任何为请求添加标签的规则或规则组结合使用，以限制各种类别的请求数量。为此，您需要按如下方式配置 Web ACL：

- 添加添加标签的规则或规则组，并对其进行配置，使其不会阻止或允许您想要限制速率的请求。如果您使用托管规则组，则可能需要将某些规则组规则操作覆盖为 Count 才能实施此行为。
- 将基于速率的规则添加到您的 Web ACL 中，其优先级设置要高于标签规则和规则组。 AWS WAF 按数字顺序评估规则，从最低顺序开始，因此基于速率的规则将在标签规则之后运行。在规则的范围缩小语句中结合使用标签匹配和标签聚合，从而在标签上配置速率限制。

以下示例使用 Amazon IP 信誉列表 AWS 托管规则组。规则组规则 `AWSManagedIPDDoSList` 会检测并标记已知其 IP 正在积极参与 DDoS 活动的请求。规则的操作在规则组定义中配置为 Count。有关规则组的更多信息，请参阅 the section called “Amazon IP 声誉列表”。

以下 Web ACL JSON 列表使用 IP 声誉规则组，后面是基于标签匹配速率的规则。基于速率的规则使用范围缩小语句来筛选已由规则组规则标记的请求。基于速率的规则语句按其 IP 地址对筛选后的请求进行聚合和速率限制。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
```

```
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

对具有指定标签命名空间的标签的请求进行速率限制

机器人控制功能托管规则组中的通用级别规则为各种类别的机器人添加了标签，但它们仅阻止来自未经验证的机器人的请求。有关这些规则的信息，请参阅 机器人控制功能规则列表。

如果您使用机器人控制功能托管规则组，则可以为来自各个已验证机器人的请求添加速率限制。为此，您需要添加一条基于速率的规则，该规则在机器人控制功能规则组之后运行，并按机器人名称标

签聚合请求。您可以指定标签命名空间聚合键并将命名空间键设置为 awswaf:managed:aws:bot-control:bot:name:。每个具有指定命名空间的唯一标签都将定义一个聚合实例。例如，标签 awswaf:managed:aws:bot-control:bot:name:axios 和 awswaf:managed:aws:bot-control:bot:name:curl 分别定义一个聚合实例。

以下 Web ACL JSON 列表显示了此配置。此示例中的规则将任何单个机器人聚合实例的请求限制为两分钟内的 1,000 个。

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
```

```
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

列出基于速率的规则实施速率限制的 IP 地址

如果您的基于速率的规则仅聚合 IP 地址或转发的 IP 地址，则可以检索该规则当前限制速率的 IP 地址列表。 AWS WAF 将这些 IP 地址存储在规则的托管密钥列表中。

> **Note**
>
> 只有在仅聚合 IP 地址或仅聚合标头中的 IP 地址时，此选项才可用。如果您使用自定义键请求聚合，则即使您在自定义键中使用了其中一个 IP 地址规范，也无法检索速率受限的 IP 地址列表。

基于速率的规则将其规则操作应用于规则的托管键列表中与规则的范围缩小语句相匹配的请求。当规则没有范围缩小语句时，它会将操作应用于来自列表中 IP 地址的所有请求。默认情况下，规则操作为 Block，但它可以是除 Allow 之外的任何有效规则操作。使用单个基于速率的规则实例 AWS WAF 可以限制速率的最大 IP 地址数为 10,000。如果超过 10,000 个地址超过速率 AWS WAF 限制，则限制速率最高的地址。

您可以使用 CLI、API 或任何软件开发工具包访问基于速率的规则的托管键列表。本主题介绍使用 CLI 和 API 进行访问。控制台目前不提供对列表的访问权限。

对于 AWS WAF API，命令为GetRateBasedStatementManagedKeys。

对于 AWS WAF CLI，命令是 get-rate-based-statement-managed-key s。

以下显示了检索 Ama CloudFront zon 分配上网页 ACL 中使用的基于费率的规则的限速 IP 地址列表的语法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

下面显示了区域应用程序、Amazon API Gateway REST API、应用程序负载均衡器、 AWS AppSync GraphQL API、Amazon Cognito 用户池、服务或 AWS 已验证访问 AWS App Runner 实例的语法。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF 监控 Web 请求并独立管理 Web ACL、可选规则组和基于速率的规则的每个唯一组合的密钥。例如，如果在规则组内定义基于速率的规则，然后在 Web ACL 中使用该规则组，则 AWS WAF 会监视 Web 请求并管理该 Web ACL 的键、规则组参考语句和基于速率的规则实例。如果您在第二个 Web ACL 中使用相同的规则组，则会 AWS WAF 监控 Web 请求并管理第二次使用的密钥，完全独立于第一次使用。

对于您在规则组中定义的基于速率的规则，除了 Web ACL 名称和规则组内基于速率的规则的名称外，还需要在请求中提供规则组参考语句的名称。下面显示了区域应用程序的语法，其中基于速率的规则是在规则组内定义的，而规则组则在 Web ACL 中使用。

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --rule-name=RuleName
```

规则组规则语句

规则组规则语句不可嵌套。

本节介绍您可以在 Web ACL 中使用的规则组规则语句。规则组 Web ACL 容量单位 (WCU) 由规则组所有者在创建时设置。有关 WCU 的信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU)。

规则组语句	描述	WCU
托管规则组	运行在指定托管规则组中定义的规则。 您可以通过添加范围缩小语句来缩小规则组评估的请求范围。 您不能将托管规则组语句嵌套在任何其他语句类型中。	由规则组以及范围缩小语句的任何其他 WCU 定义。
规则组	运行在您管理的规则组中定义的规则。 您无法向自己的规则组引用语句添加范围缩小语句。 您不能将规则组语句嵌套在任何其他语句类型中。	在创建规则组时，您可以为其定义 WCU 限制。

托管规则组语句

托管规则组规则语句会在您的 Web ACL 规则列表中添加对托管规则组的引用。您不会在控制台的规则语句下看到此选项，但是当您使用 Web ACL 的 JSON 格式时，您添加的任何托管规则组都会以这种类型显示在 Web ACL 规则下。

托管规则组可以是 AWS 托管规则组（其中大多数对 AWS WAF 客户免费开放），也可以是 AWS Marketplace 托管规则组。当您将付费 AWS 托管规则组添加到 Web ACL 时，您会自动订阅这些规则组。您可以通过订阅 AWS Marketplace 托管规则组 AWS Marketplace。有关更多信息，请参阅 托管规则组。

将规则组添加到 Web ACL 时，您可以将规则组中规则的操作覆盖为 Count 或其他规则操作。有关更多信息，请参阅 规则组的操作覆盖选项。

您可以缩小使用规则组 AWS WAF 进行评估的请求的范围。为此，您需要在规则组语句中添加范围缩小语句。有关范围缩小语句的信息，请参阅 范围缩小语句。这可以帮助您管理规则组如何影响您的流量，还可以帮助您在使用规则组时控制与流量相关的成本。有关在 AWS WAF Bot Control 托管规则组中使用范围缩小语句的信息和示例，请参阅。AWS WAF 机器人控制

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

（可选）范围缩小语句 – 此规则类型采用可选的范围缩小语句，以缩小规则组评估的请求范围。有关更多信息，请参阅 范围缩小语句。

WCU – 在创建时为规则组设置。

在何处查找规则语句

- 控制台 – 在创建 Web ACL 的过程中，在添加规则和规则组页面上，选择添加托管规则组，然后查找并选择要使用的规则组。
- API — ManagedRuleGroupStatement

规则组语句

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

将规则组添加到 Web ACL 时，您可以将规则组中规则的操作覆盖为 Count 或其他规则操作。有关更多信息，请参阅 规则组的操作覆盖选项。

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

WCU – 在创建时为规则组设置。

在何处查找规则语句

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

在中处理超大请求组件 AWS WAF

AWS WAF 不支持检查 Web 请求组件正文、标头或 Cookie 的超大内容。底层主机服务对转发以 AWS WAF 供检查的内容有数量和大小限制。例如，主机服务向发送的标头不超过 200 个 AWS WAF，因此对于包含 205 个标头的 Web 请求， AWS WAF 无法检查最后 5 个标头。

当 AWS WAF 允许 Web 请求继续访问您的受保护资源时，将发送整个 Web 请求，包括超出可以检查的数量和大小限制的任何 AWS WAF 内容。

组件检查大小限制

组件检查尺寸限制如下：

- **`Body`**和 **`JSON Body`** — 对于 Application AWS AppSync Load Balancer 和， AWS WAF 可以检查请求正文的前 8 KB。对于 CloudFront，默认情况下，API Gateway、Amazon Cognito、App Runner 和 Verified Access AWS WAF 可以检查前 16 KB，您可以在 Web ACL 配置中将限制提高到 64 KB。有关更多信息，请参阅 管理车身检查的大小限制。
- **`Headers`**— 最多 AWS WAF 可以检查请求标头的前 8 KB（8,192 字节），最多可以检查前 200 个标头。在达到第一个限制之前 AWS WAF ，内容可供检查。
- **`Cookies`**— 最多 AWS WAF 可以检查请求的 cookie 的前 8 KB（8,192 字节），最多可以检查前 200 个 cookie。在达到第一个限制之前 AWS WAF ，内容可供检查。

规则语句的超大处理选项

在编写检查其中一种请求组件类型的规则语句时，您可以指定如何处理超大组件。超大处理 AWS WAF 告诉当规则检查的请求组件超过大小限制时，如何处理 Web 请求。

处理超大组件的选项如下：

- Continue— 根据规则检查标准通常检查请求组件。 AWS WAF 将检查大小限制范围内的请求组件内容。
- Match— 将 Web 请求视为与规则语句相匹配。 AWS WAF 将规则操作应用于请求，而不根据规则的检查标准对其进行评估。
- No match— 如果不根据规则的检查标准对其进行评估，则将 Web 请求视为与规则声明不匹配。AWS WAF 继续使用 Web ACL 中的其余规则检查 Web 请求，就像对待任何不匹配的规则一样。

在 AWS WAF 控制台中，你需要选择其中一个处理选项。在控制台之外，默认选项为 Continue。

如果您在操作设置为 Block 的规则中使用 Match 选项，则该规则将阻止被检查组件过大的请求。对于任何其他配置，请求的最终处置取决于各种因素，例如 Web ACL 中其他规则的配置以及 Web ACL 的默认操作设置。

非您拥有的规则组中的超大处理

组件大小和数量限制适用于您在 Web ACL 中使用的所有规则。这包括您在托管规则组以及其他账户与您共享的规则组中使用但未管理的任何规则。

当您使用您未管理的规则组时，该规则组可能有一条规则可以检查有限的请求组件，但不会按照您需要的方式处理超大内容。有关 AWS 托管规则如何管理超大尺寸组件的信息，请参阅AWS 托管规则规则组列表。有关其他规则组的信息，请咨询您的规则组提供程序。

管理 Web ACL 中超大组件的指导原则

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

管理超大 Web 请求组件的一般准则如下：

- 如果您需要允许某些包含超大组件内容的请求，请添加规则以明确仅允许这些请求。确定这些规则的优先级，使其在 Web ACL 中检查相同组件类型的任何其他规则之前运行。使用这种方法，您将无法使用 AWS WAF 来检查允许传递给受保护资源的超大组件的全部内容。
- 对于所有其他请求，您可以通过阻止超过限制的请求来防止任何额外的字节通过：
  - 您的规则和规则组 – 在检查有大小限制的组件的规则中，配置超大处理，以便阻止超过限制的请求。例如，如果您的规则阻止具有特定标头内容的请求，请将超大处理设置为与标头内容过大的请求相匹配。或者，如果您的 Web ACL 默认会阻止请求，并且您的规则允许特定的标头内容，则将规则的超大处理配置为不匹配任何标头内容过大的请求。
  - 您不管理的规则组 – 为了防止您不管理的规则组允许超大请求组件，您可以添加一个单独的规则来检查请求组件类型并阻止超出限制的请求。确定该 Web ACL 中规则的优先级，使其在规则组之

前运行。例如，在任何正文检查规则在 Web ACL 中运行之前，您可以阻止正文内容过大的请求。以下过程将介绍如何添加此类规则。

屏蔽超大的 Web 请求组件

您可以在 Web ACL 中添加一条规则，以阻止包含过大组件的请求。

添加阻止超大内容的规则

1. 创建或编辑 Web ACL 时，在规则设置中，选择添加规则、添加我自己的规则和规则组、规则生成器，然后选择规则可视化编辑器。有关创建或编辑 Web ACL 的指导，请参阅 使用 Web ACL。
2. 输入规则的名称，然后将类型设置保留为常规规则。
3. 将以下匹配设置更改为其默认设置：
   a. 在语句中，对于检查，打开下拉列表并选择所需的 Web 请求组件，即正文、标头或 Cookie。
   b. 对于匹配类型，选择大小大于。
   c. 在大小中，键入一个至少等于该组件类型的最小大小的数字。对于标题和 Cookie，请键入8192。在 Application Load Balancer 或 AWS AppSync Web ACL 中，对于主体，键入8192。对于 API Gateway CloudFront、Amazon Cognito、App Runner 或 Verified Access Web ACL 中的正文，如果你使用的是默认的正文大小限制，请键入。16384否则，请键入您为 Web ACL 定义的正文大小限制。
   d. 对于超大处理，请选择匹配。
4. 对于操作，选择阻止。
5. 选择 添加规则。
6. 添加规则后，在设置规则优先级页面上，将其移至 Web ACL 中检查相同组件类型的所有规则或规则组上方。这使新规则具有较低的数字优先级设置，因此 AWS WAF 需要先对其进行评估。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

中的正则表达式模式匹配 AWS WAF

AWS WAF 支持 PCRE 库`libpcre`使用的模式语法。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。

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

AWS WAF 不支持以下 PCRE 模式：

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

中的 IP 集和正则表达式模式集 AWS WAF

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

您可以在规则组或 Web ACL 中使用托管集。

- 要使用 IP 集，请参阅IP 集匹配规则语句。
- 要使用正则表达式模式集，请参见。正则表达式模式集匹配规则语句

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

主题

创建和管理 IP 集

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

要使用 Web ACL 或规则组中设置的 IP，请先`IPSet`使用您的地址规格创建一个 AWS 资源。然后，在将 IP 集规则语句添加到 Web ACL 或规则组时引用该集。

主题

创建 IP 集

按照本部分中的过程创建新的 IP 集。

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

创建 IP 集

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

   > **Note**
   >
   > IP 集在创建之后无法更改名称。

4. 对于区域，选择全局 (CloudFront) 或选择要存储 IP 集的区域。您只能在保护区域资源的 Web ACL 中使用区域 IP 集。要使用网页 ACL 中设置的 IP 来保护 Amazon CloudFront 分配，您必须使用 Global (CloudFront)。
5. 对于 IP version (IP 版本)，请选择要使用的版本。
6. 在 IP 地址文本框中，以 CIDR 表示法每行输入一个 IP 地址或 IP 地址范围。 AWS WAF 支持除 `/0`之外的所有 IPv4 和 IPv6 CIDR 范围。有关 CIDR 表示法的更多信息，请参阅维基百科条目 Classless Inter-Domain Routing。

   下面是一些示例：

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

删除 IP 集

按照本部分中的指导删除引用集。

删除引用的集合和规则组

删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时， AWS WAF 会检查该实体当前是否正在 Web ACL 中使用。如果它发现它正在使用中，则 AWS WAF 会警告你。 AWS WAF 几乎总是能够确定 Web ACL 是否引用了某个实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在您的 Web ACL 中进行检查。如果实体是引用的集合，请确保没有规则组正在使用它。

删除 IP 集

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 IP 集。
3. 选择要删除的 IP 集，然后选择 删除。

创建和管理正则表达式模式集

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

要使用 Web ACL 或规则组中设置的正则表达式模式，请先使用正则表达式模式`RegexPatternSet`规范创建一个 AWS 资源。然后，在将正则表达式模式集规则语句添加到 Web ACL 或规则组时引用该集。正则表达式模式集必须至少包含一个正则表达式模式。

如果您的正则表达式模式集包含多个正则表达式模式，则在规则中使用时，模式匹配与 `OR` 逻辑组合使用。也就是说，如果请求组件与集合中的任何模式匹配，Web 请求将匹配模式集规则语句。

AWS WAF 支持 PCRE 库使用的模式语法，但`libpcre`有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

主题

创建正则表达式模式集

按照本部分中的过程创建新的正则表达式模式集。

创建正则表达式模式集

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 正则表达式模式集，然后选择 创建正则表达式模式集。
3. 输入正则表达式模式集的名称和描述。当您想要使用集时，您可以使用这些信息来标识集。

   > **Note**
   >
   > 正则表达式模式集在创建之后无法更改名称。

4. 对于 “区域”，选择 “全局” (CloudFront) 或选择要存储正则表达式模式集的区域。您只能在保护区域资源的 Web ACL 中使用区域正则表达式模式集。要使用在 Web ACL 中设置的正则表达式模式来保护 Amazon CloudFront 分配，您必须使用 Global ()。CloudFront
5. 在 正则表达式 文本框中，每行输入一个正则表达式模式。

例如，正则表达式 `I[a@]mAB[a@]dRequest` 与以下字符串匹配：`IamABadRequest`、`IamAB@dRequest`、`I@mABadRequest` 和 `I@mAB@dRequest`。

AWS WAF 支持 PCRE 库使用的模式语法，但`libpcre`有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

6. 查看正则表达式模式集的设置，然后选择 创建正则表达式模式集。

删除正则表达式模式集

按照本部分中的指导删除引用集。

删除引用的集合和规则组

删除可以在 Web ACL 中使用的实体（例如 IP 集、正则表达式模式集或规则组）时， AWS WAF 会检查该实体当前是否正在 Web ACL 中使用。如果它发现它正在使用中，则 AWS WAF 会警告你。 AWS WAF 几乎总是能够确定 Web ACL 是否引用了某个实体。但是在极少数情况下，它可能无法确定。如果您需要确保当前没有任何实体正在使用中，请在删除实体之前先在您的 Web ACL 中进行检查。如果实体是引用的集合，请确保没有规则组正在使用它。

删除正则表达式模式集

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 正则表达式模式集。
3. 选择要删除的正则表达式模式集，然后选择 删除。

AWS WAF中的自定义 Web 请求和响应

您可以将自定义 Web 请求和响应处理行为添加到 AWS WAF 规则操作和默认 Web ACL 操作中。只要您的自定义设置所附的操作适用，就会适用。

您可以通过以下方式自定义 Web 请求和响应：

- 使用 Allow、Count、CAPTCHA 和 Challenge 操作，您可以在 Web 请求中插入自定义标头。当 AWS WAF 将 Web 请求转发到受保护的资源时，该请求将包含整个原始请求以及您插入的自定义标头。对于 CAPTCHA 和 Challenge 操作，只有在该请求通过了验证码或质询令牌检查后， AWS WAF 才会应用此自定义响应。

- 通过 Block 操作，您可以定义完整的自定义响应，包括响应代码、标头和正文。受保护的资源使用提供的自定义响应来响应请求 AWS WAF。您的自定义响应将取代 403 (Forbidden) 的默认 Block 操作响应。

您可以自定义的操作设置

在定义以下操作设置时，可以指定自定义请求或响应：

- 规则操作。有关信息，请参阅 规则操作。
- Web ACL 的默认操作。有关信息，请参阅 Web ACL 默认操作。

您无法自定义的操作设置

对于在 Web ACL 中使用的规则组，您不能在覆盖操作中指定自定义请求处理。请参阅 Web ACL 规则和规则组评估。另请参阅 托管规则组语句 和 规则组语句。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

对您使用自定义请求和响应的限制

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

主题

- 为非阻止操作插入自定义请求标头
- Block 操作的自定义响应

- 自定义响应支持的状态码

为非阻止操作插入自定义请求标头

当规则操作未阻止请求时，您可以指示 AWS WAF 在原始 HTTP 请求中插入自定义标头。使用此选项，您只需添加到请求中。您不能修改或替换原始请求的任何部分。插入自定义标头的用例包括向下游应用程序发出信号，要求其根据插入的标头以不同方式处理该请求，以及标记该请求以进行分析。

此选项适用于规则操作 Allow、Count、CAPTCHA 和 Challenge，以及设置为 Allow 的 Web ACL 默认操作。有关规则操作的更多信息，请参阅 规则操作。有关默认 Web ACL 操作的更多信息，请参阅 Web ACL 默认操作。

自定义请求标头名称

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

同名标头

如果请求中已经有 AWS WAF 正在插入的同名标头，则 AWS WAF 会覆盖该标头。因此，如果您在多个具有相同名称的规则中定义标头，则检查请求并查找匹配项的最后一条规则将添加其标头，而之前的任何规则都不会添加标头。

带有非终止规则操作的自定义标头

与Allow操作不同，该Count操作不会停止 AWS WAF 使用 Web ACL 中的其余规则处理 Web 请求。同样，当CAPTCHA并Challenge确定请求令牌有效时，这些操作不会停止 AWS WAF 处理 Web 请求。因此，如果采用具有这些操作之一的规则插入自定义标头，后续规则可能也会插入自定义标头。有关规则操作行为的更多信息，请参阅 规则操作。

例如，假设您拥有以下规则，按所示顺序排列优先级：

1. RuleA，其中包含一个 Count 操作和一个名为 `RuleAHeader` 的自定义标头。
2. RuleB，其中包含一个 Allow 操作和一个名为 `RuleBHeader` 的自定义标头。

如果请求同时匹配 ruleA 和 RuleB，则 AWS WAF 插入标头`x-amzn-waf-RuleAHeader`和`x-amzn-waf-RuleBHeader`，然后将请求转发到受保护的资源。

AWS WAF 完成对请求的检查后，在 Web 请求中插入自定义标头。因此，如果您将自定义请求处理与将操作设置为 Count 的规则一起使用，则后续规则不会检查您添加的自定义标头。

自定义请求处理示例

您可以为规则的操作或 Web ACL 的默认操作定义自定义请求处理。下表显示了 Web ACL 的默认操作中添加的用于自定义处理的 JSON。

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "SampleWebACL"
 }
}
```

Block 操作的自定义响应

对于设置 AWS WAF 为的规则操作或 Web ACL 默认操作，您可以指示将自定义 HTTP 响应发送回客户端。Block有关规则操作的更多信息，请参阅 规则操作。有关默认 Web ACL 操作的更多信息，请参阅 Web ACL 默认操作。

在为 Block 操作定义自定义响应处理时，您可以定义状态代码、标头和响应正文。有关可与配合使用的状态码列表 AWS WAF，请参阅以下部分自定义响应支持的状态码。

使用案例

自定义响应的用例包括：

- 将默认状态码发送回客户端。
- 将自定义响应标头发送回客户端。您可以为指定任何标头名称，除 content-type 外。
- 将静态错误页面发送回客户端。
- 将客户端重定向到其他 URL。为此，您需要指定一个 3xx 重定向状态码，例如 301 (Moved Permanently) 或 302 (Found)，然后以新 URL 指定一个名为 Location 的新标头。

与您在受保护资源中定义的响应进行交互

您为 AWS WAF Block操作指定的自定义响应优先于您在受保护资源中定义的任何响应规范。

您保护的 AWS 资源的主机服务 AWS WAF 可能允许对 Web 请求进行自定义响应处理。示例包括：

- 借助 Amazon CloudFront，您可以根据状态代码自定义错误页面。有关信息，请参阅《Amazon CloudFront 开发者指南》中的生成自定义错误响应。
- 使用 Amazon API Gateway，您可以为网关定义响应和状态码。有关更多信息，请参阅 Amazon API Gateway 开发人员指南中的 API Gateway 中的 Gateway 响应。

在受保护的 AWS 资源中，您不能将 AWS WAF 自定义响应设置与自定义响应设置结合使用。任何单个 Web 请求的响应规范要么完全来自 AWS WAF ，要么完全来自受保护的资源。

对于 AWS WAF 阻塞的 Web 请求，以下显示了优先顺序。

1. AWS WAF 自定义响应-如果 AWS WAF Block操作启用了自定义响应，则受保护的资源会将配置的自定义响应发送回客户端。您在受保护的资源中定义的任何响应设置（如有）均无效。
2. 在受保护资源中定义的自定义响应 – 否则，如果受保护资源有指定的自定义响应设置，则受保护资源将使用这些设置来响应客户端。
3. AWS WAF 默认Block响应-否则，受保护的资源将使用 AWS WAF 默认响应来Block响应客户端403 (Forbidden)。

对于 AWS WAF 允许的 Web 请求，您对受保护资源的配置决定了它发送回客户端的响应。您无法在中 AWS WAF 为允许的请求配置响应设置。您可以 AWS WAF 为允许的请求配置的唯一自定义是在原始请求中插入自定义标头，然后再将请求转发到受保护的资源。上一节 为非阻止操作插入自定义请求标头 中介绍了此选项。

自定义响应标头

您可以为指定任何标头名称，除 content-type 外。

自定义响应正文

您可以在要使用的 Web ACL 或规则组的上下文中定义自定义响应的正文。定义自定义响应正文后，您可以在 Web ACL 或创建它的规则组中的任何其他位置通过引用来使用它。在单个 Block 操作设置中，您可以引用要使用的自定义正文，并定义自定义响应的状态代码和标头。

在控制台中创建自定义响应时，您可以从已定义的响应正文中进行选择，也可以创建新的响应正文。在控制台之外，您可以在 Web ACL 或规则组级别定义自定义响应正文，然后从 Web ACL 或规则组中的操作设置中引用它们。这在下一节的 JSON 示例中有所体现。

自定义响应示例

以下示例列出了具有自定义响应设置的规则组的 JSON。为整个规则组定义自定义响应正文，然后由规则操作中的键来引用。

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
```

```
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
    }
   },
   "Name": "GeoMatchRule",
   "Priority": 1,
   "Statement": {
    "GeoMatchStatement": {
     "CountryCodes": [
      "US"
     ]
    }
   },
   "VisibilityConfig": {
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestRuleGroupReferenceMetric",
    "SampledRequestsEnabled": true
   }
  }
 ],
 "VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "TestRuleGroupMetric",
  "SampledRequestsEnabled": true
 }
}
```

自定义响应支持的状态码

有关 HTTP 状态码的详细信息，请参阅互联网工程任务组 (IETF) 的状态码和维基百科上的 HTTP 状态码列表。

以下是 AWS WAF 支持自定义响应的 HTTP 状态代码。

- 2xx Successful
  - 200 – OK
  - 201 – Created
  - 202 – Accepted
  - 204 – No Content

  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices
  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error
  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable

- 504 – Gateway Timeout
- 505 – HTTP Version Not Supported

AWS WAF 网络请求上的标签

标签是规则与请求匹配时规则添加到 Web 请求中的元数据。添加后，在 Web ACL 评估结束之前，该请求上的标签将保持可用。您可以使用标签匹配语句访问稍后在 Web ACL 评估中运行的规则中的标签。有关更多信息，请参阅 标签匹配规则语句。

网络请求上的标签会生成 Amazon CloudWatch 标签指标。有关指标和维度的列表，请参阅 标签指标和维度。有关通过控制台和通过 AWS WAF 控制台访问指标 CloudWatch 和指标摘要的信息，请参阅监控和调整。

标签用例

AWS WAF 标签的常见用例包括：

- 在@@ 对请求采取操作之前，根据多个规则语句评估 Web 请求-在发现与 Web ACL 中的规则匹配后，如果规则操作未终止 Web ACL 评估，则 AWS WAF 继续根据 Web ACL 评估该请求。在决定允许或阻止请求之前，您可以使用标签来评估和收集来自多个规则的信息。为此，请将现有规则的操作更改为 Count，然后将其配置为为匹配的请求添加标签。然后，添加一个或多个新规则，在其他规则之后运行，并将它们配置为根据标签匹配组合评估标签并管理请求。
- 按地理区域管理 Web 请求 – 您可以单独使用地理匹配规则来按来源国管理 Web 请求。要将位置精细调整到区域级别，您可以使用带有 Count 操作和标签匹配规则的地理匹配规则。有关地理匹配规则的信息，请参阅 地理匹配规则语句。
- 跨多个规则重复使用逻辑 – 如果您需要在多个规则中重复使用相同的逻辑，则可以使用标签对逻辑进行单一来源化，然后测试结果。当您有多个使用嵌套规则语句的公共子集的复杂规则时，在复杂的规则中复制通用规则集可能非常耗时且容易出错。使用标签，您可以使用通用规则子集创建新规则，该子集计算匹配请求并为其添加标签。您将新规则添加到 Web ACL 中，使其在最初的复杂规则之前运行。然后，在原始规则中，将共享规则子集替换为检查标签的单个规则。

  例如，假设您有多条规则，而您只想应用于您的登录路径。与其让每条规则指定相同的逻辑来匹配潜在的登录路径，不如实施一条包含该逻辑的新规则。让新规则为匹配的请求添加标签，以表明该请求位于登录路径上。在您的 Web ACL 中，为该新规则设置比原始规则更低的数字优先级，使其首先运行。然后，在您的原始规则中，将共享逻辑替换为检查标签是否存在。有关优先级设置的信息，请参阅 Web ACL 中规则和规则组的处理顺序。

- 为规则组中的规则创建例外 – 此选项对您无法查看或更改的托管规则组特别有用。许多托管规则组规则会为匹配的 Web 请求添加标签，以指示匹配的规则，并可能提供有关匹配的更多信息。当您使用向请求添加标签的规则组时，您可以覆盖规则组规则来计算匹配次数，然后根据规则组标签在处理 Web 请求的规则组之后运行规则。所有 AWS 托管规则都会将标签添加到匹配的 Web 请求。有关详细说明，请参阅 AWS 托管规则规则组列表 的规则说明。
- 使用标签指标监控流量模式 – 您可以访问您通过规则添加的标签的指标，以及您在 Web ACL 中使用的任何托管规则组添加的指标。所有 AWS 托管规则组都会为其评估的 Web 请求添加标签。有关标签指标和维度的列表，请参阅 标签指标和维度。您可以通过或通过 AWS WAF 控制台中的 Web ACL 页面访问指标 CloudWatch 和指标摘要。有关信息，请参阅监控和调整。

AWS WAF 标签的工作原理

当规则与 Web 请求匹配时，如果该规则定义了标签，则会在规则评估结束时将标签 AWS WAF 添加到请求中。在 Web ACL 中的匹配规则之后评估的规则可能与规则添加的标签进行匹配。

谁在请求中添加标签

评估请求的 Web ACL 组件可以为请求添加标签。

- 任何不是规则组参考语句的规则都可以为匹配的 Web 请求添加标签。标签标准是规则定义的一部分，当 Web 请求与规则匹配时， AWS WAF 会将规则的标签添加到请求中。有关信息，请参阅 the section called “添加标签的规则”。
- 地理匹配规则语句会为其检查的任何请求添加国家和区域标签，无论该语句是否产生匹配。有关信息，请参阅 the section called “地理匹配”。
- AWS WAF 所有人的 AWS 托管规则会为他们检查的请求添加标签。它们根据规则组中的规则匹配添加一些标签，并根据托管规则组使用的 AWS 流程添加一些标签，例如使用智能威胁缓解规则组时添加的令牌标签。有关每个托管规则组添加的标签的信息，请参阅 the section called “AWS 托管规则规则组列表”。

如何 AWS WAF 管理标签

AWS WAF 在规则对请求的检查结束时，将规则的标签添加到请求中。标记是规则匹配活动的一部分，与操作类似。

Web ACL 评估结束后，标签不会保留在 Web 请求中。为了使其他规则与您的规则添加的标签相匹配，您的规则操作不得终止 Web ACL 对 Web 请求的评估。规则操作必须设置为 Count、CAPTCHA 或 Challenge。当 Web ACL 评估未终止时，Web ACL 中的后续规则可以根据请求运行其标签匹配条件。有关规则操作的更多信息，请参阅 规则操作。

在 Web ACL 评估期间访问标签

添加后，只要 AWS WAF 根据 Web ACL 评估请求，标签就会在请求上保持可用。Web ACL 中的任何规则都可以访问已在同一 Web ACL 中运行的规则所添加的标签。这包括直接在 Web ACL 中定义的规则和在 Web ACL 中使用的规则组中定义的规则。

- 您可以使用标签匹配语句与规则的请求检查条件中的标签进行匹配。您可以与请求中附加的任何标签进行匹配。有关语句的详细信息，请参阅 标签匹配规则语句。
- 地理匹配语句会添加带或不带匹配项的标签，但只有在该语句的包含 Web ACL 规则完成请求评估后，这些标签才可用。
  - 您不能使用单个规则（例如逻辑 AND 语句）对地理标签运行地理匹配语句和标签匹配语句。您必须将标签匹配语句放在单独的规则中，该规则在包含地理匹配语句的规则之后运行。
  - 如果您在基于速率的规则语句或托管规则组参考语句中使用地理匹配语句作为范围缩小语句，则该地理匹配语句添加的标签无法由包含规则的语句进行检查。如果您需要在基于速率的规则语句或规则组中检查地理标记，则必须在事先运行的单独规则中运行地理匹配语句。

在 Web ACL 评估之外访问标签信息

Web ACL 评估结束后，标签不会保留在 Web 请求中，而是 AWS WAF 将标签信息记录在日志和指标中。

- AWS WAF 存储任意请求中前 100 个标签的 Amazon CloudWatch 指标。有关访问标签指标的信息，请参阅 使用 Amazon 进行监控 CloudWatch 和 标签指标和维度。
- AWS WAF 汇总了 AWS WAF 控制台中 Web ACL 流量概述仪表板中的 CloudWatch 标签指标。您可以在任何 Web ACL 页面上访问控制面板。有关更多信息，请参阅 Web ACL 流量概述控制面板。
- AWS WAF 在日志中记录请求中前 100 个标签的标签。您可以使用标签和规则操作来筛选 AWS WAF 记录的日志。有关信息，请参阅 记录 AWS WAF Web ACL 流量。

您的 Web ACL 评估可以将 100 多个标签应用于 Web 请求并与 100 多个标签进行匹配，但 AWS WAF 只会在日志和指标中记录前 100 个标签。

AWS WAF 标签语法和命名要求

标签是由前缀、可选命名空间和名称组成的字符串。标签的组成部分用冒号分隔。标签具有以下要求和特征：

- 标签区分大小写。

- 每个标签命名空间或标签名称最多可包含 128 个字符。
- 您最多可以在标签中指定 5 个命名空间。
- 标签的组成部分用冒号 (:) 分隔。
- 不能在为标签指定的命名空间或名称中使用以下保留字符串：awswaf、aws、waf、rulegroup、webacl、regexpatternset、ipset 和 managed。

标签语法

完全限定的标签具有前缀、可选命名空间和标签名称。前缀用于标识添加标签的规则的规则组或 Web ACL 上下文。命名空间可用于为标签添加更多上下文。标签名称提供了标签的最低详细级别。它通常表示在请求中添加标签的特定规则。

标签前缀因其来源而异。

- 您的标签 – 以下内容显示了您在 Web ACL 和规则组规则中创建的标签的完整标签语法。实体类型为 rulegroup 和 webacl。

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

  - 标签命名空间前缀：awswaf:<entity owner account id>:<entity type>:<entity name>:
  - 添加的自定义命名空间：<custom namespace>:…:

  在规则组或 Web ACL 中为规则定义标签时，您可以控制自定义命名空间字符串和标签名称。其余的由你生成 AWS WAF。 AWS WAF 自动在所有标签前加上账户awswaf和 Web ACL 或规则组实体设置。
- 托管规则组标签 – 以下内容显示了由托管规则组中的规则创建的标签的完整标签语法。

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

  - 标签命名空间前缀：awswaf:managed:<vendor>:<rule group name>:
  - 添加的自定义命名空间：<custom namespace>:…:

  所有 AWS 托管规则规则组都会添加标签。有关托管规则组的信息，请参阅托管规则组。

- 来自其他 AWS 进程的标签- AWS 托管规则规则组使用这些进程，因此您可以看到它们已添加到使用托管规则组评估的 Web 请求中。下面显示了由托管规则组调用的进程所创建的标签的完整标签语法。

  ```
  awswaf:managed:<process>:<custom namespace>:...:<label name>
  ```

  - 标签命名空间前缀：awswaf:managed:<process>:
  - 添加的自定义命名空间：<custom namespace>:…:

  这种类型的标签是为调用 AWS 进程的托管规则组而列出的。有关托管规则组的信息，请参阅托管规则组。

为您的规则添加标签的示例

以下示例标签由属于账户 111122223333 的名为 testRules 的规则组中的规则定义。

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

下面的列表显示了 JSON 中的示例标签规范。这些标签名称在结尾标签名称之前包含自定义命名空间字符串。

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> 您可以通过规则 JSON 编辑器在控制台中访问此类列表。

如果您在与前面的标签示例相同的规则组和账户中运行上述规则，则将生成以下完全限定标签：

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

托管规则组的标签示例

以下显示了 AWS 托管规则组及其调用的流程的示例标签。

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF 添加标签的规则

在几乎所有规则中，您都可以定义标签 AWS WAF ，并将其应用于任何匹配的请求。

以下规则类型是唯一的例外：

- 基于速率的规则仅在速率限制时进行标记 — 基于速率的规则仅在特定聚合实例的速率限制下为该实例的 Web 请求添加标签。 AWS WAF有关基于速率的规则的更多信息，请参阅 基于速率的规则语句。
- 不允许在规则组参考语句中添加标签 — 控制台不接受这些规则类型的标签。通过 API，为任一语句类型指定标签都会导致验证异常。有关这些语句类型的信息，请参阅 托管规则组语句 和 规则组语句。

WCU – 您在 Web ACL 或规则组规则中定义的每 5 个标签为 1 个 WCU。

此语句的查找位置

- 控制台上的规则生成器 – 在规则的操作设置中的标签下。

- API 数据类型 – `Rule RuleLabels`

通过指定要附加到标签命名空间前缀的自定义命名空间字符串和名称，可以在规则中定义标签。 AWS WAF 从定义规则的上下文中派生前缀。有关这方面的信息，请参阅 AWS WAF 标签语法和命名要求 下面的标签语法信息。

AWS WAF 与标签匹配的规则

您可以使用标签匹配语句来评估 Web 请求标签。您可以与标签（需要标签名称）或命名空间（需要命名空间规范）进行匹配。对于标签或命名空间，您可以选择在规范中包含前面的命名空间和前缀。有关此语句类型的更多信息，请参阅 标签匹配规则语句。

标签的前缀用于定义标签规则的规则组或 Web ACL 的上下文。在规则的标签匹配语句中，如果您的标签或命名空间匹配字符串未指定前缀，则 AWS WAF 使用标签匹配规则的前缀。

- 直接在 Web ACL 中定义的规则的标签具有指定 Web ACL 上下文的前缀。
- 规则组内规则的标签带有指定规则组上下文的前缀。这可以是您自己的规则组，也可以是为您管理的规则组。

有关这方面的信息，请参阅 AWS WAF 标签语法和命名要求 下面的标签语法。

> **Note**
>
> 一些托管规则组会添加标签。您可以调用 `DescribeManagedRuleGroup`，从而通过 API 来检索这些信息。标签列在响应的 `AvailableLabels` 属性中。

如果要匹配与规则上下文不同的上下文中的规则，则必须在匹配字符串中提供前缀。例如，如果要匹配由托管规则组中的规则添加的标签，可以在 Web ACL 中添加一条带有标签匹配语句的规则，其匹配字符串指定规则组的前缀，然后是附加的匹配条件。

在标签匹配语句的匹配字符串中，您可以指定标签或命名空间：

- 标签 – 匹配项的标签规范由标签的结尾部分组成。您可以添加任意数量的连续命名空间，这些命名空间紧接在标签名称之前，其后是名称。您也可以通过以前缀开头的规范来提供完全限定的标签。

  示例规范：

  - `testNS1:testNS2:LabelNameA`

  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- 命名空间 – 匹配项的命名空间规范由标签规范中除名称之外的任意连续子集组成。可以包含前缀，也可以包含一个或多个命名空间字符串。

  示例规范：

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF 标签匹配示例

本节提供标签匹配规则语句的匹配规范示例。

> **Note**
>
> 这些 JSON 列表是在控制台中创建的，方法是向 Web ACL 添加一条带有标签匹配规范的规则，然后编辑规则并切换到规则 JSON 编辑器。您还可以通过 API 或命令行界面获取规则组或 Web ACL 的 JSON。

主题

- 与本地标签匹配
- 与来自其他上下文的标签进行匹配
- 与托管规则组标签匹配
- 与本地命名空间匹配
- 与托管规则组命名空间匹配

与本地标签匹配

以下 JSON 列表显示了与本规则上下文相同的标签匹配语句，该标签添加了到本地 Web 请求中。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
```

```
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

如果您在账户 111122223333 中使用此匹配语句，则在为 Web ACL `testWebACL` 定义的规则中，它将匹配以下标签。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

它与以下标签不匹配，因为标签字符串不完全匹配。

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

它与以下标签不匹配，因为上下文不一样，因此前缀不匹配。即使您将规则组 `productionRules` 添加到定义规则的 Web ACL `testWebACL` 中，也是如此。

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

与来自其他上下文的标签进行匹配

以下 JSON 列表显示了一条标签匹配规则，该规则与用户创建的规则组内规则的标签相匹配。对于 Web ACL 中运行的所有规则（不属于已命名规则组），规范中都要求使用前缀。此示例标签规范仅匹配确切的标签。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
```

```
    ],
    Action: { Block: {} }
}
```

与托管规则组标签匹配

这是一种特殊情况，即与来自另一种上下文的标签进行匹配，而不是与匹配规则的上下文进行匹配。以下 JSON 列表显示了托管规则组标签的标签匹配语句。这仅匹配标签匹配语句的键设置中指定的确切标签。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

与本地命名空间匹配

以下 JSON 列表显示了本地命名空间的标签匹配语句。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

与本地 Label 匹配类似，如果您在账户 111122223333 中使用此语句，在为 Web ACL testWebACL 定义的规则中，它将匹配以下标签。

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

它与以下标签不匹配，因为账户不一样，因此前缀不匹配。

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

该前缀也与托管规则组应用的任何标签都不匹配，如下所示。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

与托管规则组命名空间匹配

以下 JSON 列表显示了托管规则组命名空间的标签匹配语句。对于您拥有的规则组，您还需要提供前缀，以便匹配规则上下文之外的命名空间。

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

此规范与以下示例标签相匹配。

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

它与以下标签不匹配。

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF 智能威胁缓解

本节介绍由提供的托管智能威胁缓解功能 AWS WAF。您可以实施这些高级的专业保护，以防范恶意机器人和账户盗用尝试等威胁。

> **Note**
>
> 除基本使用 AWS WAF费用外，此处描述的功能还会产生额外费用。有关更多信息，请参阅AWS WAF 定价。

本节提供的指南适用于一般了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。

主题

- 智能威胁缓解选项
- 智能威胁缓解的最佳实践
- AWS WAF 网络请求令牌
- AWS WAF 欺诈控制账户创建欺诈预防 (ACFP)
- AWS WAF 防欺诈控制账户接管 (ATP)
- AWS WAF 机器人控制
- AWS WAF 客户端应用程序集成
- CAPTCHA然后Challenge在 AWS WAF

智能威胁缓解选项

本节详细比较了实施智能威胁缓解的选项。

AWS WAF 为智能威胁缓解提供以下类型的保护。

- AWS WAF F@@ raud Control 账户创建防作弊 (ACFP)-检测和管理应用程序注册页面上的恶意账户创建尝试。核心功能由 ACFP 托管规则组提供。有关更多信息，请参阅 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP) 和 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

- AWS WAF Fraud Control 账户盗用预防 (ATP)-检测和管理应用程序登录页面上的恶意接管企图。核心功能由 ATP 托管规则组提供。有关更多信息，请参阅 AWS WAF 防欺诈控制账户接管 (ATP) 和 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。
- AWS WAF 机器人控制-识别、标记和管理友好和恶意的机器人。该功能可管理具有各种应用程序中的唯一签名的普通机器人，也可管理具有特定应用程序签名的定向机器人。核心功能由机器人控制功能托管规则组提供。有关更多信息，请参阅 AWS WAF 机器人控制 和 AWS WAF 机器人控制规则组。
- 客户端应用程序集成 SDK — 验证网页上的客户端会话和最终用户，并获取 AWS WAF 令牌供客户在其 Web 请求中使用。如果您使用 ACFP、ATP 或 机器人控制功能，请尽可能在客户端应用程序中实施应用程序集成软件开发工具包，以充分利用规则组的所有功能。我们只建议在需要快速保护关键资源而又没有足够时间进行软件开发工具包集成时，作为临时措施使用这些未集成软件开发工具包的规则组。有关实施软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。
- Challenge和CAPTCHA规则操作 — 验证客户端会话和最终用户，并获取 AWS WAF 令牌供客户在其 Web 请求中使用。您可以在任何您指定规则操作的地方以及您的规则中实施这些操作，也可以在您使用的规则组中作为替换来实施。这些操作使用 AWS WAF JavaScript 插页式广告来询问客户或最终用户，并且它们需要支持的客户端应用程序。 JavaScript有关更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

智能威胁缓解 AWS 托管规则组 ACFP、ATP 和 Bot Control 使用令牌进行高级检测。有关令牌在规则组中启用的功能的信息，请参阅 为何要在 ACFP 中使用应用程序集成软件开发工具包、为何要在 ATP 中使用应用程序集成软件开发工具包 和 为什么要将应用程序集成软件开发工具包与机器人控制功能配合使用。

实施智能威胁缓解的选项从基本使用规则操作来运行挑战和强制获取令牌，到智能威胁缓解 AWS 托管规则组提供的高级功能。

下表详细比较了基本功能和高级功能的选项。

主题

- 质询和令牌获取
- 智能威胁缓解托管规则组
- 基于速率的规则和定向机器人控制功能规则中的速率限制选项

质询和令牌获取

您可以使用 AWS WAF 应用程序集成 SDK 或规则操作来提供挑战并获取令牌，Challenge以及。CAPTCHA从广义上讲，规则操作更易于实施，但它们会产生额外的成本，更多地干扰您的客户体验，并且需要。 JavaScript这些 SDK 需要在您的客户端应用程序中进行编程，但它们可以提供更好的客户体验，可以免费使用，并且可以与 Android 或 iOS 应用程序一起使用，也可以在 Android JavaScript 或 iOS 应用程序中使用。您只能将应用程序集成软件开发工具包与使用某个付费智能威胁缓解托管规则组的 Web ACL 一起使用，如下一节所述。

质询和令牌获取选项的比较

	Challenge 规则操作	CAPTCHA 规则操作	JavaScript SDK 挑战赛	移动软件开发工具包质询
什么是	规则动作，通过向浏览器客户端提供静默质询插页式广告来强制获取 AWS WAF 令牌	通过向客户端最终用户展示视觉或音频挑战插页式广告来强制获取 AWS WAF 代币的规则操作	应用程序集成层，适用于客户端浏览器和其他执行设备JavaScript。呈现静默质询并获取令牌	应用集成层，适用于 Android 和 iOS 应用程序。原生呈现静默质询并获取令牌
不错的选择……	针对机器人会话进行静默验证，并强制支持支持的客户获取代币 JavaScript	终端用户和针对机器人会话的静默验证，并强制执行令牌获取，适用于支持的客户端 JavaScript	对机器人会话进行静默验证，并对支持的客户强制获取代币 JavaScript。 这些软件开发工具包提供了最低延迟，并且可以最好地控制质询脚本在应用程序中的运行位置。	针对 Android 和 iOS 上的原生移动应用进行静默验证和令牌强制获取。 这些软件开发工具包提供了最低延迟，并且可以最好地控制质询脚本在应用程序中的运行位置。
实施的注意事项	作为规则操作设置实施	作为规则操作设置实施	需要 Web ACL 中的 ACFP、ATP 或机器人控制功	需要 Web ACL 中的 ACFP、ATP 或机器人控制功

	Challenge 规则操作	CAPTCHA 规则操作	JavaScript SDK 挑战赛	移动软件开发工具包质询
			能付费规则组之一。 需要在客户端应用程序中进行编码。	能付费规则组之一。 需要在客户端应用程序中进行编码。
运行时系统注意事项	没有有效令牌的请求的侵入性流。客户被重定向到 AWS WAF 挑战插页式广告。添加网络往返行程，并且需要对 Web 请求进行二次评估。	没有有效令牌的请求的侵入性流。客户端被重定向到 AWS WAF 验证码插页式广告。添加网络往返行程，并且需要对 Web 请求进行二次评估。	可以在幕后运行。让您更好地控制质询体验。	可以在幕后运行。让您更好地控制质询体验。
需要 JavaScript	支持	是	是	不支持
支持的客户端	执行 Javascript 的浏览器和设备	执行 Javascript 的浏览器和设备	执行 Javascript 的浏览器和设备	Android 和 iOS 设备
支持单页应用程序 (SPA)	仅限强制执行。 您可以将 Challenge 操作与软件开发工具包结合使用，以确保请求具有有效的质询令牌。您不能使用规则操作将质询脚本传送到页面。	仅限强制执行。 您可以将 CAPTCHA 操作与软件开发工具包结合使用，以确保请求具有有效的验证码令牌。您不能使用规则操作将验证码脚本传送到页面。	支持	不适用

	Challenge 规则操作	CAPTCHA 规则操作	JavaScript SDK 挑战赛	移动软件开发工具包质询
额外费用	可以，适用于您在定义的规则中或在您使用的规则组中作为规则操作优先级明确指定的操作设置。在所有其他情况下都不是。	可以，适用于您在定义的规则中或在您使用的规则组中作为规则操作优先级明确指定的操作设置。在所有其他情况下都不是。	不需要，但需要付费规则组 ACFP、ATP 或机器人控制功能。	不需要，但需要付费规则组 ACFP、ATP 或机器人控制功能。

有关与这些选项相关的成本的详细信息，请参阅 AWS WAF 定价中的智能威胁缓解信息。

只需添加带有 Challenge 或 CAPTCHA 操作的规则，即可更轻松地运行质询并提供基本的令牌强制执行。例如，如果您无权访问应用程序代码，则可能需要使用规则操作。

但是，与使用 Challenge 操作相比，如果您可以实施软件开发工具包，则可以节省成本并减少客户端 Web 请求的 Web ACL 评估延迟：

- 您可以编写自己的软件开发工具包实施，以便在应用程序中的任何位置运行质询。您可以在后台获取令牌，然后再进行任何会向您的受保护资源发送 Web 请求的客户操作。这样，令牌就可以随客户端的第一个请求一起发送。
- 相反，如果您通过实施带有 Challenge 操作的规则来获取令牌，则在客户端首次发送请求和令牌到期时，规则和操作需要额外的 Web 请求评估和处理。Challenge 操作会阻止不具备有效的未过期令牌的请求，并将质询插页式广告发送回客户端。在客户端成功响应质询后，插页式广告会重新发送包含有效令牌的原始 Web 请求，然后由 Web ACL 对其进行第二次评估。

智能威胁缓解托管规则组

智能威胁缓解 AWS Managed Rules 规则组提供基本机器人管理、检测和缓解复杂的恶意机器人、检测和缓解账户接管企图，以及检测和缓解欺诈性账户创建尝试。这些规则组与上一节中描述的应用程序集成软件开发工具包相结合，可为您的客户端应用程序提供最先进的保护和安全耦合。

托管规则组选项的比较

	ACFP	ATP	机器人控制功能的普通级别	机器人控制功能的目标级别
什么是	在应用程序的注册和登录页面上管理可能属于欺诈账户创建尝试的请求。 不管理机器人。 请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。	管理应用程序登录页面上可能属于恶意盗用尝试一部分的请求。 不管理机器人。 请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。	管理可自我识别的普通机器人，其签名在不同应用中都是唯一的。 请参阅 AWS WAF 机器人控制规则组。	使用特定于应用程序的签名，管理无法自我识别的定向机器人。 请参阅 AWS WAF 机器人控制规则组。
不错的选择……	检查账户创建流量是否存在欺诈账户创建攻击，例如通过用户名遍历和从单个 IP 地址创建许多新账户的尝试进行攻击。	检查登录流量是否存在账户盗用攻击，例如使用密码遍历的登录尝试和来自同一 IP 地址的多次登录尝试。与令牌一起使用时，还可以提供聚合保护，例如 IP 的速率限制和针对大量失败登录尝试的客户端会话。	基本机器人保护和普通自动机器人流量标记。	针对复杂机器人的目标保护，包括客户端会话级别的速率限制以及浏览器自动化工具（例如 Selenium 和 Puppeteer）的检测和缓解。
添加表示评估结果的标签	支持	是	是	支持
添加令牌标签	支持	是	是	支持
阻止没有有效令牌的请求	不包括。	不包括。	不包括。	阻止在没有令牌的情况下发送 5

	ACFP	ATP	机器人控制功能的普通级别	机器人控制功能的目标级别
	请参阅 阻止没有有效 AWS WAF 令牌的请求。	请参阅 阻止没有有效 AWS WAF 令牌的请求。	请参阅 阻止没有有效 AWS WAF 令牌的请求。	个请求的客户端会话。
需要代 AWS WAF 币 `aws-waf-token`	要求所有规则。 请参阅 为何要在 ACFP 中使用应用程序集成软件开发工具包。	要求许多规则。 请参阅 为何要在 ATP 中使用应用程序集成软件开发工具包。	不支持	支持
获取代币 AWS WAF `aws-waf-token`	是的，由规则 `AllRequests` 强制执行	不支持	不支持	一些规则使用 Challenge 或 CAPTCHA 规则操作来获取令牌。

有关与这些选项相关的成本的详细信息，请参阅 AWS WAF 定价中的智能威胁缓解信息。

基于速率的规则和定向机器人控制功能规则中的速率限制选项

AWS WAF 机器人控制规则组的目标级别和 AWS WAF 基于速率的规则语句都提供 Web 请求速率限制。下表比较了这两个选项。

基于速率的检测和缓解选项的比较

	AWS WAF 基于费率的规则	AWS WAF 机器人控制目标规则	
如何应用速率限制	对速率过高的一组请求采取行动。您可以应用除之外的任何操作Allow。	通过使用请求令牌强制执行类似人类的访问模式并应用动态速率限制。	
基于历史流量基线？	不支持	支持	

	AWS WAF 基于费率的规则	AWS WAF 机器人控制目标规则	
累积历史流量基线所需的时间	不适用	动态阈值需要五分钟。对于缺少令牌，不适用。	
缓解延迟	通常是 30-50 秒。最多可能需要几分钟。	通常不到 10 秒。最多可能需要几分钟。	
缓解目标	可配置。您可以使用范围缩小语句和一个或多个聚合键（例如 IP 地址、HTTP 方法和查询字符串）对请求进行分组。	IP 地址和客户端会话	
触发缓解所需的流量级别	中-在指定的时间窗口内可以低至 100 个请求	低 – 旨在检测客户端模式，例如慢速抓取器	
可自定义的阈值	支持	不支持	
默认缓解操作	控制台默认值为 Block。API 中没有默认设置；该设置是必需的。 您可以将其设置为除之外的任何规则操作 Allow。	规则组规则操作设置为 Challenge（不使用令牌）和 CAPTCHA（来自单个客户端会话的大流量）。 您可以将其中任一规则设置为任何有效的规则操作。	
抵御高度分布式攻击的弹性	中-最多 10,000 个 IP 地址用于单独限制 IP 地址	中 – IP 地址和令牌之间的总数限制为 50,000	

	AWS WAF 基于费率的规则	AWS WAF 机器人控制目标规则	
AWS WAF 定价	包含在的标准费用中 AWS WAF。	包含在 Bot Control 智能威胁缓解目标级别的费用中。	
有关更多信息	基于速率的规则语句	AWS WAF 机器人控制规则组	

智能威胁缓解的最佳实践

请遵循本节中的最佳实践，以最有效、最具成本效益的方式实施智能威胁缓解功能。

- 实施 JavaScript 和移动应用程序集成 SDK — 实施应用程序集成，以尽可能有效的方式启用全套 ACFP、ATP 或 Bot Control 功能。托管规则组使用软件开发工具包提供的令牌在会话级别将合法的客户端流量与不需要的流量区分开来。应用程序集成软件开发工具包可确保这些令牌始终可用。有关详细信息，请参阅：
  - 为何要在 ACFP 中使用应用程序集成软件开发工具包
  - 为何要在 ATP 中使用应用程序集成软件开发工具包
  - 为什么要将应用程序集成软件开发工具包与机器人控制功能配合使用

  使用集成在您的客户端中实现挑战，并自定义向最终用户展示验证码拼图的方式。 JavaScript有关更多信息，请参阅 AWS WAF 客户端应用程序集成。

  如果您使用 JavaScript API 自定义验证码谜题，并且在网页 ACL 中的任何位置使用CAPTCHA规则操作，请按照客户端中处理 AWS WAF 验证码响应的指南进行操作，网址为。处理来自的验证码响应 AWS WAF本指南适用于使用该 CAPTCHA 操作的任何规则，包括 ACFP 托管规则组中的规则和机器人控制功能托管规则组的目标保护级别。
- 限制您发送到 ACFP、ATP 和 Bot Control 规则组的请求 — 使用智能威胁缓解 AWS 托管规则组会产生额外费用。ACFP 规则组检查向您指定的账户注册和创建端点发出的请求。ATP 规则组检查发往您指定的登录端点的请求。机器人控制功能规则组会在 Web ACL 评估中检查到达它的每个请求。

  请考虑以下方法来减少对这些规则组的使用：
  - 使用托管规则组语句中的范围缩小语句将请求排除在检查范围之外。您可以用任何可嵌套的语句来做到这一点。有关信息，请参阅 范围缩小语句。

  - 通过在规则组之前添加规则，将请求排除在检查范围之外。对于不能在范围缩小语句中使用的规则以及更复杂的情况（例如标签后进行标签匹配），您可能需要添加在规则组之前运行的规则。有关信息，请参阅范围缩小语句和规则语句基础知识。
  - 按照成本较低的规则运行规则组。如果您有其他标准 AWS WAF 规则出于任何原因阻止请求，请在这些付费规则组之前运行它们。有关规则和规则管理的更多信息，请参阅 规则语句基础知识。
  - 如果您使用多个智能威胁缓解托管规则组，请按以下顺序运行这些规则组以降低成本：机器人控制功能、ATP、ACFP。

  有关详细定价信息，请参阅 AWS WAF 定价。

- 在正常 Web 流量期间启用机器人控制功能规则组的目标保护级别 – 某些目标保护级别的规则需要一段时间来建立正常流量模式的基准，然后才能识别和响应不规则或恶意的流量模式。例如，`TGT_ML_*` 规则最长需要 24 小时才能预热。

  当您没有遇到攻击时，可以添加这些保护，让他们有时间确定基准，然后再期望他们对攻击做出适当的反应。如果您在攻击期间添加这些规则，则在攻击消退后，由于攻击流量会增加偏差，因此建立基准的时间通常是正常所需时间的两倍到三倍。有关规则及其所需的任何预热时间的更多信息，请参阅规则列表。

- 要获得分布式拒绝服务 (DDoS) 防护，请使用 Shield Advanced 自动应用程序层 DDoS 缓解 – 智能威胁缓解规则组不提供 DDoS 保护。ACFP 可防止有人尝试在您的应用程序的注册页面上创建欺诈账户。ATP 可防止有人企图盗用您的登录页面。机器人控制功能侧重于使用令牌强制执行类似人类的访问模式，并对客户端会话进行动态速率限制。

  当你使用启用了自动应用层 DDoS 缓解功能的 Shield Advanced 时，Shield Advanced 会通过代表你创建、评估和部署自定义 AWS WAF 缓解措施来自动响应检测到的 DDoS 攻击。有关 Shield Advanced 的更多信息，请参阅 AWS Shield Advanced 概述 和 AWS Shield Advanced 应用层（第 7 层）保护。

- 调整和配置令牌处理 – 调整 Web ACL 的令牌处理以获得最佳用户体验。
  - 要降低运营成本并改善最终用户的体验，请将令牌管理免疫时间调整为安全要求允许的最长时间。这样可以最大限度地减少使用验证码拼图和静默质询。有关信息，请参阅 时间戳过期： AWS WAF 代币免疫时间。
  - 要在受保护的应用程序之间启用令牌共享，请为您的 Web ACL 配置令牌域列表。有关信息，请参阅 AWS WAF 令牌域和域名列表。

- 拒绝具有任意主机规格的请求 – 将您的受保护资源配置为要求 Web 请求中的 `Host` 标头与目标资源匹配。您可以接受一个值或一组特定的值，例如 `myExampleHost.com` 和 `www.myExampleHost.com`，但不接受主机的任意值。

- 对于作为 CloudFront 分配来源的应用程序负载均衡器，请配置 CloudFront 并 AWS WAF 进行适当的令牌处理 — 如果您将 Web ACL 关联到应用程序负载均衡器，并将应用程序负载均衡器部署为 CloudFront 分配的源，请参阅作为来源的应用程序负载均衡器的必需配置 CloudFront 。
- 部署前进行测试和调整 – 在对 Web ACL 进行任何更改之前，请按照本指南中的测试和调整程序进行操作，以确保获得预期的行为。这对于这些付费功能特别重要。有关一般指导，请参阅 测试和调整您的 AWS WAF 保护措施。有关付费托管规则组的特定信息，请参阅 测试和部署 ACFP、测试和部署 ATP 和 测试和部署 AWS WAF 机器人控制。

AWS WAF 网络请求令牌

AWS WAF 代币是 AWS WAF 智能威胁缓解提供的增强保护不可或缺的一部分。令牌（有时也称为指纹）是有关单个客户端会话的信息的集合，客户端会话存储并随其发送的每个 Web 请求一起提供。AWS WAF 使用令牌识别恶意客户端会话并将其与合法会话区分开来，即使两者都来自单个 IP 地址。使用令牌给合法用户带来的成本可以忽略不计，但对于僵尸网络来说，大规模使用令牌的成本却很高。

AWS WAF 使用令牌来支持其浏览器和最终用户质询功能，该功能由应用程序集成 SDK 和规则操作 Challenge提供。CAPTCHA此外，令牌还支持 AWS WAF 机器人控制和账户盗用防护托管规则组的功能。

AWS WAF 为成功应对无声挑战和验证码难题的客户创建、更新和加密令牌。当拥有令牌的客户端发送 Web 请求时，它会包含加密的令牌，并 AWS WAF 解密令牌并验证其内容。

主题

- 如何 AWS WAF 使用代币
- AWS WAF 代币特征
- 时间戳过期： AWS WAF 代币免疫时间
- AWS WAF 令牌域和域名列表
- AWS WAF 由机器人和欺诈管理的规则组进行代币标记
- 阻止没有有效 AWS WAF 令牌的请求
- 作为来源的应用程序负载均衡器的必需配置 CloudFront

如何 AWS WAF 使用代币

AWS WAF 使用令牌来记录和验证以下类型的客户端会话验证：

- 验证码 – 验证码拼图有助于区分机器人和人类用户。验证码只能通过 CAPTCHA 规则操作运行。成功完成拼图后，验证码脚本会更新令牌的验证码时间戳。有关更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。
- 质询 – 质询以静默方式运行，以帮助区分常规客户端会话和机器人会话，并提高机器人的操作成本。挑战成功完成后，挑战脚本会根据需要自动从中 AWS WAF 获取新代币，然后更新代币的挑战时间戳。

  AWS WAF 在以下情况下运行挑战：

  - 应用程序集成软件开发工具包 – 应用程序集成软件开发工具包在您的客户端应用程序会话中运行，有助于确保只在客户端成功响应质询后才允许尝试登录。有关更多信息，请参阅 AWS WAF 客户端应用程序集成。
  - Challenge 规则操作 – 更多信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。
  - CAPTCHA – 当验证码插页式广告运行时，如果客户端还没有令牌，则脚本会自动先运行质询，以验证客户端会话并初始化令牌。

智能威胁 AWS 托管规则组中的许多规则都需要令牌。这些规则使用标记来区分会话级别的客户端、确定浏览器特征以及了解应用网页上的人机交互程度。这些规则组调用 AWS WAF 令牌管理，令牌管理应用令牌标签，然后规则组会检查这些标签。

- AWS WAF F@@ raud Control 账户创建防作弊 (ACFP) — ACFP 规则要求使用有效令牌进行网络请求。有关规则的更多信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。
- AWS WAF Fraud Control 账户接管预防 (ATP) — 防止大量和长期客户会话的 ATP 规则要求网络请求必须具有有效令牌和未过期的质询时间戳。有关更多信息，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。
- AWS WAF Bot Control — 此规则组中的目标规则限制了客户端在没有有效令牌的情况下可以发送的 Web 请求的数量，它们使用令牌会话跟踪进行会话级别的监控和管理。根据需要，这些规则应用 Challenge 和 CAPTCHA 规则操作来强制执行令牌获取和有效的客户行为。有关更多信息，请参阅 AWS WAF 机器人控制规则组。

AWS WAF 代币特征

每个令牌都具有以下特性：

- 令牌存储在名为 `aws-waf-token` 的 Cookie 中。
- 令牌已加密。

- 该令牌使用包含以下信息的粘性粒度标识符对客户端会话进行指纹识别：
  - 客户端最近一次成功响应静默质询的时间戳。
  - 最终用户最近一次成功响应验证码的时间戳。仅当您在保护中使用验证码时，才会出现这种情况。
  - 有关客户端和客户端行为的其他信息，可帮助将合法客户端与不想要的流量区分开来。这些信息包括可用于检测自动活动的各种客户端标识符和客户端信号。收集的信息不是唯一的，无法映射到个体上。
    - 所有令牌都包含来自客户端浏览器查询的数据，例如自动化和浏览器设置不一致的迹象。此信息由 Challenge 操作运行的脚本和客户端应用程序软件开发工具包检索。脚本会主动询问浏览器并将结果放入令牌中。
    - 此外，在实施客户端应用程序集成软件开发工具包时，令牌包括被动收集的有关最终用户与应用程序页面交互的信息。交互包括鼠标移动、按键以及与页面上存在的任何 HTML 表单的交互。这些信息有助于 AWS WAF 检测客户端中的人机交互程度，以质询看似不是人类的用户。有关客户端集成的更多信息，请参阅 AWS WAF 客户端应用程序集成。

出于安全考虑， AWS 未提供对 AWS WAF 令牌内容的完整描述或有关令牌加密过程的详细信息。

时间戳过期： AWS WAF 代币免疫时间

AWS WAF 使用质询和 CAPTCHA 免疫时间来控制向单个客户会话提出质询或 CAPTCHA 的频率。在最终用户成功响应验证码后，验证码免疫时间决定了最终用户在多长时间内不再受其他验证码的影响。同样，质询免疫时间决定了客户端会话在成功响应质询后多长时间内不再受到质询。

AWS WAF 通过更新令牌内的相应时间戳来记录对质询或 CAPTCHA 的成功响应。当 AWS WAF 检查代币是否存在挑战或验证码时，它会从当前时间中减去时间戳。如果结果大于配置的免疫时间，则时间戳过期。

您可以在 Web ACL 以及任何使用 CAPTCHA 或 Challenge 规则操作的规则中配置质询和验证码免疫时间。

- 这两项免疫时间的默认 Web ACL 设置均为 300 秒。
- 您可以为任何使用 CAPTCHA 或 Challenge 操作的规则指定免疫时间。如果您未为规则指定免疫时间，则规则将从 Web ACL 继承设置。
- 对于规则组中使用 CAPTCHA 或 Challenge 操作的规则，如果您没有为该规则指定免疫时间，则它将继承您使用该规则组的每个 Web ACL 的设置。
- 应用程序集成软件开发工具包使用 Web ACL 的质询免疫时间。

质询免疫时间的最小值为 300 秒。验证码免疫时间的最小值为 60 秒。两项免疫时间的最大值均为 259,200 秒，即三天。

您可以使用 Web ACL 和规则级别免疫时间设置来调整 CAPTCHA 操作 Challenge 或软件开发工具包质询管理行为。例如，您可以配置规则，控制对免疫时间较低的高度敏感数据的访问，然后在 Web ACL 中设置较高免疫时间，供其他规则和软件开发工具包继承。

特别是对于验证码来说，解答拼图问题会降低客户的网站体验，因此调整验证码免疫时间可以帮助您减轻对客户体验的影响，同时仍能提供您想要的保护。

有关调整免疫时间以使用 Challenge 和 CAPTCHA 规则操作的更多信息，请参阅 使用 CAPTCHA 和 Challenge 操作的最佳实践。

在哪里设置代 AWS WAF 币免疫时间

您可以在 Web ACL 以及使用 Challenge 和 CAPTCHA 规则操作的规则中设置免疫时间。

有关管理 Web ACL 及其规则的一般信息，请参阅 使用 Web ACL。

在何处设置 Web ACL 的免疫时间

- 控制台 – 编辑 Web ACL 时，在规则选项卡中，编辑和更改 Web ACL 验证码配置和 Web ACL 质询配置窗格中的设置。在控制台中，只有在创建 Web ACL 之后，您才能配置 Web ACL 验证码和质询免疫时间。
- 在控制台之外 – Web ACL 数据类型具有验证码和质询配置参数，您可以配置这些参数并将其提供给 Web ACL 上的创建和更新操作。

在何处设置规则的免疫时间

- 控制台 – 当您创建或编辑规则并指定 CAPTCHA 或 Challenge 操作时，可以修改该规则的免疫时间设置。
- 在控制台之外 – 规则数据类型具有验证码和质询配置参数，您可以在定义规则时对其进行配置。

AWS WAF 令牌域和域名列表

在为客户端 AWS WAF 创建令牌时，它会使用令牌域对其进行配置。在 AWS WAF 检查 Web 请求中的令牌时，如果该令牌的域与任何被认为对 Web ACL 有效的域都不匹配，则会将该令牌视为无效因而拒绝。

默认情况下， AWS WAF 仅接受其域设置与与 Web ACL 关联的资源的主机域完全匹配的令牌。这是 Web 请求中的 `Host` 标头的值。在浏览器中，您可以在 JavaScript `window.location.hostname`属性中找到该域名，也可以在用户在地址栏中看到的地址中找到该域名。

您还可以在您的 Web ACL 配置中指定可接受的令牌域，如下一节所述。在这种情况下， AWS WAF 接受与主机标头的精确匹配项和与令牌域列表中的域名匹配。

您可以指定令牌域 AWS WAF ，以便在设置域和评估 Web ACL 中的令牌时使用。您指定的域名不能是公共后缀，例如 `gov.au`。对于您无法使用的域名，请参阅公共后缀列表下的列表 https://publicsuffix.org/list/public_suffix_list.dat。

AWS WAF Web ACL 令牌域列表配置

您可以将 Web ACL 配置为在多个受保护资源之间共享令牌，方法是提供包含您 AWS WAF 要接受的其他域的令牌域列表。使用令牌域列表时， AWS WAF 仍然接受资源的主机域。此外，它接受令牌域列表中的所有域，包括其前缀子域。

例如，令牌域列表 `example.com` 中的域名规范与 `example.com`（来自 `http://example.com/`）、`api.example.com`（来自 `http://api.example.com/`）和 `www.example.com`（来自 `http://www.example.com/`）匹配。它与 `example.api.com`（来自 `http://example.api.com/`）或 `apiexample.com`（来自 `http://apiexample.com/`）不匹配。

创建或编辑令牌域列表时，可以在 Web ACL 中对其进行配置。有关管理 Web ACL 的一般信息，请参阅 使用 Web ACL。

AWS WAF 令牌域设置

AWS WAF 应质询脚本的请求创建令牌，这些脚本由应用程序集成 SDK 以及Challenge和CAPTCHA规则操作运行。

在令牌中 AWS WAF 设置的域名由请求令牌的质询脚本的类型以及您提供的任何其他令牌域配置决定。 AWS WAF 将令牌中的域设置为它可以在配置中找到的最短、最通用的设置。

- JavaScript SDK — 您可以使用令牌域规范配置 JavaScript SDK，该规范可以包含一个或多个域。根据受保护的主机域和 Web ACL 的 AWS WAF 令牌域列表，您配置的域必须是可以接受的域。

  当为客户端 AWS WAF 发放令牌时，它会将令牌域设置为与主机域匹配的令牌域，并且是主机域和配置列表中域中最短的令牌域。例如，如果主机域是，`api.example.com`而令牌域列表有`example.com`，则`example.com`在令牌中 AWS WAF 使用，因为它与主机域匹配并且更短。

如果您未在 JavaScript API 配置中提供令牌域列表，请 AWS WAF 将该域设置为受保护资源的主机域。

有关更多信息，请参阅 提供用于令牌的域名。

- 移动软件开发工具包 – 在应用程序代码中，必须使用令牌域属性配置移动软件开发工具包。根据受保护的主机域和 Web ACL 的令牌域列表，此属性必须是 AWS WAF 可以接受的域。

  当为客户端 AWS WAF 发放令牌时，它会使用此属性作为令牌域。 AWS WAF 在为移动 SDK 客户端发放的令牌中不使用主机域。

  有关更多信息，请参阅 移 AWS WAF 动 SDK 规范 的 `WAFConfiguration` `domainName` 设置。
- Challengeacti@@ on — 如果您在 Web ACL 中指定令牌域列表，则将令牌域 AWS WAF 设置为与主机域匹配且最短的令牌域，即主机域和列表中的域中最短的令牌域。例如，如果主机域是，`api.example.com`而令牌域列表有`example.com`，则`example.com`在令牌中 AWS WAF 使用，因为它与主机域匹配并且更短。如果您未在 Web ACL 中提供令牌域列表，请 AWS WAF 将该域设置为受保护资源的主机域。

AWS WAF 由机器人和欺诈管理的规则组进行代币标记

本节介绍令 AWS WAF 牌管理向 Web 请求添加的标签。有关标签的一般信息，请参见AWS WAF 网络请求上的标签。

当您使用任何 AWS WAF 机器人或欺诈控制托管规则组时，规则组使用 AWS WAF 令牌管理来检查 Web 请求令牌并对请求应用令牌标签。有关托管规则组的信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组、AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 和 AWS WAF 机器人控制规则组。

> **Note**
>
> AWS WAF 仅当您使用这些智能威胁缓解托管规则组之一时，才会应用令牌标签。

令牌管理可以将以下标签添加到 Web 请求中。

客户端会话标签

该标签`awswaf:managed:token:id:`*`identifier`*包含一个唯一标识符， AWS WAF 令牌管理使用该标识符来识别客户端会话。如果客户端获取了新令牌，例如在丢弃其正在使用的令牌之后，标识符可能会更改。

> **Note**
>
> AWS WAF 不报告该标签的 Amazon CloudWatch 指标。

令牌状态标签：标签命名空间前缀

令牌状态标签报告令牌的状态、质询以及其中包含的 CAPTCHA 信息。

每个令牌状态标签都以下列命名空间前缀之一开头：

- `awswaf:managed:token:` – 用于报告令牌的一般状态以及令牌的质询信息的状态。
- `awswaf:managed:captcha:` – 用于报告令牌的 CAPTCHA 信息的状态。

令牌状态标签：标签名称

在前缀之后，标签的其余部分提供详细的令牌状态信息：

- `accepted` – 请求令牌存在且包含以下内容：
  - 有效的质询或 CAPTCHA 解决方案。
  - 未过期的质询或 CAPTCHA 时间戳。
  - 对 Web ACL 有效的域规范。

  示例：标签 `awswaf:managed:token:accepted` 表明 Web 请求的令牌具有有效的质询解决方案、未过期的质询时间戳以及有效的域。
- `rejected` – 请求令牌存在但不符合接受标准。

  除了被拒绝的标签外，令牌管理还添加了一个自定义标签命名空间和名称来指示原因。
  - `rejected:not_solved` – 令牌缺少质询或 CAPTCHA 解决方案。
  - `rejected:expired` – 根据您的 Web ACL 配置的令牌免疫时间，令牌的质询或 CAPTCHA 时间戳已过期。
  - `rejected:domain_mismatch` – 令牌的域与您的 Web ACL 的令牌域配置不匹配。
  - `rejected:invalid`— AWS WAF 无法读取指示的标记。

  示例：标签 `awswaf:managed:captcha:rejected` 和 `awswaf:managed:captcha:rejected:expired` 表示请求被拒绝，因为令牌中的 CAPTCHA 时间戳已超过 Web ACL 中配置的 CAPTCHA 令牌免疫时间。

- `absent` – 请求没有令牌，或者令牌管理器无法读取它。

  示例：标签 `awswaf:managed:captcha:absent` 表示请求没有令牌。

阻止没有有效 AWS WAF 令牌的请求

当您使用智能威胁 AWS 托管规则组`AWSManagedRulesACFPRuleSet`、`AWSManagedRulesATPRuleSet`和`AWSManagedRulesBotControlRul`时，规则组会调用 AWS WAF 令牌管理来评估 Web 请求令牌的状态并相应地标记请求。

> **Note**
>
> 令牌标签仅适用于您使用其中一个托管规则组评估的 Web 请求。

有关令牌管理应用的标签的信息，请参阅前面的部分 AWS WAF 由机器人和欺诈管理的规则组进行代币标记。

然后，智能威胁缓解托管规则组按如下方式处理令牌要求：

- 该 `AWSManagedRulesACFPRuleSet` `AllRequests` 规则配置为对所有请求运行 Challenge 操作，从而有效地阻止任何没有 `accepted` 令牌标签的请求。
- `AWSManagedRulesATPRuleSet` 会阻止带有 `rejected` 令牌标签的请求，但不会阻止带有 `absent` 令牌标签的请求。
- 在客户端发送五个没有 `accepted` 令牌标签的请求后，`AWSManagedRulesBotControlRuleSet` 目标保护级别会向他们提出质询。它不会阻止没有有效令牌的单个请求。规则组的通用保护级别不管理令牌要求。

有关智能威胁规则组的其他详细信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组、AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 和 AWS WAF 机器人控制规则组。

使用机器人控制功能或 ATP 托管规则组时阻止缺少令牌的请求

使用机器人控制功能和 ATP 规则组时，没有有效令牌的请求可以退出规则组评估并继续由 Web ACL 进行评估。

要阻止所有缺少令牌或令牌被拒绝的请求，请添加一条规则，使其在托管规则组之后立即运行，以捕获并阻止该规则组未处理的请求。

以下是使用 ATP 托管规则组的 Web ACL 的 JSON 列表示例。Web ACL 添加了一条规则，用于捕获 awswaf:managed:token:absent 标签并对其进行处理。该规则将其评估范围缩小到发送到登录端点的 Web 请求，以匹配 ATP 规则组的范围。添加的规则以粗体列出。

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
                      200
                    ],
                    "FailureCodes": [
                      401,
                      403,
                      500
```

```
                    ]
                  }
                }
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesATPRuleSet"
      }
    },
    {
      "Name": "RequireTokenForLogins",
      "Priority": 2,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "Statement": {
                "LabelMatchStatement": {
                  "Scope": "LABEL",
                  "Key": "awswaf:managed:token:absent"
                }
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "/web/login",
                "FieldToMatch": {
                  "UriPath": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "STARTS_WITH"
```

```
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "POST",
              "FieldToMatch": {
                "Method": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "EXACTLY"
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "RequireTokenForLogins"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "exampleWebACL"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
}
```

作为来源的应用程序负载均衡器的必需配置 CloudFront

如果您将 Web ACL 关联到应用程序负载均衡器，并将应用程序负载均衡器部署为 CloudFront 分配的来源，请阅读本节。

使用此架构，您需要提供以下额外配置才能正确处理令牌信息。

- 配置为将 `aws-waf-token` Cookie 转发 CloudFront 到 Application Load Balancer。默认情况下， CloudFront 会先从网络请求中删除 Cookie，然后再将其转发到源。要在网络请求中保留令牌 cookie，请将 CloudFront 缓存行为配置为仅包含令牌 cookie 或所有 Cookie。有关如何执行此操作的信息，请参阅《亚马逊 CloudFront开发者指南》中的基于 Cookie 缓存内容。
- 进行配置， AWS WAF 使其将 CloudFront分配的域识别为有效的令牌域。默认情况下， CloudFront 将`Host`标头设置为 Application Load Balan AWS WAF cer 来源，并将其用作受保护资源的域。但是，客户端浏览器将 CloudFront分配视为主机域，而为客户端生成的令牌使用该 CloudFront 域作为令牌域。如果不进行任何其他配置，当根据令牌域 AWS WAF 检查受保护的资源域时，它将出现不匹配的情况。要解决此问题，请将 CloudFront 分发域名添加到 Web ACL 配置中的令牌域列表中。有关如何执行此操作的信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

AWS WAF 欺诈控制账户创建欺诈预防 (ACFP)

账户创建欺诈是一种在线非法活动，攻击者试图创建一个或多个虚假账户。攻击者使用虚假账户进行欺诈活动，例如滥用促销和注册奖金、冒充他人以及网络攻击（例如网络钓鱼）。虚假账户的存在会损害您在客户中的声誉并面临财务欺诈，从而对您的业务产生负面影响。

您可以通过实施 Fraud Control 账户创建防作 AWS WAF 弊 (ACFP) 功能来监控和控制账户创建欺诈企图。 AWS WAF 在 AWS 托管规则组中提供此功能`AWSManagedRulesACFPRuleSet`以及配套的应用程序集成 SDK。

ACFP 托管规则组标记并管理可能属于恶意账户创建尝试一部分的请求。规则组通过检查客户端发送到账户登录端点的账户创建尝试来实现此目的。

ACFP 通过监控账户注册请求中是否存在异常活动以及自动阻止可疑请求来保护您的账户注册页面。规则组使用请求标识符、行为分析和机器学习来检测欺诈性请求。

- 请求检查 – ACFP 可让您查看和控制异常账户创建尝试和使用被盗凭证的尝试，以防止创建欺诈账户。ACFP 根据被盗凭证数据库检查电子邮件和密码组合，当在暗网上发现新的泄露凭证时，会定期更新。ACFP 评估电子邮件地址中使用的域名，并监控电话号码和地址字段的使用情况，以验证条目并检测欺诈行为。ACFP 按 IP 地址和客户端会话汇总数据，以检测和阻止发送过多可疑请求的客户端。

- 响应检查 — 对于 CloudFront 分配，除了检查传入的账户创建请求外，ACFP 规则组还会检查您的应用程序对账户创建尝试的响应，以跟踪成功率和失败率。利用这些信息，ACFP 可以暂时阻止尝试失败次数过多的客户端会话或 IP 地址。 AWS WAF 异步执行响应检查，因此这不会增加 Web 流量的延迟。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

> **Note**
>
> ACFP 功能不适用于 Amazon Cognito 用户群体。

主题

ACFP 组件

F AWS WAF raud Control 账户创建防作弊 (ACFP) 的主要组成部分如下：

- **`AWSManagedRulesACFPRuleSet`**— 此 AWS 托管规则组中的规则可检测、标记和处理各种类型的欺诈性账户创建活动。规则组检查客户端发送到指定账户注册端点的 HTTP GET 文本/html 请求以及客户端发送到指定账户注册端点的 POST Web 请求。对于受保护的 CloudFront 分配，规则组还会检查分配向账户创建请求发回的响应。有关此规则组的规则列表，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。您可以使用托管规则组参考语句将此规则组包含在 Web ACL 中。有关使用规则组的信息，请参阅 将 ACFP 托管规则组添加到您的 Web ACL。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

- 有关您的应用程序的账户注册和创建页面的详细信息 – 将 `AWSManagedRulesACFPRuleSet` 规则组添加到 Web ACL 时，您必须提供有关您的账户注册和创建页面的信息。这允许规则组缩小其检查的请求范围，并正确验证账户创建 Web 请求。注册页面必须接受 `GET` 文本/html 请求。账户创建路径必须接受 `POST` 请求。ACFP 规则组使用电子邮件格式的用户名。有关更多信息，请参阅 将 ACFP 托管规则组添加到您的 Web ACL。
- 对于受保护的 CloudFront 分配，有关您的应用程序如何响应账户创建尝试的详细信息 — 您可以提供有关您的应用程序对账户创建尝试的响应的详细信息，ACFP 规则组会跟踪和管理来自单个 IP 地址或单个客户端会话的批量账户创建尝试。有关配置此选项的信息，请参阅 将 ACFP 托管规则组添加到您的 Web ACL。
- JavaScript 和移动应用程序集成 SDK — 在 ACFP 实施中实现 AWS WAF JavaScript 和移动 SDK，以启用规则组提供的全套功能。许多 ACFP 规则使用软件开发工具包提供的信息进行会话级别的客户端验证和行为聚合，这是区分合法客户端流量和机器人流量所必需的。有关 SDK 的更多信息，请参阅 AWS WAF 客户端应用程序集成。

您可以将 ACFP 实施与以下实施相结合，以帮助您监控、调整和自定义保护。

- 日志和指标 — 您可以通过配置和启用日志、Amazon Security Lake 数据收集以及您的 Web ACL 的亚马逊 CloudWatch 指标，监控您的流量，并了解 ACFP 托管规则组如何影响流量。`AWSManagedRulesACFPRuleSet`添加到您的 Web 请求中的标签包含在数据中。有关这些选项的信息，请参阅记录 AWS WAF Web ACL 流量使用 Amazon 进行监控 CloudWatch、和什么是 Amazon Security Lake？ 。

  根据您的需求和看到的流量，您可能需要自定义您的 `AWSManagedRulesACFPRuleSet` 实施。例如，您可能想将某些流量排除在ACFP评估之外，或者您可能想使用范围缩小声明或标签匹配规则等 AWS WAF 功能，更改其处理其识别的某些帐户创建欺诈企图的方式。
- 标签和标签匹配规则 – 对于 `AWSManagedRulesACFPRuleSet` 中的任何规则，您可以将阻止行为切换为计数，然后与规则添加的标签进行匹配。使用此方法自定义如何处理由 ACFP 托管规则组标识的 Web 请求。有关标记和使用标签匹配语句的更多信息，请参见 标签匹配规则语句 和 AWS WAF 网络请求上的标签。

- 自定义请求和响应 – 您可以在允许的请求中添加自定义标头，也可以为被阻止的请求发送自定义响应。为此，您需要将匹配的标签与 AWS WAF 自定义请求和响应功能配对。有关请求和响应格式的更多信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

为何要在 ACFP 中使用应用程序集成软件开发工具包

我们强烈建议实施应用程序集成软件开发工具包，以便最有效地使用 ACFP 规则组。

- 完整的规则组功能 – ACFP 规则 `SignalClientHumanInteractivityAbsentLow` 仅适用于由应用程序集成填充的令牌。该规则检测并管理与应用程序页面的异常人机交互。应用程序集成软件开发工具包可以通过鼠标移动、按键和其他方法来检测正常的人机交互。由规则操作 CAPTCHA 和 Challenge 发送但无法提供此类数据的插页式广告。
- 减少延迟 – 规则组规则 `AllRequests` 将 Challenge 规则操作应用于任何还没有质询令牌的请求。发生这种情况时，规则组会对请求进行两次评估：一次没有令牌，另一次是在通过 Challenge 操作插页式广告获取令牌之后。仅使用 `AllRequests` 规则不会向您收取任何额外费用，但是这种方法会增加您的 Web 流量开销，并增加最终用户体验的延迟。如果您使用应用程序集成在客户端获取令牌，则在发送账户创建请求之前，ACFP 规则组会对请求进行一次评估。

有关这些功能的更多信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

有关软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关 AWS WAF 令牌的信息，请参阅AWS WAF 网络请求令牌。有关规则操作的信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

将 ACFP 托管规则组添加到您的 Web ACL

要将 ACFP 托管规则组配置为识别 Web 流量中的账户创建欺诈活动，您需要提供有关客户端如何访问您的注册页面以及如何向您的应用程序发送账户创建请求的信息。对于受保护的 Amazon CloudFront 分配，您还需要提供有关您的应用程序如何响应账户创建请求的信息。此配置是对托管规则组的常规配置的补充。

有关规则组的描述和规则列表，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

> **Note**
>
> ACFP 被盗凭证数据库仅包含电子邮件格式的用户名。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。有关如何将托管规则组添加到 Web ACL 的基本信息，请参阅 通过控制台向 Web ACL 添加托管规则组。

遵循最佳实践

按照 智能威胁缓解的最佳实践 中的最佳实践使用 ACFP 规则组。

在 Web ACL 中使用 **`AWSManagedRulesACFPRuleSet`** 规则组

1. 将 AWS 托管规则组`AWSManagedRulesACFPRuleSet`添加到您的 Web ACL 中，然后在保存之前编辑规则组设置。

   > **Note**
   >
   > 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

2. 在规则组配置窗格中，提供 ACFP 规则组用于检查账户创建请求的信息。

   a. 对于 “在路径中使用正则表达式”，如果您 AWS WAF 想对注册和账户创建页面路径规范执行正则表达式匹配，请将其选中。

      AWS WAF 支持 PCRE 库使用的模式语法，但`libpcre`有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

   b. 对于注册页面路径，请提供应用程序的注册页面端点路径。此页面必须接受 GET 文本/html 请求。规则组仅检查发往您指定的注册页面端点的 HTTP GET 文本/html 请求。

      > **Note**
      >
      > 端点的匹配不区分大小写。正则表达式规范不得包含标志 `(?-i)`，该标志会禁用不区分大小写的匹配。字符串规范必须以正斜杠 / 开头。

      例如，对于 URL `https://example.com/web/registration`，您可以提供字符串路径规范 `/web/registration`。以您提供的路径开头的注册页面路径被视为匹配路径。例如，`/web/registration` 匹配注册路径 `/web/registration`、`/web/registration/`、`/web/registrationPage` 和 `/web/registration/thisPage`，但与路径 `/home/web/registration` 或 `/website/registration` 不匹配。

> **Note**
>
> 确保您的最终用户在提交账户创建请求之前加载注册页面。这有助于确保来自客户端的账户创建请求包括有效的令牌。

c. 对于账户创建路径，请在您的网站上提供接受已完成的新用户详细信息的 URI。此页面必须接受 POST 请求。

> **Note**
>
> 端点的匹配不区分大小写。正则表达式规范不得包含标志 (?-i)，该标志会禁用不区分大小写的匹配。字符串规范必须以正斜杠 / 开头。

例如，对于 URL `https://example.com/web/newaccount`，您可以提供字符串路径规范 `/web/newaccount`。以您提供的路径开头的账户创建路径被视为匹配路径。例如，`/web/newaccount` 匹配账户创建路径 `/web/newaccount`、`/web/newaccount/`、`/web/newaccountPage` 和 `/web/newaccount/thisPage`，但与路径 `/home/web/newaccount` 或 `/website/newaccount` 不匹配。

d. 对于请求检查，请提供请求负载类型以及请求正文中提供用户名、密码和其他账户创建详细信息的字段名称，从而指定您的应用程序如何接受账户创建尝试。

> **Note**
>
> 对于主要地址和电话号码字段，请按照它们在请求负载中的显示顺序提供字段。

字段名称的指定取决于有效载荷类型。

- JSON 负载类型 – 使用 JSON 指针语法指定字段名称。有关 JSON 指针语法的信息，请参阅互联网工程任务组 (IETF) 文档JavaScript对象表示法 (JSON) 指针。

  例如，对于以下 JSON 负载示例，用户名字段规范为 `/signupform/username`，主地址字段规范为 `/signupform/addrp1`、`/signupform/addrp2` 和 `/signupform/addrp3`。

```
{
```

```
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- FORM_ENCODED 有效负载类型 – 使用 HTML 表单名称。

  例如，对于用户和密码输入元素名为 `username1` 和 `password1` 的 HTML 表单，用户名字段规范为 `username1`，密码字段规范为 `password1`。

e. 如果您要保护 Amazon CloudFront 分销，请在 “响应检查” 下，指定您的应用程序在响应账户创建尝试时如何指示成功或失败。

> **Note**
>
> ACFP 响应检查仅在保护 CloudFront 发行版的 Web ACL 中可用。

在账户创建响应中指定您希望 ACFP 检查的单个组件。对于 B ody 和 JSON 组件类型，AWS WAF 可以检查组件的前 65,536 字节 (64 KB)。

如界面所示，提供组件类型的检查条件。您必须提供成功和失败条件以供在组件中进行检查。

例如，假设您的应用程序在响应的状态码中指示账户创建尝试的状态，并使用 `200 OK` 指示成功，使用 `401 Unauthorized` 或 `403 Forbidden` 指示失败。您可以将响应检查组件类型设置为状态码，然后在成功文本框中输入 `200` 并在失败文本框的第一行输入 `401`，在第二行输入 `403`。

ACFP 规则组仅计算符合您的成功或失败检查条件的响应。当客户在计入的响应中成功率太高时，规则组规则会对客户端采取行动，以减少批量创建账户的尝试。为了确保规则组规则的行为准确，请务必提供成功和失败的账户创建尝试的完整信息。

要查看检查账户创建响应的规则，请在 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组 中的规则列表中查找 `VolumetricIPSuccessfulResponse` 和 `VolumetricSessionSuccessfulResponse`。

3. 为规则组提供所需的任何其他配置。

   您可以通过在托管规则组语句中添加范围缩小语句来进一步限制规则组检查的请求范围。例如，您只能检查带有特定查询参数或 Cookie 的请求。规则组将仅检查与您的范围缩小语句中的条件相匹配且发送到您在规则组配置中指定的账户注册和账户创建路径的请求。有关范围缩小语句的信息，请参阅 范围缩小语句。

4. 保存对 Web ACL 的更改。

在为生产流量部署 ACFP 实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。有关指导，请参阅以下部分。

测试和部署 ACFP

本节提供有关为您的网站配置和测试 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 实施的一般指导。您选择遵循的具体步骤将取决于您的需求、资源和收到的 Web 请求。

此信息是对 测试和调整您的 AWS WAF 保护措施 中提供的有关测试和调整的一般信息的补充。

> **Note**
>
> AWS 托管规则旨在保护您免受常见 Web 威胁的侵害。根据文档使用 AWS 托管规则组时，可以为您的应用程序增加另一层安全保护。但是， AWS 托管规则规则组并不是用来取代您的安全职责，后者由您选择的 AWS 资源决定。请参阅分担责任模型，确保您的资源 AWS 得到适当保护。

> **生产流量风险**
>
> 在为生产流量部署 ACFP 实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。

AWS WAF 提供了可用于验证 ACFP 配置的测试凭证。在以下步骤中，您将配置测试 Web ACL 以使用 ACFP 托管规则组，配置规则以捕获规则组添加的标签，然后使用这些测试凭证尝试创建账户。您可以通过查看账户创建尝试的 Amazon CloudWatch 指标来验证您的网络 ACL 是否正确管理了该尝试。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。

配置和测试 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 实施方案

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 在计数模式下 AWS WAF 添加 Fraud Control 账户创建防作弊 (ACFP) 托管规则组

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

将 AWS 托管规则组`AWSManagedRulesACFPRuleSet`添加到新的或现有的 Web ACL 中，并对其进行配置，使其不会改变当前 Web ACL 的行为。有关此规则组的规则和标签的详细信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

- 添加托管规则组时，对其进行编辑并执行以下操作：
  - 在规则组配置窗格中，提供您的应用程序的账户注册和创建页面的详细信息。ACFP 规则组使用此信息来监控登录活动。有关更多信息，请参阅 将 ACFP 托管规则组添加到您的 Web ACL。
  - 在规则窗格中，打开覆盖所有规则操作下拉列表并选择 Count。使用此配置， AWS WAF 可以根据规则组中的所有规则评估请求，并仅计算结果的匹配项，同时仍将标签添加到请求中。有关更多信息，请参阅 覆盖规则组的规则操作。

    通过此覆盖，您可以监控 ACFP 托管规则的潜在影响，以确定是否要添加例外，例如内部用例的例外。
- 定位规则组，使其按照您在 Web ACL 中的现有规则进行评估，优先级设置在数值上要高于您已在使用的任何规则或规则组。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

  这样，您当前的流量处理就不会中断。例如，如果您有检测恶意流量的规则，例如 SQL 注入或跨站脚本，它们将继续检测并记录这些流量。或者，如果您的规则允许已知的非恶意流量，则它们可以继续允许该流量，而不必被 ACFP 托管规则组阻止。在测试和调整活动期间，您可能会决定调整处理顺序。

2. 实施应用程序集成软件开发工具包

   将 AWS WAF JavaScript SDK 集成到浏览器的账户注册和账户创建路径中。 AWS WAF 还提供用于集成 iOS 和安卓设备的移动 SDK。有关集成软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关此建议的信息，请参阅 为何要在 ACFP 中使用应用程序集成软件开发工具包。

   > **Note**
   >
   > 如果您无法使用应用程序集成软件开发工具包，则可以通过在 Web ACL 中编辑 ACL 并删除您在 `AllRequests` 规则上设置的覆盖来测试 ACFP 规则组。这将启用规则的 Challenge 操作设置，以确保请求中包含有效的质询令牌。
   > 首先在测试环境中执行此操作，然后在生产环境中要格外小心。这种方法有可能阻止用户。例如，如果您的注册页面路径不接受 GET 文本/html 请求，则此规则配置可以有效地阻止注册页面上的所有请求。

3. 为 Web ACL 启用日志记录和指标

   根据需要，为 Web ACL 配置日志、Amazon Security Lake 数据收集、请求采样和亚马逊 CloudWatch 指标。您可以使用这些可见性工具来监控 ACFP 托管规则组与您的流量的交互情况。

   - 有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。
   - 有关 Amazon Security Lake 的信息，请参阅什么是亚马逊安全湖？ 以及 Amazon Security Lake 用户指南中的从 AWS 服务中收集数据。
   - 有关 Amazon CloudWatch 指标的信息，请参阅使用 Amazon 进行监控 CloudWatch。
   - 有关 Web 请求采样的信息，请参阅 查看 Web 请求示例。

4. 将 Web ACL 与资源关联

   如果 Web ACL 尚未与测试资源关联，请将其关联。有关信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

5. 监控流量和 ACFP 规则匹配情况

   确保您的正常流量畅通，并且 ACFP 托管规则组规则正在为匹配的 Web 请求添加标签。您可以在日志中看到标签，也可以在 Amazon 指标中查看 ACFP 和标签 CloudWatch 指标。在日志中，您在规则组中覆盖计数的规则会显示在 `ruleGroupList` 中，`action` 设置为计数，`overriddenAction` 表示您覆盖的已配置规则操作。

6. 测试规则组的凭证检查功能

   尝试使用已泄露的凭证创建账户，并检查规则组是否按预期与这些凭证匹配。

   a. 访问受保护资源的账户注册页面，然后尝试添加新账户。使用以下 AWS WAF 测试凭证对并输入任意考试

      - 用户：`WAF_TEST_CREDENTIAL@wafexample.com`
      - 密码：`WAF_TEST_CREDENTIAL_PASSWORD`

      这些测试凭证被归类为已泄露的凭证，ACFP 托管规则组会将 `awswaf:managed:aws:acfp:signal:credential_compromised` 标签添加到账户创建请求中，您可以在日志中看到该标签。

   b. 在您的 Web ACL 日志中，在测试账户创建请求的日志条目 `labels` 字段中查找 `awswaf:managed:aws:acfp:signal:credential_compromised` 标签。有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。

   确认规则组按预期捕获被泄露的凭证后，您可以采取措施根据受保护资源的需要配置其实施。

7. 对于 CloudFront 分配，请测试规则组对批量账户创建尝试的管理

   针对您为 ACFP 规则组配置的每个成功响应条件运行此测试。两次测试之间应至少等待 30 分钟。

   a. 对于您的每个成功条件，请确定在响应中符合成功条件的账户创建尝试。然后，在一次客户端会话中，不到 30 分钟内应至少成功完成 5 次账户创建尝试。用户通常只能在您的网站上创建一个账户。

      首次成功创建账户后，该 `VolumetricSessionSuccessfulResponse` 规则应开始与您的其余账户创建响应进行匹配，根据您的规则操作覆盖对其进行标记并进行计数。由于延迟，该规则可能会错过前一两个。

   b. 在您的 Web ACL 日志中，在测试账户创建 Web 请求的日志条目 `labels` 字段中查找 `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_i` 标签。有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。

   这些测试通过检查规则汇总的成功计数是否超过规则的阈值，来验证您的成功条件是否与您的响应相符。达到阈值后，如果您继续从同一会话发送账户创建请求，则该规则将继续匹配，直到成功率降至阈值以下。当超过阈值时，该规则会匹配来自会话地址的成功或失败的账户创建尝试。

8. 自定义 ACFP Web 请求处理

   根据需要，添加明确允许或阻止请求的规则，以更改 ACFP 规则处理请求的方式。

   例如，您可以使用 ACFP 标签来允许或阻止请求或自定义请求处理。您可以在 ACFP 托管规则组之后添加标签匹配规则，以筛选要应用的处理的已标记请求。测试后，将相关的 ACFP 规则保持在计数模式，并在自定义规则中维护请求处理决策。有关示例，请参阅ACFP 示例：针对被泄漏凭证的自定义响应。

9. 移除您的测试规则并启用 ACFP 托管规则组设置

   根据您的情况，您可能决定将某些 ACFP 规则保留为计数模式。对于要按照规则组内的配置运行的规则，请在 Web ACL 规则组配置中禁用计数模式。完成测试后，您还可以移除测试标签匹配规则。

10. 监控和调整

    为确保按照您的要求处理 Web 请求，请在启用您打算使用的 ACFP 功能后密切监控流量。根据需要调整行为，使用规则组上的规则计数覆盖和您自己的规则。

在您完成 ACFP 规则组实现的测试后，如果您尚未将 AWS WAF JavaScript SDK 集成到浏览器的账户注册和账户创建页面，我们强烈建议您这样做。 AWS WAF 还提供用于集成 iOS 和安卓设备的移动 SDK。有关集成软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关此建议的信息，请参阅 为何要在 ACFP 中使用应用程序集成软件开发工具包。

AWS WAF 欺诈控制账户创建防作弊 (ACFP) 示例

本节例示了满足 AWS WAF 欺诈控制账户创建欺诈预防（ACFP）实施的常见用例的配置。

每个示例都提供了用例的描述，然后在 JSON 列表中显示了自定义配置规则的解决方案。

> **Note**
>
> 您可以通过控制台 Web ACL JSON 下载或规则 JSON 编辑器，或者通过 API 和命令行界面中的 `getWebACL` 操作来检索 JSON 列表，例如这些示例中所示的列表。

主题

- ACFP 示例：响应检查配置

ACFP 示例：简单配置

以下 JSON 列表显示了带有 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 托管规则组的 Web ACL 示例。注意其他 `CreationPath` 和 `RegistrationPagePath` 配置，以及有效载荷类型和在有效载荷中查找新账户信息所需的信息，以便对其进行验证。规则组使用此信息来监控和管理您的账户创建请求。此 JSON 包含 Web ACL 自动生成的设置，例如标签命名空间和 Web ACL 的应用程序集成 URL。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
```

```
                "PhoneNumberFields": [
                  {
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  }
```

```
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

ACFP 示例：针对被泄漏凭证的自定义响应

默认情况下，规则组 AWSManagedRulesACFPRuleSet 执行的凭证检查通过标记请求并阻止请求来处理被泄露的凭证。有关规则组和规则行为的详细信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

要通知用户其提供的账户凭证已被泄漏，您可以执行以下操作：

- 将 **SignalCredentialCompromised** 规则覆盖为 Count – 这会使规则仅对匹配的请求进行计数和标记。
- 添加带有自定义处理的标签匹配规则 – 配置此规则，以便与 ACFP 标签匹配并执行自定义处理。

以下 Web ACL 列表显示了前一个示例中的 ACFP 托管规则组，其中的 SignalCredentialCompromised 规则操作被覆盖为计数。使用此配置，当此规则组评估任何使用已泄露凭证的 Web 请求时，它将标记该请求，但不会阻止该请求。

此外，Web ACL 现在有一个名为 aws-waf-credential-compromised 的自定义响应和一个名为 AccountSignupCompromisedCredentialsHandling 的新规则。规则优先级是比规则组更高的数值设置，因此在 Web ACL 评估中，它在规则组之后运行。新规则将任何带有规则组已泄露凭证标签的请求进行匹配。当规则找到匹配项时，它会使用自定义响应正文将 Block 操作应用于请求。自定义响应正文向最终用户提供其凭证已被泄露的信息，并建议应对操作。

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
```

```
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
```

```
                    },
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
                "EnableRegexInPath": false
              }
            }
          ],
          "RuleActionOverrides": [
            {
              "Name": "SignalCredentialCompromised",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
```

```
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

ACFP 示例：响应检查配置

以下 JSON 列表显示了一个 Web ACL 示例，其中包含配置为检查来源响应的欺 AWS WAF 诈控制账户创建防作弊 (ACFP) 托管规则组。请注意响应检查配置，该配置指定了成功和响应状态代码。您还可以根据标题、正文和正文 JSON 匹配来配置成功和响应设置。此 JSON 包含 Web ACL 自动生成的设置，例如标签命名空间和 Web ACL 的应用程序集成 URL。

> **Note**
>
> ATP 响应检查仅在保护 CloudFront 分布的 Web ACL 中可用。

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
```

```
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "ResponseInspection": {
                "StatusCode": {
                  "SuccessCodes": [
                    200
                  ],
                  "FailureCodes": [
                    401
                  ]
                }
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
```

```
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
  }
```

AWS WAF 防欺诈控制账户接管 (ATP)

账户盗用是一种在线非法活动，在这种活动中，攻击者未经授权即可访问个人的账户。攻击者可以通过多种方式执行此操作，例如使用被盗的凭证或通过一系列尝试猜测受害者的密码。当攻击者获得访问权限时，他们可能会从受害者那里窃取金钱、信息或服务。攻击者可能冒充受害者，以获得受害者拥有的其他账户的访问权限，或者访问其他人或组织的账户。此外，他们可能会尝试更改用户的密码，以阻止受害者使用自己的账户。

您可以通过实施 AWS WAF 欺诈控制账户接管预防 (ATP) 功能来监控和控制账户盗用企图。 AWS WAF 在 “ AWS 托管规则” 规则组`AWSManagedRulesATPRuleSet`和配套的应用程序集成 SDK 中提供了此功能。

ATP 托管规则组对可能属于恶意账户盗用尝试的请求进行标记和管理。规则组通过检查客户端发送到应用程序登录端点的登录尝试来实现此目的。

- 请求检查 – ATP 允许您查看和控制异常登录尝试和使用被盗凭证的登录尝试，以防止可能导致欺诈活动的账户盗用。ATP 根据被盗凭证数据库检查电子邮件和密码组合，当在暗网上发现新的泄露凭证时，会定期更新。ATP 按 IP 地址和客户端会话汇总数据，以检测和阻止发送过多可疑请求的客户端。
- 响应检查-对于 CloudFront 分配，除了检查传入的登录请求外，ATP 规则组还会检查您的应用程序对登录尝试的响应，以跟踪成功率和失败率。利用这些信息，ATP 可以暂时阻止登录失败次数过多的客户端会话或 IP 地址。 AWS WAF 会异步执行响应检查，因此不会增加 Web流量的延迟。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

> **Note**
>
> ATP 功能不适用于 Amazon Cognito 用户群体。

主题

ATP 组件

防 AWS WAF 欺诈控制账户盗用 (ATP) 的主要组成部分如下：

- **`AWSManagedRulesATPRuleSet`**— 此 AWS 托管规则组中的规则检测、标记和处理各种类型的账户接管活动。规则组检查客户端发送到指定登录端点的 HTTP POST Web 请求。对于受保护的 CloudFront 分配，规则组还会检查分配向这些请求发回的响应。有关此规则组的规则列表，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。您可以使用托管规则组参考语句将此规则组包含在 Web ACL 中。有关使用规则组的信息，请参阅 将 ATP 托管规则组添加到您的 Web ACL。

  > **Note**
  >
  > 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

- 有关您的应用程序登录页面的详细信息 – 将 `AWSManagedRulesATPRuleSet` 规则组添加到 Web ACL 时，您必须提供有关您的登录页面的信息。这允许规则组缩小其检查的请求范围，并正确验证 Web 请求中的凭证使用。ATP 规则组使用电子邮件格式的用户名。有关更多信息，请参阅 将 ATP 托管规则组添加到您的 Web ACL。

- 对于受保护的 CloudFront 分发，有关您的应用程序如何响应登录尝试的详细信息 — 您可以提供有关应用程序对登录尝试的响应的详细信息，规则组会跟踪和管理发送过多失败登录尝试的客户端。有关配置此选项的信息，请参阅 将 ATP 托管规则组添加到您的 Web ACL。
- JavaScript 和移动应用程序集成 SDK — 在 ATP 实施中实现 AWS WAF JavaScript 和移动 SDK，以启用规则组提供的全套功能。许多 ATP 规则使用软件开发工具包提供的信息进行会话级别的客户端验证和行为聚合，这是区分合法客户端流量和机器人流量所必需的。有关 SDK 的更多信息，请参阅 AWS WAF 客户端应用程序集成。

您可以将 ATP 实施与以下内容相结合，以帮助您监控、调整和自定义保护。

- 日志和指标 — 您可以通过配置和启用日志、Amazon Security Lake 数据收集以及您的 Web ACL 的亚马逊 CloudWatch 指标，监控您的流量，并了解 ACFP 托管规则组如何影响流量。`AWSManagedRulesATPRuleSet`添加到您的 Web 请求中的标签包含在数据中。有关这些选项的信息，请参阅记录 AWS WAF Web ACL 流量使用 Amazon 进行监控 CloudWatch、和什么是 Amazon Security Lake？ 。

  根据您的需求和看到的流量，您可能需要自定义您的 `AWSManagedRulesATPRuleSet` 实施。例如，您可能想将某些流量排除在 ATP 评估之外，或者您可能想使用范围缩小语句或标签匹配规则等 AWS WAF 功能，更改其处理所识别的某些账户接管尝试的方式。
- 标签和标签匹配规则 – 对于 `AWSManagedRulesATPRuleSet` 中的任何规则，您可以将阻止行为切换为计数，然后与规则添加的标签进行匹配。使用此方法自定义如何处理由 ATP 托管规则组标识的 Web 请求。有关标记和使用标签匹配语句的更多信息，请参见 标签匹配规则语句 和 AWS WAF 网络请求上的标签。
- 自定义请求和响应 – 您可以在允许的请求中添加自定义标头，也可以为被阻止的请求发送自定义响应。为此，您需要将匹配的标签与 AWS WAF 自定义请求和响应功能配对。有关请求和响应格式的更多信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

为何要在 ATP 中使用应用程序集成软件开发工具包

ATP 托管规则组需要应用程序集成软件开发工具包生成的质询令牌。这些令牌支持规则组提供的全套保护。

我们强烈建议实施应用程序集成软件开发工具包，以便最有效地使用 ATP 规则组。质询脚本必须在 ATP 规则组之前运行，这样规则组才能从脚本获取的令牌中受益。使用应用程序集成软件开发工具包，能够自动实施此操作。如果您无法使用软件开发工具包，则可以交替配置您的 Web ACL，使其对 ATP 规则组将要检查的所有请求运行 Challenge 或 CAPTCHA 规则操作。使用 Challenge 或 CAPTCHA 规则操作可能会产生额外费用。有关定价的详细信息，请参阅 AWS WAF 定价。

不需要令牌的 ATP 规则组的功能

当 Web 请求没有令牌时，ATP 托管规则组能够阻止以下类型的流量：

- 发出大量登录请求的单个 IP 地址。
- 在短时间内发出大量失败登录请求的单个 IP 地址。
- 尝试使用密码遍历登录，使用相同的用户名但更改了密码。

需要令牌的 ATP 规则组的功能

质询令牌中提供的信息扩展了规则组的功能和您的客户端应用程序的整体安全性。

该令牌为每个 Web 请求提供客户端信息，使 ATP 规则组能够将合法的客户端会话与行为不端的客户端会话区分开来，即使两者都来自单个 IP 地址。规则组使用令牌中的信息来汇总客户端会话请求行为，以进行微调的检测和缓解。

当令牌在 Web 请求中可用时，ATP 规则组可以在会话级别检测和阻止以下其他类别的客户端：

- 无法通过软件开发工具包管理的静默质询的客户端会话。
- 遍历用户名或密码的客户端会话。这也称作凭证填充。
- 反复使用被盗凭证登录的客户端会话。
- 花费很长时间尝试登录的客户端会话。
- 发出大量登录请求的客户端会话。与 AWS WAF 基于速率的规则相比，ATP 规则组提供了更好的客户端隔离，后者可以按 IP 地址阻止客户端。ATP 规则组还使用较低的阈值。
- 在短时间内发出大量失败登录请求的客户端会话。此功能适用于受保护的 Amazon CloudFront 分配。

有关这些功能的更多信息，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。

有关软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关 AWS WAF 令牌的信息，请参阅AWS WAF 网络请求令牌。有关规则操作的信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

将 ATP 托管规则组添加到您的 Web ACL

要配置 ATP 托管规则组以识别网络流量中的账户盗用活动，您需要提供有关客户端如何向您的应用程序发送登录请求的信息。对于受保护的 Amazon CloudFront 分配，您还需要提供有关您的应用程序如何响应登录请求的信息。此配置是对托管规则组的常规配置的补充。

有关规则组的描述和规则列表，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。

> **Note**
>
> ATP 被盗凭证数据库仅包含电子邮件格式的用户名。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。有关如何将托管规则组添加到 Web ACL 的基本信息，请参阅 通过控制台向 Web ACL 添加托管规则组。

遵循最佳实践

按照 智能威胁缓解的最佳实践 中的最佳实践使用 ATP 规则组。

在 Web ACL 中使用 **`AWSManagedRulesATPRuleSet`** 规则组

1. 将 AWS 托管规则组`AWSManagedRulesATPRuleSet`添加到您的 Web ACL 中，然后在保存之前编辑规则组设置。

   > **Note**
   >
   > 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

2. 在规则组配置窗格中，提供 ATP 规则组用于检查登录请求的信息。

   a. 对于 “在路径中使用正则表达式”，如果 AWS WAF 要对登录页面路径规范执行正则表达式匹配，请将其选中。

      AWS WAF 支持 PCRE 库使用的模式语法，但`libpcre`有一些例外。该库记录在 PCRE - 与 Perl 兼容的正则表达式中。有关 AWS WAF 支持的信息，请参阅中的正则表达式模式匹配 AWS WAF。

   b. 对于登录路径，提供应用程序登录端点的路径。规则组仅检查发往您指定的登录端点的 HTTP `POST` 请求。

      > **Note**
      >
      > 端点的匹配不区分大小写。正则表达式规范不得包含标志 `(?-i)`，该标志会禁用不区分大小写的匹配。字符串规范必须以正斜杠 `/` 开头。

例如，对于 URL `https://example.com/web/login`，您可以提供字符串路径规范 `/web/login`。以您提供的路径开头的登录路径被视为匹配路径。例如，`/web/login` 匹配登录路径 `/web/login`、`/web/login/`、`/web/loginPage` 和 `/web/login/thisPage`，但与登录路径 `/home/web/login` 或 `/website/login` 不匹配。

c. 对于请求检查，请通过提供请求负载类型以及请求正文中提供用户名和密码的字段的名称来指定您的应用程序如何接受登录尝试。字段名称的指定取决于有效载荷类型。

- JSON 负载类型 – 使用 JSON 指针语法指定字段名称。有关 JSON 指针语法的信息，请参阅互联网工程任务组 (IETF) 文档JavaScript对象表示法 (JSON) 指针。

  例如，对于以下示例 JSON 负载，用户名字段规范为 `/login/username`，密码字段规范为 `/login/password`。

```
{
    "login": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD"
    }
}
```

- FORM_ENCODED 有效负载类型 – 使用 HTML 表单名称。

  例如，对于输入元素名为 `username1` 和 `password1` 的 HTML 表单，用户名字段规范为 `username1`，密码字段规范为 `password1`。

d. 如果您要保护 Amazon CloudFront 分配，请在 “响应检查” 下，指定您的应用程序在响应登录尝试时如何指示成功或失败。

> **Note**
>
> ATP 响应检查仅在保护 CloudFront 分布的 Web ACL 中可用。

在登录响应中指定您希望 ATP 检查的单个组件。对于正文和 JSON 组件类型， AWS WAF 可以检查组件的前 65,536 字节 (64 KB)。

如界面所示，提供组件类型的检查条件。您必须提供成功和失败条件以供在组件中进行检查。

例如，假设您的应用程序在响应的状态码中指示登录尝试的状态，并使用 `200 OK` 指示成功，使用 `401 Unauthorized` 或 `403 Forbidden` 指示失败。您可以将响应检查组件类型设置为状态码，然后在成功文本框中输入 `200` 并在失败文本框的第一行输入 `401`，在第二行输入 `403`。

ATP 规则组仅计算符合您的成功或失败检查条件的响应。当客户端在计算的响应中失败率太高时，规则组规则会对客户端采取行动。为了确保规则组规则的行为准确，请务必提供成功和失败的登录尝试的完整信息。

要查看检查登录响应的规则，请在 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 中的规则列表中查找 `VolumetricIpFailedLoginResponseHigh` 和 `VolumetricSessionFailedLoginResponseHigh`。

3. 为规则组提供所需的任何其他配置。

   您可以通过在托管规则组语句中添加范围缩小语句来进一步限制规则组检查的请求范围。例如，您只能检查带有特定查询参数或 Cookie 的请求。规则组将仅检查发往您指定的登录端点的、与您的范围缩小语句中的条件相匹配的 HTTP POST 请求。有关范围缩小语句的信息，请参阅 范围缩小语句。

4. 保存对 Web ACL 的更改。

在为生产流量部署 ATP 实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。有关指导，请参阅以下部分。

测试和部署 ATP

本节提供有关为您的网站配置和测试 AWS WAF 欺诈控制账户接管预防 (ATP) 实施的一般指导。您选择遵循的具体步骤将取决于您的需求、资源和收到的 Web 请求。

此信息是对 测试和调整您的 AWS WAF 保护措施 中提供的有关测试和调整的一般信息的补充。

> **Note**
>
> AWS 托管规则旨在保护您免受常见 Web 威胁的侵害。根据文档使用 AWS 托管规则组时，可以为您的应用程序增加另一层安全保护。但是， AWS 托管规则规则组并不是用来取代您的安全职责，后者由您选择的 AWS 资源决定。请参阅分担责任模型，确保您的资源 AWS 得到适当保护。

⚠ 生产流量风险

在为生产流量部署 ATP 实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。

AWS WAF 提供了可用于验证 ATP 配置的测试凭证。在以下步骤中，您将配置测试 Web ACL 以使用 ATP 托管规则组，配置规则以捕获规则组添加的标签，然后使用这些测试凭证尝试登录。您可以通过检查登录尝试的 Amazon CloudWatch 指标来验证您的网络 ACL 是否正确管理了该尝试。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。

配置和测试 AWS WAF 欺诈控制账户接管预防 (ATP) 实施方案

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 在计数模式下添加 F AWS WAF raud Control 账户接管预防 (ATP) 托管规则组

   Note

   使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

   将 AWS 托管规则组`AWSManagedRulesATPRuleSet`添加到新的或现有的 Web ACL 中，并对其进行配置，使其不会改变当前 Web ACL 的行为。有关此规则组的规则和标签的详细信息，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。

   - 添加托管规则组时，对其进行编辑并执行以下操作：
     - 在规则组配置窗格中，提供您的应用程序的登录页面的详细信息。ATP 规则组使用此信息来监控登录活动。有关更多信息，请参阅 将 ATP 托管规则组添加到您的 Web ACL。
     - 在规则窗格中，打开覆盖所有规则操作下拉列表并选择 Count。使用此配置， AWS WAF 可以根据规则组中的所有规则评估请求，并仅计算结果的匹配项，同时仍将标签添加到请求中。有关更多信息，请参阅 覆盖规则组的规则操作。

       通过此覆盖，您可以监控 ATP 托管规则的潜在影响，以确定是否要添加例外，例如内部用例的例外。

- 定位规则组，使其按照您在 Web ACL 中的现有规则进行评估，优先级设置在数值上要高于您已在使用的任何规则或规则组。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

  这样，您当前的流量处理就不会中断。例如，如果您有检测恶意流量的规则，例如 SQL 注入或跨站脚本，它们将继续检测并记录这些流量。或者，如果您的规则允许已知的非恶意流量，则它们可以继续允许该流量，而不必被 ATP 托管规则组阻止。在测试和调整活动期间，您可能会决定调整处理顺序。

2. 为 Web ACL 启用日志记录和指标

   根据需要，为 Web ACL 配置日志、Amazon Security Lake 数据收集、请求采样和亚马逊 CloudWatch 指标。您可以使用这些可见性工具来监控 ATP 托管规则组与您的流量的交互情况。

   - 有关配置和使用日志记录的信息，请参阅 记录 AWS WAF Web ACL 流量。
   - 有关亚马逊安全湖的信息，请参阅什么是亚马逊安全湖？ 以及 Amazon Security Lake 用户指南中的从 AWS 服务中收集数据。
   - 有关 Amazon CloudWatch 指标的信息，请参阅使用 Amazon 进行监控 CloudWatch。
   - 有关 Web 请求采样的信息，请参阅 查看 Web 请求示例。

3. 将 Web ACL 与资源关联

   如果 Web ACL 尚未与测试资源关联，请将其关联。有关信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

4. 监控流量和 ATP 规则匹配情况

   确保您的正常流量畅通，并且 ATP 托管规则组规则正在为匹配的 Web 请求添加标签。您可以在日志中看到标签，也可以在 Amazon 指标中查看 ATP 和标签 CloudWatch 指标。在日志中，您在规则组中覆盖计数的规则会显示在 `ruleGroupList` 中，`action` 设置为计数，`overriddenAction` 表示您覆盖的已配置规则操作。

5. 测试规则组的凭证检查功能

   尝试使用已泄露的凭证进行登录，并检查规则组是否按预期与这些凭证匹配。

   a. 使用以下 AWS WAF 测试凭据对登录到受保护资源的登录页面：

      - 用户：`WAF_TEST_CREDENTIAL@wafexample.com`
      - 密码：`WAF_TEST_CREDENTIAL_PASSWORD`

这些测试凭证被归类为已泄露的凭证，ATP 托管规则组会将 `awswaf:managed:aws:atp:signal:credential_compromised` 标签添加到登录请求中，您可以在日志中看到该标签。

b. 在 Web ACL 日志中，在测试登录 Web 请求的日志条目 `labels` 字段中查找 `awswaf:managed:aws:atp:signal:credential_compromised` 标签。有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。

确认规则组按预期捕获被泄露的凭证后，您可以采取措施根据受保护资源的需要配置其实施。

6. 对于 CloudFront 分配，请测试规则组的登录失败管理

a. 针对您为 ATP 规则组配置的每个失败响应条件运行测试。两次测试之间应至少等待 10 分钟。

要测试单个失败条件，请在响应中根据该条件确定将失败的登录尝试。然后，在不到 10 分钟的时间内，从单个客户端 IP 地址执行至少 10 次失败的登录尝试。

在前 6 次失败之后，容量失败登录规则应开始与您的其余尝试进行匹配，对其进行标记和计数。由于延迟，该规则可能会错过前一两个。

b. 在 Web ACL 日志中，在测试登录 Web 请求的日志条目 `labels` 字段中查找 `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` 标签。有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。

这些测试通过检查失败的登录计数是否超过规则 `VolumetricIpFailedLoginResponseHigh` 的阈值来验证您的失败条件是否与您的响应相符。达到阈值后，如果您继续从同一 IP 地址发送登录请求，则该规则将继续匹配，直到失败率降至阈值以下。当超过阈值时，该规则会匹配从 IP 地址成功或失败的登录。

7. 自定义 ATP Web 请求处理

根据需要，添加您自己的明确允许或阻止请求的规则，以更改 ATP 规则处理请求的方式。

例如，您可以使用 ATP 标签来允许或阻止请求或自定义请求处理。您可以在 ATP 托管规则组之后添加标签匹配规则，以筛选要应用的处理的带标签的请求。测试后，将相关的 ATP 规则保持在计数模式，并在自定义规则中维护请求处理决策。有关示例，请参阅ATP 示例：针对缺失和被盗凭证的自定义处理。

8. 移除您的测试规则并启用 ATP 托管规则组设置

   根据您的情况，您可能已经决定将某些 ATP 规则保留为计数模式。对于要按照规则组内的配置运行的规则，请在 Web ACL 规则组配置中禁用计数模式。完成测试后，您还可以移除测试标签匹配规则。

9. 监控和调整

   为确保 Web 请求按您的意愿处理，请在启用要使用的 ATP 功能后密切监控您的流量。根据需要调整行为，使用规则组上的规则计数覆盖和您自己的规则。

在您完成 ATP 规则组实现的测试后，如果您还没有这样做，我们强烈建议您将 AWS WAF JavaScript 软件开发工具包集成到浏览器登录页面中，以增强检测功能。 AWS WAF 还提供用于集成 iOS 和安卓设备的移动 SDK。有关集成软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关此建议的信息，请参阅 为何要在 ATP 中使用应用程序集成软件开发工具包。

AWS WAF 防欺诈控制账户接管 (ATP) 示例

本节显示了满足 AWS WAF 欺诈控制账户盗用防护（ATP）实施常见用例的配置示例。

每个示例都提供了用例的描述，然后在 JSON 列表中显示了自定义配置规则的解决方案。

> **Note**
>
> 您可以通过控制台 Web ACL JSON 下载或规则 JSON 编辑器，或者通过 API 和命令行界面中的 `getWebACL` 操作来检索 JSON 列表，例如这些示例中所示的列表。

主题

- ATP 示例：简单配置
- ATP 示例：针对缺失和被盗凭证的自定义处理
- ATP 示例：响应检查配置

ATP 示例：简单配置

以下 JSON 列表显示了带有防 AWS WAF 欺诈控制账户接管 (ATP) 托管规则组的 Web ACL 示例。请注意额外的登录页面配置，它为规则组提供了监控和管理您的登录请求所需的信息。此 JSON 包含 Web ACL 自动生成的设置，例如标签命名空间和 Web ACL 的应用程序集成 URL。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
```

```
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

ATP 示例：针对缺失和被盗凭证的自定义处理

默认情况下，规则组 AWSManagedRulesATPRuleSet 执行的凭证检查按如下方式处理 Web 请求：

- 缺少凭证 – 标记和阻止请求。
- 凭证泄露 – 为请求添加标签，但不要将其阻止或计数。

有关规则组和规则行为的详细信息，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。

您可以通过执行以下操作为凭证缺失或泄露的 Web 请求添加自定义处理：

- 将 **MissingCredential** 规则覆盖为 Count – 此规则操作覆盖会使规则仅对匹配的请求进行计数和标记。
- 添加带有自定义处理的标签匹配规则 – 配置此规则以匹配两个 ATP 标签并执行您的自定义处理。例如，您可以将客户重定向到您的注册页面。

以下规则显示了前一个示例中的 ATP 托管规则组，其中的 MissingCredential 规则操作被覆盖为计数。这会导致规则将其标签应用于匹配的请求，然后只计算请求数，而不是阻止请求。

```
"Rules": [
    {
        "Priority": 1,
```

```
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

使用此配置，当此规则组评估任何缺少凭证或已泄露的 Web 请求时，它将标记该请求，但不会阻止该请求。

以下规则的优先级设置在数字上高于前面的规则组。 AWS WAF 按数字顺序评估规则，从最低开始，因此将在规则组评估之后评估此规则。该规则配置为匹配任一凭证标签，并为匹配的请求发送自定义响应。

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

ATP 示例：响应检查配置

以下 JSON 列表显示了一个 Web ACL 示例，其中包含配置为检查来源响应的 AWS WAF 欺诈控制账户接管预防 (ATP) 托管规则组。请注意响应检查配置，该配置指定了成功和响应状态代码。您还可以根据标题、正文和正文 JSON 匹配来配置成功和响应设置。此 JSON 包含 Web ACL 自动生成的设置，例如标签命名空间和 Web ACL 的应用程序集成 URL。

> **Note**
>
> ATP 响应检查仅在保护 CloudFront 分布的 Web ACL 中可用。

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
```

```
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "ResponseInspection": {
                                "StatusCode": {
                                  "SuccessCodes": [
                                    200
                                  ],
                                  "FailureCodes": [
                                    401
                                  ]
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF 机器人控制

借助机器人控制功能，您可以轻松监控、阻止机器人或限制速率，例如抓取器、扫描器、爬虫、状态监视器和搜索引擎。如果您使用规则组的目标检查级别，则还可以质询无法自我识别的机器人，这使得恶意机器人对您的网站进行操作变得更加困难，成本也更高。您可以单独使用 Bot Control 托管规则组来保护您的应用程序，也可以与其他 AWS 托管规则组和您自己的自定义 AWS WAF 规则结合使用。

机器人控制功能包括一个控制台控制面板，根据请求采样显示您当前的流量中有多少来自机器人。将机器人控制功能托管规则组添加到 Web ACL 后，您可以对机器人流量采取操作，并接收有关进入应用程序的常见机器人流量的详细、实时信息。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

机器人控制功能托管规则组提供了基本的通用保护级别，可为自我识别的机器人添加标签，验证普遍需要的机器人，并检测高度可信的机器人签名。这使您能够监控和控制常见的机器人流量类别。

机器人控制功能规则组还提供目标保护级别，增加了对无法自我识别的复杂机器人的检测。所有目标保护都使用浏览器查询、指纹识别和行为启发式等检测技术来识别恶意机器人流量。此外，目标保护还可对网站流量统计数据进行可选的自动机器学习分析，以检测与机器人相关的活动。启用机器学习后，AWS WAF 会使用有关网站流量的统计信息（例如时间戳、浏览器特征和之前访问的 URL）来改进机器人控制功能机器学习模型。

有关机器人控制功能托管规则组的更多信息，请参阅 AWS WAF 机器人控制规则组。

在根据 Bot Control 托管规则组 AWS WAF 评估 Web 请求时，规则组会为其检测为与机器人相关的请求添加标签，例如机器人类别和机器人名称。您可以在自己的 AWS WAF 规则中与这些标签进行匹配以自定义处理。Bot Control 托管规则组生成的标签包含在 Amazon CloudWatch 指标和您的 Web ACL 日志中。

您还可以使用 AWS Firewall Manager AWS WAF 策略在属于您组织的多个账户中跨应用程序部署 Bot Control 托管规则组 AWS Organizations。

机器人控制功能组件

机器人控制功能实施的主要组件如下：

- **`AWSManagedRulesBotControlRuleSet`** – 机器人控制功能托管规则组，其规则可检测和处理各种类别的机器人。此规则组为其检测为机器人流量的 Web 请求添加标签。

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

机器人控制功能托管规则组提供两种保护级别供您选择：

- 常见 – 检测各种自我识别的机器人，例如 Web 抓取框架、搜索引擎和自动浏览器。此级别的机器人控制功能保护使用传统的机器人检测技术（例如静态请求数据分析）来识别常见的机器人。这些规则会标记来自这些机器人的流量，并阻止他们无法验证的流量。
- 定向 – 包括通用级保护，并针对无法自我识别的复杂机器人添加定向检测。目标保护结合了速率限制和验证码以及后台浏览器质询，缓解了机器人活动。
  - **TGT_** – 提供目标保护的规则的名称以 TGT_ 开头。所有目标保护都使用浏览器查询、指纹识别和行为启发式等检测技术来识别恶意机器人流量。
  - **TGT_ML_** – 使用机器学习的目标保护规则的名称以 TGT_ML_ 开头。这些规则使用对网站流量统计数据的自动机器学习分析来检测表明分布式、协调的机器人活动的异常行为。 AWS WAF 分析有关您的网站流量的统计信息，例如时间戳、浏览器特征和之前访问的 URL，以改进 Bot Control 机器学习模型。默认情况下，机器学习功能处于启用状态，但您可以在规则组配置中将其禁用。禁用机器学习时， AWS WAF 不评估这些规则。

有关详细信息（包括有关规则组规则的信息），请参阅 AWS WAF 机器人控制规则组。

您可以使用托管规则组参考语句将此规则组包含在 Web ACL 中，并指明要使用的检查级别。对于目标关卡，您还需要指示是否启用机器学习。有关在 Web ACL 中使用托管规则组的更多信息，请参阅将 AWS WAF Bot Control 托管规则组添加到 Web ACL。

- 机器人控制功能面板 – Web ACL 的机器人监控控制面板，可通过 Web ACL 机器人控制功能选项卡访问。使用此控制面板监控您的流量，并了解其中有多少来自各种类型的机器人。如本主题所述，这可以作为自定义机器人管理的起点。您还可以使用它来验证您的更改并监控各种机器人和机器人类别的活动。
- JavaScript 和移动应用程序集成 SDK — 如果您使用 Bot Control 规则组的目标保护级别，则应实现 AWS WAF JavaScript 和移动 SDK。目标规则使用客户端令牌中的软件开发工具包提供的信息来增强对恶意机器人的检测。有关 SDK 的更多信息，请参阅 AWS WAF 客户端应用程序集成。
- 日志和指标 — 通过研究 AWS WAF 日志、Amazon Security Lake 和 Amazon 为你的网页 ACL 收集的数据，您可以监控您的机器人流量，了解机器人控制托管规则组如何评估和处理您的流量。CloudWatchBot Control 为你的网络请求添加的标签包含在数据中。有关这些选项的信息，请参

阅记录 AWS WAF Web ACL 流量使用 Amazon 进行监控 CloudWatch、和什么是 Amazon Security Lake？ 。

根据您的需求和看到的流量，您可能需要自定义机器人控制功能实施。以下是一些最常用的选项。

- 范围缩小语句 – 通过在机器人控制功能托管规则组参考语句中添加范围缩小语句，可以从机器人控制功能托管规则组评估的 Web 请求中排除一些流量。范围缩小语句可以是任何可嵌套的规则语句。当请求与 scope-down 语句不匹配时， AWS WAF 会将其评估为与规则组参考语句不匹配，而不根据规则组对其进行评估。有范围缩小语句的更多信息，请参阅 范围缩小语句。

  机器人控制功能托管规则组的定价会随着 AWS WAF 使用该规则组评估的 Web 请求数量而增加。您可以使用范围缩小语句来限制规则组评估的请求，从而帮助降低这些成本。例如，您可能希望允许所有人（包括机器人）加载您的主页，然后将规则组规则应用于发送到您的应用程序 API 或包含特定类型内容的请求。
- 标签和标签匹配规则-您可以使用 AWS WAF 标签匹配规则语句自定义 Bot Control 规则组如何处理其识别的某些机器人流量。机器人控制功能规则组会为您的 Web 请求添加标签。您可以在机器人控制功能规则组之后添加与机器人控制功能标签匹配的标签匹配规则，然后应用所需的处理。有关标记和使用标签匹配语句的更多信息，请参见 标签匹配规则语句 和 AWS WAF 网络请求上的标签。
- 自定义请求和响应 — 您可以向允许的请求添加自定义标头，也可以通过将标签与自定义请求和响应功能匹配来为您屏蔽的请求发送 AWS WAF 自定义响应。有关请求和响应格式的更多信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

为什么要将应用程序集成软件开发工具包与机器人控制功能配合使用

机器人控制功能托管规则组的大多数目标保护都需要应用程序集成软件开发工具包生成的质询令牌。不需要在请求中使用质询令牌的规则是机器人控制功能通用级别保护和目标级别机器学习规则。有关规则组中保护级别和规则的描述，请参阅 AWS WAF 机器人控制规则组。

我们强烈建议实施应用程序集成软件开发工具包，以便最有效地使用机器人控制功能规则组。质询脚本必须在机器人控制功能规则组之前运行，这样规则组才能从脚本获取的令牌中受益。

- 使用应用程序集成软件开发工具包时，脚本会自动运行。
- 如果您无法使用软件开发工具包，则可以配置您的 Web ACL，使其对机器人控制功能规则组将要检查的所有请求运行 Challenge 或 CAPTCHA 规则操作。使用 Challenge 或 CAPTCHA 规则操作可能会产生额外费用。有关定价的详细信息，请参阅 AWS WAF 定价。

当您在客户端中实施应用程序集成软件开发工具包或使用运行质询脚本的规则操作之一时，可以扩展规则组和整体客户端应用程序安全的功能。

令牌为每个 Web 请求提供客户信息。这些附加信息使机器人控制功能规则组能够将合法的客户端会话与行为不端的客户端会话区分开来，即使两者都来自单个 IP 地址。规则组使用令牌中的信息来汇总客户端会话请求行为，以实施目标保护级别提供的微调检测和缓解。

有关软件开发工具包的更多信息，请参阅 AWS WAF 客户端应用程序集成。有关 AWS WAF 令牌的信息，请参阅AWS WAF 网络请求令牌。有关规则操作的信息，请参阅 CAPTCHA然后Challenge在 AWS WAF。

将 AWS WAF Bot Control 托管规则组添加到 Web ACL

机器人控制功能托管规则组 `AWSManagedRulesBotControlRuleSet` 需要额外的配置才能确定要实施的保护级别。

有关规则组的描述和规则列表，请参阅 AWS WAF 机器人控制规则组。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。有关如何将托管规则组添加到 Web ACL 的基本信息，请参阅 通过控制台向 Web ACL 添加托管规则组。

遵循最佳实践

按照 智能威胁缓解的最佳实践 中的最佳实践使用机器人控制功能规则组。

在 Web ACL 中使用 **`AWSManagedRulesBotControlRuleSet`** 规则组

1. 将 AWS 托管规则组`AWSManagedRulesBotControlRuleSet`添加到您的 Web ACL。有关规则组的完整描述，请参阅 the section called “机器人控制功能规则组”。

   > **Note**
   >
   > 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

   添加规则组时，对其进行编辑以打开规则组的配置页面。

2. 在规则组的配置页面的检查级别窗格中，选择要使用的检查级别。

   - 常见 – 检测各种自我识别的机器人，例如 Web 抓取框架、搜索引擎和自动浏览器。此级别的机器人控制功能保护使用传统的机器人检测技术（例如静态请求数据分析）来识别常见的机器人。这些规则会标记来自这些机器人的流量，并阻止他们无法验证的流量。

- 定向 – 包括通用级保护，并针对无法自我识别的复杂机器人添加定向检测。目标保护结合了速率限制和验证码以及后台浏览器质询，缓解了机器人活动。
  - **TGT_** – 提供目标保护的规则的名称以 TGT_ 开头。所有目标保护都使用浏览器查询、指纹识别和行为启发式等检测技术来识别恶意机器人流量。
  - **TGT_ML_** – 使用机器学习的目标保护规则的名称以 TGT_ML_ 开头。这些规则使用对网站流量统计数据的自动机器学习分析来检测表明分布式、协调的机器人活动的异常行为。 AWS WAF 分析有关您的网站流量的统计信息，例如时间戳、浏览器特征和之前访问的 URL，以改进 Bot Control 机器学习模型。默认情况下，机器学习功能处于启用状态，但您可以在规则组配置中将其禁用。禁用机器学习时， AWS WAF 不评估这些规则。

3. 如果您使用的是目标保护级别，并且不想 AWS WAF 使用机器学习 (ML) 来分析分布式、协调的机器人活动的网络流量，请禁用机器学习选项。名称以 TGT_ML_ 开头的机器人控制功能规则需要机器学习。有关这些规则的详细信息，请参阅 机器人控制功能规则列表。
4. 为规则组添加范围缩小语句，以包含使用规则组的成本。范围缩小语句缩小了规则组检查的请求集的范围。例如用例，请以 机器人控制示例：仅对登录页面使用机器人控制 和 机器人控制示例：仅对动态内容使用机器人控制 开头。
5. 提供规则组所需的任何其他配置。
6. 保存对 Web ACL 的更改。

在为生产流量部署机器人控制功能实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。有关指导，请参阅以下各节。

AWS WAF Bot Control 的误报

我们精心选择了 AWS WAF Bot Control 托管规则组中的规则，以最大限度地减少误报。我们根据全局流量测试规则，并监控其对测试 Web ACL 的影响。但是，由于流量模式的变化，仍然有可能出现误报。此外，已知某些用例会导致误报，因此需要根据您的 Web 流量进行自定义。

您可能会遇到误报的情况包括：

- 移动应用程序通常具有非浏览器用户代理，`SignalNonBrowserUserAgent` 规则在默认情况下会阻止这些代理。如果您期望来自移动应用程序的流量，或者任何其他来自非浏览器用户代理的合法流量，则需要添加例外才能允许。
- 您可能会依赖一些特定的机器人流量来执行诸如正常运行时间监控、集成测试或营销工具之类的操作。如果机器人控制功能识别并阻止了您想要允许的机器人流量，则需要通过添加自己的规则来更改处理方式。虽然这不是所有客户的误报情况，但如果是针对您，则需要像处理误报一样处理。

- Bot Control 托管规则组使用来自 AWS WAF的 IP 地址验证机器人。如果您使用机器人控制功能，并且已经验证了通过代理或负载均衡器进行路由的机器人，则您可能需要使用自定义规则明确允许它们。有关如何创建此类型规则的自定义规则的更多信息，请参阅 转发的 IP 地址。
- 全局误报率较低的机器人控制功能规则可能会严重影响特定的设备或应用程序。例如，在测试和验证中，我们可能没有观察到来自低流量应用程序或来自不太常见的浏览器或设备的请求。
- 误报率处于历史最低水平的机器人控制功能规则可能会增加有效流量的误报。这可能是由于新的流量模式或请求属性随有效流量一起出现，导致其与以前没有的规则相匹配。这些更改可能是由于以下情况所致：
  - 流量详细信息随着流量流经网络设备（例如负载均衡器或内容分配网络 (CDN)）而发生变化。
  - 流量数据的新变化，例如新浏览器或现有浏览器的新版本。

有关如何处理可能从 AWS WAF 机器人控制功能托管规则组中获得的误报的信息，请参阅以下部分中的指导 测试和部署 AWS WAF 机器人控制。

测试和部署 AWS WAF 机器人控制

本节提供有关为您的网站配置和测试 AWS WAF Bot Control 实现的一般指导。您选择遵循的具体步骤将取决于您的需求、资源和收到的 Web 请求。

此信息是对 测试和调整您的 AWS WAF 保护措施 中提供的有关测试和调整的一般信息的补充。

> **Note**
>
> AWS 托管规则旨在保护您免受常见网络威胁的侵害。根据文档使用 AWS 托管规则组时，可以为您的应用程序增加另一层安全保护。但是， AWS 托管规则规则组并不是用来取代您的安全职责，后者由您选择的 AWS 资源决定。请参阅分担责任模型，确保您的资源 AWS 得到适当保护。

> **生产流量风险**
>
> 在为生产流量部署机器人控制功能实施之前，请在暂存或测试环境中对其进行测试和调整，直到您能够适应对流量的潜在影响。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。

本指导适用于大致了解如何创建和管理 AWS WAF Web ACL、规则和规则组的用户。这些主题将在本指南的前面章节中介绍。

配置和测试机器人控制功能实施

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 添加机器人控制功能托管规则组

> **Note**
>
> 使用此托管规则组时，您需要额外付费。有关更多信息，请参阅AWS WAF 定价。

将托管 AWS 规则组`AWSManagedRulesBotControlRuleSet`添加到新的或现有的 Web ACL 中，并对其进行配置，使其不会改变当前的 Web ACL 行为。

- 添加托管规则组时，对其进行编辑并执行以下操作：
  - 在检查级别窗格中，选择要使用的检查级别。
    - 常见 – 检测各种自我识别的机器人，例如 Web 抓取框架、搜索引擎和自动浏览器。此级别的机器人控制功能保护使用传统的机器人检测技术（例如静态请求数据分析）来识别常见的机器人。这些规则会标记来自这些机器人的流量，并阻止他们无法验证的流量。
    - 定向 – 包括通用级保护，并针对无法自我识别的复杂机器人添加定向检测。目标保护结合了速率限制和验证码以及后台浏览器质询，缓解了机器人活动。
      - **`TGT_`** – 提供目标保护的规则的名称以 `TGT_` 开头。所有目标保护都使用浏览器查询、指纹识别和行为启发式等检测技术来识别恶意机器人流量。
      - **`TGT_ML_`** – 使用机器学习的目标保护规则的名称以 `TGT_ML_` 开头。这些规则使用对网站流量统计数据的自动机器学习分析来检测表明分布式、协调的机器人活动的异常行为。AWS WAF 分析有关您的网站流量的统计信息，例如时间戳、浏览器特征和之前访问的 URL，以改进 Bot Control 机器学习模型。默认情况下，机器学习功能处于启用状态，但您可以在规则组配置中将其禁用。禁用机器学习时， AWS WAF 不评估这些规则。

    有关此选择的更多信息，请参阅 AWS WAF 机器人控制规则组。
  - 在规则窗格中，打开覆盖所有规则操作下拉列表并选择 Count。使用此配置，可以根据规则组中的所有规则 AWS WAF 评估请求，并仅计算结果的匹配项，同时仍将标签添加到请求中。有关更多信息，请参阅 覆盖规则组的规则操作。

通过此替换，您可以监控机器人控制功能规则对您的流量的潜在影响，以确定是否要为内部用例或所需的机器人添加例外。

- 定位规则组，使其在 Web ACL 中最后进行评估，优先级设置在数字上要高于您已在使用的任何其他规则或规则组。有关更多信息，请参阅 Web ACL 中规则和规则组的处理顺序。

  这样，您当前的流量处理就不会中断。例如，如果您有检测恶意流量的规则，例如 SQL 注入或跨站脚本，它们将继续检测和记录这些请求。或者，如果您的规则允许已知的非恶意流量，则它们可以继续允许该流量，而不必被机器人控制功能托管规则组阻止。在测试和调整活动期间，您可能会决定调整处理顺序，但这是一个不错的起点。

2. 为 Web ACL 启用日志记录和指标

   根据需要，为 Web ACL 配置日志、Amazon Security Lake 数据收集、请求采样和亚马逊 CloudWatch 指标。您可以使用这些可见性工具来监控 Bot Control 托管规则组与您的流量的交互情况。

   - 有关日志记录的信息，请参阅记录 AWS WAF Web ACL 流量。
   - 有关亚马逊安全湖的信息，请参阅什么是亚马逊安全湖？ 以及 Amazon Security Lake 用户指南中的从 AWS 服务中收集数据。
   - 有关 Amazon CloudWatch 指标的信息，请参阅使用 Amazon 进行监控 CloudWatch。
   - 有关 Web 请求采样的信息，请参阅 查看 Web 请求示例。

3. 将 Web ACL 与资源关联

   如果 Web ACL 尚未与资源关联，请将其关联。有关信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

4. 监控流量和机器人控制功能规则匹配情况

   确保流量畅通，并且机器人控制功能托管规则组规则正在为匹配的 Web 请求添加标签。您可以在日志中看到标签，也可以在 Amazon 指标中查看机器人和标签 CloudWatch 指标。在日志中，您在规则组中覆盖计数的规则会显示在 `ruleGroupList` 中，`action` 设置为计数，`overriddenAction` 表示您覆盖的已配置规则操作。

   > **Note**
   >
   > 机器人控制功能托管规则组使用来自 AWS WAF的 IP 地址验证机器人。如果您使用机器人控制功能，并且已经验证了通过代理或负载均衡器进行路由的机器人，则您可能需要使

用自定义规则明确允许它们。有关如何创建自定义规则的更多信息，请参阅 转发的 IP 地址。有关如何使用该规则自定义机器人控制功能 Web 请求处理的信息，请参阅下一步。

请仔细检查 Web 请求处理中是否存在任何可能需要通过自定义处理来缓解的误报。有关误报的示例，请参阅 AWS WAF Bot Control 的误报。

5. 自定义机器人控制功能 Web 请求处理

根据需要，添加您自己的明确允许或阻止请求的规则，以更改机器人控制功能规则处理请求的方式。

如何执行此操作取决于您的用例，但以下是常见的解决方案：

- 明确允许具有在机器人控制功能托管规则组之前添加的规则的请求。这样，允许的请求就永远不会到达规则组进行评估。这有助于控制使用机器人控制功能托管规则组的成本。
- 通过在机器人控制功能托管规则组语句中添加范围缩小语句，将请求排除在机器人控制功能评估之外。此功能与前面的选项相同。它可能有助于控制使用机器人控制功能托管规则组的费用，因为与范围缩小语句不匹配的请求永远不会进入规则组评估。有关范围缩小语句的信息，请参阅范围缩小语句。

  有关 示例，请参阅以下内容：

  - 从机器人管理中排除 IP 范围
  - 允许来自您控制的机器人的流量
- 在请求处理中使用机器人控制功能标签来允许或阻止请求。在机器人控制功能托管规则组之后添加标签匹配规则，从要阻止的请求中筛选出要允许的带标签的请求。

  测试后，将相关的机器人控制功能规则保持在计数模式，并在您的自定义规则中维护请求处理决策。有关标签匹配语句的信息，请参阅 标签匹配规则语句。

  有关此类型自定义的示例，请参阅以下内容：

  - 为被阻止的用户代理创建例外
  - 允许特定的被阻止机器人
  - 阻止已验证机器人

有关其他示例，请参阅 AWS WAF 机器人控制示例。

6. 根据需要启用机器人控制功能托管规则组设置

   根据您的情况，您可能已经决定要将某些机器人控制功能规则保留为计数模式或使用不同的操作覆盖。对于要按照规则组内部配置的方式运行的规则，请启用常规规则配置。为此，请编辑 Web ACL 中的规则组语句，然后在规则窗格中进行更改。

AWS WAF 机器人控制示例

本节显示了满足 AWS WAF Bot Control 实现的各种常见用例的示例配置。

每个示例都提供了用例的描述，然后在 JSON 列表中显示了自定义配置规则的解决方案。

> **Note**
>
> 这些示例中显示的 JSON 列表是在控制台中创建的，方法是配置规则，然后使用规则 JSON 编辑器对其进行编辑。

主题

机器人控制示例：简单配置

以下 JSON 列表显示了带有 AWS WAF 机器人控制托管规则组的 Web ACL 示例。请注意可见性配置，该配置会 AWS WAF 导致存储请求样本和指标以供监控之用。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

机器人控制示例：明确允许经过验证的机器人

AWS WAF Bot Control 不会阻止已知是常见且可验证的机器人。 AWS 当机器人控制功能将 Web 请求识别为来自已验证机器人时，它会添加一个命名该机器人的标签和一个表明它是已验证机器人的标签。机器人控制功能不会添加任何其他标签，例如信号标签，以防止已知良好的机器人被阻止。

您可能还有其他 AWS WAF 规则可以屏蔽经过验证的机器人。如果要确保允许已验证机器人，请根据机器人控制功能标签添加自定义规则以允许使用它们。您的新规则必须在机器人控制功能托管规则组之后运行，这样标签才能与之匹配。

以下规则明确允许已验证机器人。

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

机器人控制示例：屏蔽经过验证的机器人

要阻止已验证机器人，您必须添加一条规则来阻止它们，该规则在 AWS WAF 机器人控制功能托管规则组之后运行。为此，请确定要阻止的机器人名称，然后使用标签匹配语句来识别和阻止它们。如果您只想阻止所有已验证机器人，您可以省略与 `bot:name:` 标签的匹配项。

以下规则仅阻止 `bingbot` 已验证机器人。此规则必须在机器人控制功能托管规则组之后运行。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
```

```
            "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
          }
        },
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:verified"
          }
        }
      ]
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  }
}
```

以下规则会阻止所有已验证机器人。

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

机器人控制示例：允许特定被屏蔽的机器人

机器人可能会被多条机器人控制功能规则阻止。对每条阻止规则执行以下步骤。

如果 AWS WAF 机器人控制规则正在屏蔽您不想屏蔽的机器人，请执行以下操作：

1. 通过查看日志，识别阻止机器人的机器人控制功能规则。将在日志中名称以 `terminatingRule` 开头的字段中指定阻止规则。有关 Web ACL 日志的更多信息，请参阅 记录 AWS WAF Web ACL 流量。请注意规则添加到请求中的标签。

2. 在您的 Web ACL 中，覆盖阻止规则的操作以计数。要在控制台中执行此操作，请编辑 Web ACL 中的规则组规则，然后为该规则选择 Count 规则操作覆盖。这样可以确保机器人不会被规则阻止，但规则仍会将其标签应用于匹配的请求。
3. 在 Web ACL 中，在机器人控制功能托管规则组后添加标签匹配规则。将规则配置为与被覆盖的规则的标签相匹配，并阻止除您不想阻止的机器人之外的所有匹配请求。

   现在，您的 Web ACL 已配置完毕，因此您要允许的机器人不再被您通过日志识别的阻止规则所阻止。

再次检查流量和您的日志，确保机器人被允许通过。如果不是，请再次执行上述步骤。

例如，假设您需要阻止除 pingdom 以外的所有监控机器人。在这种情况下，您可以将 CategoryMonitoring 规则覆盖为计数，然后编写一条规则来阻止除带有机器人名称标签 pingdom 的机器人之外的所有监控机器人。

以下规则使用机器人控制功能托管规则组，但会将 CategoryMonitoring 规则操作覆盖为计数。类别监控规则像往常一样将其标签应用于匹配的请求，但仅对它们进行计数，而不是执行通常的阻止操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
```

```
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

以下规则与前面的 CategoryMonitoring 规则添加到匹配的 Web 请求中的类别监控标签相匹配。在类别监控请求中，该规则会阻止所有请求，除带有机器人名称 pingdom 标签的请求外。

以下规则必须在 Web ACL 处理顺序中前面的机器人控制功能托管规则组之后运行。

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
```

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

Bot Control 示例：为被屏蔽的用户代理创建例外

如果来自某些非浏览器用户代理的流量被错误屏蔽，则可以通过将违规的 Bot Control 规则设置为 Coun AWS WAF t，然后将该规则的标签与您的例外标准结合起来`SignalNonBrowserUserAgent`来创建例外。

> **Note**
>
> 移动应用程序通常具有非浏览器用户代理，`SignalNonBrowserUserAgent` 规则在默认情况下会阻止这些代理。

以下规则使用机器人控制功能托管规则组，但会将 `SignalNonBrowserUserAgent` 规则操作覆盖为计数。信号规则像往常一样将其标签应用于匹配的请求，但仅对它们进行计数，而不是执行通常的阻塞操作。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
```

```
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

以下规则与机器人控制功能 SignalNonBrowserUserAgent 规则添加到其匹配的 Web 请求中的信号标签相匹配。在信号请求中，除了那些拥有我们想要允许的用户代理的请求外，该规则会阻止所有请求。

以下规则必须在 Web ACL 处理顺序中前面的机器人控制功能托管规则组之后运行。

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
```

```
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          }
        }
      ]
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

机器人控制示例：仅对登录页面使用机器人控制

以下示例使用 scope-down 语句仅对进入网站登录页面的流量应用 AWS WAF Bot Control，该页面由 URI 路径标识。`login`登录页面的 URI 路径可能与示例不同，具体取决于您的应用程序和环境。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
```

```
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

机器人控制示例：仅对动态内容使用机器人控制

此示例使用 scope-down 语句将 AWS WAF 机器人控制仅应用于动态内容。

范围缩小语句通过否定正则表达式模式集的匹配结果来排除静态内容：

- 正则表达式模式集配置为匹配静态内容的扩展。例如，正则表达式模式集规范可能是 `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`。有关正则表达式模式集和语句的信息，请参阅 正则表达式模式集匹配规则语句。
- 在范围缩小语句中，我们通过在 NOT 语句内部嵌套正则表达式模式集语句来排除匹配的静态内容。有关 NOT 语句的信息，请参阅 NOT 规则语句。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
```

```
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

机器人控制示例：从机器人管理中排除 IP 范围

如果您想从 AWS WAF Bot Control 管理中排除一部分 Web 流量，并且可以使用规则语句识别该子集，则可以通过在 Bot Control 托管的规则组语句中添加范围缩小语句来将其排除。

以下规则对所有 Web 流量执行常规的机器人控制功能机器人管理，除来自特定 IP 地址范围的 Web 请求外。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

机器人控制示例：允许来自你控制的机器人的流量

您可以配置一些站点监控机器人和自定义机器人来发送自定义标头。如果要允许来自这些类型的机器人的流量，可以将其配置为在标头中添加共享密钥。然后，您可以通过向 AWS WAF Bot Control 托管规则组语句添加范围缩小语句来排除带有标题的消息。

以下示例规则将带有密钥标头的流量排除在机器人控制功能检查之外。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
```

```
    }
  }
}
```

机器人控制示例：目标检查级别

要获得增强的保护级别，您可以在 AWS WAF Bot Control 托管规则组中启用目标检查级别。

在以下示例中，启用了机器学习功能。您可以通过将设置EnableMachineLearning为来选择退出此行为false。

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
  }
}
```

Bot Control 示例：使用两个语句来限制目标检查级别的使用

作为成本优化，您可以在 Web ACL 中使用两个 AWS WAF Bot Control 托管规则组语句，它们具有不同的检查级别和范围。例如，您可以将目标检查级别声明的范围仅限于更敏感的应用程序端点。

以下示例中的两个语句具有相互排斥的作用域。如果没有此配置，请求可能会导致两次计费评估。

> **Note**
>
> 控制台的可视化编辑AWSManagedRulesBotControlRuleSet器不支持引用多个语句。请改用 JSON 编辑器。

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
             "ManagedRuleGroupConfigs": [
               {
                 "AWSManagedRulesBotControlRuleSet": {
                   "InspectionLevel": "COMMON"
                 }
               }
             ],
             "RuleActionOverrides": [],
             "ExcludedRules": []
          },
          "VisibilityConfig": {
             "SampledRequestsEnabled": true,
             "CloudWatchMetricsEnabled": true,
             "MetricName": "AWS-AWSBotControl-Common"
           },
           "ScopeDownStatement": {
              "NotStatement": {
```

```
            "Statement": {
              "ByteMatchStatement": {
                "FieldToMatch": {
                  "UriPath": {}
                },
                "PositionalConstraint": "STARTS_WITH",
                "SearchString": "/sensitive-endpoint",
                "TextTransformations": [
                  {
                    "Type": "NONE",
                    "Priority": 0
                  }
                ]
              }
            }
          }
        }
      }
    },
    {
     "Name": "AWS-AWSBotControl-Targeted",
     "Priority": 6,
     "Statement": {
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesBotControlRuleSet",
           "ManagedRuleGroupConfigs": [
             {
               "AWSManagedRulesBotControlRuleSet": {
                 "InspectionLevel": "TARGETED",
                 "EnableMachineLearning": true
               }
             }
           ],
           "RuleActionOverrides": [],
           "ExcludedRules": []
        },
        "VisibilityConfig": {
           "SampledRequestsEnabled": true,
           "CloudWatchMetricsEnabled": true,
           "MetricName": "AWS-AWSBotControl-Targeted"
         },
         "ScopeDownStatement": {
            "Statement": {
```

```
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "UriPath": {}
                  },
                  "PositionalConstraint": "STARTS_WITH",
                  "SearchString": "/sensitive-endpoint",
                  "TextTransformations": [
                    {
                      "Type": "NONE",
                      "Priority": 0
                    }
                  ]
                }
              }
            }
          }
        }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF 客户端应用程序集成

使用 AWS WAF 客户端应用程序集成 API 将客户端保护与 AWS 服务器端 Web ACL 保护相结合，以帮助验证向受保护资源发送 Web 请求的客户端应用程序是否为目标客户端，以及您的最终用户是否为人类。

使用客户端集成来管理静默浏览器质询和验证码拼图，获取带有成功浏览器和最终用户响应证明的令牌，并将这些令牌包含在对受保护端点的请求中。有关 AWS WAF 代币的一般信息，请参阅AWS WAF 网络请求令牌。

将您的客户端集成与 Web ACL 保护相结合，后者需要有效的令牌才能访问您的资源。您可以在 智能威胁集成和 AWS 托管规则 使用检查和监控挑战令牌的规则组（如下一节中列出的规则组），也可以使用 CAPTCHA 和 Challenge 规则操作进行检查，如 CAPTCHA然后Challenge在 AWS WAF 中所述。

AWS WAF 为应用程序提供两个集成级别，为移动 JavaScript 应用程序提供一个集成级别：

- 智能威胁集成-验证客户端应用程序并提供 AWS 令牌获取和管理。这与 AWS WAF Challenge规则操作提供的功能类似。此功能将您的客户端应用程序与 `AWSManagedRulesACFPRuleSet` 托管规则组、`AWSManagedRulesATPRuleSet` 托管规则组和 `AWSManagedRulesBotControlRuleSet` 托管规则组的目标保护级别完全集成。

  智能威胁集成 API 使用 AWS WAF 静默浏览器质询来帮助确保只有在客户端获取有效令牌后才允许对受保护资源进行登录尝试和其他调用。这些 API 管理您的客户端应用程序会话的令牌授权，并收集有关客户端的信息，以帮助确定它是由机器人操作还是由人类操作。

  > **Note**
  >
  > 这适用于安卓 JavaScript 和 iOS 移动应用程序。

- 验证码集成 – 使用您在应用程序中管理的自定义验证码拼图验证最终用户。这与 AWS WAF CAPTCHA规则动作提供的功能类似，但增加了对拼图位置和行为的控制。

  这种集成利用 JavaScript 智能威胁集成来运行静默挑战，并为客户的页面提供 AWS WAF 令牌。

  > **Note**
  >
  > 这适用于 JavaScript 应用程序。

主题

- 智能威胁集成和 AWS 托管规则
- 访问 AWS WAF 客户端应用程序集成 API
- AWS WAF JavaScript 集成
- AWS WAF 移动应用程序集成

智能威胁集成和 AWS 托管规则

智能威胁集成 API 与使用智能威胁规则组的 Web ACL 配合使用，以启用这些高级托管规则组的全部功能。

- AWS WAF 欺诈控制账户创建欺诈预防 (ACFP) 托管规则组`AWSManagedRulesACFPRuleSet`。

  账户创建欺诈是一种在线非法活动，攻击者在您的应用程序中创建无效账户，其目的包括获得注册奖金或冒充他人。ACFP 托管规则组提供规则，用于阻止、标记和管理可能属于欺诈账户创建尝试的请

求。这些 API 支持经过微调的客户端浏览器验证和人机交互信息，ACFP 规则使用这些信息将有效的客户端流量与恶意流量区分开来。

有关更多信息，请参阅 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组 和 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP)。

- AWS WAF 防欺诈控制账户接管 (ATP) 管理的规则组`AWSManagedRulesATPRuleSet`。

  账户盗用是一种在线非法活动，在这种活动中，攻击者未经授权即可访问个人的账户。ATP 托管规则组提供规则，用于阻止、标记和管理可能属于恶意账户盗用尝试的请求。这些 API 支持经过微调的客户端验证和行为聚合，ATP 规则使用这些验证和行为聚合将有效的客户端流量与恶意流量区分开来。

  有关更多信息，请参阅 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组 和 AWS WAF 防欺诈控制账户接管 (ATP)。

- AWS WAF Bot Control 托管规则组的目标保护级别`AWSManagedRulesBotControlRuleSet`。

  机器人从自我识别和有用的机器人（例如大多数搜索引擎和爬虫）到针对您的网站运行且无法自我识别的恶意机器人。机器人控制功能托管规则组提供用于监控、标记和管理 Web 流量中的机器人活动的规则。当您使用此规则组的目标保护级别时，目标规则会使用 API 提供的客户端会话信息来更好地检测恶意机器人。

  有关更多信息，请参阅 AWS WAF 机器人控制规则组 和 AWS WAF 机器人控制。

要将其中一个托管规则组添加到 Web ACL，请参阅步骤 将 ACFP 托管规则组添加到您的 Web ACL、将 ATP 托管规则组添加到您的 Web ACL 和 将 AWS WAF Bot Control 托管规则组添加到 Web ACL。

> **Note**
>
> 托管规则组目前不会阻止缺少令牌的请求。要阻止缺少令牌的请求，请在实施应用程序集成 API 后，按照 阻止没有有效 AWS WAF 令牌的请求 中的指导进行操作。

访问 AWS WAF 客户端应用程序集成 API

集 JavaScript 成 API 现已公开发布，您可以将其用于浏览器和其他执行设备 JavaScript。

AWS WAF 提供适用于 Android 和 iOS 移动应用程序的定制智能威胁集成 SDK。

- 对于安卓移动应用程序， AWS WAF 软件开发工具包适用于安卓 API 版本 23（安卓版本 6）及更高版本。有关 Android 版本的信息，请参阅软件开发工具包平台发行说明。
- 对于 iOS 移动应用程序， AWS WAF 软件开发工具包适用于 iOS 版本 13 及更高版本。有关 iOS 版本的信息，请参阅 iOS 和 iPadOS 发行说明。

通过控制台访问集成 API

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中选择 应用程序集成，然后选择您感兴趣的选项卡。

   - 智能威胁集成可用于 JavaScript 和移动应用程序。

     该选项卡包含以下内容：

     - 为智能威胁应用程序集成启用的 Web ACL 列表。该列表包括使用 `AWSManagedRulesACFPRuleSet` 托管规则组、`AWSManagedRulesATPRuleSet` 托管规则组或 `AWSManagedRulesBotControlRuleSet` 托管规则组的目标保护级别的每个 Web ACL。在实施智能威胁 API 时，您需要使用要与之集成的 Web ACL 的集成 URL。
     - 您有权访问的 API。这 JavaScript 些 API 始终可用。要访问移动软件开发工具包，请通过联系 AWS 联系支持人员。
   - 验证码集成可用于应用程序。 JavaScript

     该选项卡包含以下内容：

     - 在您的集成中使用的集成 URL。
     - 您为客户端应用程序域创建的 API 密钥。使用验证码API需要加密的API密钥，该密钥使客户有权从其域名访问 AWS WAF 验证码。对于您与之集成的每个客户端，请使用包含该客户端域名的 API 密钥。有关这些要求以及有关管理这些密钥的更多信息，请参阅 管理 JS 验证码 API 的 API 密钥。

AWS WAF JavaScript 集成

您可以使用 JavaScript 集成 API 在浏览器和其他执行设备中实现 AWS WAF 应用程序集成。JavaScript

只有当浏览器访问 HTTPS 端点时，才能运行验证码谜题和静默挑战。浏览器客户端必须在安全的环境中运行才能获取令牌。

- 智能威胁 API 允许您通过静默的客户端浏览器质询来管理令牌授权，并在发送到受保护资源的请求中包含令牌。
- 验证码集成 API 增加了智能威胁 API，允许您自定义验证码拼图在客户端应用程序中的位置和特征。此 API 利用智能威胁 API 获取 AWS WAF 令牌，以便在最终用户成功完成验证码拼图后在页面中使用。

通过使用这些集成，可以确保客户端的远程过程调用包含有效的令牌。当这些集成 API 出现在您的应用程序页面上时，您可以在 Web ACL 中实施缓解规则，例如阻止不包含有效令牌的请求。您还可以通过在规则中使用 Challenge 或 CAPTCHA 操作来实施强制使用客户端应用程序获取的令牌的规则。

下表显示了 Web 应用程序页面中智能威胁 API 的典型实施的基本组件。

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

验证码集成 API 可让您自定义最终用户的验证码拼图体验。CAPTCHA 集成利用 JavaScript 智能威胁集成进行浏览器验证和令牌管理，并添加了配置和呈现 CAPTCHA 拼图的功能。

以下列表显示了 Web 应用程序页面中典型的 CAPTCHA JavaScript API 实现的基本组件。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
```

```
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

主题

- 提供用于令牌的域名
- 将 JavaScript API 与内容安全策略配合使用
- 使用智能威胁 JavaScript API
- 使用验证码 API JavaScript

提供用于令牌的域名

默认情况下，在 AWS WAF 创建令牌时，它使用与 Web ACL 关联的资源的主机域。您可以为为 JavaScript API AWS WAF 创建的令牌提供其他域名。为此，请使用一个或多个令牌域配置全局变量 `window.awsWafCookieDomainList`。

AWS WAF 创建令牌时，它会使用中域名`window.awsWafCookieDomainList`和与 Web ACL 关联的资源的主机域组合中最合适、最短的域。

设置示例：

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

您不能在此列表中使用公共后缀。例如，您不能在列表中使用 gov.au 或 co.uk 作为令牌域。

您在此列表中指定的域名必须与您的其他域名和域名配置兼容：

- 根据受保护的主机域和为 Web ACL 配置的令牌域列表，这些域必须是可以接受的域。 AWS WAF 有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。
- 如果您使用 CAP JavaScript TCHA API，则您的 CAPTCHA API 密钥中至少有一个域名必须与中的一个令牌域名完全匹配，window.awsWafCookieDomainList或者该域名必须是其中一个令牌域的顶点域。

  例如，对于令牌域 mySubdomain.myApex.com，API 密钥 mySubdomain.myApex.com 完全匹配，API 密钥 myApex.com 是顶点域。任一密钥都与令牌域相匹配。

  有关 API 密钥的更多信息，请参阅 管理 JS 验证码 API 的 API 密钥。

如果您使用 AWSManagedRulesACFPRuleSet 托管规则组，则可以配置一个与您在规则组配置中提供的账户创建路径中的域名相匹配的域。有关此配置的更多信息，请参阅将 ACFP 托管规则组添加到您的 Web ACL。

如果您使用 AWSManagedRulesATPRuleSet 托管规则组，则可以配置一个与您在规则组配置中提供的登录路径中的域名相匹配的域。有关此配置的更多信息，请参阅将 ATP 托管规则组添加到您的 Web ACL。

将 JavaScript API 与内容安全策略配合使用

如果您将内容安全策略 (CSP) 应用于您的资源，则需要将 AWS WAF apex 域列入许可名单。JavaScript awswaf.comS JavaScript DK 会调用不同的 AWS WAF 端点，因此将此域列入许可名单可提供 SDK 操作所需的权限。

以下显示了将 AWS WAF apex 域列入许可名单的配置示例：

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

如果您尝试将 JavaScript SDK 与使用 CSP 的资源一起使用，但尚未将该 AWS WAF 域列入许可名单，则会收到如下错误：

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

使用智能威胁 JavaScript API

智能威胁 API 提供了针对用户的浏览器运行静默挑战的操作，以及处理提供成功挑战和验证码响应证明的 AWS WAF 令牌的操作。

首先在测试环境中实施 JavaScript 集成，然后在生产环境中实现集成。有关其他编码指导，请参阅以下各节。

使用智能威胁 API

1. 安装 API

   如果您使用验证码 API，可以跳过此步骤。当您安装验证码 API时，脚本会自动安装智能威胁 API。

   a. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   b. 在导航窗格中，选择 应用程序集成。在应用程序集成页面上，您可以看到选项卡式选项。

   c. 选择智能威胁集成

   d. 在该选项卡中，选择要与之集成的Web ACL。Web ACL 列表仅包括使用 `AWSManagedRulesACFPRuleSet` 托管规则组、`AWSManagedRulesATPRuleSet` 托管规则组或 `AWSManagedRulesBotControlRuleSet` 托管规则组的目标保护级别的 Web ACL。

   e. 打开 S JavaScript DK 窗格，复制脚本标签以便在集成中使用。

   f. 在应用程序页面代码的 <head> 部分中，插入您为 Web ACL 复制的脚本标记。此包含会使您的客户端应用程序在页面加载时自动在后台检索令牌。

   ```
   <head>
       <script type="text/javascript" src="Web ACL integration URL/challenge.js”
    defer></script>
   <head>
   ```

此 <script> 列表使用 defer 属性进行配置，但如果您想让页面有不同的行为，则可以将设置更改为 async。

2. （可选）为客户端的令牌添加域配置-默认情况下，在 AWS WAF 创建令牌时，它使用与 Web ACL 关联的资源的主机域。要为 JavaScript API 提供其他域名，请按照中的指南进行操作提供用于令牌的域名。
3. 对智能威胁集成进行编码 – 编写代码以确保在客户端向受保护的端点发送请求之前完成令牌检索。如果您已经在使用 fetch API 进行调用，则可以替换 AWS WAF 集成 fetch 封装器。如果您不使用 fetch API，则可以改用 AWS WAF 集成getToken操作。有关编码指导，请参阅以下部分。
4. 在您的 Web ACL 中添加令牌验证 – 在您的 Web ACL 中添加至少一条规则，用于检查您的客户端发送的 Web 请求中是否存在有效的质询令牌。您可以使用规则组来检查和监控质询令牌，例如机器人控制功能托管规则组的目标级别，也可以使用 Challenge 规则操作进行检查，如 CAPTCHA 然后Challenge在 AWS WAF 中所述。

   新增的 Web ACL 可验证对受保护端点的请求是否包含您在客户端集成中获取的令牌。包含有效、未过期令牌的请求将通过 Challenge 检查，并且不会向您的客户发送另一个静默质询。
5. （可选）阻止缺少令牌的请求 – 如果您将 API 与 ACFP 托管规则组、ATP 托管规则组或机器人控制功能规则组的目标规则一起使用，则这些规则不会阻止缺少令牌的请求。要阻止缺少令牌的请求，请按照 阻止没有有效 AWS WAF 令牌的请求 中的指导进行操作。

主题

- 智能威胁 API 规范
- 如何使用集成 fetch 包装程序
- 如何使用集成 getToken

智能威胁 API 规范

本节列出了智能威胁缓解 JavaScript API 的方法和属性的规范。使用这些 API 进行智能威胁和验证码集成。

`AwsWafIntegration.fetch()`

使用 AWS WAF 集成实现向服务器发送 HTTP fetch 请求。

AwsWafIntegration.getToken()

检索存储的 AWS WAF 令牌并将其存储在当前页面上的 Cookie 中aws-waf-token，名称和值设置为令牌值。

AwsWafIntegration.hasToken()

返回一个布尔值，指示 aws-waf-token Cookie 当前是否包含未过期的令牌。

如果您也在使用验证码集成，请参阅相关规范，网址为 验证码 API 规范 JavaScript 。

如何使用集成 **fetch** 包装程序

你可以通过更改AwsWafIntegration命名空间下对 fetch API 的常规fetch调用来使用 AWS WAF fetch包装器。 AWS WAF 包装器支持所有与标准 JavaScript fetch API 调用相同的选项，并为集成添加了令牌处理。这种方法通常是集成应用程序的最简单方法。

在包装程序实施之前

以下示例列表显示了实施 AwsWafIntegration fetch 包装程序之前的标准代码。

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

包装程序实施后

以下列表显示了与 AwsWafIntegration fetch 包装程序实施相同的代码。

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

如何使用集成 **getToken**

AWS WAF 要求您向受保护端点发出的请求中包含以当前令牌值命名aws-waf-token的 Cookie。

该 getToken 操作是一个异步 API 调用，用于检索 AWS WAF 令牌并将其存储在名为 aws-waf-token 的当前页面的 Cookie 中，值设置为令牌值。您可以根据需要在页面中使用此令牌 Cookie。

当您调用 getToken，它会执行以下操作：

- 如果未过期的令牌已经可用，则调用会立即将其返回。
- 否则，该调用将从令牌提供程序那里检索新令牌，等待最多 2 秒钟才能完成令牌获取工作流程，然后超时。如果操作超时，则会引发错误，您的调用代码必须处理该错误。

该 getToken 操作有一个附带的 hasToken 操作，用于指示 aws-waf-token Cookie 当前是否包含未过期的令牌。

AwsWafIntegration.getToken()检索有效的令牌并将其存储为 Cookie。大多数客户调用会自动附加此 Cookie，但有些则不会。例如，跨主机域发出的呼叫不会附加 Cookie。在接下来的实现细节中，我们将展示如何处理这两种类型的客户端调用。

基本**getToken**实现，适用于附加 **aws-waf-token** cookie 的调用

以下示例列表显示了通过登录请求实施 getToken 操作的标准代码。

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

只有在 **getToken** 提供令牌后才能提交表格

以下列表显示了如何注册事件侦听器以拦截表单提交，直到有有效的令牌可供使用。

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

当您的客户端默认不附加 **aws-waf-token** Cookie 时附加令牌

AwsWafIntegration.getToken()检索有效的令牌并将其存储为 Cookie，但并非所有客户端调用都会默认附加此 Cookie。例如，跨主机域发出的呼叫不会附加 Cookie。

fetch包装器会自动处理这些情况，但是如果您无法使用fetch包装器，则可以使用自定义x-aws-waf-token标题来处理此问题。 AWS WAF 除了从 aws-waf-token Cookie 中读取令牌外，还会从该标头中读取令牌。以下代码显示了设置标题的示例。

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
```

```
});
```

默认情况下，AWS WAF 仅接受包含与请求的主机域相同域名的令牌。任何跨域令牌都需要在 Web ACL 令牌域列表中输入相应的条目。有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

有关跨域令牌使用的更多信息，请参阅 aws-s aws-waf-bot-control amples/-。api-protection-with-captcha

使用验证码 API JavaScript

CAPTCHA JavaScript API 允许您配置验证码拼图并将其放置在客户端应用程序中所需的位置。在最终用户成功完成验证码拼图后，此 JavaScript API 利用智能威胁 API 的功能来获取和使用 AWS WAF 令牌。

首先在测试环境中实施 JavaScript 集成，然后在生产环境中实现集成。有关其他编码指导，请参阅以下各节。

使用验证码集成 API

1. 安装 API

   a. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
   b. 在导航窗格中，选择 应用程序集成。在应用程序集成页面上，您可以看到选项卡式选项。
   c. 选择验证码集成。
   d. 复制列出的 JavaScript 集成脚本标签，以便在集成中使用。
   e. 在应用程序页面代码的 <head> 部分中，插入您复制的脚本标签。此功能使验证码拼图可供配置和使用。

      ```
      <head>
          <script type="text/javascript" src="integrationURL/jsapi.js" defer></
      script>
      </head>
      ```

      此 <script> 列表使用 defer 属性进行配置，但如果您想让页面有不同的行为，则可以将设置更改为 async。

      如果智能威胁集成脚本尚不存在，验证码脚本还会自动加载该脚本。智能威胁集成脚本使您的客户端应用程序在页面加载时自动在后台检索令牌，并提供您使用验证码 API 所需的其他令牌管理功能。

2. （可选）为客户端的令牌添加域配置-默认情况下，在 AWS WAF 创建令牌时，它将使用与 Web ACL 关联的资源的主机域。要为 JavaScript API 提供其他域名，请按照中的指南进行操作提供用于令牌的域名。
3. 获取客户端的加密 API 密钥 — CAPTCHA API 需要一个包含有效客户端域列表的加密 API 密钥。 AWS WAF 使用此密钥来验证您在集成中使用的客户端域是否已获准使用 AWS WAF CAPTCHA。要生成 API 密钥，请按照 管理 JS 验证码 API 的 API 密钥 中的指导进行操作。
4. 编写验证码控件实施代码 – 在页面中要使用它的位置实施 `renderCaptcha()` API 调用。有关配置和使用此功能的信息，请参阅以下各节 验证码 API 规范 JavaScript 和 如何显示验证码拼图。

   CAPTCHA 实现与智能威胁集成 API 集成，用于令牌管理和运行使用令牌的提取调用。 AWS WAF 有关使用这些 API 的指导，请参阅 使用智能威胁 JavaScript API。
5. 在您的 Web ACL 中添加令牌验证 – 在 Web ACL 中添加至少一条规则，用于检查客户端发送的 Web 请求中是否存在有效的验证码令牌。您可以使用 CAPTCHA 规则操作进行检查，如 CAPTCHA然后Challenge在 AWS WAF 中所述。

   新增的 Web ACL 可验证发往受保护端点的请求是否包含您在客户端集成中获取的令牌。包含有效、未过期的验证码令牌的请求会通过 CAPTCHA 规则操作检查，并且不会向您的最终用户显示其他验证码拼图。

主题

- 验证码 API 规范 JavaScript
- 如何显示验证码拼图
- 处理来自的验证码响应 AWS WAF
- 管理 JS 验证码 API 的 API 密钥

验证码 API 规范 JavaScript

本节列出了 CAPTCHA AP JavaScript I 的方法和属性的规范。使用 CAPTCHA JavaScript API 在您的客户端应用程序中运行自定义的验证码拼图。

此 API 建立在智能威胁 API 的基础上，您可以使用这些API来配置和管理 AWS WAF 令牌的获取和使用。请参阅 智能威胁 API 规范。

AwsWafCaptcha.renderCaptcha(container, configuration)

向最终用户展示 AWS WAF 验证码拼图，成功后，使用验证码验证更新客户端令牌。这仅在集成了验证码时可用。使用此调用和智能威胁 API 来管理令牌检索并在您的 `fetch` 调用中提供令牌。请参阅智能威胁 API，网址为 智能威胁 API 规范。

与 AWS WAF 发送的 CAPTCHA 插页式广告不同，通过这种方法渲染的 CAPTCHA 拼图会立即显示拼图，而无需初始标题屏幕。

container

页面上目标容器元素的 `Element` 对象。这通常是通过调用 `document.getElementById()` 或 `document.querySelector()` 来检索的。

必需：是

类型：`Element`

配置

一个包含验证码配置设置的对象，如下所示 ：

apiKey

启用客户端域权限的加密 API 密钥。使用 AWS WAF 控制台为您的客户端域生成 API 密钥。一个密钥最多可用于五个域。有关信息，请参阅 管理 JS 验证码 API 的 API 密钥。

必需：是

类型：`string`

onSuccess: (wafToken: string) => void;

当最终用户成功完成验证码拼图时，使用有效 AWS WAF 令牌调用。在发送到使用 AWS WAF Web ACL 保护的终端节点的请求中使用该令牌。该令牌提供了最近成功完成拼图的证明和时间戳。

必需：是

onError?: (error: CaptchaError) => void;

在验证码操作期间发生错误时，使用错误对象调用。

必需：否

CaptchaError 类定义 – `onError` 处理程序使用以下类定义提供错误类型。

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- kind – 返回的错误类型。
- statusCode – HTTP 状态码（如果有）。如果错误是由于 HTTP 错误造成的，则 network_error 将使用此选项。

onLoad?: () => void;

在加载新的验证码拼图时调用。

必需：否

onPuzzleTimeout?: () => void;

在验证码拼图过期前未完成时调用。

必需：否

onPuzzleCorrect?: () => void;

当有人为验证码拼图提供正确答案时调用。

必需：否

onPuzzleIncorrect?: () => void;

当有人为验证码拼图提供不正确答案时调用。

必需：否

defaultLocale

用于验证码拼图的默认语言环境。验证码拼图的书面说明有阿拉伯语 (ar-SA)、简体中文 (zh-CN)、荷兰语 (nl-NL)、英语 (en-US)、法语 (fr-FR)、德语 (de-DE)、意大利语 (it-IT)、日语 (ja-JP)、巴西葡萄牙语 (pt-BR)、西班牙语 (es-ES) 和土耳其语 (tr-TR)。除了中文和日语（默认为英语）外，所有书面语言都提供音频指令。要更改默认语言，请提供国际语言和区域代码，例如ar-SA。

默认：最终用户浏览器中当前使用的语言

必需：否

类型：string

disableLanguageSelector

如果设置为 true，则验证码拼图会隐藏语言选择器。

默认值：false

必需：否

类型：boolean

dynamicWidth

如果设置为 true，则验证码拼图会更改宽度以与浏览器窗口宽度兼容。

默认值：false

必需：否

类型：boolean

skipTitle

如果设置为 true，则验证码拼图不会显示拼图标题完成拼图。

默认值：false

必需：否

类型：boolean

如何显示验证码拼图

你可以在客户端界面中随心所欲地使用该 AWS WAF renderCaptcha呼叫。该呼叫从中检索验证码拼图 AWS WAF，对其进行渲染，然后将结果发送到进行验证。 AWS WAF 调用时，您需要提供拼图显示配置以及最终用户完成拼图时要运行的回调。有关选项的更多信息，请参阅上一部分 验证码 API 规范 JavaScript 。

将此调用与智能威胁集成 API 的令牌管理功能结合使用。该调用将为您的客户端提供一个令牌，用于验证验证码拼图是否成功完成。使用智能威胁集成 API 来管理令牌，并在客户端对受 AWS WAF Web ACL 保护的端点的调用中提供令牌。有关智能威胁 API 的信息，请参阅 使用智能威胁 JavaScript API。

实施示例

以下示例列表显示了标准的 CAPTCHA 实现，包括 AWS WAF 集成 URL 在该部分中的<head>位置。

该列表将使用智能威胁集成 API 的 AwsWafIntegration.fetch 包装程序配置带有成功回调的 renderCaptcha 函数。有关此函数的信息，请参阅 如何使用集成 fetch 包装程序。

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
```

```
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

配置设置示例

以下示例列表显示了宽度和标题选项的非默认设置 `renderCaptcha`。

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

有关配置选项的全部信息，请参阅 验证码 API 规范 JavaScript 。

处理来自的验证码响应 AWS WAF

如果匹配的 Web 请求没有带有有效 CAPTCHA 时间戳的令牌，则带有CAPTCHA操作的 AWS WAF 规则将终止对该请求的评估。如果请求是 GET 文本/html 调用，则该 CAPTCHA 操作将向客户端提供带有验证码拼图的插页式广告。当你不集成 CAPTCHA JavaScript API 时，插页式广告会运行拼图，如果最终用户成功解决了这个问题，则会自动重新提交请求。

当你集成 CAPTCHA JavaScript API 并自定义验证码处理时，你需要检测终止的验证码响应，提供你的自定义 CAPTCHA，然后如果最终用户成功解决了难题，则重新提交客户的 Web 请求。

以下代码示例演示如何执行此操作。

> **Note**
>
> AWS WAF CAPTCHA操作响应的状态码为 HTTP 405，我们用它来识别此代码中的CAPTCHA响应。如果您的受保护端点使用 HTTP 405 状态代码为同一调用传递任何其他类型的响应，本示例代码也会为这些响应显示验证码拼图。

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
```

```
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

管理 JS 验证码 API 的 API 密钥

要将 AWS WAF 验证码集成到带有 JavaScript API 的客户端应用程序中，您需要用于运行验证码拼图的客户端域的 API 集成标签和加密 API 密钥。 JavaScript

的 CAPTCHA 应用程序集成 JavaScript 使用加密的 API 密钥来验证客户端应用程序域是否有权使用 AWS WAF CAPTCHA API。当您从 JavaScript 客户端调用 CAPTCHA API 时，您需要提供一个 API 密钥和一个包含当前客户端域名的域名列表。您最多可以在一个加密密钥中列出 5 个域名。

API 密钥要求

您在验证码集成中使用的 API 密钥必须包含一个适用于您使用密钥的客户端的域。

- 如果您在客户的智能威胁集成中指定了 `window.awsWafCookieDomainList`，那么您的 API 密钥中至少有一个域必须与 `window.awsWafCookieDomainList` 中的一个令牌域完全匹配，或者必须是其中一个令牌域的顶点域。

  例如，对于令牌域 `mySubdomain.myApex.com`，API 密钥 `mySubdomain.myApex.com` 完全匹配，API 密钥 `myApex.com` 是顶点域。任一密钥都与令牌域相匹配。

  有关设置令牌域列表的信息，请参阅 提供用于令牌的域名。
- 否则，当前域名必须包含在 API 密钥中。当前域名是您可以在浏览器地址栏中看到的域名。

根据受保护的主机域和为 Web ACL 配置的令牌域列表，您使用的域必须是可以接受的域。 AWS WAF 有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

如何为 API 密钥选择区域

AWS WAF 可以在任何可用的区域生成验证码 API 密钥。 AWS WAF

通常，您应使用与网页 ACL 相同的区域作为验证码 API 密钥。但是，如果您希望全球受众使用区域性网络 ACL，则可以获取范围为的 CAPTCHA JavaScript 集成标签 CloudFront 和作用域为 API 密钥，然后将其与区域网络 ACL 一起使用。 CloudFront这种方法允许客户从离他们最近的区域加载验证码拼图，从而减少延迟。

不支持在多个区域之间使用的 CAPTCHA API 密钥范围以外的 CloudFront 区域。它们只能在适用范围内的区域中使用。

为您的客户端域生成 API 密钥

通过控制台获取集成 URL 并生成和检索 API 密钥。

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 应用程序集成。
3. 在为应用程序集成启用的 Web ACL 窗格中，选择要用于 API 密钥的区域。您也可以在验证码集成选项卡的 API 密钥窗格中选择区域。
4. 选择验证码集成选项卡。此选项卡提供可在 JavaScript 集成中使用的 CAPTCHA 集成标签以及 API 密钥列表。两者的作用域均限于所选区域。
5. 在 API 密钥窗格中，选择生成密钥。此时将显示生成密钥对话框。
6. 输入要包含在密钥中的客户端域。您最多可以输入 5 个。完成后，选择生成密钥。界面返回到验证码集成选项卡，其中列出了您的新密钥。

   API 密钥一经创建，即不可变。如果您需要更改密钥，请生成一个新密钥并改用该密钥。
7. （可选）复制新生成的密钥以用于集成。

您也可以使用 REST API 或特定语言的 AWS 软件开发工具包来完成这项工作。REST API 调用是 createApiKey 和 listapiK eys。

删除 API 密钥

要删除 API 密钥，必须使用 REST API 或特定语言的 AWS 软件开发工具包。REST API 调用是 deleteaPiKey。您无法使用控制台删除密钥。

删除密钥后，最长可能需要 24 小时 AWS WAF 才能禁止在所有地区使用该密钥。

AWS WAF 移动应用程序集成

您可以使用 AWS WAF 移动软件开发工具包实现适用于 Android 和 iOS 移动应用程序的 AWS WAF 智能威胁集成 SDK。

- 对于安卓移动应用程序， AWS WAF 软件开发工具包适用于安卓 API 版本 23（安卓版本 6）及更高版本。有关 Android 版本的信息，请参阅软件开发工具包平台发行说明。
- 对于 iOS 移动应用程序， AWS WAF 软件开发工具包适用于 iOS 版本 13 及更高版本。有关 iOS 版本的信息，请参阅 iOS 和 iPadOS 发行说明。

使用移动软件开发工具包，您可以管理令牌授权，并将令牌包含在发送到受保护资源的请求中。通过使用软件开发工具包，可以确保客户端的这些远程过程调用包含有效的令牌。此外，在应用程序页面上进行这种集成后，您可以在 Web ACL 中实施缓解规则，例如阻止不包含有效令牌的请求。

要访问移动软件开发工具包，请通过联系 AWS 联系支持人员。

> **Note**
>
> 移 AWS WAF 动 SDK 不可用于验证码自定义。

使用 SDK 的基本方法是使用配置对象创建令牌提供者，然后使用令牌提供者从中检索令牌 AWS WAF。默认情况下，令牌提供程序会在您向受保护资源发出的 Web 请求中包含检索到的令牌。

以下是软件开发工具包实施的部分列表，其中显示了主要组件。有关更多详细示例，请参阅为 AWS WAF 移动 SDK 编写代码。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

安装 AWS WAF 移动 SDK

要访问移动软件开发工具包，请通过联系 AWS 联系支持人员。

首先在测试环境中实施移动软件开发工具包，然后在生产环境中实施。

安装移 AWS WAF 动 SDK

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 应用程序集成。
3. 在智能威胁集成选项卡中，执行以下操作：
   a. 在为应用程序集成启用的 Web ACL窗格中，找到要与之集成的 Web ACL。复制并保存 Web ACL 集成 URL，以便在实施中使用。您也可以通过 API 调用 `GetWebACL` 获取此 URL。
   b. 选择移动设备类型和版本，然后选择下载。你可以选择任何你喜欢的版本，但我们建议使用最新版本。 AWS WAF 将设备上的`zip`文件下载到您的标准下载位置。
4. 在您的应用程序开发环境中，将文件解压缩到您选择的工作位置。在 zip 文件的顶级目录中，找到并打开 `README`。按照`README`文件中的说明安装 AWS WAF 移动 SDK，以便在您的移动应用程序代码中使用。
5. 根据以下各部分中的指导对您的应用程序进行编程。

移 AWS WAF 动 SDK 规范

本节列出了最新可用版本的 AWS WAF 移动软件开发工具包的软件开发工具包对象、操作和配置设置。有关令牌提供程序和操作如何处理各种配置设置组合的详细信息，请参阅 AWS WAF 移动 SDK 的工作原理。

`WAFToken`

持有 AWS WAF 代币。

`getValue()`

检索 `WAFToken` 的 `String` 表示形式。

`WAFTokenProvider`

在您的移动应用程序中管理令牌。使用 `WAFConfiguration` 对象实施此目的。

`getToken()`

如果启用了后台刷新，则会返回缓存的令牌。如果禁用了后台刷新，则会对进行同步阻塞调用，AWS WAF 以检索新令牌。

onTokenReady(WAFTokenResultCallback)

指示令牌提供程序刷新令牌并在活动令牌准备就绪时调用提供的回调。当令牌被缓存并准备就绪时，令牌提供程序将在后台线程中调用您的回调。在应用程序首次加载和恢复活动状态时调用此函数。有关返回活动状态的更多信息，请参阅 the section called “在应用程序处于非活动状态后检索令牌”。

对于 Android 或 iOS 应用程序，您可以设置 `WAFTokenResultCallback` 为希望令牌提供程序在请求的令牌准备就绪时调用的操作。您的 `WAFTokenResultCallback` 实施必须采用参数 `WAFToken`，`SdkError`。对于 iOS 应用程序，您可以交替创建内联函数。

storeTokenInCookieStorage(WAFToken)

指示将指定的 AWS WAF 令牌存储`WAFTokenProvider`到软件开发工具包的 Cookie 管理器中。默认情况下，只有在首次获取令牌和刷新令牌时，才会将其添加到 Cookie 存储中。如果应用程序出于任何原因清除了共享 Cookie 存储，则在下次刷新之前，SDK 不会自动重新添加 AWS WAF 令牌。

WAFConfiguration

保存 `WAFTokenProvider` 实施的配置。实施此操作时，您需要提供 Web ACL 的集成 URL、要在令牌中使用的域名以及您希望令牌提供程序使用的任何非默认设置。

以下列表指定了可以在 `WAFConfiguration` 对象中管理的配置设置。

applicationIntegrationUrl

应用程序集成 URL。从 AWS WAF 控制台或通过 `getWebACL` API 调用获取。

必需：是

类型：应用程序专用 URL。对于 iOS，请参阅 iOS URL。对于 Android 系统，请参阅 java.net URL。

backgroundRefreshEnabled

表示您是否希望令牌提供程序在后台刷新令牌。如果您设置了此选项，则令牌提供程序会根据管理自动令牌刷新活动的配置设置在后台刷新您的令牌。

必需：否

类型：`Boolean`

默认值：TRUE

domainName

要在令牌中使用的域名，用于令牌获取和 Cookie 存储。例如，example.com 或 aws.amazon.com。这通常是与 Web ACL 关联的资源的主机域，您将在其中发送 Web 请求。对于 ACFP 托管规则组 AWSManagedRulesACFPRuleSet，这通常是一个与您在规则组配置中提供的账户创建路径中的域相匹配的单个域。对于 ATP 托管规则组 AWSManagedRulesATPRuleSet，这通常是一个与您在规则组配置中提供的登录路径中的域相匹配的单个域。

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

根据受保护的主机域和 Web ACL 的令牌域列表，该域必须是可以接受的域。 AWS WAF 有关更多信息，请参阅 AWS WAF Web ACL 令牌域列表配置。

必需：是

类型：String

maxErrorTokenRefreshDelayMsec

尝试失败后，重复令牌刷新之前等待的最长时间（以毫秒为单位）。此值在令牌检索失败且重试 maxRetryCount 次后使用。

必需：否

类型：Integer

默认值：5000（5 秒）

允许的最小值：1（1 毫秒）

允许的最大值：30000（30 秒）

maxRetryCount

请求令牌时使用指数回退执行的最大重试次数。

必需：否

类型：Integer

默认值：如果启用了背景刷新，则为 5。否则为 3。

允许的最小值：0

允许的最大值：10

setTokenCookie

表示您是否希望软件开发工具包的 Cookie 管理器在您的请求中添加令牌 Cookie。默认情况下，这会向所有请求添加一个令牌 Cookie。Cookie 管理器会向任何路径在 tokenCookiePath 中指定的路径之下的请求添加令牌 Cookie。

必需：否

类型：Boolean

默认值：TRUE

tokenCookiePath

当 setTokenCookie 是 TRUE 时使用。表示您希望软件开发工具包的 Cookie 管理器在其中添加令牌 Cookie 的顶级路径。管理员会将令牌 Cookie 添加到您发送到该路径的所有请求以及所有子路径中。

例如，如果您将其设置为 /web/login，则管理器将包含发送到 /web/login 的所有内容及其任何子路径的令牌 Cookie，例如 /web/login/help。它不包括发送到其他路径的请求的令牌，例如 /、/web 或 /web/order。

必需：否

类型：String

默认值：/

tokenRefreshDelaySec

用于背景刷新。后台令牌刷新之间的最长时间（以秒为单位）。

必需：否

类型：Integer

默认值：88

允许的最小值：88

允许的最大值：300（5 分钟）

AWS WAF 移动 SDK 的工作原理

移动软件开发工具包为您提供可配置的令牌提供程序，可用于令牌检索和使用。令牌提供程序会验证您允许的请求是否来自合法客户。当你向你保护的 AWS 资源发送请求时 AWS WAF，你需要在 Cookie 中加入令牌来验证请求。您可以手动处理令牌 Cookie，也可以让令牌提供程序为您处理。

本节介绍移动软件开发工具包中包含的类、属性和方法之间的交互。有关软件开发工具包规范，请参阅移 AWS WAF 动 SDK 规范。

令牌检索和缓存

在移动应用程序中创建令牌提供程序实例时，您可以配置您希望它如何管理令牌和令牌检索。您的主要选择是如何维护有效的、未过期的令牌，以便在应用的 Web 请求中使用：

- 启用后台刷新 – 这是默认设置。令牌提供程序会在后台自动刷新令牌并将其缓存。启用后台刷新后，当您调用 `getToken()` 时，该操作将检索缓存的令牌。

  令牌提供程序以可配置的时间间隔执行令牌刷新，以便在应用程序处于活动状态时，缓存中始终有未过期的令牌可用。当您的应用程序处于非活动状态时，后台刷新会暂停。有关此问题的信息，请参阅在应用程序处于非活动状态后检索令牌。
- 禁用后台刷新 – 您可以禁用后台令牌刷新，然后仅按需检索令牌。按需检索的令牌不会被缓存，您可以根据需要检索多个令牌。每个令牌都独立于您检索的任何其他令牌，并且每个令牌都有自己的时间戳，用于计算到期时间。

  禁用后台刷新后，您可以选择以下令牌检索：
  - **`getToken()`**— 当您在禁`getToken()`用后台刷新的情况下呼叫时，调用会同步从中检索新令牌。 AWS WAF这可能是一个阻塞调用，如果在主线程上调用，可能会影响应用程序的响应速度。
  - **`onTokenReady(WAFTokenResultCallback)`** – 此调用异步检索新令牌，然后在令牌准备就绪时在后台线程中调用提供的结果回调。

令牌提供程序如何重试失败的令牌检索

检索失败时，令牌提供程序会自动重试令牌检索。重试最初是使用指数回退来执行的，起始重试等待时间为 100 ms。有关指数重试的信息，请参阅 AWS中的错误重试和指数回退。

当重试次数达到配置的 maxRetryCount 时，令牌提供程序要么停止尝试，要么切换为每 maxErrorTokenRefreshDelayMsec 毫秒尝试一次，具体取决于令牌检索的类型：

- **onTokenReady()** – 令牌提供程序切换到两次尝试之间的等待 maxErrorTokenRefreshDelayMsec 毫秒，并继续尝试检索令牌。
- 后台刷新 – 令牌提供程序切换到两次尝试之间的等待 maxErrorTokenRefreshDelayMsec 毫秒，并继续尝试检索令牌。
- 禁用后台刷新时按需 **getToken()** 调用 – 令牌提供程序停止尝试检索令牌并返回之前的令牌值，如果没有以前的令牌，则返回空值。

在应用程序处于非活动状态后检索令牌

仅当您的应用类型被视为处于活动状态时，才会执行后台刷新：

- iOS – 当应用程序位于前台时，将执行后台刷新。
- Android – 无论是在前台还是在后台，都是在应用程序未关闭时执行后台刷新。

如果您的应用程序处于任何不支持后台刷新的状态的时间超过您配置的 tokenRefreshDelaySec 秒数，则令牌提供程序会暂停后台刷新。例如，对于 iOS 应用程序，如果 tokenRefreshDelaySec 为 300 并且应用程序关闭或进入后台超过 300 秒，则令牌提供程序将停止刷新令牌。当应用程序恢复到活动状态时，令牌提供程序会自动重新启动后台刷新。

当您的应用程序恢复到活动状态时，请调用 onTokenReady()，以便在令牌提供程序检索并缓存新令牌时通知您。不要随便调用 getToken()，因为缓存中可能还不包含当前有效的令牌。

为 AWS WAF 移动 SDK 编写代码

此部分提供使用软件开发工具包的代码示例。

初始化令牌提供程序并获取令牌

您可以使用配置对象启动令牌提供程序实例。然后，您可以使用可用操作检索令牌。以下是所需代码的基本组件。

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
```

```
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

Java 示例：

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);
```

```
// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Kotlin 示例：

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
}
```

允许软件开发工具包在您的 HTTP 请求中提供令牌 Cookie

如果 setTokenCookie 是 TRUE，令牌提供者会在您向 tokenCookiePath 中指定的路径下的所有位置发出的网络请求中为您包含令牌 Cookie。默认情况下，setTokenCookie 为 TRUE，tokenCookiePath 为 /。

您可以通过指定令牌 Cookie 路径来缩小包含令牌 Cookie 的请求的范围，例如 /web/login。如果您这样做，请检查您的 AWS WAF 规则是否未检查您发送到其他路径的请求中的令牌。使用 AWSManagedRulesACFPRuleSet 规则组时，您可以配置账户注册和创建路径，规则组会检查发送到这些路径的请求中的令牌。有关更多信息，请参阅 将 ACFP 托管规则组添加到您的 Web ACL。同样，当您使用 AWSManagedRulesATPRuleSet 规则组时，您可以配置登录路径，规则组会检查发送到该路径的请求中的令牌。有关更多信息，请参阅 将 ATP 托管规则组添加到您的 Web ACL。

iOS

如果setTokenCookie是TRUE，则令牌提供者会将 AWS WAF 令牌存储在 a 中，HTTPCookieStorage.shared并自动将该 Cookie 包含在对您在中指定的域的请求中WAFConfiguration。

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

如果setTokenCookie是TRUE，则令牌提供者将 AWS WAF 令牌存储在应用程序范围内共享的CookieHandler实例中。令牌提供程序会自动将 Cookie 包含在对您在 WAFConfiguration 中指定的域的请求中。

Java 示例：

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Kotlin 示例：

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
```

```
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

如果您已经初始化了 CookieHandler 默认实例，则令牌提供程序将使用它来管理 Cookie。否则，令牌提供者将使用该令 AWS WAF 牌初始化一个新CookieManager实例，CookiePolicy.ACCEPT_ORIGINAL_SERVER然后将此新实例设置为中的默认实例CookieHandler。

以下代码显示了当 Cookie 管理器和 Cookie 处理程序在您的应用程序中不可用时，软件开发工具包如何对其进行初始化。

Java 示例：

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Kotlin 示例：

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

在您的 HTTP 请求中手动提供令牌 Cookie

如果您将 setTokenCookie 设置为 FALSE，则需要在向受保护端点发出的请求中手动提供令牌 Cookie，作为 Cookie HTTP 请求标头。以下代码演示了如何执行此操作。

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
```

```
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

Java 示例：

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Kotlin 示例：

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHA然后Challenge在 AWS WAF

您可以将 AWS WAF 规则配置为对符合规则检查标准的 Web 请求运行CAPTCHA或Challenge操作。您还可以对 JavaScript 客户端应用程序进行编程，使其在本地运行 CAPTCHA 拼图和浏览器挑战。

只有当浏览器访问 HTTPS 端点时，才能运行验证码谜题和静默挑战。浏览器客户端必须在安全的环境中运行才能获取令牌。

- CAPTCHA— 要求最终用户解开 CAPTCHA 难题，以证明有人在发送请求。验证码拼图旨在让人类相当容易和快速地成功完成拼图，而计算机很难成功完成或随机完成。

  在 Web ACL 规则中，CAPTCHA 通常用于某项Block操作会阻止过多的合法请求，但允许所有流量通过会导致大量不想要的请求（例如来自机器人的请求）。有关规则操作行为的信息，请参阅AWS WAFCAPTCHA 和 Challenge 规则操作的工作原理。

  您还可以在客户端应用程序集成 API 中编程 CAPTCHA 拼图实现。当你这样做时，你可以自定义拼图在客户端应用程序中的行为和位置。有关更多信息，请参阅 AWS WAF 客户端应用程序集成。
- Challenge— 运行静默挑战，要求客户端会话验证它是浏览器，而不是机器人。验证在后台运行，不涉及最终用户。这是一个不错的选择，可以验证您怀疑无效的客户端，而不会通过验证码拼图对最终

用户体验产生负面影响。有关规则操作行为的信息，请参阅AWS WAFCAPTCHA 和 Challenge 规则操作的工作原理。

Challenge 规则操作类似于客户端智能威胁集成 API 运行的质询，如 AWS WAF 客户端应用程序集成 中所述。

> **Note**
>
> 当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中将其作为规则操作覆盖时，您需要支付额外费用。有关更多信息，请参阅AWS WAF 定价。

有关所有规则操作选项的说明，请参阅规则操作。

主题

- AWS WAF 验证码拼图
- AWS WAFCAPTCHA 和 Challenge 规则操作的工作原理
- 使用 CAPTCHA 和Challenge 操作的最佳实践

AWS WAF 验证码拼图

AWS WAF 提供标准的 CAPTCHA 功能，要求用户确认自己是人类。验证码代表完全自动化的公共图灵测试，用于区分计算机和人类。验证码拼图旨在验证人类是否在发送请求，并防止网页抓取、凭证填充和垃圾邮件等活动。验证码谜题无法清除所有不需要的请求。使用机器学习和人工智能已经解决了许多难题。为了规避验证码，一些组织通过人工干预来补充自动化技术。尽管如此，验证码仍然是防止不太复杂的机器人流量和增加大规模运营所需资源的有用工具。

AWS WAF 随机生成其 CAPTCHA 谜题并轮流浏览它们，以确保向用户提供独特的挑战。 AWS WAF 定期添加新的谜题类型和风格，以保持对抗自动化技术的有效性。除了谜题之外， AWS WAF CAPTCHA脚本还收集有关客户端的数据，以确保任务由人类完成并防止重播攻击。

每个验证码拼图都包含一组标准控件，供最终用户申请新拼图、在音频和视觉拼图之间切换、访问其他说明以及提交拼图解决方案。所有拼图都支持屏幕阅读器、键盘控制和对比色。

AWS WAF CAPTCHA 拼图符合《网络内容无障碍指南》(WCAG) 的要求。有关信息，请参阅万维网联盟 (W3C) 网站上的网络内容无障碍指南 (WCAG) 概述。

主题

验证码拼图语言支持

CAPTCHA 拼图从客户端浏览器语言的书面说明开始，如果浏览器语言不支持，则使用英语。拼图通过下拉菜单提供了其他语言选项。

用户可以通过选择页面底部的耳机图标来切换到音频指令。拼图的音频版本提供了有关文本的口语说明，用户应在文本框中键入这些文本，并被背景噪音覆盖。

下表列出了您可以为验证码拼图中的书面说明选择的语言以及每种选择的音频支持。

AWS WAF CAPTCHA 拼图支持的语言

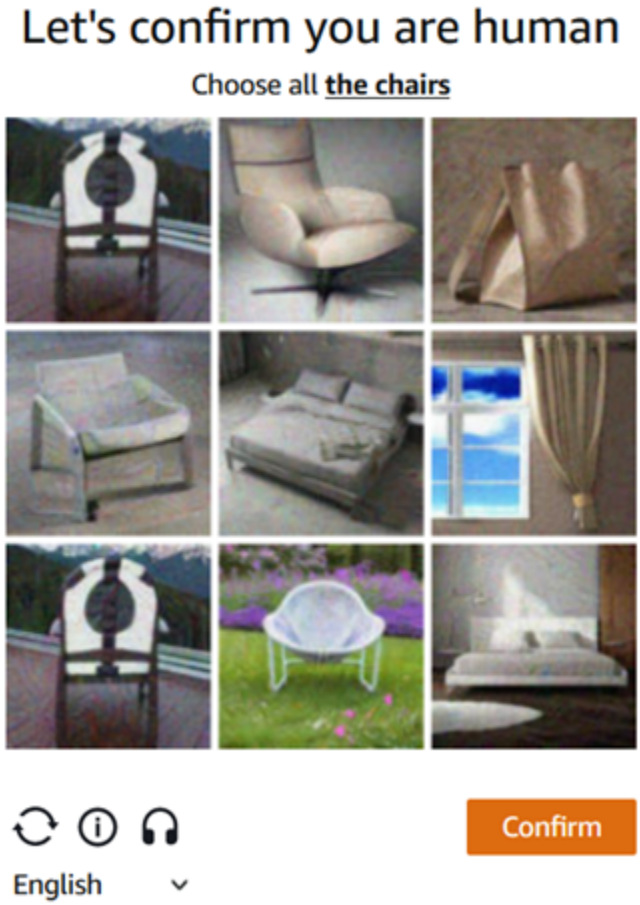
书面说明支持	区域代码	支持音频指令
阿拉伯语	ar-sa	阿拉伯语
简体中文	zh-CN	英语音频
荷兰语	nl-NL	荷兰语
English	en-US	English
French	fr-FR	法语
德语	de-DE	德语
意大利语	it-IT	意大利语
日语	ja-JP	英语音频
巴西葡萄牙语	pt-BR	巴西葡萄牙语

书面说明支持	区域代码	支持音频指令
西班牙语	es-ES	西班牙语
土耳其语	tr-TR	土耳其语

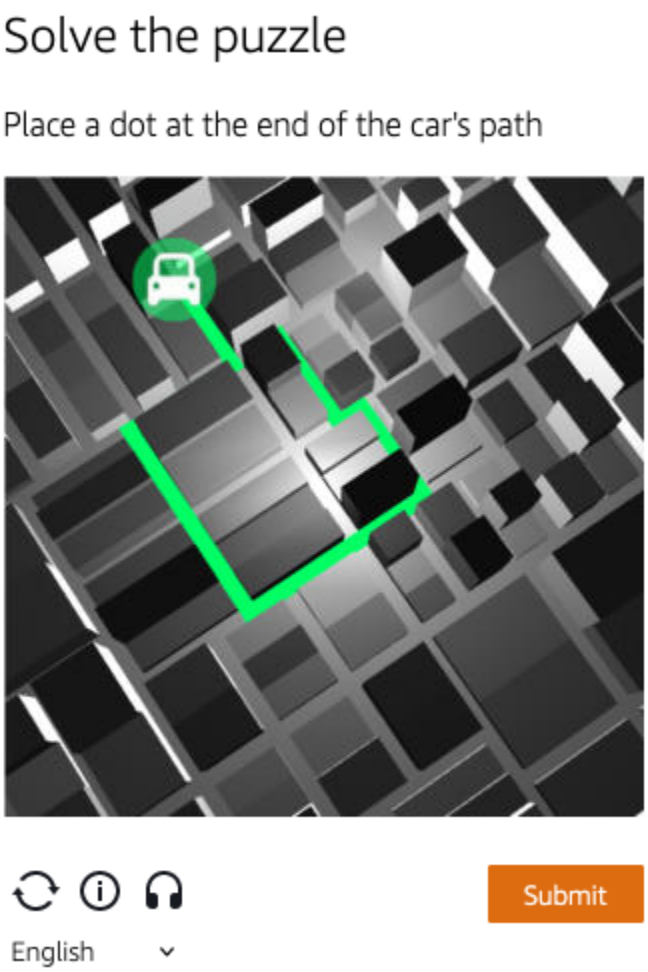
验证码拼图示例

典型的视觉验证码拼图需要交互才能表明用户可以理解一张或多张图像并与之交互。

以下屏幕截图显示了图片网格拼图的示例。这个拼图需要你选择网格中包含特定类型物体的所有图片。

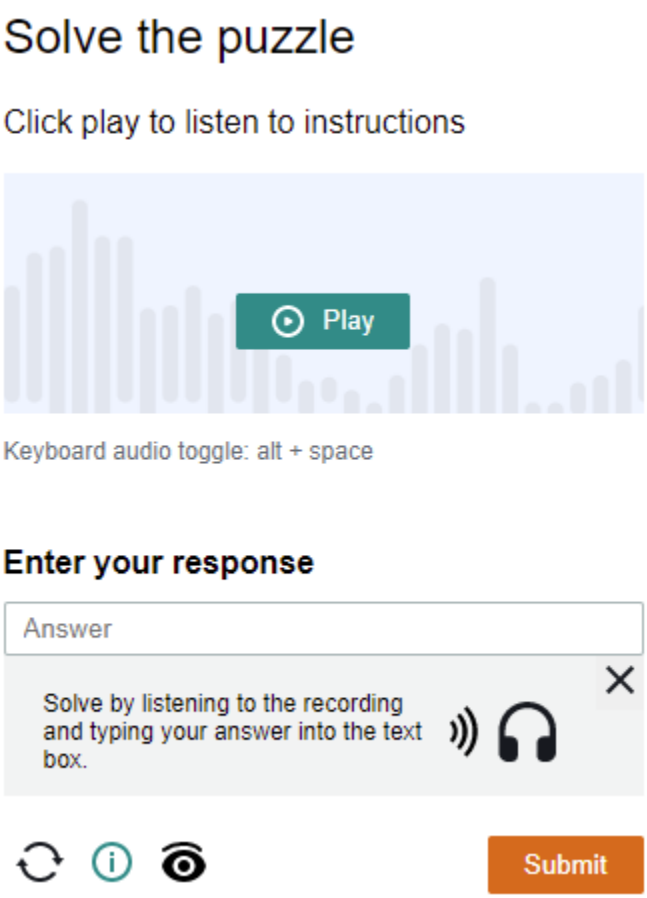


以下屏幕截图显示了一个示例拼图，它要求您在绘图中识别汽车路径的终点。



音频拼图提供背景噪音，上面有关于用户应在文本框中键入的文本的口语说明。

以下屏幕截图显示音频拼图选项的显示。



AWS WAFCAPTCHA 和 Challenge 规则操作的工作原理

AWS WAF CAPTCHA并且Challenge是标准规则操作，因此它们相对容易实现。要使用其中任何一个，您需要为规则创建检查条件，以确定要检查的请求，然后指定两个规则操作之一。有关规则操作选项的一般信息，请参阅 规则操作。

除了从服务器端实现静默挑战和验证码谜题外，你还可以在你的 JavaScript iOS 和 Android 客户端应用程序中集成静默挑战，也可以在客户端中渲染验证码拼图。 JavaScript 这些集成使您能够为最终用户提供更好的性能和验证码拼图体验，还可以降低与使用规则操作和智能威胁缓解规则组相关的成本。有关这些选项的详细信息，请参阅 AWS WAF 客户端应用程序集成。有关定价信息，请参阅 AWS WAF 定价。

主题

- CAPTCHA 和 Challenge 操作行为
- CAPTCHA 和 Challenge 日志和指标中的操作

CAPTCHA 和 Challenge 操作行为

当 Web 请求与规则的检查标准相匹配CAPTCHA或Challenge操作时，将根据其令牌状态和免疫时间配置来 AWS WAF 决定如何处理请求。 AWS WAF 还会考虑请求是否可以处理验证码拼图或挑战脚本插页式广告。这些脚本被设计为作为 HTML 内容处理，只有期望 HTML 内容的客户端才能正确处理它们。

> **Note**
>
> 当您在其中一个规则中使用 CAPTCHA 或 Challenge 规则操作或在规则组中将其作为规则操作覆盖时，您需要支付额外费用。有关更多信息，请参阅AWS WAF 定价。

操作如何处理 Web 请求

AWS WAF 按如下方式对 Web 请求应用CAPTCHA或Challenge操作：

- 有效令牌 — AWS WAF 处理方式与Count操作类似。 AWS WAF 应用您为规则操作配置的所有标签和请求自定义，然后使用 Web ACL 中的其余规则继续评估请求。
- 令牌缺失、无效或已过期 — AWS WAF 停止对请求进行 Web ACL 评估并阻止其前往预期目的地。

  AWS WAF 根据规则操作类型生成一个响应，然后将其发送回客户端：

  - Challenge – AWS WAF 在响应字段中包含以下内容：
    - 值为 `challenge` 的标头 `x-amzn-waf-action`。

      > **Note**
      >
      > 在客户端浏览器中运行的 JavaScript 应用程序无法使用此标头。有关详细信息，请参阅以下部分。

    - HTTP 状态代码 `202 Request Accepted`。
    - 如果请求包含值为的`Accept`标头`text/html`，则响应将包括带有质询脚本的JavaScript 页面插页式广告。
  - CAPTCHA— 在响应中 AWS WAF 包括以下内容：
    - 值为 `captcha` 的标头 `x-amzn-waf-action`。

> **Note**
>
> 在客户端浏览器中运行的 JavaScript 应用程序无法使用此标头。有关详细信息，请参阅以下部分。

- HTTP 状态代码 `405 Method Not Allowed`。
- 如果请求包含值为的`Accept`标头`text/html`，则响应将包含带有验证码脚本的JavaScript 页面插页式广告。

要在 Web ACL 或规则级别配置令牌到期时间，请参阅 时间戳过期： AWS WAF 代币免疫时间。

在客户端浏览器中运行的 JavaScript 应用程序无法使用标头

当使用验证码或质询 AWS WAF 响应来响应客户端请求时，它不包括跨源资源共享 (CORS) 标头。CORS 标头是一组访问控制标头，它们告诉客户端 Web 浏览器 JavaScript应用程序可以使用哪些域、HTTP 方法和 HTTP 标头。如果没有 CORS 标头，在客户端浏览器中运行的 JavaScript 应用程序将无法访问 HTTP 标头，因此无法读取CAPTCHA和Challenge响应中提供的`x-amzn-waf-action`标头。

质询和验证码插页式广告的用途

当质询插页式广告运行时，在客户端成功响应之后，如果它还没有令牌，则插页式广告会为其初始化一个令牌。然后，它会使用质询解题时间戳更新令牌。

当验证码插页式广告运行时，如果客户端还没有令牌，验证码插页式广告会首先调用质询脚本来质询浏览器并初始化令牌。然后，插页式广告运行了验证码拼图。当最终用户成功完成拼图后，插页式广告会使用验证码解算时间戳更新令牌。

无论哪种情况，在客户端成功响应并且脚本更新令牌后，脚本都会使用更新的令牌重新提交原始 Web 请求。

您可以配置如何 AWS WAF 处理令牌。有关信息，请参阅AWS WAF 网络请求令牌。

CAPTCHA 和 Challenge 日志和指标中的操作

CAPTCHA 和 Challenge 操作可以是非终止的，如 Count，也可以是终止的，如 Block。结果取决于请求是否具有有效令牌以及该操作类型的未过期时间戳。

- 有效令牌-当操作找到有效令牌且未阻止请求时，会按以下方式 AWS WAF 捕获指标和日志：

- 增加 CaptchaRequests 和 RequestsWithValidCaptchaToken 或 ChallengeRequests 和 RequestsWithValidChallengeToken 的指标。
- 将匹配项记录为带有 CAPTCHA 或 Challenge 操作的 nonTerminatingMatchingRules 条目。以下列表显示了与 CAPTCHA 操作相关的此类匹配的日志部分。

```
  "nonTerminatingMatchingRules": [
  {
    "ruleId": "captcha-rule",
    "action": "CAPTCHA",
    "ruleMatchDetails": [],
    "captchaResponse": {
      "responseCode": 0,
      "solveTimestamp": 1632420429
    }
  }
]
```

- 令牌@@ 丢失、无效或已过期-当操作因令牌丢失或无效而阻止请求时，会按以下方式 AWS WAF 捕获指标和日志：
  - 增加 CaptchaRequests 或 ChallengeRequests 的指标。
  - 将匹配项记录为带有 HTTP 405 状态码的 CaptchaResponse 条目或带有 HTTP 202 状态码的 ChallengeResponse 条目。该日志会显示请求是缺少令牌还是时间戳已过期。该日志还会显示是 AWS WAF 向客户端发送了 CAPTCHA 插页式页面还是向客户端浏览器发送了静默质询。以下列表显示了与 CAPTCHA 操作相关的此类匹配的日志部分。

```
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  ...
  "responseCodeSent": 405,
  ...
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
```

有关 AWS WAF 日志的信息，请参阅记录 AWS WAF Web ACL 流量。

有关 AWS WAF 指标的信息，请参阅AWS WAF 指标和维度。

有关规则操作选项的信息，请参阅 规则操作。

使用 CAPTCHA 和Challenge 操作的最佳实践

按照本节中的指导来计划和实施 AWS WAF CAPTCHA 或质疑。

规划您的验证码并质询实施

根据您的网站使用情况、要保护的数据的敏感度以及请求的类型，确定在哪里放置验证码拼图或静默质询。选择您要应用验证码的请求，这样您就可以根据需要展示拼图，但要避免在没有用处且可能降低用户体验的地方展示拼图。使用该Challenge操作来运行静默挑战，这些挑战对最终用户影响较小，但仍有助于验证请求是否来自 JavaScript 已启用的浏览器。

只有当浏览器访问 HTTPS 端点时，才能运行验证码谜题和静默挑战。浏览器客户端必须在安全的环境中运行才能获取令牌。

决定在哪里对您的客户进行验证码拼图和静默质询

确定您不希望受到验证码影响的请求，例如对 CSS 或图像的请求。仅在必要时使用验证码。例如，如果您计划在登录时进行验证码检查，并且用户总是直接从登录到另一个屏幕，则可能不需要在第二个屏幕上进行验证码检查，这可能会降低您的最终用户体验。

配置Challenge并CAPTCHA使用，以便 AWS WAF 仅在响应请求时发送验证码谜题和静默挑战。`GET` `text/html`您不能运行拼图或质询来响应 `POST` 请求、跨源资源共享 (CORS) 预检 `OPTIONS` 请求或任何其他非 `GET` 请求类型。其他请求类型的浏览器行为可能有所不同，可能无法正确处理插页式广告。

客户可以接受 HTML，但仍然无法处理验证码或质询插页式广告。例如，带有小 iFrame 的网页上的控件可能接受 HTML，但无法显示或处理验证码。避免为这些类型的请求设置规则操作，就像对不接受 HTML 的请求一样。

使用 CAPTCHA 或 Challenge 验证之前的令牌获取

在合法用户应始终拥有有效令牌的地方，您只能使用规则操作来验证是否存在有效令牌。在这些情况下，请求能否处理插页式广告并不重要。

例如，如果您实现了 JavaScript 客户端应用程序 CAPTCHA API，并在向受保护的端点发送第一个请求之前立即在客户端上运行 CAPTCHA 拼图，则您的第一个请求应始终包含对质询和验证码均有效的令牌。有关 JavaScript 客户端应用程序集成的信息，请参见AWS WAF JavaScript 集成。

对于这种情况，您可以在 Web ACL 中添加与第一个调用匹配的规则，并使用 Challenge 或 CAPTCHA 规则操作对其进行配置。当规则与合法的最终用户和浏览器匹配时，该操作将找到有效的令牌，因此不会阻止请求或发送质询或验证码拼图作为响应。有关规则操作的工作原理的更多信息，请参阅 CAPTCHA 和 Challenge 操作行为。

使用和保护带有 CAPTCHA 和 Challenge 的敏感非 HTML 数据

您可以通过以下方法对敏感的非 HTML 数据（例如 API）使用验证码和 Challenge 保护。

1. 识别接受 HTML 响应且与敏感的非 HTML 数据的请求非常接近的请求。
2. 编写与 HTML 请求相匹配且与敏感数据请求相匹配的 CAPTCHA 或 Challenge 规则。
3. 调整您的 CAPTCHA 和 Challenge 免疫时间设置，以便在正常的用户交互中，客户端从 HTML 请求中获得的令牌在请求您的敏感数据时可用且未过期。有关调整信息，请参阅 时间戳过期： AWS WAF 代币免疫时间。

当对您的敏感数据的请求与 CAPTCHA 或 Challenge 规则匹配时，如果客户端仍有来自先前拼图或质询的有效令牌，则该请求不会被阻止。如果令牌不可用或时间戳已过期，则访问您的敏感数据的请求将失败。有关规则操作的工作原理的更多信息，请参阅 CAPTCHA 和 Challenge 操作行为。

使用验证码和 Challenge 以调整现有规则

查看您的现有规则，看看是否要修改或添加这些规则。以下是一些需要考虑的常见情况。

- 如果您有阻止流量的基于速率的规则，但为了避免阻止合法用户，则将速率限制保持在相对较高的水平，请考虑在阻止规则之后添加第二条基于速率的规则。为第二条规则指定比阻止规则更低的限制，并将规则操作设置为 CAPTCHA 或 Challenge。阻止规则仍会阻止速率过高的请求，而新规则将以更低的速率阻止大多数自动流量。有关基于速率的规则的更多信息，请参阅 基于速率的规则语句。
- 如果您有阻止请求的托管规则组，则可以将部分或全部规则的行为从 Block 切换到 CAPTCHA 或 Challenge。为此，请在托管规则组配置中，覆盖规则操作设置。有关覆盖规则操作的信息，请参阅 规则组规则操作优先于规则。

在部署之前先测试您的验证码和质疑实施方案

至于所有新功能，请按照 the section called “测试和调整您的保护” 中的指导进行操作。

在测试期间，请查看您的令牌时间戳到期要求，并设置您的 Web ACL 和规则级别免疫时间配置，以便在控制网站访问权限和为客户提供良好体验之间取得良好的平衡。有关信息，请参阅时间戳过期： AWS WAF 代币免疫时间。

记录 AWS WAF Web ACL 流量

您可以启用日志记录，以获取有关 Web ACL 对流量进行分析的详细信息。记录的信息包括从您的 AWS 资源 AWS WAF 收到网络请求的时间、有关该请求的详细信息以及请求匹配的规则的详细信息。您可以将 Web ACL 日志发送到亚马逊 CloudWatch 日志组、亚马逊简单存储服务 (Amazon S3) Service 存储桶或亚马逊数据 Firehose 传输流。

其他数据收集和分析选项

除了记录之外，您还可以启用以下数据收集和分析选项：

- Amazon Secur ity Lake — 您可以将安全湖配置为收集 Web ACL 数据。Security Lake 从各种来源收集日志和事件数据，用于标准化、分析和管理。有关此选项的信息，请参阅什么是 Amazon 安全湖？ 以及 Amazon Security Lake 用户指南中的从 AWS 服务中收集数据。

  AWS WAF 不会向您收取使用此选项的费用。有关定价信息，请参阅 Amazon Security Lak e 用户指南中的安全湖定价和如何确定安全湖定价。
- 请求采样 — 您可以将 Web ACL 配置为对其评估的 Web 请求进行采样，从而了解您的应用程序正在接收的流量类型。有关此选项的更多信息，请参阅查看 Web 请求示例。

> **Note**
>
> Web ACL 日志配置仅影响日 AWS WAF 志。特别是，经过编辑的日志记录字段配置对请求采样或 Security Lake 数据收集没有影响。Security Lake 数据收集完全通过 Security Lake 服务进行配置。从抽样请求中排除字段的唯一方法是禁用 Web ACL 的采样。

主题

记录 Web ACL 流量信息的定价

根据与每种日志目标类型相关的费用，您需要为记录 Web ACL 流量信息付费。这些费用是对 AWS WAF使用费的补充。您的费用可能会有所不同，具体取决于您选择的目标类型和记录的数据量等因素。

以下提供了指向每种日志记录目标类型的定价信息的链接：

- CloudWatch 日志-费用适用于已售日志传输。参见 Amazon CloudWatch 日志定价。在 “付费套餐” 下，选择 “日志” 选项卡，然后在 “Vended Logs” 下，查看 CloudWatch 日志传送信息。
- Amazon S3 存储桶 — Amazon S3 费用是向亚马逊 S3 存储桶交付日志和使用 Amazon S3 存储桶的合并费用。 CloudWatch
  - 有关 Amazon S3，请参阅 Amazon S3 定价。
  - 有关 CloudWatch 向 Amazon S3 发送日志的信息，请参阅 Ama zon CloudWatch 日志定价。在付费套餐下，选择日志选项卡，然后在提供的日志下，查看传输到 S3的信息
- Firehose — 参见亚马逊数据 Firehose 定价。

有关 AWS WAF 定价的信息，请参阅AWS WAF 定价。

AWS WAF 登录目的地

本部分将介绍您可以从日志中选择的 AWS WAF 日志记录选项。每个部分都提供了配置日志记录的指导，包括有关目标类型特定行为的信息。配置日志记录目标后，就可以向 Web ACL 日志配置提供其规范，以开始向其记录日志。

主题

- Amazon Log CloudWatch s 日志组
- Amazon 简单存储服务存储桶
- 亚马逊 Data Firehose 传送流

Amazon Log CloudWatch s 日志组

本主题提供有关将 Web ACL 流量日志发送到 CloudWatch 日志组的信息。

> **Note**
>
> 除了 AWS WAF使用费用外，您还需要支付登录费用。有关信息，请参阅 记录 Web ACL 流量信息的定价。

要向 Amazon CloudWatch Logs 发送日志，您需要创建一个 CloudWatch 日志日志组。启用登录功能时 AWS WAF，您需要提供日志组 ARN。启用 Web ACL 的日志记录后，会将日志 AWS WAF 传送到 CloudWatch 日志流中的日志日志组。

使用 CloudWatch 日志时，可以在 AWS WAF 控制台中浏览 Web ACL 的日志。在您的 Web ACL 页面中，选择日志记录见解选项卡。此选项是对通过 CloudWatch 控制台为日志提供的 CloudWatch 日志见解的补充。

配置 AWS WAF Web ACL 日志的日志组与 Web ACL 位于同一区域，并使用与管理 Web ACL 相同的帐户。有关配置 CloudWatch 日志组的信息，请参阅使用日志组和日志流。

CloudWatch 日志日志组的配额

CloudWatch 日志具有默认的最大吞吐量配额，该配额在区域内的所有日志组中共享，您可以请求增加该配额。如果您的日志记录要求对于当前的吞吐量设置PutLogEvents来说过高，您将看到账户的限制指标。要在 Service Quotas 控制台中查看限制并申请提高配额，请参阅CloudWatch 日志 PutLogEvents 配额。

日志组命名

您的日志组名称必须以 `aws-waf-logs-` 开头，但可以按照您的喜好以任何后缀结尾，例如 `aws-waf-logs-testLogGroup2`。

所产生的 ARN 格式如下所示：

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

日志流的命名格式如下所示：

```
Region_web-acl-name_log-stream-number
```

以下显示了 `us-east-1` 区域中 Web ACL `TestWebACL` 的日志流示例。

```
us-east-1_TestWebACL_0
```

将日志发布到 CloudWatch 日志所需的权限

为日志组配置 Web ACL 流量 CloudWatch 日志记录需要本节所述的权限设置。这些权限是在您使用 AWS WAF 完全访问托管策略之一时为您设置的，AWSWAFConsoleFullAccess或AWSWAFFullAccess。如果您想更精细地管理对日志记录和 AWS WAF 资源的访问权限，则可以自己设置权限。有关管理权限的信息，请参阅 IAM 用户指南中的AWS 资源访问管理。有关 AWS WAF 托管策略的信息，请参阅 AWS 的托管策略 AWS WAF。

这些权限允许您更改 Web ACL 日志配置、为 CloudWatch 日志配置日志传送以及检索有关您的日志组的信息。这些权限必须附加到您用来管理 AWS WAF的用户。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

如果允许对所有 AWS 资源执行操作，则会在策略中指明，"Resource"设置为"*"。这意味着允许对每个操作支持的所有 AWS 资源执行这些操作。例如，只有 wafv2 日志记录配置资源支持操作 wafv2:PutLoggingConfiguration。

Amazon 简单存储服务存储桶

本主题提供有关将 Web ACL 流量日志发送到 Amazon S3 存储桶的信息。

> **Note**
>
> 除了 AWS WAF使用费用外，您还需要支付登录费用。有关信息，请参阅 记录 Web ACL 流量信息的定价。

要将您的 Web ACL 流量日志发送到 Amazon S3，您需要使用与管理Web ACL 相同的账户设置一个 Amazon S3 存储桶，并以 aws-waf-logs- 开头命名该存储桶。启用登录功能时 AWS WAF，您需要提供存储桶名称。有关创建日志记录桶的信息，请参阅 Amazon Simple Storage Service 用户指南中的创建桶。

您可以使用Amazon Athena 交互式查询服务访问和分析您的 Amazon S3 日志。Athena 可让您轻松地使用标准 SQL 直接分析 Amazon S3 中的数据。只需在中执行一些操作 AWS Management Console，您就可以将 Athena 指向存储在 Amazon S3 中的数据，然后快速开始使用标准 SQL 来运行临时查询并获得结果。有关更多信息，请参阅 Amazon Athen a 用户指南中的查询 AWS WAF 日志。

> **Note**
>
> AWS WAF 支持使用亚马逊 S3 存储桶对密钥类型亚马逊 S3 密钥 (SSE-S3) 和 AWS Key Management Service (SSE-KMS) 进行加密。 AWS KMS keys AWS WAF 不支持对由管理的 AWS Key Management Service 密钥进行加密 AWS。

您的Web ACL 每隔 5 分钟将日志文件发布到 Amazon S3 存储桶。每个日志文件都包含前 5 分钟记录的流量日志记录。

日志文件的最大文件大小为 75 MB。如果日志文件在 5 分钟期间内达到文件大小限制，流日志会停止向它添加流日志记录，将它发布到 Amazon S3 存储桶，然后创建一个新的日志文件。

日志文件是压缩文件。如果使用 Amazon S3 控制台打开文件，Amazon S3 会解压日志记录并显示它们。如果您下载日志文件，则必须对其进行解压才能查看记录。

单个日志文件包含包含多条记录的交错条目。要查看 Web ACL 的所有日志文件，请查找按 Web ACL 名称、区域和您的账户 ID 汇总的条目。

命名要求和语法

用于 AWS WAF 记录的存储桶名称必须以您想要的任何后缀开头，`aws-waf-logs-`并且可以以任何后缀结尾。例如，`aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`。

存储桶位置

存储桶位置使用以下语法：

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

存储桶 ARN

存储桶的 Amazon 资源名称（ARN）格式如下：

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

带有前缀的存储桶位置

如果您在对象键名称中使用前缀来组织存储在存储桶中的数据，则可以在日志存储桶名称中提供前缀。

> **Note**
>
> 此选项在控制台中不可用。使用 AWS WAF API、CLI 或 AWS CloudFormation。

有关在 Amazon S3 中使用前缀的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用前缀组织对象。

带有前缀的存储桶位置使用以下语法：

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

存储桶文件夹和文件名

在您的存储桶中，按照您提供的任何前缀，您的 AWS WAF 日志将写入一个文件夹结构，该结构由您的账户 ID、区域、Web ACL 名称以及日期和时间决定。

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

在文件夹中，日志文件名遵循类似的格式：

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

文件夹结构和日志文件名中使用的时间规范符合时间戳格式规范 YYYYMMddTHHmmZ。

下面显示了 Amazon S3 存储桶中名为 DOC-EXAMPLE-BUCKET 的存储桶的示例日志文件。那 AWS 账户 是11111111111。Web ACL 是 TEST-WEBACL，区域是 us-east-1。

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> 用于 AWS WAF 记录的存储桶名称必须以您想要的任何后缀开头，aws-waf-logs-并且可以以任何后缀结尾。

向 Amazon S3 存储桶发布日志的所需的权限

为 Amazon S3 存储桶配置 Web ACL 流量日志需要以下权限设置。这些权限是在您使用 AWS WAF 完全访问托管策略 AWSWAFConsoleFullAccess 或 AWSWAFFullAccess 时为您设置的，。如果您想更精细地管理对日志和 AWS WAF 资源的访问权限，则可以自己设置这些权限。有关管理权限的信息，请参阅IAM 用户指南中的 AWS 资源的访问权限管理。有关 AWS WAF 托管策略的信息，请参阅AWS 的托管策略 AWS WAF。

以下权限允许您更改 Web ACL 日志配置和配置向 Amazon S3 存储桶的日志传输。这些权限必须附加到您用来管理 AWS WAF的用户。

> **Note**
>
> 当你设置下面列出的权限时，你可能会在 AWS CloudTrail 日志中看到错误，表明访问被拒绝，但 AWS WAF 记录权限是正确的。

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
         ],
         "Effect":"Allow"
      }
   ]
}
```

如果允许对所有 AWS 资源执行操作，则会在策略中以"Resource"设置为"*"。这意味着允许对每个操作支持的所有 AWS 资源执行这些操作。例如，只有 wafv2 日志记录配置资源支持操作 wafv2:PutLoggingConfiguration。

默认情况下，Amazon S3 存储桶以及其中包含的对象都是私有的。只有存储桶拥有者才能访问存储桶和其中存储的对象。不过，存储桶拥有者可以通过编写访问策略来向其他资源和用户授予访问权限。

如果创建日志的用户拥有存储桶，服务会自动向存储桶附加以下策略，以授予日志将日志发布到存储桶的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
```

```
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> 用于 AWS WAF 记录的存储桶名称必须以您想要的任何后缀开头，aws-waf-logs-并且可以以任何后缀结尾。

如果创建日志的用户不拥有存储桶，也没有存储桶的 GetBucketPolicy 和 PutBucketPolicy 权限，日志创建操作会失败。在这种情况下，存储桶拥有者必须手动将上述策略添加到存储桶，并指定日志创建者的 AWS 账户 ID。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南 中的如何添加 S3 存储桶策略？ 如果存储桶从多个账户接收日志，则将 Resource 元素条目添加到每个账户的 AWSLogDeliveryWrite 策略语句。

例如，以下存储桶策略允许 AWS 账户 111122223333向名为的存储桶发布日志aws-waf-logs-*DOC-EXAMPLE-BUCKET*：

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
```

```
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

使用 AWS Key Management Service KMS 密钥的权限

如果您的登录目标使用服务器端加密，密钥存储在 AWS Key Management Service (SSE-KMS) 中，并且您使用客户托管密钥（KMS 密钥），则必须授予使用您的 KMS 密钥的 AWS WAF 权限。为此，您需要为所选目标的 KMS 密钥添加密钥政策。这允许 AWS WAF 日志记录将您的日志文件写入您的目标。

将以下密钥策略添加到您的 KMS 密钥中，以允许登录 AWS WAF 到您的 Amazon S3 存储桶。

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
```

```
    "Resource": "*"
}
```

访问 Amazon S3 日志文件所需的权限

Amazon S3 使用访问控制列表 (ACL) 管理对 AWS WAF 日志创建的日志文件的访问。默认情况下，存储桶拥有者对每个日志文件具有 FULL_CONTROL 权限。如果日志传输拥有者与存储桶拥有者不同，则没有权限。日志传输账户具有 READ 和 WRITE 权限。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南 中的访问控制列表 (ACL) 概述。

亚马逊 Data Firehose 传送流

本节提供有关将您的网页 ACL 流量日志发送到 Amazon Data Firehose 传输流的信息。

> **Note**
>
> 除了 AWS WAF使用费用外，您还需要支付登录费用。有关信息，请参阅 记录 Web ACL 流量信息的定价。

要将日志发送到亚马逊数据 Firehose，您需要将网页 ACL 中的日志发送到您在 Firehose 中配置的亚马逊数据 Firehose 传输流。启用日志记录后，通过 Firehose 的 HTTPS 端点将日志 AWS WAF 传送到您的存储目标。

一个 AWS WAF 日志等同于一个 Firehose 记录。如果您通常每秒收到 10,000 个请求并启用完整日志，则应在 Firehose 中设置每秒 10,000 条记录。如果您未正确配置 Firehose，则 AWS WAF 不会记录所有日志。有关更多信息，请参阅亚马逊 Kinesis Data Firehose 配额。

有关如何创建亚马逊数据 Firehose 传输流和查看您存储的日志的信息，请参阅什么是亚马逊数据 Firehose？

有关创建传输流的信息，请参阅创建 Amazon Data Firehose 传送流。

为您的网页 ACL 配置 Amazon Data Firehose 传输流

按如下方式为您的网络 ACL 配置 Amazon Data Firehose 传输流。

- 使用与管理 Web ACL 相同的账户来创建它。
- 将其创建在与 Web ACL 相同的区域中。如果您要为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）地区创建 firehose。us-east-1

- 为数据消防队指定一个以前缀 `aws-waf-logs-` 开头的名称。例如，`aws-waf-logs-us-east-2-analytics`。
- 将其配置为直接放置，这样应用程序就可以直接访问传送流。在 Amazon Data Firehose 控制台中，对于传送流来源设置，选择直接 PUT 或其他来源。通过 API，将传送流属性 `DeliveryStreamType` 设置 为 `DirectPut`。

> **Note**
>
> 请勿使用 `Kinesis stream` 作为来源。

向 Amazon Data Firehose 传输流发布日志所需的权限

要了解 Kinesis Data Firehose 配置所需的权限，请参阅 使用 Amazon Kinesis Data Firehose 控制访问。

您必须具有以下权限才能成功启用 Amazon Data Firehose 传输流的网页 ACL 日志记录。

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

有关服务相关角色以及 `iam:CreateServiceLinkedRole` 权限的信息，请参阅将服务相关角色用于 AWS WAF。

Web ACL 日志记录配置

您可以随时对 Web ACL 启用和禁用日志记录功能。

> **Note**
>
> 除了 AWS WAF使用费用外，您还需要支付登录费用。有关信息，请参阅 记录 Web ACL 流量信息的定价。

如果在日志中找不到日志记录

在极少数情况下， AWS WAF 日志传输可能会降至100%以下，而日志的交付会尽力而为。该 AWS WAF 架构将应用程序的安全性置于所有其他考虑因素之上。某些情况下，例如，当日志流遇到流量节

流时，这可能会导致记录被丢弃。这不应该影响多个记录。如果您注意到一些丢失的日志条目，请与 AWS Support 中心联系。

在 Web ACL 的日志配置中，您可以自定义 AWS WAF 发送到日志的内容。

- 字段密文 – 对于使用相应匹配设置的规则，您可以从日志记录中删除以下字段：URI 路径、查询字符串、单标头和 HTTP 方法。编辑后的字段在日志中显示为 REDACTED。例如，如果您在日志中编辑查询字符串字段，则该字段将与使用查询字符串匹配组件设置的所有规则的 REDACTED 一样列出。编辑仅适用于您在规则中指定匹配的请求组件，因此单个标头组件的编辑不适用于在标头上匹配的规则。有关日志字段的列表，请参阅 日志字段。

  > **Note**
  >
  > 此设置对请求采样没有影响。对于请求采样，排除字段的唯一方法是禁用 Web ACL 的采样。

- 日志筛选 – 您可以添加筛选功能以指定哪些 Web 请求保留在日志中，哪些将丢弃的筛选。您可以根据在 Web 请求评估期间 AWS WAF 适用的设置进行筛选。您可以按以下设置进行筛选：
  - 完全限定的标签 – 完全限定的标签具有前缀、可选命名空间和标签名称。前缀用于标识添加标签的规则的规则组或 Web ACL 上下文。有关标签的信息，请参阅 AWS WAF 网络请求上的标签。
  - 规则操作 – 您可以根据任何普通规则操作设置进行筛选，也可以根据规则组规则的旧版 EXCLUDED_AS_COUNT 覆盖选项进行筛选。有关规则操作设置的信息，请参阅 规则操作。有关规则组规则的当前和旧规则操作覆盖的信息，请参阅 规则组的操作覆盖选项。
    - 普通规则操作筛选器适用于在规则中配置的操作，也适用于使用当前选项配置的用于覆盖规则组规则操作的操作。
    - EXCLUDED_AS_COUNT 日志筛选器与 Count 操作日志筛选器重叠。EXCLUDED_AS_COUNT 筛选当前和旧版选项，用于将规则组规则操作覆盖为 Count。

为 Web ACL 启用日志记录

要启用 Web ACL 的日志记录，必须已经配置了日志记录目标。有关您的目标选择和每个目标的要求的信息，请参阅 AWS WAF 登录目的地。

为 Web ACL 启用日志记录

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

2. 在导航窗格中，选择 Web ACL。
3. 选择您要启用日志记录的 Web ACL 名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。
4. 在 日志记录 选项卡上，选择 启用日志记录。
5. 选择日志记录目标类型，然后选择您配置的日志记录目标。必须选择名称以 `aws-waf-logs-` 开头的日志记录目标。
6. （可选）如果您不希望某些字段包含在日志中，请对其进行编辑。选择要编辑的字段，然后选择添加。根据需要重复操作来编辑其他字段。

   > **Note**
   >
   > 此设置对请求采样没有影响。对于请求采样，排除字段的唯一方法是禁用 Web ACL 的采样。

7. （可选）如果您不想向日志发送所有请求，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个筛选器，选择添加筛选条件，然后选择您的筛选条件并指定是要保留还是删除符合条件的请求。添加完筛选条件后，如果需要，可以修改默认日志记录行为。
8. 选择启用日志记录。

   > **Note**
   >
   > 成功启用日志记录后， AWS WAF 将创建一个服务关联角色，该角色具有将日志写入日志目标所需的权限。有关更多信息，请参阅 将服务相关角色用于 AWS WAF。

日志字段

以下列表介绍了可能的日志字段。

action

AWS WAF 应用于请求的终止操作。这表示允许、阻止、验证码或质询。当 Web 请求不包含有效令牌时，CAPTCHA 和 Challenge 操作将终止。

args

查询字符串。

验证码响应

请求的 CAPTCHA 操作状态，在对请求应用CAPTCHA操作时填充。无论是终止操作还是非终止CAPTCHA操作，都将填充此字段。如果请求多次应用该CAPTCHA操作，则从上次应用该操作时起填充此字段。

当请求不包含令牌或者令牌无效或已过期时，该 CAPTCHA 操作将终止 Web 请求检查。如果CAPTCHA操作即将终止，则此字段包含响应代码和失败原因。如果操作未终止，则此字段包含求解时间戳。要区分终止操作和非终止操作，可以在此字段中筛选非空`failureReason`属性。

challengeResponses

请求的质疑操作状态，在对请求应用Challenge操作时填充。无论是终止操作还是非终止Challenge操作，都将填充此字段。如果请求多次应用该Challenge操作，则从上次应用该操作时起填充此字段。

当请求不包含令牌或者令牌无效或已过期时，该 Challenge 操作将终止 Web 请求检查。如果Challenge操作即将终止，则此字段包含响应代码和失败原因。如果操作未终止，则此字段包含求解时间戳。要区分终止操作和非终止操作，可以在此字段中筛选非空`failureReason`属性。

clientIp

发送请求的客户端的 IP。

country

请求的源国家/地区。 AWS WAF 如果无法确定原产国，则会将此字段设置为`-`。

excludedRules

仅用于规则组规则。规则组中您排除的规则的列表。这些规则的操作设置为 Count。

如果您使用覆盖规则操作选项覆盖要计数的规则，则此处不会列出匹配项。它们被列为操作对`action` 和 `overriddenAction`.

exclusionType

一种类型，指示排除的规则具有操作 Count。

ruleId

规则组中排除的规则的 ID。

formatVersion

日志的格式版本。

标头

标头的列表。

httpMethod

请求中的 HTTP 方法。

httpRequest

关于请求的元数据。

httpSourceId

关联资源的ID。

- 对于 Amazon CloudFront 分配，编号为 ARN *distribution-id* 语法：

  arn:*partition*cloudfront::*account-id*:distribution/*distribution-id*
- 对于应用程序负载均衡器，ID 是 *load-balancer-id*，采用 ARN 语法：

  arn:*partition*:elasticloadbalancing:*region*:*account-id*:loadbalancer/app/*load-balancer-name/load-balancer-id*
- 对于 Amazon API Gateway REST API，ID 是 *api-id*，采用 ARN 语法：

  arn:*partition*:apigateway:*region*::/restapis/*api-id*/stages/*stage-name*
- 对于 AWS AppSync GraphQL API，编号是 ARN 语法*GraphQLApiId*中的：

  arn:*partition*:appsync:*region*:*account-id*:apis/*GraphQLApiId*
- 对于 Amazon Cognito 用户群体，ID 是 *user-pool-id*，采用 ARN 语法：

  arn:*partition*:cognito-idp:*region*:*account-id*:userpool/*user-pool-id*
- 对于 AWS App Runner 服务，ID 是 ARN 语法*apprunner-service-id*中的：

  arn:*partition*:apprunner:*region*:*account-id*:service/*apprunner-service-name/apprunner-service-id*

httpSourceName

请求的源。可能CF的值：亚马逊 CloudFront、APIGW亚马逊 API Gateway、应用程序负载均衡器、ALB Amazon Cognito AWS AppSync、COGNITOIDP Amazon Cognito、APPRUNNER App Runner 以及经过验证VERIFIED_ACCESS的访问权限。APPSYNC

httpVersion

HTTP 版本。

ja3Fingerprint

请求的 JA3 指纹。

> **Note**
>
> JA3 指纹检查仅适用于 Amazon CloudFront 发行版和应用程序负载均衡器。

JA3 指纹是一个 32 字符的哈希值，源自传入请求的 TLS Client Hello。此指纹用作客户端 TLS 配置的唯一标识符。 AWS WAF 计算并记录每个具有足够的 TLS Client Hello 信息用于计算的请求的此指纹。

在 Web ACL 规则中配置 JA3 指纹匹配时，需要提供此值。有关创建与 JA3 指纹的匹配项的信息，请参阅 请求组件选项 中的 JA3 指纹，以了解规则语句。

标签

Web 请求上的标签。这些标签是由用来评估请求的规则应用的。 AWS WAF 记录前 100 个标签。

nonTerminatingMatching规则

与请求匹配的非终止规则列表。列表中的每个项目都包含以下信息。

action

AWS WAF 应用于请求的操作。这表示计数、验证码或质询。当 Web 请求包含有效令牌时，CAPTCHA 和 Challenge 不会终止。

ruleId

与请求匹配并且为非终止规则的 ID。

ruleMatchDetails

有关与请求匹配的规则的详细信息。此字段仅适用于 SQL 注入和跨站脚本攻击（XSS）匹配规则语句。匹配规则可能需要匹配多个检查条件，因此这些匹配详细信息以匹配条件的形式提供。

为每条规则提供的任何其他信息会因规则配置、规则匹配类型和匹配详细信息等因素而异。例如，对于带有CAPTCHA或Challenge操作的规则，`challengeResponse`将列

出captchaResponse或。如果匹配的规则位于规则组中，并且您已覆盖其配置的规则操作，则中将提供配置的操作。overriddenAction

超大字段

Web 请求中经过 Web ACL 检查且超出 AWS WAF 检查限制的字段列表。如果字段过大，但 Web ACL 未对其进行检查，则不会在此处列出该字段。

此列表可以包含以下零个或多个
值：REQUEST_BODY、REQUEST_JSON_BODY、REQUEST_HEADERS 和 REQUEST_COOKIES。有关超大字段的更多信息，请参阅 在中处理超大请求组件 AWS WAF。

rateBasedRule名单

对请求执行操作的基于速率的规则列表。有关基于速率的规则的更多信息，请参阅 基于速率的规则语句。

rateBasedRule我是

作用于请求的基于速率的规则的 ID。如果这已终止请求，则 rateBasedRuleId 的 ID 与 terminatingRuleId 的 ID 相同。

rateBasedRule姓名

作用于请求的基于速率的规则的名称。

limitKey

规则使用的聚合类型。可能的值包括：对于 Web 请求来源为 IP，请求标头中转发的 IP 为FORWARDED_IP，自定义聚合键设置为 CUSTOMKEYS，将所有请求合并计数（不进行聚合）为 CONSTANT。

limitValue

仅在按单个 IP 地址类型限制速率时使用。如果请求包含无效的 IP 地址，则 limitvalue 为 INVALID。

maxRateAllowed

特定聚合实例在指定时间窗口内允许的最大请求数。聚合实例由limitKey加上您在基于速率的规则配置中提供的任何其他密钥规范来定义。

evaluationWindowSec

请求中 AWS WAF 包含的时间长度，以秒为单位。

customValue

请求中基于速率的规则标识的唯一值。对于字符串值，日志会打印字符串值的前 32 个字符。根据密钥类型，这些值可能仅用于密钥，例如 HTTP 方法或查询字符串，也可能用于密钥和名称，例如标头和标头名称。

requestHeadersInserted

为处理自定义请求而插入的标头列表。

requestId

请求的 ID，由底层主机服务生成。对于应用程序负载均衡器，这是跟踪 ID。对于所有其他人，这是请求 ID。

responseCodeSent

与自定义响应一起发送的响应代码。

ruleGroupId

规则组的 ID。如果规则阻止了请求，则 `ruleGroupID` 的 ID 与 `terminatingRuleId` 的 ID 相同。

ruleGroupList

对该请求进行操作的规则组列表，包含匹配信息。

terminatingRule

终止请求的规则。如果存在，则它包含以下信息。

action

AWS WAF 应用于请求的终止操作。这表示允许、阻止、验证码或质询。当 Web 请求不包含有效令牌时，CAPTCHA 和 Challenge 操作将终止。

ruleId

匹配请求的规则的 ID。

ruleMatchDetails

有关与请求匹配的规则的详细信息。此字段仅适用于 SQL 注入和跨站脚本攻击（XSS）匹配规则语句。匹配规则可能需要匹配多个检查条件，因此这些匹配详细信息以匹配条件的形式提供。

为每条规则提供的任何其他信息会因规则配置、规则匹配类型和匹配详细信息等因素而异。例如，对于带有CAPTCHA或Challenge操作的规则，`challengeResponse`将列

出captchaResponse或。如果匹配的规则位于规则组中，并且您已覆盖其配置的规则操作，则中将提供配置的操作。overriddenAction

terminatingRuleId

终止请求的规则的 ID。如果没有任何情况会终止请求，则值为 Default_Action。

terminatingRuleMatch详情

有关与请求匹配的终止规则的详细信息。终止规则具有针对 Web 请求结束检查过程的操作。终止规则可能的操作包括Allow、Block、CAPTCHA 和 Challenge。在检查 Web 请求期间，在与请求匹配且具有终止操作的第一条规则处， AWS WAF 停止检查并应用操作。除了日志中报告的匹配终止规则的威胁外，Web 请求可能还包含其他威胁。

这仅适用于 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。匹配规则可能需要匹配多个检查条件，因此这些匹配详细信息以匹配条件的形式提供。

terminatingRuleType

终止请求的规则的类型。可能的值：RATE_BASED、REGULAR、GROUP 和 MANAGED_RULE_GROUP。

时间戳

时间戳，以毫秒为单位。

uri

请求的 URI。

webaclId

Web ACL 的 GUID。

日志示例

Example 基于速率的规则 1：使用一个键配置规则，设置为 **Header:dogname**

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
```

```
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 基于速率的规则 1：被基于速率的规则阻止的请求的日志条目

```
{
   "timestamp":1683355579981,
   "formatVersion":1,
   "webaclId": ...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
```

```
      {
         "rateBasedRuleId": ...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            }
         ]
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
   "requestHeadersInserted":null,
   "responseCodeSent":null,
   "httpRequest":{
      "clientIp":"52.46.82.45",
      "country":"FR",
      "headers":[
         {
            "name":"X-Forwarded-For",
            "value":"52.46.82.45"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
```

```
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example 基于速率的规则 2：使用两个键进行规则配置，设置为 **Header:dogname** 和 **Header:catname**

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
```

```
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 基于速率的规则 2：被基于速率的规则阻止的请求的日志条目

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
```

```
         "rateBasedRuleId":...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            },
            {
               "key":"HEADER",
               "name":"catname",
               "value":"goofie"
            }
         ]
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
   "requestHeadersInserted":null,
   "responseCodeSent":null,
   "httpRequest":{
      "clientIp":"52.46.82.35",
      "country":"FR",
      "headers":[
         {
            "name":"X-Forwarded-For",
            "value":"52.46.82.35"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
         },
```

```
          {
             "name":"X-Amzn-Trace-Id",
             "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
          },
          {
             "name":"catname",
             "value":"goofie"
          },
          {
             "name":"dogname",
             "value":"ella"
          },
          {
             "name":"User-Agent",
             "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
          },
          {
             "name":"Accept-Encoding",
             "value":"gzip,deflate"
          }
       ],
       "uri":"/CanaryTest",
       "args":"",
       "httpVersion":"HTTP/1.1",
       "httpMethod":"GET",
       "requestId":"EdzmlH5OCGYF1vQ="
    }
}
```

Example 在 SQLi 检测时触发的规则的日志输出（终止）

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
```

```
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
```

```
    ]
}
```

Example 在 SQLi 检测时触发的规则的日志输出（未终止）

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
```

```
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 在规则组内触发的多个规则的日志输出（RuleA-XSS 正在终止，Rule-B 未终止）

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
```

```
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 为检查内容类型为 JSON 的请求正文而触发的规则的日志输出

AWS WAF 目前将 JSON 身体检查的位置报告为UNKNOWN。

```
{
    "timestamp": 1576280412771,
```

```
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 使用有效的、未过期的验证码令牌记录针对 Web 请求的验证码规则的输出

以下日志列表适用于将规则与 CAPTCHA 操作相匹配的 Web 请求。Web 请求具有有效且未过期的 CAPTCHA 令牌，并且仅被标记为验证码匹配 AWS WAF，类似于操作的行为。Count此验证码匹配在 nonTerminatingMatchingRules 标记。


```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
```

```
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
```

```
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
```

```
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example 针对没有 验证码令牌的 Web 请求记录验证码规则的输出

以下日志列表适用于将规则与 CAPTCHA 操作相匹配的 Web 请求。该网络请求没有验证码令牌，已被屏蔽。 AWS WAF

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
```

```
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
```

```
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```


测试和调整您的 AWS WAF 保护措施

我们建议您先测试和调整 AWS WAF Web ACL 的任何更改，然后再将其应用于网站或 Web 应用程序流量。

⚠ 生产流量风险

在为生产流量部署 Web ACL 实施之前，请在暂存或测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。然后，在启用之前，在计数模式下使用生产流量对规则进行测试和调整。

本节提供测试和调整 AWS WAF Web ACL、规则、规则组、IP 集和正则表达式模式集的指导。

本节还为测试您使用由其他人管理的规则组提供了一般指导。其中包括 AWS 托管规则规则组、 AWS Marketplace 托管规则组以及其他账户与您共享的规则组。对于这些规则组，还要遵循规则组提供程序提供的任何指导。

- 有关机器人控制 AWS 托管规则组的信息，另请参阅测试和部署 AWS WAF 机器人控制。
- 有关账户盗用防护 AWS 托管规则组的信息，另请参阅测试和部署 ATP。
- 有关账户创建防欺诈 AWS 托管规则组的信息，另请参阅测试和部署 ACFP。

更新期间暂时出现不一致

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

以下示例是更改传播过程中可能暂时出现的不一致：

- 创建 Web ACL 后，如果您尝试将其与资源关联，则可能会出现异常，指示 Web ACL 不可用。
- 将规则组添加到 Web ACL 后，新的规则组规则可能在某个使用 Web ACL 的区域生效，而在另一个区域不生效。
- 更改规则操作设置后，可能会在某些位置显示旧操作而在另一些位置显示新操作。
- 将 IP 地址添加到阻止规则中使用的 IP 集后，新地址可能会在一个区域中被阻止，而在另一个区域中仍然允许。

测试和调整高级步骤

本节提供了测试 Web ACL 更改的步骤列表，包括其使用的任何规则或规则组。

> **Note**
>
> 要遵循本节中的指导，您需要了解如何创建和管理 AWS WAF 保护，例如 Web ACL、规则和规则组。本指南前面部分将介绍该信息。

测试和调整您的Web ACL

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

1. 准备测试

   准备好监控环境，将新 AWS WAF 保护切换到计数模式进行测试，并创建所需的任何资源关联。

   请参阅 准备测试。

2. 在测试和生产环境中进行监控和调整

   首先在测试或暂存环境中监控和调整您的 AWS WAF 保护措施，然后在生产环境中监控和调整您的保护措施，直到您确信它们可以根据需要处理流量。

   请参阅 监控和调整。

3. 在生产环境中启用保护功能

   当您对测试保护感到满意时，请将其切换到生产模式，清理所有不必要的测试工件，然后继续监控。

   请参阅 在生产环境中启用保护。

完成变更实施后，请继续监控生产环境中的 Web 流量和保护，以确保它们按您想要的方式运行。Web 流量模式可能会随着时间的推移而发生变化，因此您可能需要偶尔调整保护。

准备测试

本节介绍如何进行设置以测试和调整您的 AWS WAF 保护措施。

> **Note**
>
> 要遵循本节中的指导，您需要大致了解如何创建和管理 AWS WAF 保护，例如 Web ACL、规则和规则组。本指南前面部分将介绍该信息。

准备测试

1. 为网页 ACL 启用网页 ACL 日志记录、Amazon CloudWatch 指标和网络请求采样

   使用日志记录、指标和采样来监控 Web ACL 规则与您的 Web 流量的交互情况。

   - 日志记录-您可以配置 AWS WAF 为记录 Web ACL 评估的 Web 请求。您可以将日志发送到日 CloudWatch 志、亚马逊 S3 存储桶或 Amazon Data Firehose 传输流。您可以编辑字段并应用筛选。有关更多信息，请参阅 记录 AWS WAF Web ACL 流量。

- Amazon Secur ity Lake — 您可以将安全湖配置为收集 Web ACL 数据。Security Lake 从各种来源收集日志和事件数据，用于标准化、分析和管理。有关此选项的信息，请参阅什么是 Amazon Security Lake？ 以及 Amazon Security Lake 用户指南中的从 AWS 服务中收集数据。
- Amazon CloudWatch 指标 — 在您的 Web ACL 配置中，为要监控的所有内容提供指标规范。您可以通过 AWS WAF 和 CloudWatch控制台查看指标。有关更多信息，请参阅 使用 Amazon 进行监控 CloudWatch。
- Web 请求采样 – 您可以查看您的 Web ACL 评估的所有 Web 请求的示例。有关 Web 请求采样的信息，请参阅 查看 Web 请求示例。

2. 将保护设置为 Count 模式

在 Web ACL 配置中，将要测试的任何内容切换到计数模式。这会使测试保护在不改变请求处理方式的情况下记录与 Web 请求的匹配情况。您将能够在指标、日志和采样请求中看到匹配项，以验证匹配条件并了解可能对您的 Web 流量产生的影响。无论规则操作如何，向匹配请求添加标签的规则都将添加标签。

- Web ACL 中定义的规则 – 编辑 Web ACL 中的规则并将其操作设置为 Count。
- 规则组 – 在 Web ACL 配置中，编辑规则组的规则语句，然后在规则窗格中打开覆盖所有规则操作下拉列表并选择 Count。如果您以 JSON 格式管理 Web ACL，请将规则添加到规则组参考语句的 `RuleActionOverrides` 设置中，`ActionToUse` 设置为 Count。以下示例列表显示了“`AWSManagedRulesAnonymousIpList` AWS 托管规则” 规则组中两个规则的替代。

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
      },
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "HostingProviderIPList"
      }
    ],
    "ExcludedRules": []
```

```
    }
  },
```

有关规则操作覆盖的更多信息，请参阅 覆盖规则组的规则操作。

对于您自己的规则组，请勿修改规则组本身中的规则操作。带有 Count 操作的规则组规则不会生成测试所需的指标或其他工件。此外，更改规则组会影响使用该规则组的所有 Web ACL，而 Web ACL 配置内部的更改仅影响单个 Web ACL。

- Web ACL – 如果您正在测试新的 Web ACL，请将 Web ACL 的默认操作设置为允许请求。这使您可以试用 Web ACL，而不会以任何方式影响流量。

通常，计数模式生成的匹配项多于生产模式。这是因为计算请求数的规则不会阻止 Web ACL 对请求的评估，因此稍后在 Web ACL 中运行的规则也可能与请求匹配。当您将规则操作更改为生产设置时，允许或阻止请求的规则将终止对它们匹配的请求的评估。因此，通常会由 Web ACL 中较少的规则来检查匹配的请求。有关规则操作对 Web 请求总体评估的效果的更多信息，请参阅 规则操作。

使用这些设置，您的新保护不会改变 Web 流量，但会在指标、Web ACL 日志和请求样本中生成匹配信息。

3. 将 Web ACL 与资源关联

   如果 Web ACL 尚未与资源关联，请将其关联。

   请参阅 将 Web ACL 与资源关联或取消关联 AWS。

您现在可以监控和调整 Web ACL。

监控和调整

本节介绍如何监控和调整 AWS WAF 保护措施。

> **Note**
>
> 要遵循本节中的指导，您需要大致了解如何创建和管理 AWS WAF 保护，例如 Web ACL、规则和规则组。本指南前面部分将介绍该信息。

监控 Web 流量和规则匹配以验证 Web ACL 的行为。如果您发现问题，请调整规则以进行更正，然后进行监控以验证调整。

重复以下步骤，直到 Web ACL 根据需要管理您的 Web 流量。

监控和调整

1. 监控流量和规则匹配情况

   确保流量畅通，并且您的测试规则正在找到匹配的请求。

   请查看以下信息，了解您正在测试的保护：

   - 日志 – 访问与 Web 请求匹配的规则的相关信息：
     - 您的规则 – Web ACL 中具有 Count 操作的规则列在 `nonTerminatingMatchingRules` 下。带有 Allow 或 Block 的规则列为 `terminatingRule`. 根据规则匹配的结果，带有 CAPTCHA 或 Challenge 的规则可以是终止的，也可以是非终止的，因此列在两个类别之一下。
     - 规则组 – 在 `ruleGroupId` 字段中标识规则组，其规则匹配的分类与独立规则的分类相同。
     - 标签 – `Labels` 字段中列出了规则已应用于请求的标签。

     有关更多信息，请参阅 日志字段。
   - Amazon CloudWatch 指标 — 您可以访问以下指标来评估您的 Web ACL 请求。
     - 您的规则-指标按规则操作分组。例如，当您在Count模式下测试规则时，其匹配项将列为 Web ACL 的`Count`指标。
     - 您的规则组-规则组的指标列在规则组指标下。
     - 其他账户拥有的规则组-规则组指标通常只有规则组所有者可见。但是，如果您覆盖规则的规则操作，则该规则的指标将列在您的 Web ACL 指标下。此外，任何规则组添加的标签都会列在您的 Web ACL 指标中

       此类别中的规则组是其他账户与您共享的AWS 的托管规则 AWS WAFAWS Marketplace 托管规则组其他服务提供的规则组、、和规则组。
     - 标签-评估期间添加到 Web 请求的标签列在 Web ACL 标签指标中。您可以访问所有标签的指标，无论它们是由您的规则和规则组添加的，还是由其他账户拥有的规则组中的规则添加的。

     有关更多信息，请参阅 查看 Web ACL 的指标。
   - Web ACL 流量概述仪表板 — 访问 AWS WAF 控制台中的 Web ACL 页面并打开 “流量概述” 选项卡，即可访问 Web ACL 评估的 Web 流量的摘要。

流量概述控制面板提供了在评估您的应用程序网络流量时 AWS WAF 收集的 Amazon CloudWatch 指标的近乎实时的摘要。

有关更多信息，请参阅 Web ACL 流量概述控制面板。

- 采样的 Web 请求 – 访问与 Web 请求样本相匹配的规则的信息。示例信息通过 Web ACL 中规则的指标名称来标识匹配的规则。对于规则组，该指标标识规则组参考语句。对于规则组内的规则，该示例在中列出了匹配的规则名称 `RuleWithinRuleGroup`。

  有关更多信息，请参阅 查看 Web 请求示例。

2. 配置缓解以解决误报

   如果您确定某条规则正在生成误报，则通过在不应该出现误报的时候匹配 Web 请求，则以下选项可以帮助您调整 Web ACL 保护以缓解误报。

   更正规则检查条件

   对于您自己的规则，您通常只需要调整用于检查 Web 请求的设置即可。示例包括更改正则表达式模式集中的规范，调整在检查之前应用于请求组件的文本转换，或者切换到使用转发 IP 地址。有关导致问题的规则类型，请参阅 规则语句基础知识 下方的指南。

   更正复杂的问题

   对于您无法控制的检查条件和某些复杂的规则，您可能需要进行其他更改，例如添加明确允许或阻止请求的规则，或者通过有问题的规则将请求排除在评估范围之外的规则。托管规则组通常需要这种缓解，但其他规则也可以。示例包括基于速率的规则语句和 SQL 注入攻击规则语句。

   如何减少误报，因用例而异。以下是常规方法：

   - 添加缓解规则 – 添加一条规则，该规则在新规则之前运行，并明确允许导致误报的请求。有关 Web ACL 中规则评估顺序的信息，请参阅 Web ACL 中规则和规则组的处理顺序。

     通过这种方法，允许的请求会被发送到受保护的资源，因此它们永远不会达到新的评估规则。如果新规则是付费托管规则组，则此方法还有助于控制使用该规则组的费用。

   - 添加带有缓解规则的逻辑规则 – 使用逻辑规则语句将新规则与排除误报的规则相结合。有关信息，请参阅 逻辑规则语句。

     例如，假设您正在添加一个 SQL 注入攻击匹配语句，该语句会为某类请求生成误报。创建与这些请求相匹配的规则，然后使用逻辑规则语句组合这些规则，这样您就可以只匹配两个请求都不符合误报条件且确实符合 SQL 注入攻击条件的请求。

- 添加范围缩小语句 – 对于基于速率的语句和托管规则组引用语句，通过在主语句中添加范围向下语句，将导致误报的请求排除在评估之外。

  与范围缩小语句不匹配的请求永远不会到达规则组或基于速率的评估。有关范围缩小语句的信息，请参阅 范围缩小语句。有关示例，请参阅从机器人管理中排除 IP 范围。

- 添加标签匹配规则 – 对于使用标签的规则组，请确定有问题的规则应用于请求的标签。如果您尚未在计数模式下设置规则组规则，则可能需要先将规则组规则设置为计数模式。添加一个标签匹配规则，该规则位于规则组之后运行，该规则与有问题的规则所添加的标签相匹配。在标签匹配规则中，您可以筛选要允许的请求和要阻止的请求。

  如果您使用这种方法，则在完成测试后，请在规则组中将有问题的规则保持在计数模式，并保留您的自定义标签匹配规则。有关标签匹配语句的信息，请参阅 标签匹配规则语句。有关示例，请参阅 允许特定的被阻止机器人 和 ATP 示例：针对缺失和被盗凭证的自定义处理。

- 更改托管规则组的版本 – 对于版本控制的托管规则组，请更改您正在使用的版本。例如，您可以切换回已成功使用的最后一个静态版本。

  这通常是临时修复。在测试或暂存环境中继续测试最新版本时，或者在等待提供程序提供更兼容的版本时，您可以更改生产流量的版本。有关托管规则组版本的信息，请参阅 托管规则组。

如果您对新规则可以根据您的需要匹配请求感到满意，请进入下一阶段的测试并重复此过程。在您的生产环境中执行测试和调整的最后阶段。

查看 Web ACL 的指标

将 Web ACL 与一个或多个 AWS 资源关联后，您可以在 Amazon CloudWatch 图表中查看关联生成的指标。

有关 AWS WAF 指标的信息，请参阅AWS WAF 指标和维度。有关 CloudWatch 指标的信息，请参阅 Amazon CloudWatch 用户指南。

对于 Web ACL 中的每条规则以及关联资源转发给 AWS WAF Web ACL 的所有请求， CloudWatch 您可以执行以下操作：

- 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。
- 更改对数据 CloudWatch 执行的计算，例如最大值、最小值、平均值或总和。

> **Note**
>
> AWS WAF w CloudFront ith 是一项全球服务，只有当您在中选择美国东部（弗吉尼亚北部）地区时，才可使用指标 AWS Management Console。如果您选择其他区域，则CloudWatch控制台中将不会显示任何 AWS WAF 指标。

查看 Web ACL 中规则的数据

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 如有必要，请将区域更改为 AWS 资源所在的区域。对于 CloudFront，请选择美国东部（弗吉尼亚北部）区域。
3. 在导航窗格的指标下，选择所有指标，然后在浏览选项卡下搜索`AWS::WAFV2`。
4. 选中要查看其数据的 Web ACL 对应的复选框。
5. 更改适用的设置：

   Statistic

   选择对数据 CloudWatch 执行的计算。

   时间范围

   选择您要查看前一个小时还是前三个小时的数据。

   周期

   选择图表中的数据点之间的间隔。

   规则

   选择要查看其数据的规则。

   > **Note**
   >
   > 如果您更改了规则的名称，并且希望该规则的指标名称反映更改，则还必须更新该指标名称。 AWS WAF 当您更改规则名称时，不会自动更新规则的指标名称。在控制台中编辑规则时，您可以使用规则 JSON 编辑器更改指标名称。您也可以通过 API 以及在用于定义 Web ACL 或规则组的任何 JSON 列表中更改这两个名称。

请注意以下几点：

- 如果您最近将 Web ACL 与 AWS 资源相关联，则可能需要等待几分钟才能使数据显示在图表中，并让 Web ACL 的指标显示在可用指标列表中。
- 如果您将多个资源与 Web ACL 关联，则 CloudWatch数据将包括对所有资源的请求。
- 您可以将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。

有关 CloudWatch 指标的更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

Web ACL 流量概述控制面板

本节介绍 AWS WAF 控制台中的 Web ACL 流量概述仪表板。将 Web ACL 与一个或多个 AWS 资源关联并启用 Web ACL 的指标后，您可以访问 AWS WAF 控制台中的 Web ACL 的流量概述选项卡，访问该 Web ACL 评估的 Web 流量的摘要。控制面板包含在评估您的应用程序网络流量时 AWS WAF 收集的 Amazon CloudWatch 指标的近乎实时的摘要。

> **Note**
>
> 如果您在控制面板上看不到任何内容，请确保为 Web ACL 启用了指标。

Web ACL 的流量概述选项卡包含具有以下类别的信息的选项卡式控制面板：

- 所有流量 – Web ACL 评估的所有 Web 请求。

  控制面板重点是终止操作，但您可以在以下位置查看计数规则的匹配项：
  - 此控制面板的前 10 条规则窗格。切换切换到计数操作以显示计数规则匹配项。
  - Web ACL 页面的采样请求选项卡。此新选项卡包括所有规则匹配的图表。有关信息，请参阅 查看 Web 请求示例。
- 机器人控制功能 – Web ACL 使用机器人控制功能托管规则组评估的 Web 请求。

  如果您未在 Web ACL 中使用此规则组，则此选项卡会显示根据机器人控制功能规则评估您的 Web 流量样本的结果。这让您可以了解您的应用程序收到的机器人流量，并且是免费的。

此规则组是 AWS WAF 提供的智能威胁缓解选项的一部分。有关更多信息，请参阅 AWS WAF 机器人控制 和 AWS WAF 机器人控制规则组。

- 防止@@ 账户盗用 — Web ACL 使用防 AWS WAF 欺诈控制账户接管保护 (ATP) 托管规则组评估的 Web 请求。只有在 Web ACL 中使用此规则组时，此选项卡才可用。

  ATP 规则组是 AWS WAF 智能威胁缓解产品的一部分。有关更多信息，请参阅 AWS WAF 防欺诈控制账户接管 (ATP) 和 AWS WAF 防欺诈控制账户盗用 (ATP) 规则组。
- 账户创建防作弊 — Web ACL 使用 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 托管规则组评估的 Web 请求。只有在 Web ACL 中使用此规则组时，此选项卡才可用。

  ACFP 规则组是 AWS WAF 智能威胁缓解产品的一部分。有关更多信息，请参阅 AWS WAF 欺诈控制账户创建欺诈预防 (ACFP) 和 AWS WAF 欺诈控制账户创建防作弊 (ACFP) 规则组。

仪表板基于 Web ACL 的 CloudWatch 指标，通过图表可以访问中的相应指标 CloudWatch。对于智能威胁缓解控制面板（如机器人控制功能），使用的指标主要是标签指标。

- 有关 AWS WAF 提供的指标的列表，请参阅AWS WAF 指标和维度。
- 有关 CloudWatch 指标的信息，请参阅 Amazon CloudWatch 用户指南。

控制面板提供您选择的终止操作和日期范围的流量模式摘要。无论托管规则组本身是否应用终止操作，智能威胁缓解控制面板都包含相应托管规则组评估的请求。例如，如果选中 Block，则账户盗用防护控制面板将包含所有 Web 请求的信息，这些请求既由 ATP 托管规则组评估，又在 Web ACL 评估期间的某个时候被阻止。请求可以由 ATP 托管规则组、在 Web ACL 中的规则组之后运行的规则或 Web ACL 的默认操作来阻止。

查看 Web ACL 的控制面板

按照本节中的步骤访问 Web ACL 控制面板并设置数据筛选条件。如果您最近将 Web ACL 与 AWS 资源相关联，则可能需要等待几分钟才能在仪表板中显示数据。

控制面板包括对您与 Web ACL 关联的所有资源的请求。

查看 Web ACL 的流量概述控制面板

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 Web ACL，然后搜索您感兴趣的 Web ACL。

3. 选择 Web ACL。控制台会将您转到 Web ACL 的页面。流量概述默认处于选中状态。
4. 根据需要更改数据筛选器设置。

   - 终止规则操作 – 选择要包含在控制面板中的终止操作。控制面板汇总了 Web 请求的指标，这些请求具有由 Web ACL 评估应用的选定操作之一。如果您选择所有可用操作，则控制面板将包含所有已评估的 Web 请求。有关操作的信息，请参阅 如何 AWS WAF 处理 Web ACL 中的规则和规则组操作。
   - 时间范围 – 选择要在控制面板中查看的时间间隔。您可以选择查看相对于现在的时间范围，例如过去 3 小时或上周，也可以从日历中选择绝对时间范围。
   - 时区 – 当您指定绝对时间范围时，此设置适用。您可以使用浏览器的本地时区或 UTC（协调世界时）。

查看选项卡中您感兴趣的信息。数据筛选器选项适用于所有控制面板。在图表窗格中，您可以将光标悬停在数据点或区域上方以查看任何其他详细信息。

Count 行动规则

您可以在两个位置之一查看计数操作匹配的信息。

- 在此流量概述选项卡中，在所有流量控制面板上，找到前 10 条规则窗格并切换切换到计数操作。启用此切换后，窗格将显示计数规则匹配，而不是终止规则匹配。
- 在 Web ACL 的采样请求选项卡中，查看您在流量概述选项卡上设置的时间范围内的所有规则匹配项和操作的图表。有关采样请求选项卡的信息，请参阅 查看 Web 请求示例。

亚马逊 CloudWatch 指标

在仪表板图表窗格中，您可以访问图表化数据的 CloudWatch 指标。选择图表窗格顶部或窗格内⋮（垂直省略号）下拉菜单中的选项。

刷新控制面板

控制面板不会自动刷新。要更新显示，请选择刷新

图标。

Web ACL 的流量概述控制面板示例

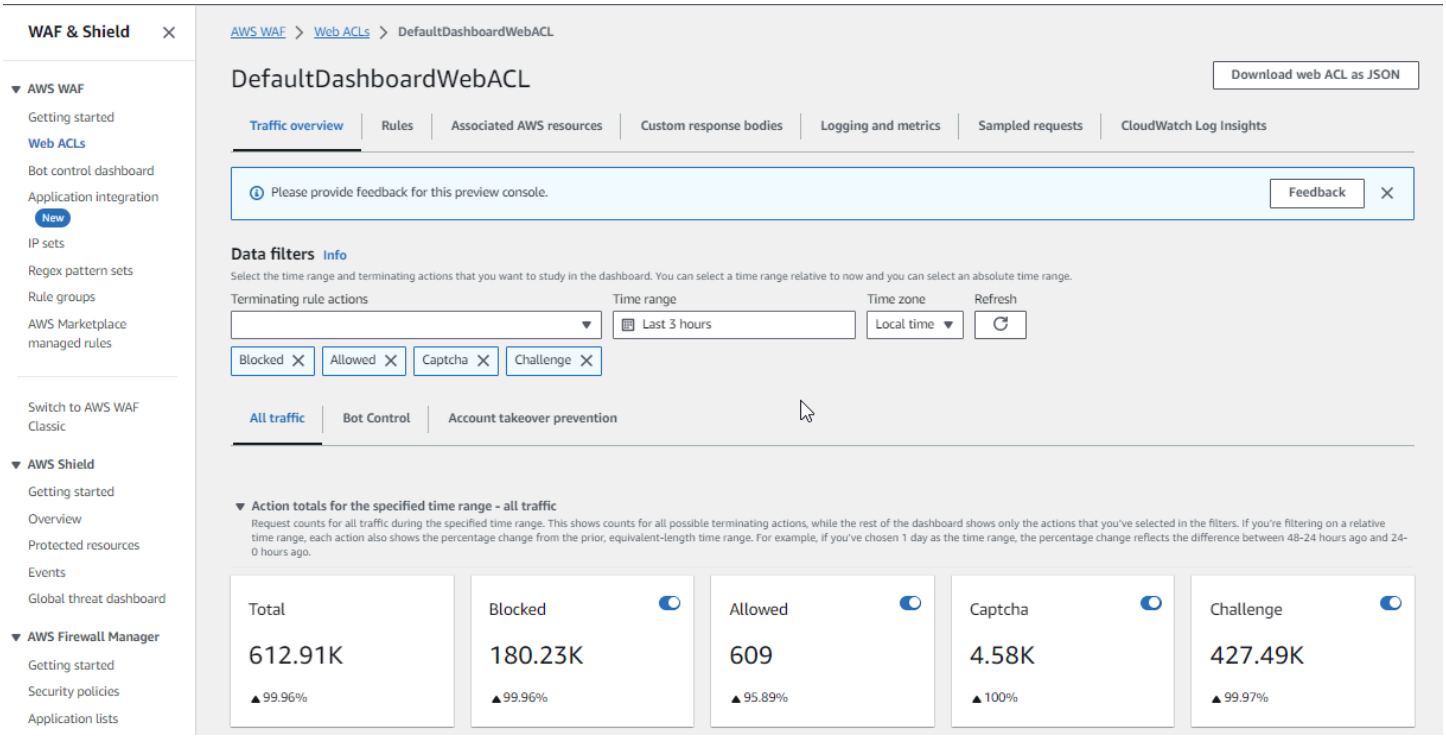
本节显示了 Web ACL 的流量概述控制面板的示例屏幕。

> **Note**
>
> 如果您已经在使用 AWS WAF 保护应用程序资源，则可以在控制台的页面上查看任何 Web ACL 的 AWS WAF 控制面板。有关信息，请参阅 查看 Web ACL 的控制面板。

屏幕示例：数据筛选器和所有流量控制面板操作计数

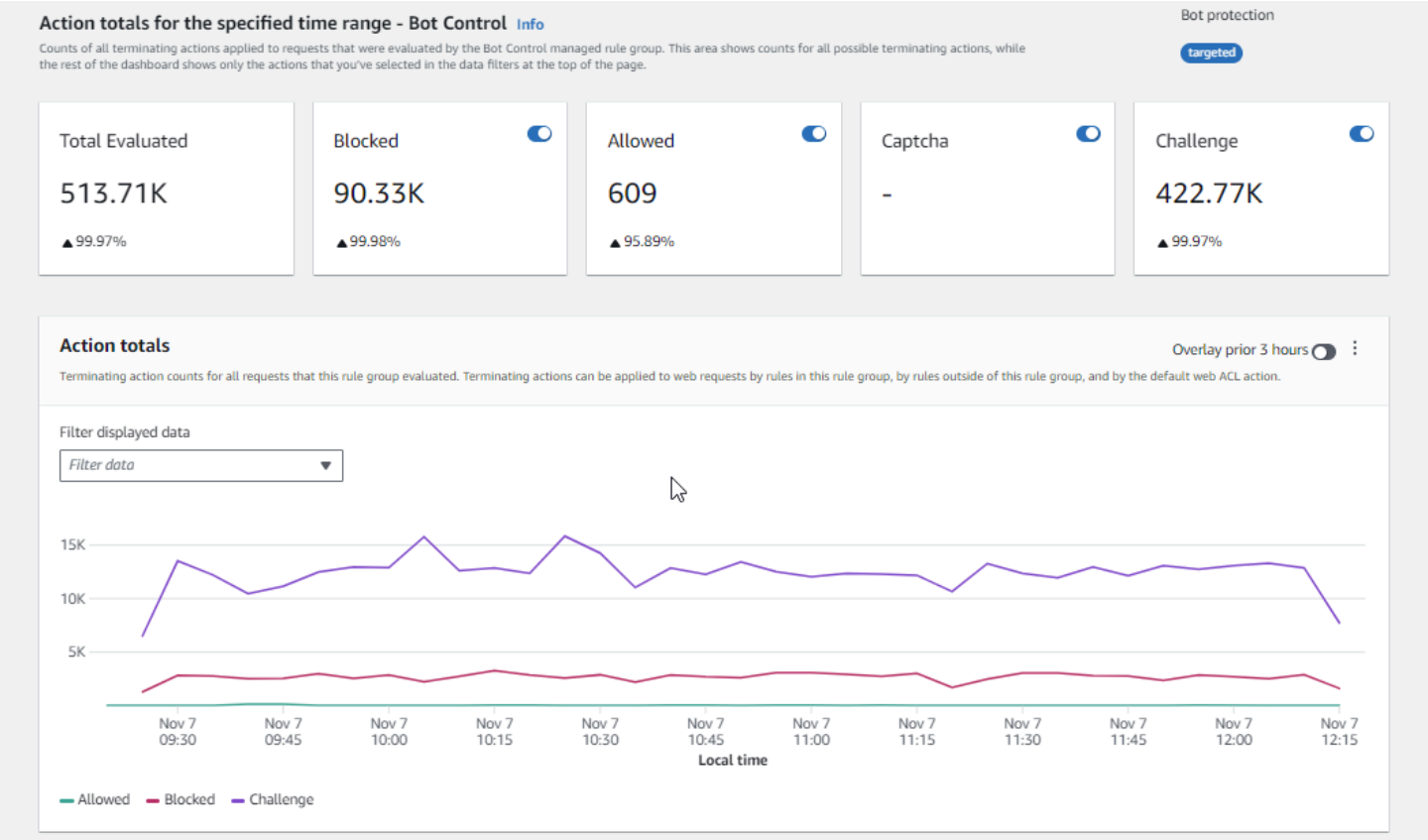
以下屏幕截图描绘了选中所有流量选项卡的 Web ACL 的流量概览。数据筛选器设置为默认值：过去三个小时内的所有终止操作。

所有流量控制面板内是各种终止操作的操作总数。每个窗格都列出了请求计数，并显示一个向上/向下箭头，表示自前三个小时的时间范围以来的变化。



屏幕示例：机器人控制功能面板操作计数

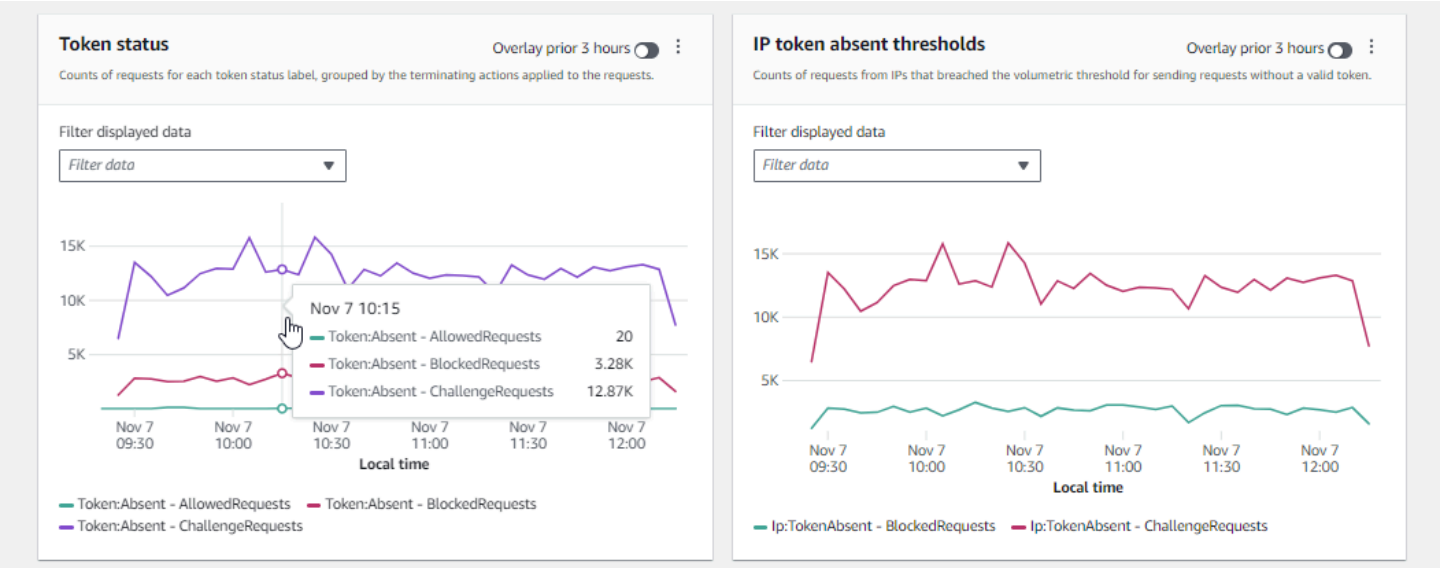
以下屏幕截图描绘了机器人控制功能控制面板的操作计数。这显示了时间范围内的相同总数窗格，但计数仅适用于机器人控制功能规则组评估的请求。再往下看，在操作总计窗格中，您可以看到指定的三小时时间范围内的操作计数。在此时间范围内，该 CAPTCHA 操作未应用于规则组评估的任何请求。



屏幕示例：机器人控制功能控制面板令牌状态摘要图表

以下屏幕截图描绘了机器人控制功能控制面板中提供的两个摘要图形。令牌状态窗格显示各种令牌状态标签的计数，以及应用于请求的规则操作。IP 令牌缺失阈值窗格显示了来自 IP 的请求的数据，这些请求在没有令牌的情况下发送了太多请求。

将鼠标悬停在图表中的任何区域上方会显示可用的信息详细信息。在此屏幕截图的令牌状态窗格中，鼠标将鼠标悬停在某个时间点上，而不在任何图形线上，因此控制台会显示该时间点所有线的数据。



本部分仅显示 Web ACL 流量概述控制面板中提供的部分流量摘要。要查看任何 Web ACL 的控制面板，请在控制台中打开 Web ACL 的页面。有关如何执行此操作的信息，请参阅 查看 Web ACL 的控制面板 上的指导。

查看 Web 请求示例

本节介绍 AWS WAF 控制台中的 Web ACL 采样请求选项卡。在此选项卡中，您可以查看 AWS WAF 已检查的 Web 请求的所有规则匹配项的图表。此外，如果您为 Web ACL 启用了请求采样，则可以看到 AWS WAF 已检查的 Web 请求样本的表格视图。您也可以通过 API 调用`GetSampledRequests`检索抽样请求信息。

请求采样包含多达 100 个符合 Web ACL 规则条件的请求，另有 100 个请求不符合任何规则，但应用了 Web ACL 默认操作。样本中的请求来自所有受保护的资源，这些资源在过去三小时内收到了对您内容的请求。

当 Web 请求与规则中的条件相匹配且该规则的操作未终止请求评估时， AWS WAF 将继续使用 Web ACL 中的后续规则检查 Web 请求。因此，Web 请求可能会多次出现。有关规则操作行为的信息，请参阅 规则操作。

查看所有规则图表和采样请求

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中，选择 Web ACL。
3. 选择要查看其请求的 Web ACL 的名称。控制台会将您转到 Web ACL 的描述，您可以在其中对其进行编辑。

4. 在采样请求选项卡中，您可以看到以下内容：

- 所有规则图表 – 此图表显示在指定时间范围内执行的所有 Web 请求评估的匹配规则和规则操作。

> **Note**
>
> 此图表的时间范围在 Web ACL 的流量概述选项卡的数据筛选器部分中设置。有关信息，请参阅 查看 Web ACL 的控制面板。

- 采样请求表 - 此表显示过去 3 小时的采样请求数据。对于每个条目，该表显示下列数据：

  指标名称

  Web ACL 中与请求匹配的规则的 CloudWatch 指标名称。如果 Web 请求与 Web ACL 中的任何规则都不匹配，则此值为默认值。

  > **Note**
  >
  > 如果您更改了规则的名称，并且希望该规则的指标名称反映更改，则还必须更新该指标名称。 AWS WAF 当您更改规则名称时，不会自动更新规则的指标名称。在控制台中编辑规则时，您可以使用规则 JSON 编辑器更改指标名称。您也可以通过 API 以及在用于定义 Web ACL 或规则组的任何 JSON 列表中更改这两个名称。

  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`)。

  规则组中的规则数

  如果指标名称标识了规则组参考语句，则该语句标识了规则组中与该请求相匹配的规则。

  操作

  指示对应规则的操作。有关可能的规则操作的信息，请参阅 规则操作。

时间

从受保护资源 AWS WAF 收到请求的时间。

要显示有关 Web 请求组成部分的其他信息，请在请求行中选择 URI 的名称。

在生产环境中启用保护

在生产环境中完成最后阶段的测试和调整后，请在生产模式下启用保护。

> **生产流量风险**
>
> 在为生产流量部署 Web ACL 实施之前，请在测试环境中对其进行测试和调整，直到您对流量可能产生的影响感到满意。在启用对生产流量的保护之前，还要在计数模式下对其进行测试和调整。

> **Note**
>
> 要遵循本节中的指导，您需要大致了解如何创建和管理 AWS WAF 保护，例如 Web ACL、规则和规则组。本指南前面部分将介绍该信息。

首先在测试环境中执行这些步骤，然后在生产环境中执行这些步骤。

在生产环境中启用 AWS WAF 保护

1. 切换到您的生产保护

   更新您的 Web ACL 并切换您的生产设置。

   a. 删除您不需要的所有测试规则

      如果您添加了在生产中不需要的测试规则，请将其删除。如果您使用任何标签匹配规则来筛选托管规则组规则的结果，请务必保留这些规则。

   b. 切换为生产操作

      将新规则的操作设置更改为预期的生产设置。

- Web ACL 中定义的规则 – 编辑 Web ACL 中的规则，并将其操作从 Count 更改为生产操作。
- 规则组 – 在规则组的 Web ACL 配置中，根据测试和调整活动的结果，将规则切换为使用自己的操作或保留 Count 操作覆盖。如果您使用标签匹配规则来筛选规则组规则的结果，请务必保留该规则的替代规则。

  要切换到使用规则的操作，请在您的 Web ACL 配置中，编辑规则组的规则语句并删除该规则的 Count 覆盖。如果您以 JSON 格式管理 Web ACL，则在规则组参考语句中，从 `RuleActionOverrides` 列表中删除该规则的条目。
- Web ACL – 如果您更改了测试的 Web ACL 默认操作，请将其切换到生产设置。

通过这些设置，您的新保护将按照您的意图管理 Web 流量。

保存 Web ACL 时，与之关联的资源将使用您的生产设置。

2. 监控和调整

   为确保按照您的要求处理 Web 请求，请在启用新功能后密切监控流量。您将监控生产规则操作的指标和日志，而不是您在调整工作中监控的计数操作。继续监控并根据需要调整行为，以适应 Web 流量的变化。

如何 AWS WAF 使用 Amazon CloudFront 功能

创建 Web ACL 时，可以指定 AWS WAF 要检查的一个或多个 CloudFront 分配。 AWS WAF 开始根据您在 Web ACL 中确定的标准检查和管理针对这些分发的 Web 请求。 CloudFront 提供了一些增强 AWS WAF 功能的功能。本章介绍几种您可以配置的方法，CloudFront 以便 CloudFront 更好地协同 AWS WAF 工作。

主题

AWS WAF 与 CloudFront 自定义错误页面一起使用

默认情况下，当根据您指定的条件 AWS WAF 阻止 Web 请求时，它会403 （Forbidden)向查看者返回 HTTP 状态码 CloudFront，并将该状态代码 CloudFront 返回给查看者。然后，查看器显示简要且采用稀疏格式的默认消息，如下所示：

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

您可以通过定义自定义响应来覆盖您的 AWS WAF Web ACL 规则中的此行为。有关使用 AWS WAF 规则自定义响应行为的更多信息，请参阅Block 操作的自定义响应。

> **Note**
>
> 使用 AWS WAF 规则自定义的响应优先于您在 CloudFront 自定义错误页面中定义的任何响应规范。

如果您希望通过 CloudFront显示自定义错误消息（可能使用与网站其余部分相同的格式），则可以配置 CloudFront 为向查看者返回包含自定义错误消息的对象（例如 HTML 文件）。

> **Note**
>
> CloudFront 无法区分您的来源返回的 HTTP 状态码 403 和请求被阻止 AWS WAF 时返回的 HTTP 状态码 403。这意味着，您无法根据 HTTP 状态代码 403 的不同原因返回不同的自定义错误页面。

有关 CloudFront 自定义错误页面的更多信息，请参阅 Amazon CloudFront 开发者指南中的生成自定义错误响应。

AWS WAF 与一起 CloudFront用于在您自己的 HTTP 服务器上运行的应用程序

AWS WAF 与一起使用时 CloudFront，您可以保护在任何 HTTP 网络服务器上运行的应用程序，无论是在亚马逊弹性计算云 (Amazon EC2) 中运行的网络服务器，还是您私下管理的网络服务器。您也可以配置 CloudFront 为要求在 CloudFront和您自己的 Web 服务器之间以及查看者和 CloudFront之间使用 HTTPS。

需要在 CloudFront 和你自己的网络服务器之间使用 HTTPS

要要求在 CloudFront 和您自己的网络服务器之间使用 HTTPS，您可以使用 CloudFront 自定义源功能，并为特定来源配置源协议策略和源域名设置。在您的 CloudFront 配置中，您可以指定服务器的 DNS 名称以及从源中获取对象时 CloudFront 要使用的端口和协议。您还应确保自定义源服务器上的 SSL/TLS 证书与您已配置的源域名匹配。在以外使用自己的 HTTP Web 服务器时 AWS，必须使用由受信任的第三方证书颁发机构 (CA) 签名的证书，例如 Comodo 或 Symante DigiCert c。有关要求在 CloudFront和您自己的网络服务器之间进行通信时需要 HTTPS 的更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的 “需要使用 HTTPS 才能 CloudFront 与您的自定义源进行通信” 主题。

要求在查看者和之间使用 HTTPS CloudFront

要要求在查看者和之间使用 HTTPS CloudFront，您可以更改 CloudFront分配中一个或多个缓存行为的查看者协议策略。有关在观看者和之间使用 HTTPS 的更多信息 CloudFront，请参阅 Amazon CloudFront 开发者指南 CloudFront中的 “观看者之间需要使用 HTTPS 才能进行通信” 主题。您也可以带上自己的 SSL 证书，这样观众就可以使用自己的域名（例如 https://www.mysite.com）通过 HTTPS 连接到您的 CloudFront 发行版。有关更多信息，请参阅 Amazon CloudFront 开发者指南中的配置备用域名和 HTTPS 主题。

选择 CloudFront响应的 HTTP 方法

创建 Amazon CloudFront 网络分配时，您可以选择要 CloudFront 处理的 HTTP 方法并将其转发到您的来源。可从以下选项中进行选择：

- **GET**，**HEAD**— 您 CloudFront 只能使用从原点获取对象或获取对象标题。
- **GET**,**HEAD**, **OPTIONS** — 您 CloudFront 只能使用从您的来源获取对象、获取对象标头或检索源服务器支持的选项列表。
- **GET**、**HEAD**、**OPTIONS**、**PUTPOST**、**PATCH**、、**DELETE** — 您可以使用获 CloudFront 取、添加、更新和删除对象以及获取对象标题。此外，您可以执行其他 POST 操作，例如从 Web 表格提交数据。

您还可以使用 AWS WAF 字节匹配规则语句来允许或阻止基于 HTTP 方法的请求，如中所述字符串匹配规则语句。如果您想使用 CloudFront 支持的方法组合，例如GET和HEAD，则无需配置 AWS WAF 以阻止使用其他方法的请求。如果要允许组合 CloudFront 不支持的方法，例如GETHEADPOST、和，则可以配置 CloudFront 为响应所有方法，然后使用 AWS WAF 来阻止使用其他方法的请求。

有关选择 CloudFront 响应方法的更多信息，请参阅《Amazon CloudFront 开发者指南》中 “您在创建或更新 Web 分配时指定的值” 主题中的 “允许的 HTTP 方法”。

您使用 AWS WAF 服务的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

> **Note**
>
> 本节为您使用 AWS WAF 服务及其 AWS 资源（例如 AWS WAF Web ACL 和规则组）提供标准 AWS 安全指南。
> 有关使用保护 AWS 资源的信息 AWS WAF，请参阅 AWS WAF 指南的其余部分。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用的合规计划 AWS WAF，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS WAF。以下主题向您介绍如何进行配置 AWS WAF 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS WAF 资源。

主题

- 中的数据保护 AWS WAF
- 的身份和访问管理 AWS WAF
- 登录和监控 AWS WAF
- 合规性验证 AWS WAF
- 韧性在 AWS WAF
- AWS WAF中的基础设施安全性

中的数据保护 AWS WAF

分 AWS 担责任模型适用于中的数据保护 AWS WAF。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的

AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API AWS WAF 或 SDK 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或 AWS SDK 的情况。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

AWS WAF 实体（例如 Web ACL、规则组和 IP 集）采用静态加密，但某些不提供加密的地区除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

删除 AWS WAF 资源

您可以删除您在 AWS WAF中创建的资源。请参阅以下各节中每种资源类型的指南。

- 删除 Web ACL
- 删除规则组
- 删除 IP 集
- 删除正则表达式模式集

的身份和访问管理 AWS WAF

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS WAF 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 AWS WAF。

服务用户-如果您使用 AWS WAF 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 AWS WAF 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AWS WAF中的特征，请参阅 对 AWS WAF 身份和访问进行故障排除。

服务管理员-如果您负责公司的 AWS WAF 资源，则可能拥有完全访问权限 AWS WAF。您的工作是确定您的服务用户应访问哪些 AWS WAF 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与配合使用 AWS WAF，请参阅如何 AWS WAF 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 AWS WAF的访问权限的详细信息。要查看您可以在 IAM 中使用的 AWS WAF 基于身份的策略示例，请参阅。适用于 AWS WAF的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（ MFA ）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定

的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon QLDB 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他

AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策

略（SCP）。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。

- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS WAF 与 IAM 配合使用

在使用 IAM 管理访问权限之前 AWS WAF，请先了解有哪些 IAM 功能可供使用 AWS WAF。

您可以搭配使用的 IAM 功能 AWS WAF

IAM 功能	AWS WAF 支持
基于身份的策略	是
基于资源的策略	支持
策略操作	是
策略资源	支持
策略条件键（特定于服务）	支持
ACL	否
ABAC（策略中的标签）	部分
临时凭证	支持
转发访问会话（FAS）	支持
服务角色	支持

IAM 功能	AWS WAF 支持
服务相关角色	支持

要全面了解 AWS WAF 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 AWS WAF

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

要查看 AWS WAF 基于身份的策略的示例，请参阅。适用于 AWS WAF的基于身份的策略示例

内部基于资源的政策 AWS WAF

支持基于资源的策略	支持

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予

访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

AWS WAF 使用基于资源的策略来支持跨账户共享规则组。通过向 AWS WAF API 调用或等效的 CLI PutPermissionPolicy 或 SDK 调用提供基于资源的策略设置，您可以与其他 AWS 账户共享您拥有的规则组。如需了解更多信息，包括其他可用语言的示例和文档链接，请参阅 AWS WAF API 参考PutPermissionPolicy中的。此功能无法通过其他方式使用，例如控制台或 AWS CloudFormation。

的政策行动 AWS WAF

支持策略操作	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看每个 AWS WAF 操作和权限的列表，请参阅《服务授权参考》中的 AWS WAF V2 定义的操作。

正在执行的策略操作在操作前 AWS WAF 使用以下前缀：

```
wafv2
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以开头的所有操作List，请包括以下操作：AWS WAF

```
"Action": "wafv2:List*"
```

要查看 AWS WAF 基于身份的策略的示例，请参阅。适用于 AWS WAF的基于身份的策略示例

需要额外权限设置的操作

有些操作需要的权限无法在《服务授权参考》中的 AWS WAF V2 定义的操作中进行完整描述。本节提供其他权限信息。

主题

- AssociateWebACL 权限
- DisassociateWebACL 权限
- GetWebACLForResource 权限
- ListResourcesForWebACL 权限

AssociateWebACL 权限

本节列出了使用 AWS WAF 操作 `AssociateWebACL` 将 Web ACL 与资源关联所需的权限。

对于 Amazon CloudFront 分配，请使用操作代替此 CloudFront 操作`UpdateDistribution`。有关信息，请参阅`UpdateDistribution`《亚马逊 CloudFront API 参考》。

Amazon API Gateway REST API

需要权限才能在 REST API 资源类型`SetWebACL`上调用 API Gateway，以及调用 AWS WAF `AssociateWebACL` Web ACL 的权限。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
```

```
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

应用程序负载均衡器

需要权限才能在 Applicati `elasticloadbalancing:SetWebACL` on Load Balancer 资源类型 AWS WAF `AssociateWebACL`上调用操作并调用 Web ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

需要权限才能调用 AWS AppSync `SetWebACL` GraphQL API 资源类型和通过 Web ACL AWS WAF `AssociateWebACL` 进行调用。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
```

```
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 用户池

需要权限才能对用户池资源类型调用 Amazon Cognito `AssociateWebACL` 操作并调用 Web AWS WAF `AssociateWebACL` ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服务

需要权限才能对 App Runner 服务资源类型调用 App Runner `AssociateWebACL` 操作并调用 AWS WAF `AssociateWebACL` Web ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 已验证访问实例

需要权限才能在 “已验证访问权限” 实例资源类型上调用`ec2:AssociateVerifiedAccessInstanceWebAcl`操作并调用 AWS WAF `AssociateWebACL` Web ACL。

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
```

```
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`DisassociateWebACL` 权限

本节列出了使用 AWS WAF 操作 `DisassociateWebACL` 将 Web ACL 与资源取消关联所需的权限。

对于 Amazon CloudFront 分配，请使用`UpdateDistribution`带有空网页 ACL ID 的 CloudFront 操作来代替此操作。有关信息，请参阅UpdateDistribution《亚马逊 CloudFront API 参考》。

Amazon API Gateway REST API

需要权限才能在 REST API 资源类型上调用 API Gateway `SetWebACL`。不需要通话许可 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

应用程序负载均衡器

需要权限才能在应用程序负载均衡器资源类型上调用 `elasticloadbalancing:SetWebACL` 操作。不需要通话许可 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
```

```
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

需要权限才能调用 AWS AppSync `SetWebACL` GraphQL API 资源类型。不需要通话许可 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 用户池

需要权限才能对用户池资源类型调用 Amazon Cognito `DisassociateWebACL` 操作并进行调用。AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
```

```
}
```

AWS App Runner 服务

需要权限才能在 App Runner 服务资源类型上调用 App Runner `DisassociateWebACL` 操作并进行调用 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 已验证访问实例

需要权限才能在 “已验证访问权限” 实例资源类型上调用`ec2:DisassociateVerifiedAccessInstanceWebAcl`操作并进行调用 AWS WAF `DisassociateWebACL`。

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
```

```
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`GetWebACLForResource` 权限

本节列出了使用 AWS WAF 操作 `GetWebACLForResource` 获取受保护资源的 Web ACL 所需的权限。

对于 Amazon CloudFront 分配，请使用操作代替此 CloudFront 操作`GetDistributionConfig`。有关信息，请参阅GetDistributionConfig《亚马逊 CloudFront API 参考》。

> **Note**
>
> `GetWebACLForResource` 需要调用 `GetWebACL` 的权限。在这种情况下，`GetWebACL`仅 AWS WAF 用于验证您的账户是否具有访问`GetWebACLForResource`返回的 Web ACL 所需的权限。当您致电时`GetWebACLForResource`，您可能会收到一条错误消息，表明您的账户无权使用`wafv2:GetWebACL`该资源。 AWS WAF 不会将此类错误添加到 AWS CloudTrail 事件历史记录中。

亚马逊 API Gateway REST API、Application Load Balancer 和 AWS AppSync GraphQL API

需要通话 AWS WAF `GetWebACLForResource`权限才能获`GetWebACL`得 Web ACL。

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Amazon Cognito 用户池

需要权限才能对用户池资源类型调用 Amazon Cognito `GetWebACLForResource` 操作以及调 AWS WAF `GetWebACLForResource`用和。`GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:GetWebACLForResource"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服务

需要权限才能调用 App Runner 服务资源类型的 App Runner `DescribeWebAclForService` 操作以及调用 AWS WAF `GetWebACLForResource`和`GetWebACL`。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
```

```
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 已验证访问实例

需要权限才能在 “已验证访问权限” 实例资源类型上调用`ec2:GetVerifiedAccessInstanceWebAcl`操作并调用 AWS WAF `GetWebACLForResource`和`GetWebACL`。

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`ListResourcesForWebACL` 权限

本节列出了使用 AWS WAF 操作 `ListResourcesForWebACL` 检索 Web ACL 的受保护资源列表所需的权限。

对于 Amazon CloudFront 分配，请使用操作代替此 CloudFront 操作`ListDistributionsByWebACLId`。有关信息，请参阅《亚马逊 CloudFront API 参考》中的 ListDistributionsByWebAC Lid。

亚马逊 API Gateway REST API、Application Load Balancer 和 AWS AppSync GraphQL API

需要权限才能调 AWS WAF `ListResourcesForWebACL`用 Web ACL。

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Amazon Cognito 用户池

需要权限才能在用户群体资源类型上调用 Amazon Cognito `ListResourcesForWebACL` 操作并调用 AWS WAF `ListResourcesForWebACL`。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 服务

需要权限才能在 App Runner 服务资源类型上调用 App Runner `ListAssociatedServicesForWebAcl` 操作并进行调用 AWS WAF `ListResourcesForWebACL`。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 已验证访问实例

需要权限才能在 Verified Access 实例资源类型上调用 `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` 操作并调用 AWS WAF `ListResourcesForWebACL`。

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
```

```
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

的政策资源 AWS WAF

支持策略资源	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 AWS WAF 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 AWS WAF V2 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 V2 定义的 AWS WAF 操作。要允许或拒绝对 AWS WAF 资源子集的访问，请在策略的resource元素中包含该资源的 ARN。

AWS WAF wafv2资源的 ARN 格式如下：

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

有关 ARN 的信息，请参阅 Amazon Web Services 一般参考中的 Amazon 资源名称 (ARN)。

以下列出了特定于 wafv2 资源 ARN 的要求：

- ##：对于用于保护 Amazon CloudFront 分配的 AWS WAF 资源，请将其设置为us-east-1。否则，请将其设置为您正在使用受保护区域资源的区域。

- s@@ *co* pe：将范围设置为，以便`global`在 Amazon CloudFront 配送中使用或`regional`与 AWS WAF 支持的任何区域资源一起使用。区域资源是 Amazon API Gateway REST API、应用程序负载均衡器、 AWS AppSync GraphQL API、Amazon Cognito 用户池、服务和 AWS 已验证访问实 AWS App Runner 例。
- *####*：指定以下值之一：`webacl`、`rulegroup`、`ipset`、`regexpatternset` 或 `managedruleset`。
- *####*：指定您为 AWS WAF 资源提供的名称，或指定通配符 (*) 以表示满足 ARN 中其他规格的所有资源。您必须指定资源名称和资源 ID，或者为两者指定通配符。
- *resource-id*：指定 AWS WAF 资源的 ID，或指定通配符 (*) 以表示满足 ARN 中其他规格的所有资源。您必须指定资源名称和资源 ID，或者为两者指定通配符。

例如，以下 ARN 指定区域 `us-west-1` 中具有账户 `111122223333` 的区域作用域的所有 Web ACL：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

以下 ARN 为区域 `us-east-1` 中的账户 `111122223333` 指定了名为 `MyIPManagementRuleGroup` 全局范围规则组：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

要查看 AWS WAF 基于身份的策略的示例，请参阅。适用于 AWS WAF的基于身份的策略示例

的策略条件密钥 AWS WAF

支持特定于服务的策略条件键	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

此外，还 AWS WAF 支持以下条件键，您可以使用这些条件键为您的 IAM 策略提供精细筛选：

- wafv2：LogDestinationResource

  此条件密钥采用日志目标的 Amazon 资源名称 (ARN) 规范。这是您在使用 REST API 调用时为日志目标提供的 ARN。`PutLoggingConfiguration`

  您可以明确指定 ARN，也可以为 ARN 指定过滤。以下示例指定筛选具有特定位置和前缀的 Amazon S3 存储桶 ARN。

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2：LogScope

  此条件键以字符串形式定义日志配置的来源。当前，它始终设置为默认值`Customer`，这表示日志记录目标归您所有和管理。

要查看 AWS WAF 条件键列表，请参阅《服务授权参考》中的 AWS WAF V2 条件密钥。要了解可以使用条件键的操作和资源，请参阅 AWS WAF V2 定义的操作。

要查看 AWS WAF 基于身份的策略的示例，请参阅。适用于 AWS WAF的基于身份的策略示例

输入的 ACL AWS WAF

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC with AWS WAF

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与 AWS WAF

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发服务的访问会话 AWS WAF

支持转发访问会话 (FAS)	支持

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求

时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

AWS WAF的服务角色

支持服务角色	支持

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 AWS WAF 功能。只有在 AWS WAF 提供操作指导时才编辑服务角色。

的服务相关角色 AWS WAF

支持服务相关角色	支持

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 AWS WAF 服务相关角色的详细信息，请参阅将服务相关角色用于 AWS WAF。

适用于 AWS WAF的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 AWS WAF 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关由 AWS WAF定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 AWS WAF V2 的操作、资源和条件密钥。

主题

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 AWS WAF 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略 或 工作职能的AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy 语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 AWS WAF 控制台

要访问 AWS WAF 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 AWS WAF 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色可以使用 AWS WAF 控制台，还应至少将 AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS 托管策略附加到实体。有关托管策略的信息，请参阅 AWS 托管策略： AWSWAFConsoleReadOnlyAccess。有关将托管策略附加到用户的更多信息，请参阅 IAM 用户指南中的向用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授予对 AWS WAF CloudFront、和的只读访问权限 CloudWatch

以下政策授予用户对 AWS WAF 资源、Amazon CloudFront 网络分配和亚马逊 CloudWatch 指标的只读访问权限。对于需要查看 AWS WAF 条件、规则和 Web ACL 中设置的权限的用户，可以查看哪个分配与 Web ACL 相关联，以及监控中的 CloudWatch指标和请求样本，这非常有用。这些用户无法创建、更新或删除 AWS WAF 资源：

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

授予对 AWS WAF CloudFront、和的完全访问权限 CloudWatch

以下政策允许用户在中执行任何 AWS WAF 操作、对 CloudFront Web 分配执行任何操作以及监控指标和请求示例 CloudWatch。它对 AWS WAF 管理员用户很有用。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

强烈建议您为拥有管理权限的用户配置 Multi-Factor Authentication (MFA)。有关更多信息，请参阅 IAM 用户指南中的在 AWS中使用多重身份验证（MFA）设备。

授予对单个的访问权限 AWS 账户

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。
- 读取和更新所有 CloudFront 分配的访问权限，这允许您关联 Web ACL 和 CloudFront 分配。
- 读取所有 CloudWatch 指标和指标统计信息的访问权限，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": [
```

```
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

授予对单个 Web ACL 的访问权限

以下策略允许用户通过控制台对账户中的特定 Web ACL 执行任何 AWS WAF 操作444455556666。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

授予 CLI 访问权限 Web ACL 和规则组

以下策略允许用户通过 CLI 对账户中的特定 Web ACL 和特定规则组执行任何 AWS WAF 操作444455556666。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

以下策略允许用户通过控制台对账户中的特定 Web ACL 执行任何 AWS WAF 操作444455556666。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 的托管策略 AWS WAF

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： AWSWAFReadOnlyAccess

该策略授予只读权限，允许用户访问集成服务的 AWS WAF 资源和资源，例如亚马逊、Amazon API Gateway CloudFront、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已验证访问权限。 AWS App Runner您可以将此策略附加到您的 IAM 身份。 AWS WAF 还将此策略附加 AWS WAF 到允许代表您执行操作的服务角色。

有关此策略的详细信息，请参阅 IAM 控制台AWSWAFReadOnlyAccess中的。

AWS 托管策略： AWSWAFFullAccess

该政策授予对集成服务（例如亚马逊 CloudFront、Amazon API Gateway、Application Load Balancer、Amazon Cognito 和 AWS 已验证访问权限）的资源和资源的完全访问权限。 AWS WAF AWS AppSync AWS App Runner您可以将此策略附加到您的 IAM 身份。 AWS WAF 还将此策略附加 AWS WAF 到允许代表您执行操作的服务角色。

有关此策略的详细信息，请参阅 IAM 控制台AWSWAFFullAccess中的。

AWS 托管策略： AWSWAFConsoleReadOnlyAccess

该策略向 AWS WAF 控制台授予只读权限，其中包括用于 AWS WAF 集成服务的资源，例如亚马逊 CloudFront、Amazon API Gateway、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已验证访问权限。 AWS App Runner您可以将此策略附加到您的 IAM 身份。 AWS WAF 还将此策略附加 AWS WAF 到允许代表您执行操作的服务角色。

有关此策略的详细信息，请参阅 IAM 控制台AWSWAFConsoleReadOnlyAccess中的。

AWS 托管策略： AWSWAFConsoleFullAccess

该政策授予对 AWS WAF 控制台的完全访问权限，其中包括用于 AWS WAF 集成服务的资源，例如亚马逊、Amazon API Gateway CloudFront、Application Load Balancer AWS AppSync、Amazon Cognito 和 AWS 已验证访问权限。 AWS App Runner您可以将此策略附加到您的 IAM 身份。 AWS WAF 还将此策略附加 AWS WAF 到允许代表您执行操作的服务角色。

有关此策略的详细信息，请参阅 IAM 控制台AWSWAFConsoleFullAccess中的。

AWS WAFAWS 托管策略的更新

查看 AWS WAF 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 AWS WAF 文档历史记录页面上的 RSS feed，网址为文档历史记录。

Policy	更改的说明	Date
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源	扩展了权限，可将 AWS 已验证访问权限实例添加到您可以保护的资源类型中 AWS WAF。	2023-06-17

Policy	更改的说明	Date
AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息：AWSWAFFullAccess.		
AWSWAFReadOnlyAccess 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息：AWSWAFReadOnlyAccess.	扩展了权限，可将 AWS 已验证访问权限实例添加到您可以保护的资源类型中 AWS WAF。	2023-06-17
AWSWAFConsoleFullAccess 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleFullAccess.	扩展了权限，可将 AWS 已验证访问权限实例添加到您可以保护的资源类型中 AWS WAF。	2023-06-17
AWSWAFConsoleReadOnlyAccess 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleReadOnlyAccess.	扩展了权限，可将 AWS 已验证访问权限实例添加到您可以保护的资源类型中 AWS WAF。	2023-06-17

Policy	更改的说明	Date
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息 :AWSWAFFullAccess.	扩展了权限以更正 AWS App Runner 服务的访问设置。	2023-06-06
`AWSWAFReadOnlyAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息 :AWSWAFReadOnlyAccess.	扩展了权限以更正 AWS App Runner 服务的访问设置。	2023-06-06
`AWSWAFConsoleFullAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息 :AWSWAFConsoleFullAccess.	扩展了权限以更正 AWS App Runner 服务的访问设置。	2023-06-06

Policy	更改的说明	Date
`AWSWAFConsoleReadOnlyAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleReadOnlyAccess.	扩展了权限以更正 AWS App Runner 服务的访问设置。	2023-06-06
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息：AWSWAFFullAccess.	扩展了向可用来保护的资源类型添加 AWS App Runner 服务的权限 AWS WAF。	2023-03-30
`AWSWAFReadOnlyAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息：AWSWAFReadOnlyAccess.	扩展了向可用来保护的资源类型添加 AWS App Runner 服务的权限 AWS WAF。	2023-03-30

Policy	更改的说明	Date
`AWSWAFConsoleFullAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleFullAccess.	扩展了向可用来保护的资源类型添加 AWS App Runner 服务的权限 AWS WAF。	2023-03-30
`AWSWAFConsoleReadOnlyAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息：AWSWAFConsoleReadOnlyAccess.	扩展了向可用来保护的资源类型添加 AWS App Runner 服务的权限 AWS WAF。	2023-03-30
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息：AWSWAFFullAccess.	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中。 AWS WAF	2022-08-25

Policy	更改的说明	Date
`AWSWAFReadOnlyAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息 :AWSWAFReadOnlyAccess.	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中。 AWS WAF	2022-08-25
`AWSWAFConsoleFullAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息 :AWSWAFConsoleFullAccess.	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中。 AWS WAF	2022-08-25
`AWSWAFConsoleReadOnlyAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息 :AWSWAFConsoleReadOnlyAccess.	扩展了权限，将 Amazon Cognito 用户池添加到您可以保护的资源类型中。 AWS WAF	2022-08-25

Policy	更改的说明	Date
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息 :AWSWAFFullAccess.	更正了亚马逊简单存储服务 (Amazon S3) 和亚马逊 CloudWatch 日志的日志传输权限设置。此更改解决了日志配置期间出现的拒绝访问错误。有关记录 Web ACL 流量的信息，请参阅 记录 AWS WAF Web ACL 流量。	2022-01-11
`AWSWAFConsoleFullAccess` 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息 :AWSWAFConsoleFullAccess.	更正了亚马逊简单存储服务 (Amazon S3) 和亚马逊 CloudWatch 日志的日志传输权限设置。此更改解决了日志配置期间发生的访问错误。有关记录 Web ACL 流量的信息，请参阅 记录 AWS WAF Web ACL 流量。	2022-01-11
`AWSWAFFullAccess` 该政策 AWS WAF 允许代表您管理集成服务中的 AWS 资源 AWS WAF 和集成服务中的资源。 IAM 控制台中的详细信息 :AWSWAFFullAccess.	为扩展的日志记录选项添加了新权限。 此更改 AWS WAF 允许访问其他日志目标亚马逊简单存储服务 (Amazon S3) 和 Amazon Logs。 CloudWatch 有关记录 Web ACL 流量的信息，请参阅 记录 AWS WAF Web ACL 流量。	2021-11-15

Policy	更改的说明	Date
AWSWAFConsoleFullAccess 此政策 AWS WAF 允许您代表您在集成服务中和集成服务中 AWS WAF 管理 AWS 控制台 AWS 资源和其他资源。 IAM 控制台中的详细信息 :AWSWAFConsoleFullAccess.	为扩展的日志记录选项添加了新权限。 此更改 AWS WAF 允许访问其他日志目标亚马逊简单存储服务 (Amazon S3) 和 Amazon Logs。 CloudWatch 有关记录 Web ACL 流量的信息，请参阅记录 AWS WAF Web ACL 流量。	2021-11-15
AWS WAF 已开始跟踪更改	AWS WAF 开始跟踪其 AWS 托管策略的更改。	2021-3-01

对 AWS WAF 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 AWS WAF 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 AWS WAF
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 AWS WAF 资源

我无权在以下位置执行操作 AWS WAF

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 wafv2:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 wafv2:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 AWS WAF。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 AWS WAF中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AWS WAF 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解是否 AWS WAF 支持这些功能，请参阅如何 AWS WAF 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

将服务相关角色用于 AWS WAF

AWS WAF 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS WAF服务相关角色由服务预定义 AWS WAF ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS WAF 更加容易，因为您不必手动添加必要的权限。 AWS WAF 定义其服务相关角色的权限，除非另有定义，否则 AWS WAF 只能担任其角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这样可以保护您的 AWS WAF 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

AWS WAF的服务相关角色权限

AWS WAF 使用服务相关角色`AWSServiceRoleForWAFV2Logging`。

AWS WAF 使用此服务相关角色向 Amazon Data Firehose 写入日志。只有在启用登录功能后才会使用此角色 AWS WAF。有关更多信息，请参阅 记录 AWS WAF Web ACL 流量。

`AWSServiceRoleForWAFV2Logging` 服务相关角色信任 `wafv2.amazonaws.com` 服务来代入角色。

该角色的权限策略 AWS WAF 允许对指定资源完成以下操作：

- 操作：`firehose:PutRecord`firehose:PutRecordBatch在 Amazon Data 上，Firehose 的数据流资源名称以 “aws-waf-logs-” 开头。例如，`aws-waf-logs-us-east-2-analytics`。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS WAF创建服务相关角色

您无需手动创建服务相关角色。当您启用 AWS WAF 登录功能 AWS Management Console，或者在 CLI 或 AWS WAF AP AWS WAF I 中`PutLoggingConfiguration`发出请求时， AWS WAF 会为您创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。启用 AWS WAF 日志记录后， AWS WAF 会再次为您创建服务相关角色。

为 AWS WAF编辑服务相关角色

AWS WAF 不允许您编辑AWSServiceRoleForWAFV2Logging服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AWS WAF的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 AWS WAF 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除使用的 AWS WAF 资源 **AWSServiceRoleForWAFV2Logging**

1. 在 AWS WAF 控制台上，从每个 Web ACL 中删除日志记录。有关更多信息，请参阅 记录 AWS WAF Web ACL 流量。
2. 使用 API 或 CLI，为已启用日志记录的每个 Web ACL 提交 DeleteLoggingConfiguration 请求。有关更多信息，请参阅 AWS WAF API 参考。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForWAFV2Logging 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AWS WAF 服务相关角色的受支持区域

AWS WAF 支持在提供服务的所有地区使用服务相关角色。有关更多信息，请参阅 AWS WAF 终端节点和限额。

登录和监控 AWS WAF

监控是维护 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS WAF 您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控您的 AWS WAF 资源和响应潜在事件的工具：

亚马逊 CloudWatch 警报

使用 CloudWatch 警报，您可以监视您指定的时间段内的单个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 AWS Auto Scaling 政策 CloudWatch 发送通知。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

AWS CloudTrail 日志

CloudTrail 提供了用户、角色或 AWS 服务在中执行的操作的记录 AWS WAF。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 AWS WAF、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。有关更多信息，请参阅 使用 记录 AWS CloudTrail API 调用。

AWS WAF Web ACL 流量记录

AWS WAF 为您的 Web ACL 分析的流量提供日志记录。日志包含诸如从您的受保护 AWS 资源 AWS WAF 收到请求的时间、有关该请求的详细信息以及请求匹配的规则的操作设置等信息。有关更多信息，请参阅 记录 AWS WAF Web ACL 流量。

合规性验证 AWS WAF

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

  > **Note**
  >
  > 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS WAF

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS WAF中的基础设施安全性

作为一项托管服务 AWS WAF ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用 AWS WAF 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

AWS WAF 配额

> **Note**
>
> 这是的最新版本 AWS WAF。有关 AWS WAF 经典版的信息，请参阅AWS WAF 经典。

AWS WAF 受以下配额（以前称为限制）的约束。这些配额适用于所有可用区域。 AWS WAF 每个区域分别受这些限额的约束。限额不会跨区域累积。

AWS WAF 在每个账户可以拥有的最大实体数量上有默认配额。您可以请求提高这些限额。

资源	每个区域每个账户的默认限额
最大 Web ACL 数	100
最大规则组数	100
最大 IP 集数	100
每个 Web ACL 每秒的最大请求数	25000
每个 Web ACL 或规则组的最大自定义请求标头数	100
每个 Web ACL 或规则组的最大自定义响应标头数	100
每个 Web ACL 或规则组的最大自定义响应正文数	50
Web ACL 令牌域列表中令牌域的最大数量	10

允许的最大每秒请求数 (RPS) CloudFront 由 AWS WAF 《CloudFront 开发者指南》设置 CloudFront 和描述。

AWS WAF 每个地区的每个账户的以下实体设置都有固定的配额。无法更改这些限额。

资源	每区域每账户的限额
每个 Web ACL 的最大 Web ACL 容量单位 (WCU)*	5000
每个规则组的最大 WCU	5000
每个规则组的最大参考语句数。在规则组中，参考语句可以引用 IP 集或正则表达式模式集。	50
每个 Web ACL 的最大参考语句数。在 Web ACL 中，参考语句可以引用规则组、IP 集或正则表达式模式集。	50
每个 IP 集以 CIDR 表示法表示的 IP 地址 的最大数量	10000

资源	每区域每账户的限额
每个 Web ACL 基于速率的规则的最大数量	10
每个规则组基于速率的规则的最大数量	4
可为基于速率的规则定义的最小请求速率	100
每个基于速率的规则可以限制的唯一 IP 地址的最大数量	10000
字符串匹配语句中的最大字符数	200
每个正则表达式模式中的最大字符数	200
每个正则表达式集唯一正则表达式模式的最大数量	10
正则表达式集的最大数量	10
可以检查 Application Load Balancer AWS AppSync 和保护措施的 Web 请求正文的最大大小	8 KB
可以检查的 Web 请求正文的最大大小为 API Gateway CloudFront、Amazon Cognito、App Runner 和已验证访问保护**	64 KB
每条规则语句的最大文本转换次数	10
单个自定义响应定义的自定义响应正文内容的最大大小	4 KB
单个自定义响应定义的最大自定义标头数	10
单个自定义请求定义的最大自定义标头数	10
单个规则组或单个 Web ACL 的所有响应正文内容的最大组合大小	50 KB

* 在 Web ACL 中使用超过 1,500 个 WCU 所产生的成本超出了基本 Web ACL 的价格。有关更多信息，请参阅 AWS WAF 网络 ACL 容量单位 (WCU) 和 AWS WAF 定价。

**默认情况下，API Gateway、Amazon Cognito CloudFront、Amazon Cognito、App Runner 和已验证访问权限资源的身体检查限制设置为 16 KB，但您可以在 Web ACL 配置中将这些资源中的任何资源提高到列出的最大值。有关更多信息，请参阅 管理车身检查的大小限制。

AWS WAF 每个地区的每个账户有以下固定通话配额。这些限额适用于通过任何可用方式（包括控制台、CLI、 AWS CloudFormation、REST API 和开发工具包）对服务的总调用次数。无法更改这些限额。

调用类型	每区域每账户的限额
调用 AssociateWebACL 的最大次数	每 2 秒一个请求
调用 DisassociateWebACL 的最大次数	每 2 秒一个请求
调用 GetWebACLForResource 的最大次数	每秒一个请求
调用 ListResourcesForWebACL 的最大次数	每秒一个请求
对任何单个 Get 或 List 操作的最大调用次数（如果未为其定义其他限额）	每秒五个请求
对任何单个 Create、Put 或 Update 操作的最大调用次数（如果未为其定义其他限额）	每秒一个请求

将您的 AWS WAF 经典资源迁移到 AWS WAF

本节提供将您的规则和 Web ACL 从 AWS WAF 经典版迁移到经典版的 AWS WAF指南。 AWS WAF 已于 2019 年 11 月发布。如果您使用 Cl AWS WAF assic 创建了诸如规则和 Web ACL 之类的资源，则要么需要使用 Cl AWS WAF assic 来处理它们，要么将其迁移到最新版本。

在开始迁移工作之前，请 AWS WAF 通过通读来熟悉一下。AWS WAF

主题

- 为什么要迁移到 AWS WAF？
- 迁移的工作原理
- 迁移注意事项和限制
- 将 Web ACL 从 AWS WAF 经典版迁移到 AWS WAF

为什么要迁移到 AWS WAF？

与之前的版本相比，最新版本 AWS WAF 提供了许多改进，同时保留了您习惯的大部分概念和术语。

以下列表介绍 AWS WAF最新版本中的主要更改。在继续迁移之前，请花点时间查看此列表并熟悉指南的 AWS WAF 其余部分。

- AWS 的托管规则 AWS WAF-现在可通过 AWS 托管规则提供的规则组提供针对常见 Web 威胁的防护。这些规则组中的大多数都是免费包含的 AWS WAF。有关更多信息，请参阅AWS 托管规则规则组列表和博客文章宣布的 AWS 托管规则 AWS WAF。
- 新 AWS WAF API — 新 API 允许您使用一组 API 配置所有 AWS WAF 资源。为了区分区域和全球应用程序，新 API 包括一个 `scope` 设置。有关此 API 的更多信息，请参阅 AWS WAFV2 操作和 AWS WAFV2 数据类型。

  在 API、SDK、CLI 和 CI AWS WAF assic 中 AWS CloudFormation，Classic 保留了其命名方案，并根据上下文添加了V2或v2，引用了最新版本的。 AWS WAF
- 简化的服务配额（限制）— AWS WAF 现在允许每个 Web ACL 有更多规则，并允许您表达更长的正则表达式模式。有关更多信息，请参阅 AWS WAF 配额。
- Web ACL 限制现在基于计算需求 — Web ACL 限制现在基于 Web ACL 容量单位 (WCU)。 AWS WAF 根据运行规则所需的操作容量计算规则的 WCU。Web ACL 的 WCU 是 Web ACL 中所有规则和规则组的 WCU 总和。

  有关 WCU 的一般信息，请参阅 如何 AWS WAF 运作。有关每个规则的 WCU 使用情况的信息，请参阅 规则语句基础知识。
- 基于文档的规则编写 – 您现在可以采用 JSON 格式编写和表达规则、规则组和 Web ACL。您不再需要使用单独的 API 调用来创建不同的条件，然后将条件与规则相关联。这极大地简化了编写和维护代码的方式。在查看 Web ACL 时，您可以通过控制台访问 Web ACL 的 JSON 格式，方法是选择将 Web ACL 下载为 JSON。创建自己的规则时，可以通过选择 规则 JSON 编辑器 来访问其 JSON 表示形式。
- 规则嵌套和完全逻辑操作支持 – 您可以使用逻辑规则语句和使用嵌套来编写复杂的组合规则。您可以创建语句，如 `[A AND NOT(B OR C)]`。有关更多信息，请参阅 逻辑规则语句。
- 改进的基于速率的规则-在的最新版本中 AWS WAF，您可以自定义规则评估的时间窗口以及规则聚合请求的方式。您可以使用多个 Web 请求特征的组合来自定义聚合。此外，最新的基于费率的规则可以更快地对流量变化做出反应。有关更多信息，请参阅 基于速率的规则语句。
- 对于 IP 集的可变 CIDR 范围支持 – IP 设置规范现在对于 IP 范围具有更大的灵活性。对于 IPv4，则 AWS WAF 支持/1。/32对于 IPv6，/1则 AWS WAF 支持/128。有关 IP 集的更多信息，请参阅 IP 集匹配规则语句。

- 可链接的文本转换 — AWS WAF 可以在检查网络请求内容之前对其进行多次文本转换。有关更多信息，请参阅 文本转换选项。
- 改善了控制台体验 — 新的 AWS WAF 控制台具有可视化规则生成器和更直观的控制台设计。
- Fi@@ rewall Manager AWS WAF 策略的扩展选项-在 Firewall Manager 的 AWS WAF Web ACL 管理中，您现在可以创建一组先 AWS WAF 处理的规则组和一组最后 AWS WAF 处理的规则组。应用 AWS WAF 策略后，本地账户所有者可以添加自己的规则组，这些规则组在这两个规则组之间进行 AWS WAF 处理。有关 Firewall Manager AWS WAF 策略的更多信息，请参阅 AWS WAF 政策。
- AWS CloudFormation 支持所有规则语句类型 — AWS WAF 中 AWS CloudFormation 支持 AWS WAF 控制台和 API 支持的所有规则语句类型。此外，您可以轻松地将您以 JSON 格式编写的规则转换为 YAML 格式。

迁移的工作原理

自动迁移会继承您的大部分 AWS WAF 经典 Web ACL 配置，剩下一些需要手动处理的事情。

以下列出了迁移 Web ACL 的概要步骤。

1. 自动迁移会读取与现有 Web ACL 相关的所有内容，而无需在 Cl AWS WAF assic 中修改或删除任何内容。它创建 Web ACL 及其相关资源的表示形式，与兼容 AWS WAF。它为新的 Web ACL 生成一个 AWS CloudFormation 模板，并将其存储在 Amazon S3 存储桶中。
2. 您可以将模板部署到中 AWS CloudFormation，以便在中重新创建 Web ACL 和相关资源。 AWS WAF
3. 您可以查看 Web ACL 并手动完成迁移，同时确保您的新 Web ACL 充分利用最新 AWS WAF的功能。
4. 您可以手动将受保护的资源切换到新的 Web ACL。

迁移注意事项和限制

迁移并不会全然转入您在 AWS WAF Classic 中的所有设置。有些事物（如托管规则）不会在两个版本之间确切地映射。其他设置（如 Web ACL 与受保护 AWS 资源的关联）最初会在新版本中禁用，以便您可以在准备就绪后添加它们。

以下列表介绍迁移的注意事项，并说明您可能要采取的任何应对步骤。使用此概览来规划迁移。稍后的详细迁移步骤将指导您完成建议的迁移步骤。

- 单一账户-您只能将任何账户的 AWS WAF 经典资源迁移到同一账户的 AWS WAF 资源。
- 托管规则-迁移不会从 AWS Marketplace 卖家那里移交任何托管规则。有些 AWS Marketplace 卖家有同等的托管规则 AWS WAF ，您可以再次订阅。在执行此操作之前，请查看最新版本附带的 AWS 托管规则 AWS WAF。其中大多数对 AWS WAF 用户都是免费的。有关托管规则的信息，请参阅托管规则组。
- Web ACL 关联 – 迁移不会带入 Web ACL 和受保护资源之间的任何关联。这是设计使然，目的是避免影响生产工作负载。验证所有内容都已正确迁移后，请将新的 Web ACL 与您的资源关联。
- 日志记录 – 默认情况下，已迁移 Web ACL 的日志记录处于禁用状态。这是设计使然。准备好从 Classic 切换到 C AWS WAF lassic 时启用日志记录 AWS WAF。
- AWS Firewall Manager 规则组-迁移不处理由 Firewall Manager 管理的规则组。您可以迁移由 Firewall Manager 管理的 Web ACL，但迁移不会带入规则组。应在 Firewall Manager 中为新的 AWS WAF 创建策略，而不是为这些 Web ACL 使用迁移工具。

  > **Note**
  >
  > Firewall Manager 为 AWS WAF 经典版管理的规则组是 Firewall Manager 规则组。在新版本中 AWS WAF，规则组就是 AWS WAF 规则组。在功能上，它们是一样的。

- AWS WAF 安全自动化-不要尝试迁移任何AWS WAF 安全自动化。迁移不会转换自动化过程可能正在使用的 Lambda 函数。当有与最新版本兼容的新 AWS WAF 安全自动化解决方案可用时 AWS WAF，请重新部署该解决方案。

将 Web ACL 从 AWS WAF 经典版迁移到 AWS WAF

要迁移 Web ACL 并切换到它，请执行自动迁移，然后完成一系列手动步骤。

主题

- 迁移 Web ACL：自动迁移
- 迁移 Web ACL：手动后续操作
- 迁移 Web ACL：其他注意事项
- 迁移 Web ACL：切换

迁移 Web ACL：自动迁移

自动将 Web ACL 配置从 AWS WAF 经典版迁移到 AWS WAF

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 选择 “切换到 AWS WAF 经典版”，然后查看 Web ACL 的配置设置。记下这些设置，同时考虑到前一节迁移注意事项和限制中介绍的注意事项和限制。
3. 在顶部的信息对话框中，找到以迁移 Web ACL开头的句子，并选择迁移向导链接。这将启动迁移向导。

   如果您没有看到信息对话框，则可能是自启动 C AWS WAF lassic 主机以来已将其关闭。在导航栏中，选择 “切换到新建”， AWS WAF然后选择 “切换到 AWS WAF 经典”，信息对话框就会重新出现。
4. 选择要迁移的 Web ACL。
5. 对于迁移配置，提供要用于模板的 Amazon S3 存储桶。您需要为迁移 API 正确配置的 Amazon S3 存储桶来存储迁移 API 生成的 AWS CloudFormation 模板。

   - 如果存储桶已加密，则必须使用 Amazon S3 (SSE-S3) 密钥。迁移不支持使用 AWS Key Management Service (SSE-KMS) 密钥进行加密。
   - 存储桶名称必须以 `aws-waf-migration-` 开头。例如，`aws-waf-migration-my-web-acl`。
   - 存储桶必须位于您要部署此模板的区域中。例如，对于 `us-west-2` 中的 Web ACL，您必须使用 `us-west-2` 中的 Amazon S3 存储桶，并且必须将模板堆栈部署到 `us-west-2`。
6. 对于 S3 存储桶策略，我们建议选择 自动应用迁移所需的存储桶策略。或者，如果您想自行管理存储桶，则必须手动应用以下存储桶策略：

   - 对于全球 Amazon CloudFront 应用程序 (`waf`)：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
```

```
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

- 对于区域性 Amazon API Gateway 或应用程序负载均衡器应用程序 (`waf-regional`)：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. 在 选择如何处理无法迁移的规则 中，选择排除无法迁移的规则或选择停止迁移。有关无法迁移的规则的信息，请参阅迁移注意事项和限制。
8. 选择下一步。
9. 对于创建 AWS CloudFormation 模板，请验证您的设置，然后选择开始创建 AWS CloudFormation 模板以开始迁移过程。这可能需要几分钟时间，具体取决于 Web ACL 的复杂性。
10. 在 “创建并运行 AWS CloudFormation 堆栈以完成迁移” 中，您可以选择进入 AWS CloudFormation 控制台根据模板创建堆栈，创建新的 Web ACL 及其资源。为此，请选择创建 AWS CloudFormation 堆栈。

自动迁移过程完成后，您可以继续执行手动后续步骤。请参阅 迁移 Web ACL：手动后续操作。

迁移 Web ACL：手动后续操作

自动迁移完成后，请查看新创建的 Web ACL 并填入迁移过程未带入的组件。以下过程介绍迁移未处理的 Web ACL 管理的各个方面。有关列表，请参阅迁移注意事项和限制。

完成基本迁移 - 手动步骤

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 控制台应自动使用最新版本的 AWS WAF。要验证这一点，请在导航窗格中查看是否可以看到 “切换到 AWS WAF 经典版” 选项。如果您看到 “切换到新版本” AWS WAF，请选择该选项以切换到最新版本。
3. 在导航窗格中，选择 Web ACL。
4. 在 Web ACL 页面中，在创建新 Web ACL 的区域的列表中找到新的 Web ACL。选择 Web ACL 的名称以显示 Web ACL 的设置。
5. 对照之前的 AWS WAF 经典 Web ACL，查看新 Web ACL 的所有设置。默认情况下，日志记录和受保护的资源关联处于禁用状态。您可以在准备好进行切换时启用这些功能。
6. 如果您的 AWS WAF Classic Web ACL 具有带条件的基于速率的规则，则迁移中不会引入该条件。您可以在新的 Web ACL 中向规则添加条件。

   a. 在 Web ACL 设置页面中，选择 规则 选项卡。

   b. 在列表中找到基于费率的规则，选择该规则，然后选择 编辑。

   c. 对于 将请求计入费率限制的标准，选择 仅考虑与规则语句中的标准匹配的请求，然后提供附加标准。您可以使用任何可嵌套的规则语句（包括逻辑语句）添加标准。有关选择的信息，请参阅基于速率的规则语句。
7. 如果您的 AWS WAF 经典 Web ACL 具有托管规则组，则迁移中不会包含该规则组。您可以将托管规则组添加到新的 Web ACL 中。查看有关托管规则组的信息，包括新版本中可用的 AWS 托管规则列表 AWS WAF，网址为托管规则组。要添加托管规则组，请执行以下操作：

   a. 在 Web ACL 设置页面中，选择 Web ACL 规则 选项卡。

   b. 选择 添加规则，然后选择 添加托管规则组。

   c. 展开您选择的供应商的列表，然后选择要添加的规则组。对于 AWS Marketplace 卖家，您可能需要订阅规则组。有关在 Web ACL 中使用托管规则组的更多信息，请参阅托管规则组和 Web ACL 规则和规则组评估。

完成基本迁移过程后，我们建议您查看您的需求并考虑其他选项，以确保新配置尽可能高效并使用最新的可用安全选项。请参阅 迁移 Web ACL：其他注意事项。

迁移 Web ACL：其他注意事项

查看您的新 Web ACL 并考虑新 AWS WAF 的 Web ACL 中可用的选项，以确保配置尽可能高效，并且使用的是最新的可用安全选项。

其他 AWS 托管规则

考虑在 Web ACL 中实施其他 AWS 托管规则，以提高应用程序的安全状况。这些都包含 AWS WAF 在内，不收取额外费用。 AWS 托管规则具有以下类型的规则组：

- 基准规则组针对各种常见威胁提供了一般保护，例如阻止已知错误输入进入应用程序并防止访问管理页面。
- 使用案例特定的规则组为许多不同的使用案例和环境提供增量保护。
- IP 声誉列表基于客户端的源 IP 提供威胁情报。

有关更多信息，请参阅 AWS 的托管规则 AWS WAF。

规则优化和清理

重新访问旧规则，并考虑通过重写它们或删除过时的规则来优化它们。例如，如果您过去部署了技术论文《OWASP 十大 Web 应用程序漏洞》、《为 OWASP 十大 Web 应用程序漏洞使用做好准备》AWS WAF 和《我们的新白皮书》中的 AWS CloudFormation 模板，则应考虑将其替换为托管规则。AWS 虽然文档中的概念仍然适用，可以帮助您编写自己的规则，但模板创建的规则在很大程度上已被 AWS 托管规则所取代。

Amazon CloudWatch 指标和警报

重新访问您的 Amazon CloudWatch 指标并根据需要设置警报。迁移不会延续CloudWatch 警报，而且您的指标名称可能不是您想要的。

与您的应用程序团队一起审核

与您的应用程序团队合作并检查安全状况。找出应用程序经常解析哪些字段，并添加规则以相应地清理输入。如果应用程序的业务逻辑无法处理边缘案例，请检查是否存在任何边缘案例，并添加规则以捕获这些案例。

规划切换

与您的应用程序团队一起规划切换的时间。从旧的 Web ACL 关联切换到新的 Web ACL 关联可能需要很少的时间才能传播到存储资源的所有区域。传播时间可以从几秒钟到几分钟不等。在此期间，有些请求将由旧的 Web ACL 处理，而其他请求将由新的 Web ACL 处理。在整个交换过程中，您的资源都将受到保护，但是您可能会注意到在切换进行期间请求处理存在不一致之处。

准备好切换时，请按照迁移 Web ACL：切换中的步骤操作。

迁移 Web ACL：切换

验证新的 Web ACL 设置后，可以开始使用它来代替 AWS WAF Classic Web ACL。

开始使用您的新 AWS WAF Web ACL

1. 按照中的指导，将 AWS WAF Web ACL 与要保护的资源相关联将 Web ACL 与资源关联或取消关联 AWS。这会自动断开资源与旧 Web ACL 的关联。

   切换可能需要几秒到几分钟的传播时间。在此期间，一些请求可能会由旧的 Web ACL 处理，而另一些则由新的 Web ACL 处理。在整个交换过程中，您的资源都将受到保护，但是在请求处理完成之前，您可能会注意到请求处理存在不一致之处。
2. 按照记录 AWS WAF Web ACL 流量中的指导为新的 Web ACL 配置日志记录。
3. （可选）如果您的 AWS WAF 经典 Web ACL 不再与任何资源关联，请考虑将其完全从 AWS WAF Classic 中删除。有关信息，请参阅删除 Web ACL。

AWS WAF 经典

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF Classic 是一款 Web 应用程序防火墙，允许您监控转发到 Amazon API Gateway API、亚马逊 CloudFront 或应用程序负载均衡器的 HTTP 和 HTTPS 请求。 AWS WAF Classic 还允许您控制对内容的访问权限。根据您指定的条件，例如请求来源的 IP 地址或查询字符串的值，API Gateway 或 Application Load Balancer 使用请求的内容或 HTTP 403 状态代码（禁止）来响应请求。 CloudFront 您还可以配置 CloudFront 为在请求被阻止时返回自定义错误页面。

主题

设置 AWS WAF 经典版

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

本主题介绍准备使用 C AWS WAF lassic 的初步步骤，例如创建用户帐户。您无需为这些付费。您只需为所使用的 AWS 服务付费。

> **Note**
>
> 如果您是新用户，请不要按照 C AWS WAF lassic 的这些设置步骤进行操作。 AWS WAF相反，请按照最新版本的步骤操作 AWS WAF，网址为设置您的账户以使用服务。

完成这些步骤后，请参阅，AWS WAF 经典版入门继续开始使用 AWS WAF Classic。

> **Note**
>
> AWS Shield Standard 包含在 AWS WAF Classic 中，不需要额外设置。有关更多信息，请参阅 AWS Shield 和 Shield Advanced 的工作原。

在您首次使用 AWS WAF Classic 或 AWS Shield Advanced 首次使用之前，请完成本节中的步骤。

主题

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户
- 下载工具

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

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

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。
2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

下载工具

AWS Management Console 包括 C AWS WAF lassic 的主机，但如果您想以编程方式访问 AWS WAF Classic，请参阅以下内容：

- 如果您想调用 AWS WAF Classic API 而不必处理诸如组装原始 HTTP 请求之类的低级细节，则可以使用 S AWS DK。 AWS 软件开发工具包提供的函数和数据类型封装了 C AWS WAF lassic 和其他服务的功能。 AWS 要下载 S AWS DK，请参阅相应页面，其中还包括先决条件和安装说明：
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  有关软件开发工具 AWS 包的完整列表，请参阅 Amazon Web Services 工具。
- 如果您使用的编程语言 AWS 不提供 SDK，则 AWS WAF API 参考将记录 C AWS WAF lassic 支持的操作。

- AWS Command Line Interface (AWS CLI) 支持 AWS WAF 经典版。 AWS CLI 允许您从命令行控制多项 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。
- AWS Tools for Windows PowerShell 支持 AWS WAF 经典。有关更多信息，请参阅 AWS Tools for PowerShell Cmdlet 参考。

AWS WAF 经典版的工作原理

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

您可以使用 AWS WAF Classic 来控制 API Gateway、Amazon CloudFront 或 Application Load Balancer 如何响应网络请求。您首先需创建条件、规则和 Web 访问控制列表 (Web ACL)。您需要定义条件、将条件合并为规则并将规则合并为 Web ACL。

> **Note**
>
> 您还可以使用 AWS WAF Classic 来保护托管在亚马逊弹性容器服务 (Amazon ECS) 容器中的应用程序。Amazon ECS 是一项高度可扩展的快速容器管理服务，它可轻松运行、停止和管理集群上的 Docker 容器。要使用此选项，您可以将 Amazon ECS 配置为使用支持 AWS WAF 经典版的应用程序负载均衡器来路由和保护服务中任务之间的 HTTP/HTTPS（第 7 层）流量。有关更多信息，请参阅 Amazon Elastic Container Service 开发人员指南中的服务负载均衡。

Conditions

条件定义您希望 AWS WAF Classic 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

您可以将条件组合成规则，以精确定位您想要允许、阻止或计数的请求。 AWS WAF Classic 提供两种类型的规则：

常规规则

常规规则仅使用条件来锁定特定请求。例如，根据您发现的来自某个攻击者的最近请求，您可以创建一个规则，其中包含以下条件：

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

当一个规则中包括多个条件时，如本例所示， AWS WAF Classic 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。

将至少一个条件添加到常规规则。没有条件的常规规则无法匹配任何请求，因此永远不会触发规则的操作（允许、计数或阻止）。

基于速率的规则

基于速率的规则就像常规规则一样，具有额外的速率限制。基于速率的规则计算从满足规则条件的 IP 地址到达的请求。如果来自 IP 地址的请求在五分钟内超过速率限制，则该规则可能会触发操作。触发操作可能需要一两分钟的时间。

对于基于速率的规则而言，条件是可选的。如果未在基于速率的规则中添加任何条件，则速率限制适用于所有 IP 地址。如果将条件与速率限制组合在一起，则速率限制适用于与条件匹配的 IP 地址。

例如，基于您发现的来自某个攻击者的最近请求，您可以创建一个基于速率的规则，包含如下条件：

- 请求来自 192.0.2.44。
- 请求在 `User-Agent` 标头中包含值 `BadBot`。

在此基于速率的规则中，您还定义了一个速率限制。在本例中，假设您创建了速率限制 1000。当请求既符合上述两个条件又超过每 5 分钟 1000 个请求的速率限制时，将触发在 Web ACL 中定义的该规则的操作（阻止或计数）。

不符合这两个条件的请求不计入速率限制，也不受此规则的影响。

又如，假设您希望将请求限定为网站上特定页面的请求。为此，您可以向基于速率的规则中添加以下字符串匹配条件：

- Part of the request to filter on 是 `URI`。
- 匹配类型 是 `Starts with`。
- Value to match 是 `login`。

还要将 `RateLimit` 指定为 1000。

通过向 Web ACL 中添加此基于速率的规则，您可以将请求限制在登录页面，而不影响网站其余部分。

Web ACL

在您将条件合并为规则之后，您可将规则合并为 Web ACL。在其中可定义每个规则的操作允许、阻止或计数和默认操作：

每个规则的操作

当网络请求符合规则中的所有条件时，CI AWS WAF assic 可以阻止该请求，也可以允许将请求转发到 API Gateway API、 CloudFront 分发版或应用程序负载均衡器。您可以为每条规则指定希望 AWS WAF Classic 执行的操作。

AWS WAF Classic 按照您列出的规则顺序将请求与 Web ACL 中的规则进行比较。 AWS WAF 然后，Classic 会执行与请求匹配的第一条规则关联的操作。例如，如果一个 Web 请求与一条允许请求的规则和另一条阻止请求的规则相匹配，则 CI AWS WAF assic 将根据首先列出的规则来允许或阻止该请求。

如果您想在开始使用新规则之前对其进行测试，也可以将 C AWS WAF lassic 配置为计算满足该规则中所有条件的请求数。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 Classic 是允许还是阻止不符合 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。

如果请求不满足规则中的所有三个条件，并且默认操作为`ALLOW`，则 C AWS WAF lassic 会将请求转发到 API Gateway CloudFront 或 Application Load Balancer，然后服务使用请求的对象进行响应。

如果您向 Web ACL 添加两个或更多规则，则 AWS WAF Classic 仅在请求不满足任何规则中的所有条件时才会执行默认操作。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。

AWS WAF 只有当请求不满足第一条规则中的所有三个条件且不满足第二条规则中的一个条件时，Classic 才会执行默认操作。

在某些情况下， AWS WAF 可能会遇到内部错误，从而延迟对 Amazon API Gateway、Amazon CloudFront 或应用程序负载均衡器关于允许还是阻止请求的响应。在这些情况下，通常 CloudFront 会允许请求或提供内容。API 网关和 Application Load Balancer 通常会拒绝请求，不提供内容。

AWS WAF 经典定价

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

使用 AWS WAF Classic，您只需为自己创建的 Web ACL 和规则以及 CI AWS WAF assic 检查的 HTTP 请求数量付费。有关更多信息，请参阅 AWS WAF Classic 定价。

AWS WAF 经典版入门

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

本教程介绍如何使用 AWS WAF Classic 执行以下任务：

- 设置 AWS WAF 经典版。
- 使用 AWS WAF 经典版控制台创建 Web 访问控制列表 (Web ACL)，并指定要用于筛选 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 请求必须符合规则中的所有条件， AWS WAF Classic 才会根据您指定的条件阻止或允许请求。
- 向 Web ACL 中添加规则。可以在其中指定基于添加到每个规则的条件阻止还是允许 Web 请求。
- 指定默认操作 (阻止或允许)。这是 AWS WAF Classic 在网络请求与您的任何规则都不匹配时采取的操作。
- 选择您希望 C AWS WAF lassic 检查其网络请求的 Amazon CloudFront 配送。本教程仅涵盖的步骤 CloudFront，但应用程序负载均衡器和 Amazon API Gateway API API 的流程基本相同。 AWS WAF Class CloudFront ic for 适用于所有人 AWS 区域。 AWS WAF 与 API Gateway 或 Application Load Balancer 配合使用的 Classic 在AWS 服务终端节点列出的区域中可用。

> **Note**
>
> AWS 对于您在本教程中创建的资源，每天向您收取的费用通常少于 0.25 美元。当您完成本教程时，建议您删除资源以避免产生不必要的费用。

主题

步骤 1：设置 AWS WAF 经典版

如果您尚未按照 设置 AWS WAF 经典版 中的常规设置步骤操作，请立即执行操作。

步骤 2：创建 Web ACL

AWS WAF Classic 控制台将引导您完成将 CI AWS WAF assic 配置为根据您指定的条件（例如请求来源的 IP 地址或请求中的值）阻止或允许 Web 请求的过程。在此步骤中，您将创建一个 Web ACL。

创建 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 如果这是您第一次使用 AWS WAF 经典版，请选择转到 AWS WAF 经典版，然后选择配置 Web ACL。

   如果您以前使用过 AWS WAF 经典版，请在导航窗格中选择 Web AC L，然后选择创建 Web ACL。

3. 在 Name web ACL (命名 web ACL) 页面上，对于 Web ACL name (Web ACL 名称)，输入一个名称。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

4. 对于 CloudWatch metric name (&CW; 指标名称)，输入一个名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9)，且不能包含空格。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

5. 对于 区域（亚马逊云科技区域），选择一个区域。如果要将此 Web ACL 与 CloudFront 分配相关联，请选择全局 (CloudFront)。
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。

创建 IP 匹配条件

1. 在 创建条件 页面上，对于 IP 匹配条件，选择 创建条件。
2. 在 创建 IP 匹配条件 对话框中，对于 名称，输入一个名称。该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。
3. 对于 地址，输入 192.0.2.0/24。此 IP 地址范围 (采用 CIDR 表示法指定) 包含从 192.0.2.0 到 192.0.2.255 的 IP 地址。(192.0.2.0/24 IP 地址范围保留供示例使用，因此不会有 Web 请求源自这些 IP 地址。)

   AWS WAF Classic 支持 IPv4 地址范围：/8 以及介于 /16 到 /32 之间的任何范围。 AWS WAF Classic 支持 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。（要指定一个 IP 地址，如 192.0.2.44，请输入 192.0.2.44/32。）不支持其他范围。

   有关 CIDR 表示法的更多信息，请参阅维基百科条目 Classless Inter-Domain Routing。
4. 选择 创建。

步骤 4：创建地理匹配条件

地理匹配条件指定请求源自的一个或多个国家/地区。在此步骤中，您将创建一个地理匹配条件。在后面的步骤中，您会指定是允许还是阻止源自指定国家/地区的请求。

> **Note**
>
> 有关地理匹配条件的更多信息，请参阅使用地理匹配条件。

创建地理匹配条件

1. 在 创建条件 页面上，对于 Geo match conditions，选择 创建条件。
2. 在 创建地理匹配条件 对话框中，对于 名称，输入一个名称。该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。
3. 选择位置类型和国家/地区。目前，位置类型 只能是 国家/地区。
4. 选择 添加位置。
5. 选择 创建。

步骤 5：创建字符串匹配条件

字符串匹配条件用于标识您希望 AWS WAF Classic 在请求中搜索的字符串，例如标头或查询字符串中的指定值。字符串通常由可打印 ASCII 字符组成，但您可以指定从十六进制 0x00 到 0xFF (十进制 0 到 255) 的任何字符。在此步骤中，您将创建一个字符串匹配条件。在后面的步骤中，您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。

创建字符串匹配条件

1. 在 创建条件 页面上，对于 字符串和正则表达式匹配条件，选择 创建条件。
2. 在 创建字符串匹配条件 对话框中，输入下列值：

名称

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

Type

选择 String match。

Part of the request to filter on

选择您希望 C AWS WAF lassic 检查指定字符串的 Web 请求部分。

对于此示例，选择 标头。

> **Note**
>
> 如果您选择正文作为要筛选的请求部分的值，C AWS WAF lassic 将仅检查前 8192 字节 (8 KB)，因为仅 CloudFront 转发前 8192 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 Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

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

由于您为要筛选的部分请求选择了标头，因此必须指定希望 C AWS WAF lassic 检查哪个标头。输入 User-Agent (用户代理)。（此值不区分大小写。）

Match type

选择指定字符串必须出现在 User-Agent 标头中的何处，例如，字符串开头、末尾还是其他什么地方。

在此示例中，选择 “完全匹配”，这表示 AWS WAF Classic 会检查 Web 请求中是否存在与您指定的值相同的标头值。

Transformation

为了绕过 AWS WAF Classic，攻击者在网络请求中使用不寻常的格式，例如，通过添加空格或对部分或全部请求进行网址编码。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 要匹配的值 中输入的值已进行了 base64 编码时，选中此复选框。

对于此示例，不要选中此复选框。

Value to match

指定您希望 AWS WAF Classic 在 Web 请求的部分中搜索的值，这些请求是您在请求的一部分中筛选的。

对于此示例，请输入BadBot。 AWS WAF Classic 将检查 Web 请求中的`User-Agent`标头以获取该值BadBot。

Value to match 的最大长度是 50 个字符。如果您要指定 base64 编码值，您可以提供最多 50 个字符（编码前）。

3. 如果您希望 AWS WAF Classic 检查网络请求中是否有多个值，例如包含的`User-Agent`标头`BadBot`和包含的查询字符串`BadParameter`，则有两种选择：

   - 如果您希望仅当 Web 请求同时包含两个值 (AND) 时才允许或阻止请求，则为每个值创建一个字符串匹配条件。
   - 如果您希望在 Web 请求包含任意一个值或同时包含两个值 (OR) 时允许或阻止请求，则将两个值添加到同一个字符串匹配条件。

   对于此示例，选择 Create。

步骤 5A：创建正则表达式条件（可选）

正则表达式条件是一种字符串匹配条件，其类似之处在于它标识您希望 AWS WAF Classic 在请求中搜索的字符串，例如标头或查询字符串中的指定值。主要区别在于，您使用正则表达式 (regex) 来指定希望 C AWS WAF lassic 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。

创建正则表达式匹配条件

1. 在 创建条件 页面上，对于 字符串匹配和正则表达式条件，选择 创建条件。
2. 在 创建字符串匹配条件 对话框中，输入下列值：

名称

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

Type

选择 RegEx 匹配。

Part of the request to filter on

选择您希望 C AWS WAF lassic 检查指定字符串的 Web 请求部分。

对于此示例，选择 Body。

> **Note**
>
> 如果您选择正文作为要筛选的请求部分的值，C AWS WAF lassic 将仅检查前 8192 字节 (8 KB)，因为仅 CloudFront 转发前 8192 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 Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

Transformation

为了绕过 AWS WAF Classic，攻击者在网络请求中使用不寻常的格式，例如，通过添加空格或对部分或全部请求进行网址编码。转换会通过删除空格、通过对请求进行 URL 解码或是通过执行可消除攻击者常用的许多不寻常格式的其他操作，将 Web 请求转换为更标准的格式。

您只能指定一个类型的文本转换。

对于此示例，选择 None。

与请求匹配的正则表达式模式

选择 Create regex pattern set。

新模式集名称

输入名称，然后指定您希望 CI AWS WAF assic 搜索的正则表达式模式。

接下来，输入正则表达式 I [a@] maB [a@] dRequest。 AWS WAF Classic 将检查 Web 请求中的`User-Agent`标头中的值：

- iAMA BadRequest
- IamAB@dRequest
- 我 @mA BadRequest
- I@mAB@dRequest

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

步骤 6：创建 SQL 注入匹配条件

SQL 注入匹配条件用于标识您希望 C AWS WAF lassic 检查的部分 Web 请求中是否存在恶意 SQL 代码，例如标头或查询字符串。攻击者使用 SQL 查询从数据库中提取数据。在此步骤中，您将创建一个 SQL 注入匹配条件。在后面的步骤中，您会指定是允许还是阻止表现为包含恶意 SQL 代码的请求。

> **Note**
>
> 有关字符串匹配条件的更多信息，请参阅使用 SQL 注入匹配条件。

创建 SQL 注入匹配条件

1. 在 Create conditions 页面上，对于 SQL 注入匹配条件，选择 Create condition。
2. 在 创建 SQL 注入匹配条件 对话框中，输入下列值：

名称

输入名称。

Part of the request to filter on

选择您希望 C AWS WAF lassic 检查恶意 SQL 代码的 Web 请求部分。

对于此示例，选择 Query string。

> **Note**
>
> 如果您选择正文作为要筛选的请求部分的值，C AWS WAF lassic 将仅检查前 8192 字节 (8 KB)，因为仅 CloudFront 转发前 8192 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 Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

Transformation

对于此示例，选择 URL decode。

攻击者使用不寻常的格式，例如 URL 编码，试图绕过 AWS WAF Classic。URL decode (URL 解码) 选项可在 AWS WAF Classic 检查 Web 请求之前消除请求中的一些这类格式。

您只能指定一个类型的文本转换。

3. 选择 创建。
4. 选择下一步。

步骤 7：（可选）创建其他条件

AWS WAF Classic 包括其他条件，包括：

- 大小限制条件-标识您希望 C AWS WAF lassic 检查长度的 Web 请求部分，例如标题或查询字符串。有关更多信息，请参阅 使用大小约束条件。
- 跨站点脚本匹配条件-标识要 AWS WAF 检查恶意脚本的 Web 请求部分，例如标题或查询字符串。有关更多信息，请参阅 使用跨站点脚本匹配条件。

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。

步骤 8：创建规则并添加条件

您可以创建一条规则来指定您希望 AWS WAF Classic 在 Web 请求中搜索的条件。如果您向规则添加多个条件，则 Web 请求必须匹配规则中的所有条件，CI AWS WAF assic 才能根据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。

创建规则并添加条件

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

   名称

   输入名称。

   CloudWatch 指标名称

   输入 C AWS WAF lassic 将创建并与规则关联的 CloudWatch 指标的名称。该名称只能包含字母数字字符 (A-Z、a-z、0-9)，且不能包含空格。

   Rule type

   选择 常规规则 或 基于速率的规则。基于速率的规则与常规规则基本相同，但还考虑到任何五分钟时段来自标识的 IP 地址的请求数。有关这些规则类型的更多信息，请参阅 AWS WAF 经典版的工作原理。对于此示例，请选择 `Regular rule`。

   速率限制

   对于基于速率的规则，请输入与规则条件匹配的 IP 地址在任何五分钟内允许的最大请求数。
3. 对于要添加到规则的第一个条件，指定以下设置：

   - 根据网络请求是否符合条件中的设置，选择您希望 Cl AWS WAF assic 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 添加条件。

5. 添加您之前创建的地理匹配条件。指定以下值：
   - When a request does
   - originate from a geographic location in
   - 选择您的地理匹配条件。
6. 选择添加另一个条件。
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 添加条件。
9. 添加您之前创建的 SQL 注入匹配条件。指定以下值：
   - When a request does
   - match at least one of the filters in the SQL injection match condition
   - 选择您的 SQL 注入匹配条件。
10. 选择 添加条件。
11. 添加您之前创建的大小约束条件。指定以下值：
    - When a request does
    - match at least one of the filters in the size constraint condition
    - 选择您的大小约束条件。
12. 如果您创建了任何其他条件 (如正则表达式条件)，以类似方式添加这些条件。
13. 选择 创建。
14. 对于 Default action，选择 Allow all requests that don't match any rules。
15. 选择 检查并创建。

步骤 9：将规则添加 Web ACL

向 Web ACL 中添加规则时，您可指定以下设置：

- 您希望 AWS WAF Classic 对符合规则中所有条件的 Web 请求执行的操作：允许、阻止或计算请求。

- Web ACL 的默认操作。这是您希望 AWS WAF Classic 对不符合规则中所有条件的 Web 请求采取的操作：允许或阻止请求。

AWS WAF Classic 开始屏蔽符合以下所有条件（以及您可能已添加的任何其他条件）的 CloudFront Web 请求：

- `User-Agent` 标头的值是 `BadBot`
- (如果您创建并添加了正则表达式条件) `Body` 的值是四个字符串中与模式 `I[a@]mAB[a@]dRequest` 匹配的任一个字符串
- 请求源自 192.0.2.0-192.0.2.255 范围中的 IP 地址
- 请求源自您在地理匹配条件中所选的国家/地区
- 请求表现为在查询字符串中包含恶意 SQL 代码

AWS WAF Classic CloudFront 允许响应任何不符合这三个条件的请求。

步骤 10：清除资源

现在您已成功完成了教程。为了防止您的账户产生额外的 AWS WAF 经典版费用，您应该清理您创建的 AWS WAF 经典版对象。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**
>
> AWS 对于您在本教程中创建的资源，每天向您收取的费用通常少于 0.25 美元。完成后，建议您删除资源以防止产生不必要的费用。

删除 C AWS WAF lassic 收费的对象

1. 取消您的 Web ACL 与您的 CloudFront 分配的关联：

   a. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

      如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。

   b. 选择要删除的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。

c. 在右窗格中，在规则选项卡上，转到使用此 Web ACL 的AWS 资源部分。对于与 Web ACL 关联的 CloudFront 分发，请在 “类型” 列中选择 x。

2. 从规则中删除条件：

   a. 在导航窗格中，选择 规则。
   b. 选择在教程中创建的规则。
   c. 选择 Edit rule。
   d. 选择每个条件标题右侧的 x。
   e. 选择更新。

3. 从 Web ACL 中删除规则，然后删除 Web ACL：

   a. 在导航窗格中，选择 Web ACL。
   b. 选择在教程中创建的 Web ACL 名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
   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 规则。
   b. 选择在教程中创建的规则。
   c. 选择 Delete （删除)。
   d. 在 Delete 对话框中，再次选择 Delete 以确认。

AWS WAF Classic 不对条件收费，但如果您想完成清理，请执行以下步骤从条件中移除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 经典版控制台的导航窗格中，选择 IP 地址。
   b. 选择在教程中创建的 IP 匹配条件。
   c. 选中您添加的 IP 地址范围的复选框。
   d. 选择 Delete IP address or range。

e. 在 IP match conditions 窗格中，选择 Delete。

f. 在 Delete 对话框中，再次选择 Delete 以确认。

2. 删除 SQL 注入匹配条件中的筛选条件，然后删除 SQL 注入匹配条件：

a. 在导航窗格中，选择 SQL 注入。

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 删除筛选器。

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 删除筛选器。

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 删除筛选器。

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 删除筛选器。

e. 在 Size constraint conditions 窗格中，选择 Delete。

f. 在 Delete 对话框中，再次选择 Delete 以确认。

创建和配置 Web 访问控制列表 (Web ACL)

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

通过网络访问控制列表 (Web ACL)，您可以精细控制您的 Amazon API Gateway API、亚马逊 CloudFront 分发或应用程序负载均衡器响应的网络请求。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。
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。
   - 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。

- 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。
- 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。
- 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。
- 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。
- 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。

3. 将条件添加到一个或多个规则。如果您向同一规则添加多个条件，则 Web 请求必须符合所有条件，CI AWS WAF assic 才能根据该规则允许或阻止请求。有关更多信息，请参阅 使用规则。（可选）您可以使用基于速率的规则而不是常规规则来限制来自满足条件的任何 IP 地址的请求数。
4. 将规则添加到 Web ACL。对于每条规则，指定您希望 AWS WAF Classic 根据您添加到规则中的条件允许还是阻止请求。如果您向 Web ACL 添加多个规则，则 CI AWS WAF assic 会按照规则在 Web ACL 中列出的顺序对这些规则进行评估。有关更多信息，请参阅 使用 Web ACL。

   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

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。

主题

使用跨站点脚本匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

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脚本匹配条件来识别希望 C AWS WAF lassic 检查可能存在恶意脚本的 Web 请求部分，例如 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
- 创建或编辑跨站点脚本匹配条件时指定的值
- 在跨站点脚本匹配条件中添加和删除筛选条件
- 删除跨站点脚本匹配条件

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。过滤器表示您希望 C AWS WAF lassic 检查哪一部分 Web 请求中是否存在恶意脚本，例如 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。以下是每种配置如何影响 AWS WAF 经典行为：

- 每个跨站脚本匹配条件不止一个过滤器（推荐）— 当您将包含多个过滤器的跨站脚本匹配条件添加到规则并将该规则添加到 Web ACL 时，Web 请求必须仅匹配跨站脚本匹配条件中的一个过滤器，Cl AWS WAF assic 才能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。一个过滤器指示 AWS WAF Classic 检查 URI 中是否存在恶意脚本，另一个过滤器指示 AWS WAF Classic 检查查询字符串。 AWS WAF 如果请求在 URI 或查询字符串中似乎包含恶意脚本，Classic 会允许或阻止这些请求。
- 每个跨站脚本匹配条件一个过滤器 — 当您将单独的跨站脚本匹配条件添加到规则并将该规则添加到 Web ACL 时，Web 请求必须匹配所有条件，Cl AWS WAF assic 才能根据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。当您将两个条件添加到同一个规则并将该规则添加到 Web ACL 时，仅当 URI 和查询字符串都显示包含恶意脚本时，C AWS WAF lassic 才允许或阻止请求。

> **Note**
>
> 向规则添加跨站脚本匹配条件时，还可以将 CI AWS WAF assic 配置为允许或阻止看似不包含恶意脚本的 Web 请求。

创建跨站点脚本匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Cross-site scripting。
3. 选择 创建条件。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 创建或编辑跨站点脚本匹配条件时指定的值。
5. 选择 再添加一个筛选条件。
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

选择每个 Web 请求中您希望 AWS WAF Classic 检查恶意脚本的部分：

标题

指定的请求标头，例如 `User-Agent` 或 `Referer` 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：DELETE、GET、HEAD、OPTIONS、PATCH、POST、和PUT。

查询字符串

URL 中在 ？字符之后出现的部分 (如果有)。

> **Note**
>
> 对于跨站点脚本匹配条件，我们建议您为要作为筛选条件的请求部分选择所有查询参数（仅限值），而不是查询字符串。

URI

请求的 URI 路径，用于标识资源，例如 /images/daily-ad.jpg。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

除非指定了转换，否则不会对 URI 进行标准化，而是像在请求中从客户端 AWS 收到的那样对其进行检查。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**
>
> 如果选择正文作为要作为筛选条件的请求部分 的值，则 AWS WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。（AWS WAF Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

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，如果网址是 “www.xyz.com？UserName=abc& SalesRegion =seattle”，则可以向或参数添加过滤器。UserNameSalesRegion

如果您选择 单一查询参数（仅限值），您还将指定 查询参数名称。这是您要检查的查询字符串中的参数，例如UserName或SalesRegion。查询参数名称 的最大长度为 30 个字符。查询参数名称 不区分大小写。例如，如果您指定UserName为查询参数名称，它将匹配的所有变体UserName，例如用户名和用户名。

所有查询参数（仅限值）

与单一查询参数（仅限值）类似，但C AWS WAF lassic不会检查单个参数的值，而是检查查询字符串中的所有参数值中是否存在可能的恶意脚本。例如，如果网址为 “www.xyz.com？UserName=abc& SalesRegion =seattle”，并且您选择了所有查询参数（仅限值），则如果值为或包含可能的恶意脚本，C AWS WAF lassic 将触发匹配。UserNameSalesRegion

标题

如果您为要筛选的部分请求选择了标头，请从常用标头列表中选择标头，或者输入希望 C AWS WAF lassic 检查是否存在恶意脚本的标头的名称。

Transformation

在 C AWS WAF lassic 检查请求之前，转换会重新格式化 Web 请求。这消除了攻击者为了绕过 C AWS WAF lassic 而在 Web 请求中使用的一些不寻常的格式。

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 Valu e 中的字符串是否匹配之前，Classic 不会对 Web 请求执行任何文本转换。

转换为小写形式

AWS WAF 经典版将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF Classic 用未编码的字符替换 HTML 编码的字符：

- 将 " 替换为 &
- 将   替换为不间断空格
- 将 < 替换为 <
- 将 > 替换为 >
- 将以十六进制格式表示的字符 &#xhhhh; 替换为对应字符

- 将以十进制格式表示的字符 &#nnnn; 替换为对应字符

规范化空格

AWS WAF Classic 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。
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 添加筛选条件。
   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。
   c. 选择 添加。
5. 要删除筛选条件，请执行以下步骤：
   a. 选择要删除的筛选条件。
   b. 选择 删除筛选器。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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 关联的规则 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，选择规则。
   b. 选择使用要删除的跨站点脚本匹配条件的规则的名称。
   c. 在右窗格中，选择要从规则中删除的跨站点脚本匹配条件，然后选择 Remove selected condition。
   d. 对使用要删除的跨站点脚本匹配条件的所有其余规则重复步骤 b 和 c。

e. 在导航窗格中，选择 Cross-site scripting。

f. 在 Cross-site scripting match conditions 窗格中，选择要删除的跨站点脚本匹配条件。

6. 选择 删除 删除所选条件。

使用 IP 匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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
- 编辑 IP 匹配条件
- 删除 IP 匹配条件

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**
>
> 向规则添加 IP 匹配条件时，还可以将 AWS WAF Classic 配置为允许或阻止不是来自您在条件中指定的 IP 地址的 Web 请求。

创建 IP 匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 IP 地址。
3. 选择 创建条件。
4. 在 名称 字段中输入名称。

   该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。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 0:0:0:0:0:ffff:c000:22c，请键入 0:0:0:0:0:ffff:c000:22c/128。
   - 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请键入 192.0.2.0/24。
   - 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。

   AWS WAF Classic 支持 IPv4 地址范围：/8 以及介于 /16 到 /32 之间的任何范围。 AWS WAF Classic 支持 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。有关 CIDR 表示法的更多信息，请参阅维基百科条目无类别域间路由。
6. 选择 Add another IP address or range。
7. 如果要添加其他 IP 地址或范围，请重复步骤 5 和 6。
8. 添加完值后，选择 Create IP match condition。

编辑 IP 匹配条件

您可以将 IP 地址范围添加到 IP 匹配条件或删除范围。要更改范围，请添加新范围并删除旧范围。

编辑 IP 匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 在导航窗格中，选择 IP 地址。
3. 在 IP match conditions 窗格中，选择要编辑的 IP 匹配条件。
4. 添加 IP 地址范围：

   a. 在右窗格中，选择 Add IP address or range。

   b. 选择正确的 IP 版本并使用 CIDR 表示法输入 IP 地址范围。下面是一些示例：

      - 要指定 IPv4 地址 192.0.2.44，请输入 192.0.2.44/32。
      - 要指定 IPv6 地址 0:0:0:0:0:ffff:c000:22c，请输入 0:0:0:0:0:ffff:c000:22c/128。
      - 要指定从 192.0.2.0 至 192.0.2.255 的 IPv4 地址范围，请输入 192.0.2.0/24。
      - 要指定从 2620:0:2d0:200:0:0:0:0 到 2620:0:2d0:200:ffff:ffff:ffff:ffff 的 IPv6 地址范围，请输入 2620:0:2d0:200::/64。

      AWS WAF Classic 支持 IPv4 地址范围：/8 以及介于 /16 到 /32 之间的任何范围。 AWS WAF Classic 支持 IPv6 地址范围：/24、/32、/48、/56、/64 和 /128。有关 CIDR 表示法的更多信息，请参阅维基百科条目无类别域间路由。

   c. 要添加更多 IP 地址，请选择 添加其他 IP 地址 并输入值。

   d. 选择 添加。

5. 删除 IP 地址或范围：

   a. 在右窗格中，选择要删除的值。

   b. 选择 Delete IP address or range。

删除 IP 匹配条件

如果要删除某个 IP 匹配条件，则必须先删除该条件中的所有 IP 地址和范围，然后从使用该条件的所有规则中将其删除，如以下过程中所述。

删除 IP 匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 在导航窗格中，选择 IP 地址。
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，选择规则。

   b. 选择使用要删除的 IP 匹配条件的规则的名称。

   c. 在右窗格中，选择要从规则中删除的 IP 匹配条件，然后选择 Remove selected condition。

   d. 对使用要删除的 IP 匹配条件的所有其余规则重复步骤 b 和 c。

   e. 在导航窗格中，选择 IP match conditions。

   f. 在 IP match conditions 窗格中，选择要删除的 IP 匹配条件。

6. 选择 删除 删除所选条件。

使用地理匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

如果要基于请求源自的国家/地区允许或阻止 Web 请求，请创建一个或多个地理匹配条件。地理匹配条件列出了您的请求源自的国家/地区。在这个过程中的稍后阶段，在创建 Web ACL 时，需要指定是允许还是阻止来自这些国家/地区的请求。

您可以将地理匹配条件与其他 AWS WAF 经典条件或规则一起使用来构建复杂的筛选。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，则来自该国家/地区的所有请求都将被屏蔽，并且不会转发到 AWS WAF Classic。因此，如果您想根据地理位置和其他 AWS WAF 经典条件允许或阻止请求，则不应使用 CloudFront 地理限制功能。相反，您应该使用 AWS WAF 经典地理匹配条件。

主题

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**
>
> 向规则添加地理匹配条件时，您还可以将 AWS WAF Classic 配置为允许或阻止并非来自您在条件中指定的国家/地区的 Web 请求。

创建地理匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Geo match。
3. 选择 创建条件。
4. 在 名称 字段中输入名称。

   该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。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。位置类型 目前只能是 国家/地区。
7. 选择 添加位置。
8. 选择 创建。

编辑地理匹配条件

您可以向地理匹配条件中添加国家/地区或从地理匹配条件中删除国家/地区。

编辑地理匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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 添加筛选条件。
   b. 选择位置类型和国家/地区。位置类型 目前只能是 国家/地区。
   c. 选择 添加。
5. 要删除国家/地区，请按照下列步骤操作：

   a. 在右窗格中，选择要删除的值。
   b. 选择 删除筛选器。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

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，选择规则。
   b. 选择使用要删除的地理匹配条件的规则的名称。
   c. 在右窗格中，选择 编辑规则。
   d. 选择要删除的条件旁边的 X。
   e. 选择更新。
   f. 对使用要删除的地理匹配条件的所有其余规则重复这些步骤。
3. 从要删除的条件中删除筛选条件：
   a. 在导航窗格中，选择 Geo match。
   b. 选择要删除的地理匹配条件的名称。
   c. 在右窗格中，选中 筛选条件 旁边的复选框来选择所有筛选条件。
   d. 选择 删除筛选器。
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 删除 删除所选条件。

使用大小约束条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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。大小限制条件用于标识您希望 C AWS WAF lassic 查看的 Web 请求部分、您希望 C AWS WAF lassic 查找的字节数以及运算符，例如大于 (>) 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，如果您将 AWS WAF Classic 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 Classic 仅检查前 8192 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

创建大小限制条件时，您可以指定过滤器来标识希望 C AWS WAF lassic 评估长度的 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。以下是每种配置如何影响 AWS WAF 经典行为：

- 每个大小限制条件一个过滤器-将单独的大小限制条件添加到规则并将该规则添加到 Web ACL 时，Web 请求必须符合所有条件，CI AWS WAF assic 才能根据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。当您将两个条件添加到同一个规则并将该规则添加到 Web ACL 时，CI AWS WAF assic 仅在两个条件都为真时才允许或阻止请求。
- 每个大小限制条件不止一个过滤器-当您将包含多个过滤器的大小限制条件添加到规则并将该规则添加到 Web ACL 时，Web 请求只需要匹配大小限制条件中的一个过滤器，CI AWS WAF assic 即可根据该条件允许或阻止请求。

  假设您创建了一个而不是两个条件，并且其中一个条件包含与前面示例相同的两个筛选条件。 AWS WAF 如果查询字符串大于 100 字节或请求正文大于 1024 字节，Classic 将允许或阻止请求。

> **Note**
>
> 向规则添加大小限制条件时，还可以将 CI AWS WAF assic 配置为允许或阻止与条件中的值不匹配的 Web 请求。

创建大小约束条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Size constraints。
3. 选择 创建条件。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 创建或编辑大小约束条件时指定的值。
5. 选择 再添加一个筛选条件。
6. 如果要添加其他筛选条件，请重复步骤 4 和 5。
7. 添加完筛选器后，选择 Create size constraint condition。

创建或编辑大小约束条件时指定的值

创建或更新大小约束条件时，需要指定以下值：

名称

为大小约束条件输入名称。

该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。条件的名称在创建后不可更改。

Part of the request to filter on

选择每个 Web 请求中您希望 AWS WAF Classic 评估长度的部分：

标题

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

请求的 URI 路径，用于标识资源，例如 `/images/daily-ad.jpg`。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

除非指定了转换，否则不会对 URI 进行标准化，而是像在请求中从客户端 AWS 收到的那样对其进行检查。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，如果网址是 “www.xyz.com？UserName=abc& SalesRegion =seattle”，则可以向或参数添加过滤器。UserNameSalesRegion

如果您选择 单一查询参数（仅限值），您还将指定 查询参数名称。这是您要检查的查询字符串中的参数，例如UserName。查询参数名称 的最大长度为 30 个字符。查询参数名称 不区分大小写。例如，如果您指定UserName为查询参数名称，它将匹配的所有变体 UserName，例如用户名和用户名。

所有查询参数（仅限值）

与单一查询参数（仅限值）类似，但C AWS WAF lassic不会检查单个参数的值，而是检查查询字符串中所有参数的值以了解大小约束。例如，如果网址为 “www.xyz.com？UserName=abc& SalesRegion =seattle”，并且您选择了所有查询参数（仅限值），则如果超过指定大小，则 C AWS WAF lassic 将触发匹配值的匹配。UserNameSalesRegion

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

如果您为要筛选的请求的一部分选择了标头，请从常用标头列表中选择标头，或者键入希望 C AWS WAF lassic 评估其长度的标头的名称。

比较运算符

选择您希望 AWS WAF Classic 如何根据您为 “大小” 指定的值来评估 Web 请求中查询字符串的长度。

例如，如果您为比较运算符选择大于，在 “大小” 中键入 100，则 AWS WAF Classic 会评估长度超过 100 字节的查询字符串的 Web 请求。

大小

输入您希望 C AWS WAF lassic 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 路径 `/logo.jpg` 的长度是 9 个字符。

Transformation

在 C AWS WAF lassic 评估请求中指定部分的长度之前，转换会重新格式化 Web 请求。这消除了攻击者为了绕过 C AWS WAF lassic 而在 Web 请求中使用的一些不寻常的格式。

> **Note**
>
> 如果您为请求的一部分选择正文进行筛选，则无法将 C AWS WAF lassic 配置为执行转换，因为只有前 8192 字节会被转发以供检查。但是，您仍然可以基于 HTTP 请求正文的大小筛选流量，并将转换指定为无。（AWS WAF Classic 从请求标头中获取正文的长度。）

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，Classic 不会对 Web 请求执行任何文本转换。

转换为小写形式

AWS WAF 经典版将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF Classic 用未编码的字符替换 HTML 编码的字符：

- 将 `&quot;` 替换为 &
- 将 ` ` 替换为不间断空格
- 将 `<` 替换为 <
- 将 `>` 替换为 >
- 将以十六进制格式表示的字符 `&#xhhhh;` 替换为对应字符
- 将以十进制格式表示的字符 `&#nnnn;` 替换为对应字符

规范化空格

AWS WAF Classic 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。
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 添加筛选条件。

   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。

   c. 选择 添加。

5. 要删除筛选条件，请执行以下步骤：

   a. 选择要删除的筛选条件。

   b. 选择 删除筛选器。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

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 关联的规则 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，选择规则。

   b. 选择使用要删除的大小约束条件的规则的名称。

   c. 在右窗格中，选择要从规则中删除的大小约束条件，然后选择 Remove selected condition。

   d. 对使用要删除的大小约束条件的所有其余规则重复步骤 b 和 c。

   e. 在导航窗格中，选择 Size constraint。

   f. 在 Size constraint conditions 窗格中，选择要删除的大小限制条件。

6. 选择 删除 删除所选条件。

使用 SQL 注入匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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 注入匹配条件用于标识您希望 C AWS WAF lassic 检查的 Web 请求部分，例如 URI 路径或查询字符串。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
- 创建或编辑 SQL 注入匹配条件时指定的值
- 在 SQL 注入匹配条件中添加和删除筛选条件
- 删除 SQL 注入匹配条件

创建 SQL 注入匹配条件

创建 SQL 注入匹配条件时，需要指定过滤器，这些过滤器指明希望 C AWS WAF lassic 检查哪一部分 Web 请求中是否存在恶意 SQL 代码，例如 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。以下是每种配置如何影响 AWS WAF 经典行为：

- 每个 SQL 注入匹配条件都有一个以上的过滤器（推荐）— 当您在规则中添加包含多个过滤器的 SQL 注入匹配条件并将该规则添加到 Web ACL 时，Web 请求只需要与 SQL 注入匹配条件中的一个过滤器匹配，CI AWS WAF assic 即可根据该条件允许或阻止请求。

  例如，假设您创建一个 SQL 注入匹配条件，并且该条件包含两个筛选条件。一个过滤器指示 AWS WAF Classic 检查 URI 中是否有恶意 SQL 代码，另一个过滤器指示 AWS WAF Classic 检查查询字符串。 AWS WAF 如果请求在 URI 或查询字符串中似乎包含恶意 SQL 代码，Classic 会允许或阻止这些请求。

- 每个 SQL 注入匹配条件一个过滤器-将单独的 SQL 注入匹配条件添加到规则并将该规则添加到 Web ACL 时，Web 请求必须匹配所有条件，CI AWS WAF assic 才能根据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。当您将两个条件添加到同一个规则并将该规则添加到 Web ACL 时，CI AWS WAF assic 仅在 URI 和查询字符串似乎都包含恶意 SQL 代码时才允许或阻止请求。

> **Note**
>
> 向规则添加 SQL 注入匹配条件时，还可以将 AWS WAF Classic 配置为允许或阻止看似不包含恶意 SQL 代码的 Web 请求。

创建 SQL 注入匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 SQL 注入。
3. 选择 创建条件。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 创建或编辑 SQL 注入匹配条件时指定的值。
5. 选择 再添加一个筛选条件。
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 创建。

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）或以下特殊字符：_-!"#`+*},./。条件的名称在创建后不可更改。

Part of the request to filter on

选择每个 Web 请求中您希望 AWS WAF Classic 检查恶意 SQL 代码的部分：

标题

指定的请求标头，例如 `User-Agent` 或 `Referer` 标头。如果选择 Header，则在 Header 字段中指定标头的名称。

HTTP method

HTTP 方法，指示请求要求源执行的操作的类型。CloudFront 支持以下方法：`DELETE`、`GET`、`HEAD`、`OPTIONS`、`PATCH`、`POST`、和`PUT`。

查询字符串

URL 中在 ？字符之后出现的部分 (如果有)。

> **Note**
>
> 对于 SQL 注入匹配条件，我们建议您通过所有查询参数（仅限值），而不是查询字符串，来选择要作为筛选条件的请求部分。

URI

请求的 URI 路径，用于标识资源，例如 `/images/daily-ad.jpg`。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

除非指定了转换，否则不会对 URI 进行标准化，而是像请求中从客户端 AWS 接收的那样对其进行检查。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**
>
> 如果选择正文作为要作为筛选条件的请求部分 的值，则 AWS WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。（AWS WAF Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

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，如果网址是 “www.xyz.com？UserName=abc& SalesRegion =seattle”，则可以向或参数添加过滤器。UserNameSalesRegion

如果您选择 单一查询参数（仅限值），您还将指定 查询参数名称。这是您要检查的查询字符串中的参数，例如UserName或SalesRegion。查询参数名称 的最大长度为 30 个字符。查询参数名称 不区分大小写。例如，如果您指定UserName为查询参数名称，它将匹配的所有变体UserName，例如用户名和用户名。

所有查询参数（仅限值）

与单一查询参数（仅限值）类似，但是 C AWS WAF lassic 不会检查单个参数的值，而是检查查询字符串中所有参数的值是否存在可能的恶意 SQL 代码。例如，如果网址为 “www.xyz.com？UserName=abc& SalesRegion =seattle”，并且您选择了所有查询参数（仅限值），则如果其中一个或UserName的值可能包含恶意 SQL 代码，C AWS WAF lassic 将触发匹配。SalesRegion

标题

如果您为要筛选的部分请求选择了标头，请从常用标头列表中选择标头，或者输入希望 C AWS WAF lassic 检查是否存在恶意 SQL 代码的标头的名称。

Transformation

在 C AWS WAF lassic 检查请求之前，转换会重新格式化 Web 请求。这消除了攻击者为了绕过 C AWS WAF lassic 而在 Web 请求中使用的一些不寻常的格式。

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 Valu e 中的字符串是否匹配之前，Classic 不会对 Web 请求执行任何文本转换。

转换为小写形式

AWS WAF 经典版将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF Classic 用未编码的字符替换 HTML 编码的字符：

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

规范化空格

AWS WAF Classic 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 SQL 注入。
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 添加筛选条件。

   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。

   c. 选择 添加。
5. 要删除筛选条件，请执行以下步骤：

   a. 选择要删除的筛选条件。

   b. 选择 删除筛选器。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 SQL 注入。
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 关联的规则 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，选择规则。

b. 选择使用要删除的 SQL 注入匹配条件的规则的名称。

c. 在右窗格中，选择要从规则中删除的 SQL 注入匹配条件，然后选择 Remove selected condition。

d. 对使用要删除的 SQL 注入匹配条件的所有其余规则重复步骤 b 和 c。

e. 在导航窗格中，选择 SQL 注入。

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 删除 删除所选条件。

使用字符串匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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。字符串匹配条件用于标识您要搜索的字符串以及您希望 C AWS WAF lassic 检查该字符串的 Web 请求部分，例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字符串的请求。

主题

- 创建字符串匹配条件
- 创建或编辑字符串匹配条件时指定的值
- 在字符串匹配条件中添加和删除筛选条件
- 删除字符串匹配条件

创建字符串匹配条件

创建字符串匹配条件时，需要指定筛选器来识别要搜索的字符串以及希望 C AWS WAF lassic 检查该字符串的 Web 请求部分，例如 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。以下是每种配置如何影响 AWS WAF 经典行为：

- 每个字符串匹配条件一个过滤器-将单独的字符串匹配条件添加到规则并将该规则添加到 Web ACL 时，Web 请求必须匹配所有条件，CI AWS WAF assic 才能根据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。当您将两个条件添加到同一个规则并将该规则添加到 Web ACL 时，CI AWS WAF assic 仅允许或阻止包含两个值的请求。
- 每个字符串匹配条件不止一个过滤器-当您将包含多个过滤器的字符串匹配条件添加到规则并将该规则添加到 Web ACL 时，Web 请求只需要匹配字符串匹配条件中的一个过滤器，CI AWS WAF assic 即可根据一个条件允许或阻止请求。

  假设您创建了一个而不是两个条件，并且其中一个条件包含与前面示例相同的两个筛选条件。 AWS WAF 如果请求包含在*`User-Agent`*标题或查询字符串*`BadBot`*中，Classic 将允许或*`BadParameter`*阻止请求。

> **Note**
>
> 向规则添加字符串匹配条件时，还可以将 CI AWS WAF assic 配置为允许或阻止与条件中的值不匹配的 Web 请求。

创建字符串匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 String and regex matching。
3. 选择 创建条件。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 创建或编辑字符串匹配条件时指定的值。
5. 选择 添加筛选条件。
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 创建。

创建或编辑字符串匹配条件时指定的值

创建或更新字符串匹配条件时，需要指定以下值：

名称

为字符串匹配条件输入名称。该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。条件的名称在创建后不可更改。

Type

选择 String match。

Part of the request to filter on

选择每个 Web 请求中您希望 AWS WAF Classic 检查的部分，以查找您在要匹配的值中指定的字符串：

标题

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

请求的 URI 路径，用于标识资源，例如 `/images/daily-ad.jpg`。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

除非指定了转换，否则不会对 URI 进行标准化，而是像在请求中从客户端 AWS 收到的那样对其进行检查。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**
>
> 如果选择正文作为要作为筛选条件的请求部分 的值，则 AWS WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。（AWS WAF Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

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，如果网址是 “www.xyz.com？UserName=abc& SalesRegion =seattle”，则可以向或参数添加过滤器。UserNameSalesRegion

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，“要匹配的值”中的 “波士顿” 或 “西雅图” 都将触发匹配。

如果您选择 单一查询参数（仅限值），您还将指定 查询参数名称。这是您要检查的查询字符串中的参数，例如UserName或SalesRegion。查询参数名称 的最大长度为 30 个字符。查询参数名称 不区分大小写。例如，如果您指定UserName为查询参数名称，它将匹配的所有变体 UserName，例如用户名和用户名。

所有查询参数（仅限值）

与单一查询参数（仅限值）类似，但C AWS WAF lassic不会检查单个参数的值，而是检查查询字符串中所有参数的值以匹配该值。例如，如果网址为 “www.xyz.com？UserName=abc& SalesRegion =seattle”，并且您选择了所有查询参数（仅限值），则如果将UserName或的值指定为要匹配的值，C AWS WAF lass SalesRegionic 将触发匹配。

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

如果您从请求的部分中选择标题以在列表中进行筛选，请从常用标题列表中选择标题，或者输入希望 C AWS WAF lassic 检查的标题的名称。

Match type

在您希望 AWS WAF Classic 检查的请求部分中，选择要匹配的值中的字符串必须出现在哪个位置才能匹配此过滤器：

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 要匹配的值，并且 要匹配的值 必须仅包含字母数字字符或下划线 (A-Z、a-z、0-9 或 _)。此外，要匹配的值 必须是单词，这表示以下一种情况：

- 要匹配的值 与 Web 请求的指定部分的值精确匹配，如标头的值。
- 要匹配的值 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;)。
- 要匹配的值 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)。
- 要匹配的值 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。

开始于

字符串出现在请求的指定部分的开头。

结束于

字符串出现在请求的指定部分的末尾。

Transformation

在 C AWS WAF lassic 检查请求之前，转换会重新格式化 Web 请求。这消除了攻击者为了绕过 C AWS WAF lassic 而在 Web 请求中使用的一些不寻常的格式。

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 Valu e 中的字符串是否匹配之前，Classic 不会对 Web 请求执行任何文本转换。

转换为小写形式

AWS WAF 经典版将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF Classic 用未编码的字符替换 HTML 编码的字符：

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

规范化空格

AWS WAF Classic 将以下字符替换为空格字符（十进制 32）：

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

此外，此选项将多个空格替换为一个空格。

Simplify command line

如果您担心攻击者注入操作系统命令行命令并使用异常格式伪装部分或所有命令，使用此选项可执行以下转换：

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

URL decode

解码 URL 编码的请求。

Value is base64 encoded

如果 要匹配的值 中的值进行了 base64 编码，则选中此复选框。使用 base64 编码可指定攻击者在其请求中包含的不可打印的字符 (如制表符和换行符)。

Value to match

指定您希望 AWS WAF Classic 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 字节的最大长度适用于编码之前的值。

在字符串匹配条件中添加和删除筛选条件

您可以将筛选条件添加到字符串匹配条件或删除筛选条件。要更改筛选条件，请添加一个新筛选条件并删除旧条件。

在字符串匹配条件中添加或删除筛选条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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 添加筛选条件。

   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。

   c. 选择 添加。
5. 要删除筛选条件，请执行以下步骤：

   a. 选择要删除的筛选条件。

   b. 选择 删除筛选条件。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

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，选择规则。

   b. 选择使用要删除的字符串匹配条件的规则的名称。

   c. 在右窗格中，选择 编辑规则。

   d. 选择要删除的条件旁边的 X。

   e. 选择更新。

   f. 对使用要删除的字符串匹配条件的所有其余规则重复这些步骤。

3. 从要删除的条件中删除筛选条件：

   a. 在导航窗格中，选择 String and regex matching。

   b. 选择要删除的字符串匹配条件的名称。

   c. 在右窗格中，选中 筛选条件 旁边的复选框来选择所有筛选条件。

   d. 选择 删除筛选器。

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 删除 删除所选条件。

使用正则表达式匹配条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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，用于标识您要搜索的模式以及您希望 C AWS WAF lassic 检查该模式的 Web 请求部分，例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

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，您可以将这些模式集添加到过滤器中，这些过滤器指定您希望 AWS WAF Classic 检查该模式集的 Web 请求部分，例如 URI 或查询字符串。

您可以将多个正则表达式添加到单个模式集中。如果您这样做，这些表达式将使用 OR 进行组合。也就是说，如果请求的适当部分与列出的任何表达式匹配，则 Web 请求将与模式集匹配。

向规则添加正则表达式匹配条件时，还可以将 CI AWS WAF assic 配置为允许或阻止与条件中的值不匹配的 Web 请求。

AWS WAF Classic 支持大多数标准的 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 在导航窗格中，选择 String and regex matching。
3. 选择 创建条件。
4. 指定适用的筛选条件设置。有关更多信息，请参阅 您在创建或编辑 RegEx 匹配条件时指定的值。
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 创建。

您在创建或编辑 RegEx 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输入名称。该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。条件的名称在创建后不可更改。

Type

选择 RegEx 匹配。

Part of the request to filter on

在每个 Web 请求中，选择您希望 AWS WAF Classic 检查的部分，以匹配您在值中指定的模式：

标题

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

请求的 URI 路径，用于标识资源，例如 `/images/daily-ad.jpg`。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

除非指定了转换，否则不会对 URI 进行标准化，而是像在请求中从客户端 AWS 收到的那样对其进行检查。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**
>
> 如果选择正文作为要作为筛选条件的请求部分 的值，则 AWS WAF Classic 只检查前 8192 个字节 (8 KB)。要允许或阻止正文长度超过 8192 个字节的请求，可以创建大小约束条件。（AWS WAF Classic 从请求标头中获取正文的长度。）有关更多信息，请参阅 使用大小约束条件。

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，如果网址是 “www.xyz.com？UserName=abc& SalesRegion =seattle”，则可以向或参数添加过滤器。UserNameSalesRegion

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，匹配值中的 “波士顿” 或 “西雅图” 的模式将触发匹配。

如果您选择 单一查询参数（仅限值），您还将指定 查询参数名称。这是您要检查的查询字符串中的参数，例如UserName或SalesRegion。查询参数名称 的最大长度为 30 个字符。查询参数名称 不区分大小写。例如，如果您指定UserName为查询参数名称，它将匹配的所有变体 UserName，例如用户名和用户名。

所有查询参数（仅限值）

与单一查询参数（仅限值）类似，但C AWS WAF lassic不会检查单个参数的值，而是检查查询字符串中所有参数的值以匹配在值中指定的模式。例如，在 URL “www.xyz.com？UserName=abc& SalesRegion =seattle” 中，要匹配的值中的一个模式与中的值匹配或将触发匹配。UserNameSalesRegion

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

如果您从请求的部分中选择标题以在列表中进行筛选，请从常用标题列表中选择标题，或者输入希望 C AWS WAF lassic 检查的标题的名称。

Transformation

在 C AWS WAF lassic 检查请求之前，转换会重新格式化 Web 请求。这消除了攻击者为了绕过 C AWS WAF lassic 而在 Web 请求中使用的一些不寻常的格式。

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 Valu e 中的字符串是否匹配之前，Classic 不会对 Web 请求执行任何文本转换。

转换为小写形式

AWS WAF 经典版将大写字母 (A-Z) 转换为小写字母 (a-z)。

HTML decode

AWS WAF Classic 用未编码的字符替换 HTML 编码的字符：

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

规范化空格

AWS WAF Classic 将以下字符替换为空格字符（十进制 32）：

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

此外，此选项将多个空格替换为一个空格。

Simplify command line

如果您担心攻击者注入操作系统命令行命令并使用异常格式伪装部分或所有命令，使用此选项可执行以下转换：

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

URL decode

解码 URL 编码的请求。

与请求匹配的正则表达式模式

您可以选择现有的模式集或创建新的模式集。如果您创建新的模式集，请指定以下内容：

新模式集名称

输入名称，然后指定您希望 CI AWS WAF assic 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。

要匹配的值 的最大长度是 70 个字符。

编辑正则表达式匹配条件

您可以对现有正则表达式匹配条件进行以下更改：

- 从现有模式集中删除模式
- 向现有模式集中添加模式
- 从现有的正则表达式匹配条件中删除筛选条件
- 向现有的正则表达式匹配条件添加筛选器（在一个正则表达式匹配条件中只能有一个筛选器。因此，要添加筛选器，您必须先删除该现有筛选器。）
- 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。
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. 选择编辑。
6. 选择要删除的模式旁边的 X。
7. 选择保存。

向现有模式集中添加模式

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。
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. 选择编辑。
6. 输入新的正则表达式模式。
7. 选择新模式旁边的 +。
8. 选择保存。

从现有的正则表达式匹配条件中删除筛选条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到“切换到 AWS WAF 经典版”，请将其选中。
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 删除筛选器。

删除正则表达式匹配条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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。
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，选择规则。
   b. 选择使用要删除的正则表达式匹配条件的规则的名称。
   c. 在右窗格中，选择 编辑规则。
   d. 选择要删除的条件旁边的 X。
   e. 选择更新。
   f. 对使用要删除的正则表达式匹配条件的所有其余规则重复这些步骤。
4. 在导航窗格中，选择 String and regex matching。
5. 选择要删除的条件旁边的按钮。
6. 选择 Delete （ 删除)。

向现有的正则表达式匹配条件中添加筛选条件或更改其中的筛选条件

正则表达式匹配条件中只能具有一个筛选条件。如果要添加或更改筛选条件，您必须首先删除现有的筛选条件。

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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。
3. 在导航窗格中，选择 String and regex matching。

4. 选择要更改的条件的名称。
5. 选择 添加筛选条件。
6. 为新的筛选条件输入适当的值，然后选择 添加。

使用规则

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

规则允许您通过指定希望 CI AWS WAF assic 监视的确切条件，精确定位希望 CI AWS WAF assic 允许或阻止的 Web 请求。例如， AWS WAF Classic 可以监视请求来源的 IP 地址、请求包含的字符串和字符串的显示位置，以及请求是否包含恶意 SQL 代码。

主题

- 创建规则并添加条件
- 在规则中添加和删除条件
- 删除规则
- AWS Marketplace 规则组

创建规则并添加条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

如果您向规则添加多个条件，则 Web 请求必须符合所有条件，CI AWS WAF assic 才能根据该规则允许或阻止请求。

创建规则并添加条件

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 在导航窗格中，选择规则。
3. 选择 创建规则。
4. 输入以下值：

   名称

   输入名称。

   CloudWatch 指标名称

   输入 C AWS WAF lassic 将创建并与规则关联的 CloudWatch 指标的名称。该名称只能包含字母数字字符（A-Z、a-z、0-9），最大长度为 128 和最小长度为 1。它不能包含为 C AWS WAF lassic 保留的空格或指标名称，包括 “全部” 和 “Default_Action”。

   Rule type

   选择 `Regular rule` 或 `Rate-based rule`。基于速率的规则与常规规则基本相同，但还考虑到任何五分钟时段来自标识的 IP 地址的请求数。有关这些规则类型的详细信息，请参阅 AWS WAF 经典版的工作原理。

   速率限制

   对于基于速率的规则，请输入与规则条件匹配的 IP 地址在任何五分钟内允许的最大请求数。速率限制必须至少为 100。

   您可以单独指定速率限制，也可以指定速率限制和条件。如果仅指定速率限制， AWS WAF 则对所有 IP 地址施加限制。如果您指定速率限制和条件， AWS WAF 则会对符合条件的 IP 地址设置限制。

   当 IP 地址达到速率限制阈值时，通常在 30 秒内尽快 AWS WAF 应用分配的操作（封锁或计数）。操作完成后，如果五分钟过去了，没有来自该 IP 地址的请求，则将计数器 AWS WAF 重置为零。

5. 要将条件添加到规则，请指定以下值：

When a request does/does not

如果您希望 AWS WAF Classic 根据条件中的筛选条件允许或阻止请求，请选择 d oes。例如，如果 IP 匹配条件包括 IP 地址范围 192.0.2.0/24，并且您希望 CI AWS WAF assic 允许或阻止来自这些 IP 地址的请求，则选择允许。

如果您希望 AWS WAF Classic 根据条件中过滤器的反向来允许或阻止请求，请选择 “不是”。例如，如果 IP 匹配条件包括 IP 地址范围 192.0.2.0/24，并且您希望 CI AWS WAF assic 允许或阻止不是来自这些 IP 地址的请求，则选择 “不是”。

match/originate from

选择要添加到规则的条件的类型：

- 跨站点脚本匹配条件：选择在跨站点脚本匹配条件中匹配至少一个筛选条件
- IP 匹配条件：选择源自 IP 地址
- 地理匹配条件：选择源自地理位置
- 大小约束条件：选择在大小约束条件中匹配至少一个筛选条件
- SQL 注入匹配条件：选择在 SQL 注入匹配条件中匹配至少一个筛选条件
- 字符串匹配条件：选择在字符串匹配条件中匹配至少一个筛选条件
- 正则表达式匹配条件：选择(在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的条件。列表仅显示在上一步选择的类型的条件。

6. 要将另一个条件添加到规则中，请选择 添加另一个条件，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 请求必须在每个条件中至少匹配一个筛选条件，CI AWS WAF assic 才能根据该规则允许或阻止请求
   - 如果您向同一规则添加两个 IP 匹配条件，则 CI AWS WAF assic 将仅允许或阻止来自两个 IP 匹配条件中都出现的 IP 地址的请求

7. 添加完条件后，选择 创建。

在规则中添加和删除条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择规则。
3. 选择要在其中添加或删除条件的规则的名称。
4. 选择 添加规则。
5. 要添加条件，请选择 添加条件 并指定以下值：

   When a request does/does not

   如果您希望 AWS WAF Classic 根据条件中的过滤器来允许或阻止请求，例如，源自 IP 地址范围 192.0.2.0/24 的 Web 请求，请选择允许。

   如果您希望 AWS WAF Classic 根据条件中过滤条件的反向来允许或阻止请求，请选择 “不是”。例如，如果 IP 匹配条件包括 IP 地址范围 192.0.2.0/24，并且您希望 CI AWS WAF assic 允许或阻止不是来自这些 IP 地址的请求，则选择 “不是”。

   match/originate from

   选择要添加到规则的条件的类型：

   - 跨站点脚本匹配条件：选择在跨站点脚本匹配条件中匹配至少一个筛选条件
   - IP 匹配条件：选择源自 IP 地址
   - 地理匹配条件：选择源自地理位置

- 大小约束条件：选择在大小约束条件中匹配至少一个筛选条件
- SQL 注入匹配条件：选择在 SQL 注入匹配条件中匹配至少一个筛选条件
- 字符串匹配条件：选择在字符串匹配条件中匹配至少一个筛选条件
- 正则表达式匹配条件：选择(在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的条件。列表仅显示在上一步选择的类型的条件。

6. 要删除条件，请选择条件名称右侧的 X
7. 选择更新。

删除规则

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

如果要删除某个规则，需要先从使用该规则的 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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 要从使用某个规则的 Web ACL 中将其删除，请对每个 Web ACL 执行以下步骤：

   a. 在导航窗格中，选择 Web ACL。
   b. 选择使用待删除规则的 Web ACL 的名称。
   c. 选择 规则 选项卡。
   d. 选择 Edit web ACL。
   e. 选择要删除的规则右侧的 X，然后选择更新。
3. 在导航窗格中，选择规则。

4. 选择要删除的规则的名称。
5. 选择 删除。

AWS Marketplace 规则组

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF Classic 提供AWS Marketplace 规则组来帮助您保护资源。 AWS Marketplace 规则组是由 AWS AWS 合作伙伴公司编写和更新的预定义 ready-to-use 规则的集合。

某些 AWS Marketplace 规则组旨在帮助保护特定类型的 Web 应用程序 WordPress，例如 Joomla 或 PHP。其他 AWS Marketplace 规则组针对已知威胁或常见的 Web 应用程序漏洞（例如 OWASP 前十名中列出的漏洞）提供了广泛的保护。

您可以安装来自首选 AWS 合作伙伴的单个 AWS Marketplace 规则组，也可以添加自己的自定义 AWS WAF Classic 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 规则组来满足 Web 应用程序防火墙要求。

AWS Marketplace 规则组没有长期合同，也没有最低承诺。当您订阅规则组时，将按月收取费用（按小时比例）和根据数量收取持续请求费用。有关更多信息，请参阅 AWS WAF Classic Pricing 和上每个 AWS Marketplace 规则组的描述 AWS Marketplace。

自动更新

及时了解不断变化的威胁形势可能既耗时又昂贵。 AWS Marketplace 当您实现和使用 C AWS WAF lassic 时，规则组可以为您节省时间。另一个好处是，当出现新的漏洞 AWS 和威胁时，我们的 AWS 合作伙伴会自动更新 AWS Marketplace 规则组。

我们的许多合作伙伴会在新漏洞公开披露之前收到通知。他们可以在新威胁广为人知之前更新其规则组并为您部署它们。许多合作伙伴还拥有威胁研究团队，可调查和分析最近出现的威胁，以便编写最相关的规则。

访问规则组中的 AWS Marketplace 规则

每个 AWS Marketplace 规则组都全面描述了其旨在防范的攻击和漏洞类型。为了保护规则组提供程序的知识产权，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。

由于您无法查看规则组中的单个 AWS Marketplace 规则，因此也无法编辑规则组中的任何规则。AWS Marketplace 但是，您可以从规则组中排除特定规则。这称为“规则组例外”。排除规则不会删除这些规则。相反，它将规则的操作更改为 COUNT。因此，与已排除规则匹配的请求会计入总数，但不会受到阻止。您将收到每个排除规则的 COUNT 指标。

在对意外阻止流量的规则组进行故障排除时，排除规则会很有用（误报）。一种故障排除技术是识别规则组中阻止所需流量的特定规则，然后禁用（排除）该特定规则。

除了排除特定规则外，您还可以通过启用或禁用整个规则组以及选择要执行的规则组操作来优化保护。有关更多信息，请参阅 使用 AWS Marketplace 规则组。

配额

您只能启用一个 AWS Marketplace 规则组。您也可以启用一个使用创建的自定义规则组 AWS Firewall Manager。这些规则组计入每个 Web ACL 10 个规则的最大配额。因此，在一个 AWS Marketplace Web ACL 中可以有一个规则组、一个自定义规则组和最多八个自定义规则。

定价

有关 AWS Marketplace 规则组定价，请参阅AWS WAF 经典定价和上每个 AWS Marketplace 规则组的描述 AWS Marketplace。

使用 AWS Marketplace 规则组

您可以在 C AWS WAF lassic 控制台上订阅和取消订阅 AWS Marketplace 规则组。您还可以从规则组中排除特定规则。

订阅和使用 AWS Marketplace 规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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或编辑 Web ACL。

> **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。

取消订阅 AWS Marketplace 规则组

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
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。
3. 在导航窗格中，选择 Marketplace。
4. 选择 管理您的订阅。
5. 选择您想取消订阅的规则组旁边的取消订阅。
6. 选择是，取消订阅。

从规则组中排除规则（规则组例外）

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 如果尚未启用，请启用 AWS WAF 经典日志记录。有关更多信息，请参阅 记录 Web ACL 流量信息。使用 AWS WAF 经典日志来标识要排除的规则的 ID。这些规则通常是阻止合法请求的规则。

3. 在导航窗格中，选择 Web ACL。
4. 选择要编辑的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。

> **Note**
>
> 在您可以从该规则组中排除规则之前，您要编辑的规则组必须与 Web ACL 相关联。

5. 在右窗格中的 规则 选项卡上，选择 Edit web ACL。
6. 在 规则组例外 部分中，展开您要编辑的规则组。
7. 选择要排除的规则旁边的 X。您可以使用 AWS WAF 经典日志来识别正确的规则 ID。
8. 选择更新。

排除规则不会从规则组中删除这些规则。相反，它将规则的操作更改为 COUNT。因此，与已排除规则匹配的请求会计入总数，但不会受到阻止。您将收到每个排除规则的 COUNT 指标。

> **Note**
>
> 您可以使用相同的过程从您在 AWS Firewall Manager中创建的自定义规则组中排除规则。但是，除了使用这些步骤从自定义规则组中排除规则之外，您还可以使用在 AWS WAF 经典规则组中添加和删除规则中描述的步骤编辑自定义规则组。

规则组覆盖

AWS Marketplace 规则组有两种可能的操作：“不覆盖” 和 “覆盖要计数”。如果您要测试规则组，请将操作设置为覆盖以计数。此规则组操作会覆盖该规则组中包含的单个规则指定的任何数据块操作。也就是说，如果规则组的操作设置为覆盖以计数，这些请求则不会阻止基于单个规则操作的匹配请求，而会被进行计数。相反，如果您把规则组的操作设置为无覆盖，则会使用该规则组中单个规则的操作。

AWS Marketplace 规则组问题排查

如果您发现某个 AWS Marketplace 规则组阻止了合法流量，请执行以下步骤。

AWS Marketplace 规则组故障排除

1. 排除阻止合法流量的特定规则。您可以使用 C AWS WAF lassic 日志确定哪些规则阻止了哪些请求。有关排除规则的更多信息，请参阅从规则组中排除规则（规则组例外）。

2. 如果排除特定规则不能解决问题，则可以将 AWS Marketplace 规则组的操作从 “不覆盖” 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。
3. 将 AWS Marketplace 规则组操作设置为 O verride to count 后，请联系规则组提供商的客户支持团队以进一步解决问题。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

如果 AWS WAF Classic 或由管理的规则组存在问题 AWS，请联系 AWS Support。如果 AWS 合作伙伴管理的规则组存在问题，请联系该合作伙伴的客户支持团队。要查找合作伙伴的联系信息，请参阅合作伙伴的列表 AWS Marketplace。

创建并销售 AWS Marketplace 规则组

如果您想在上销售 AWS Marketplace 规则组 AWS Marketplace，请参阅 “如何销售您的软件” AWS Marketplace。

使用 Web ACL

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

向 Web ACL 添加规则时，您可以根据规则中的条件指定是希望 CI AWS WAF assic 允许还是阻止请求。如果您向 Web ACL 添加多个规则，则 CI AWS WAF assic 会按照您在 Web ACL 中列出的顺序对每个请求进行评估。当 Web 请求符合规则中的所有条件时， AWS WAF Classic 会立即采取相应的操作（允许或阻止），并且不会根据 Web ACL 中的其余规则（如果有）评估请求。

如果 Web 请求与 Web ACL 中的任何规则都不匹配，CI AWS WAF assic 将执行您为 Web ACL 指定的默认操作。有关更多信息，请参阅 确定 Web ACL 的默认操作。

如果要在开始使用规则来允许或阻止请求之前对其进行测试，则可以将 CI AWS WAF assic 配置为计算符合规则条件的 Web 请求。有关更多信息，请参阅 测试 Web ACL。

主题

确定 Web ACL 的默认操作

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

创建和配置 Web ACL 时，必须做出的第一个也是最重要的决定是 C AWS WAF lassic 的默认操作是允许 Web 请求还是阻止 Web 请求。默认操作指示 AWS WAF Classic 在检查 Web 请求中是否符合您指定的所有条件后要执行的操作，而 Web 请求与这些条件都不匹配：

- 允许：如果要允许大多数用户访问您的网站，但是阻止其请求源自指定 IP 地址或其请求表现为包含恶意 SQL 代码或指定值的攻击者进行访问，请选择允许作为默认操作。
- 阻止：如果要阻止大多数准用户访问您的网站，但是允许其请求源自指定 IP 地址或其请求包含指定值的用户进行访问，请选择阻止作为默认操作。

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

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

创建 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 如果这是您第一次使用 AWS WAF 经典版，请选择转到 AWS WAF 经典版，然后选择 “配置 Web ACL”。如果您以前使用过 AWS WAF 经典版，请在导航窗格中选择 Web AC L，然后选择创建 Web ACL。

3. 对于 Web ACL 名称，输入一个名称。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

4. 对于CloudWatch 指标名称，如果适用，请更改默认名称。该名称只能包含字母数字字符（A-Z、a-z、0-9），最大长度为 128 和最小长度为 1。它不能包含为 C AWS WAF lassic 保留的空格或指标名称，包括 “全部” 和 “Default_Action”。

   > **Note**
   >
   > Web ACL 在创建之后无法更改名称。

5. 对于 区域（亚马逊云科技区域），选择一个区域。

6. 对于 AWS 资源，选择要与此 Web ACL 关联的资源，然后选择 下一步。

7. 如果您已经创建了希望 AWS WAF Classic 用来检查您的 Web 请求的条件，请选择 “下一步”，然后继续下一步。

如果尚未创建条件，请创建条件。有关更多信息，请参阅以下主题：

- 使用跨站点脚本匹配条件
- 使用 IP 匹配条件
- 使用地理匹配条件
- 使用大小约束条件
- 使用 SQL 注入匹配条件
- 使用字符串匹配条件
- 使用正则表达式匹配条件

8. 如果您已经创建了要添加到此 Web ACL 的规则或 AWS Marketplace 规则组（或订阅了规则组），请将这些规则添加到 Web ACL：

   a. 在 规则 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 创建规则。

   b. 输入以下值：

      名称

      输入名称。

      CloudWatch 指标名称

      输入 C AWS WAF lassic 将创建并与规则关联的 CloudWatch 指标的名称。该名称只能包含字母数字字符（A-Z、a-z、0-9），最大长度为 128 和最小长度为 1。它不能包含空格或为 AWS WAF Classic 预留的指标名称，包括“All”和“Default_Action”。

      > **Note**
      > 创建规则之后，无法更改指标名称。

   c. 要将条件添加到规则，请指定以下值：

When a request does/does not

如果您希望 AWS WAF Classic 根据条件中的过滤器来允许或阻止请求，例如，源自 IP 地址范围 192.0.2.0/24 的 Web 请求，请选择允许。

如果您希望 AWS WAF Classic 根据条件中过滤器的反向来允许或阻止请求，请选择 “不是”。例如，如果 IP 匹配条件包括 IP 地址范围 192.0.2.0/24，并且您希望 CI AWS WAF assic 允许或阻止不是来自这些 IP 地址的请求，则选择 “不是”。

match/originate from

选择要添加到规则的条件的类型：

- 跨站点脚本匹配条件：选择在跨站点脚本匹配条件中匹配至少一个筛选条件
- IP 匹配条件：选择源自 IP 地址
- 地理匹配条件：选择源自地理位置
- 大小约束条件：选择在大小约束条件中匹配至少一个筛选条件
- SQL 注入匹配条件：选择在 SQL 注入匹配条件中匹配至少一个筛选条件
- 字符串匹配条件：选择在字符串匹配条件中匹配至少一个筛选条件
- 正则表达式匹配条件：选择在正则表达式匹配条件中匹配至少一个筛选条件

condition name

选择要添加到规则的条件。列表仅显示您在前面列表中选择的类型的条件。

d. 要将另一个条件添加到规则，请选择 添加另一个条件，然后重复步骤 b 和 c。请注意以下几点：

   - 如果您添加多个条件，则 Web 请求必须在每个条件中至少匹配一个筛选条件，CI AWS WAF assic 才能根据该规则允许或阻止请求。
   - 如果您在同一规则中添加两个 IP 匹配条件，则 CI AWS WAF assic 将仅允许或阻止来自两个 IP 匹配条件中出现的 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 创建。

g. 继续执行步骤 10。

10. 对于 Web ACL 中的每个规则或规则组，选择您希望 AWS WAF Classic 提供的管理类型，如下所示：

- 对于每条规则，选择是否希望 AWS WAF Classic 根据规则中的条件允许、阻止或计数 Web 请求：
  - 允许 — API Gateway CloudFront 或 Application Load Balancer 使用请求的对象进行响应。如果是 CloudFront，如果对象不在边缘缓存中，则将请求 CloudFront 转发到源。
  - 阻止 — API Gateway CloudFront 或 Application Load Balancer 使用 HTTP 403（禁止）状态代码响应请求。CloudFront 也可以使用自定义错误页面进行响应。有关更多信息，请参阅 在 CloudFront 自定义错误页面上使用 AWS WAF 经典版。
  - 计数 — AWS WAF Classic 会增加符合规则条件的请求计数器，然后根据 Web ACL 中的其余规则继续检查 Web 请求。

    有关在开始使用 Web ACL 允许或阻止 Web 请求之前，使用 计数 测试 Web ACL 的信息，请参阅 对与 Web ACL 中的规则匹配的 Web 请求计数。
- 对于每个规则组，为其设置覆盖操作：
  - 无覆盖：促使利用规则组中各个规则的操作。
  - 覆盖以计数：覆盖组中各个规则指定的所有阻止操作，以便仅对所有匹配的请求进行计数。

  有关更多信息，请参阅 规则组覆盖。

11. 如果要更改 Web ACL 中规则的顺序，请使用顺序列中的箭头。 AWS WAF Classic 根据规则在 Web ACL 中出现的顺序来检查 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。当 Web 请求与此 Web ACL 中任何规则中的条件都不匹配时，CI AWS WAF assic 会执行此操作。有关更多信息，请参阅 确定 Web ACL 的默认操作。
14. 选择 检查并创建。
15. 查看 Web ACL 的设置，然后选择 确认并创建。

将 Web ACL 与 Amazon API Gateway API、 CloudFront 分配或应用程序负载均衡器关联或取消关联

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

要关联或取消关联 Web ACL，请执行适用的过程。请注意，在创建或更新 CloudFront 分配时，也可以将 Web ACL 与分配相关联。有关更多信息，请参阅《Amazon CloudFront 开发者指南》中的使用 AWS WAF 经典版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：

- 每个 API Gateway API、Application Load Balancer 和 CloudFront 分配只能与一个 Web ACL 关联。
- 与 CloudFront 分配关联的 Web ACL 不能与 Application Load Balancer 或 API Gateway API 关联。但是，Web ACL 可以与其他 CloudFront 发行版相关联。

将 Web ACL 与 API Gateway API、 CloudFront 发行版或应用程序负载均衡器相关联

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Web ACL。
3. 选择要与 API Gateway API、 CloudFront 分配或应用程序负载均衡器关联的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
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，使用资源列表选择要与此 Web ACL 关联的 API Gateway API、 CloudFront分布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 添加。
7. 要将此 Web ACL 与其他 API Gateway API、 CloudFront 发行版或其他应用程序负载均衡器相关联，请重复步骤 4 到 6。

解除 Web ACL 与 API Gateway API、 CloudFront 分布或应用程序负载均衡器的关联

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

2. 在导航窗格中，选择 Web ACL。
3. 选择要取消与 API Gateway API、 CloudFront 分配或应用程序负载均衡器关联的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
4. 在 “规则” 选项卡上的 “使用此 Web ACL 的AWS 资源” 下，为要取消与此 Web ACL 关联的每个 API Gateway API、 CloudFront 分配或应用程序负载均衡器选择 x。

编辑 Web ACL

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

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 Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Web ACL。
3. 选择要编辑的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
4. 在右窗格中的 规则 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 规则 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. 如果要更改 Web ACL 中规则的顺序，请使用顺序列中的箭头。 AWS WAF Classic 根据规则在 Web ACL 中出现的顺序来检查 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 Classic 中删除规则，而只是将该规则从此 Web ACL 中删除。
8. 要更改规则的操作或 Web ACL 的默认操作，请选择首选选项。

> **Note**
>
> 为规则组或规则组（而不是单个 AWS Marketplace 规则）设置操作时，您为规则组设置的操作（“不覆盖” 或 “覆盖计数”）称为覆盖操作。有关更多信息，请参阅规则组覆盖

9. 选择保存更改。

删除 Web ACL

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

要删除 Web ACL，必须删除 Web ACL 中包含的规则，并取消所有 CloudFront 分配和应用程序负载均衡器与 Web ACL 的关联。请执行以下过程。

删除 Web ACL

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择 Web ACL。
3. 选择要删除的 Web ACL 的名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
4. 在右窗格中的 规则 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 Classic 中删除规则，而只是从此 Web ACL 中删除规则。
6. 选择更新。

7. 解除 Web ACL 与所有 CloudFront 分配和应用程序负载均衡器的关联。在 “规则” 选项卡上的 “使用此 Web ACL 的AWS 资源” 下，为每个 API Gateway API、 CloudFront 分发版或 Application Load Balancer 选择 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

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

为确保您不会意外将 CI AWS WAF assic 配置为阻止要允许的 Web 请求或允许要阻止的请求，我们建议您在开始在网站或 Web 应用程序上使用 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
- 查看 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 的网络请求示例

对与 Web ACL 中的规则匹配的 Web 请求计数

向 Web ACL 添加规则时，您可以指定是否希望 AWS WAF Classic 允许、阻止或计算符合该规则中所有条件的 Web 请求。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 Classic 会根据第一条规则中的条件检查每个 Web 请求。如果 Web 请求符合该规则中的所有条件，则 AWS WAF Classic 会增加该规则的计数器。然后， AWS WAF Classic 会根据下一条规则中的条件检查 Web 请求。如果请求符合该规则中的所有条件，则 AWS WAF Classic 会增加该规则的计数器。这种情况一直持续到 AWS WAF Classic 根据您的所有规则中的条件检查请求为止。

在将网页 ACL 中的所有规则配置为对请求进行计数并将网页 ACL 与 Amazon API Gateway API、CloudFront 分配或应用程序负载均衡器关联后，即可在亚马逊 CloudWatch图表中查看生成的计数。对于 Web ACL 中的每条规则以及 API Gateway CloudFront 或 Application Load Balancer 向 AWS WAF 经典 Web ACL 转发的所有请求， 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
- 更改对数据 CloudWatch 执行的计算，例如最大值、最小值、平均值或总和

> **Note**
>
> AWS WAF Classic with CloudFront 是一项全球服务，只有当您在中选择美国东部（弗吉尼亚北部）地区时，才可使用指标 AWS Management Console。如果您选择其他区域，则 CloudWatch 控制台中将不会显示任何 AWS WAF 经典指标。

查看 Web ACL 中规则的数据

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格的 指标 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：

   Statistic

   选择对数据 CloudWatch 执行的计算。

   时间范围

   选择您要查看前一个小时还是前三个小时的数据。

   周期

   选择图表中的数据点之间的间隔。

   规则

   选择要查看其数据的规则。

请注意以下几点：

- 如果您刚刚将 Web ACL 与 API Gateway API、 CloudFront 分布或 Application Load Balancer 相关联，则可能需要等待几分钟，数据才会显示在图表中，并让 Web ACL 的指标出现在可用指标列表中。
- 如果您将多个 API Gateway API、 CloudFront 分布或 Application Load Balancer 与 Web ACL 相关联，则 CloudWatch 数据将包括与该网络 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）查看有关 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 的各个请求的详细信息。有关更多信息，请参阅 查看 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 的网络请求示例。
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)。

   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 允许 或 阻止。有关更多信息，请参阅 编辑 Web ACL。

查看 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 的网络请求示例

在 AWS WAF Classic 控制台中，您可以查看 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 进行检查的请求示例。对于每个示例请求，您可以查看关于该请求的详细数据，例如来源 IP 地址和请求中包含的标头。您还可以查看请求匹配哪个规则，以及该规则配置为允许还是阻止请求。

请求采样包含多达 100 个与每个规则中的所有条件都匹配的请求，还有用于默认操作的 100 个请求，该默认操作适用于未与任何规则中的所有条件匹配的请求。示例中的请求来自在过去 15 分钟内收到内容请求的所有 API Gateway API、 CloudFront 边缘站点或应用程序负载均衡器。

查看 API Gateway CloudFront 或 Application Load Balancer 已转发到 AWS WAF Classic 的网络请求示例

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

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 请求 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

   请求的 URI 路径，用于标识资源，例如 `/images/daily-ad.jpg`。这不包括 URI 的查询字符串或片段组件。有关信息，请参阅统一资源标识符 (URI)：一般语法。

   Matches rule

   确定 Web ACL 中 Web 请求匹配其所有条件的第一个规则。如果 Web 请求与 Web ACL 中任何规则的所有条件均不匹配，则 Matches rule 的值为 默认。

   请注意，当 Web 请求与规则中的所有条件相匹配并且该规则的操作为 C ount 时， AWS WAF Classic 会继续根据 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 计数 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 允许、区块 还是 计数。

   时间

   AWS WAF Classic 收到来自 API Gateway CloudFront 或您的应用程序负载均衡器的请求的时间。

4. 要显示有关该请求的更多信息，请选择该请求的 IP 地址左侧的箭头。 AWS WAF 经典版显示以下信息：

源 IP

与表中 源 IP 列的值相同的 IP 地址。

Country

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（请求标头）

请求中的请求标头和标头值。

5. 要刷新示例请求列表，请选择 Get new samples。

使用 AWS WAF 经典规则组以用于 AWS Firewall Manager

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF 经典规则组是您添加到 AWS WAF 经典 AWS Firewall Manager 策略的一组规则。您可以创建自己的规则组，也可以从中购买托管规则组 AWS Marketplace。

> **Important**
>
> 如果要向 Firewall Manager 策略添加 AWS Marketplace 规则组，则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 规则组。

主题

创建 AWS WAF 经典规则组

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

在创建要与之配合使用的 AWS WAF 经典规则组时 AWS Firewall Manager，需要指定要将哪些规则添加到该组中。

创建规则组 (控制台)

1. AWS Management Console 使用您在先决条件中设置的 AWS Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台https://console.aws.amazon.com/wafv2/fms。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅步骤 2：创建 AWS Firewall Manager 默认管理员帐户。

2. 在导航窗格中，选择 “切换到 AWS WAF 经典版”。
3. 在 AWS WAF 经典版导航窗格中，选择规则组。
4. 选择 创建规则组。

> **Note**
>
> 您不能将基于速率的规则添加到规则组。

5. 如果您已创建要添加到规则组的规则，请选择 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 为此规则组创建规则和条件。
6. 选择下一步。
7. 如果您选择创建规则，请按照创建规则并添加条件中的步骤创建规则。

> **Note**
>
> 使用 AWS WAF 经典版控制台创建规则。

创建所有需要的规则后，请转到下一步。

8. 键入规则组名称。
9. 要将规则添加到规则组，请选择规则，然后选择 添加规则。选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。有关选项的更多信息，请参阅AWS WAF 经典版的工作原理。
10. 在添加完规则后，请选择 创建。

您可以测试您的规则组，方法是将其添加到 WebACL 中，然后 AWS WAF 将 WebACL 操作设置为“重写为计数”。此操作将覆盖您为组中包含的规则选择的任何操作，并且仅对匹配的请求计数。有关更多信息，请参阅 创建 Web ACL。

在 AWS WAF 经典规则组中添加和删除规则

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

您可以在 C AWS WAF lassic 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. AWS Management Console 使用您在先决条件中设置的 AWS Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台https://console.aws.amazon.com/wafv2/fms。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅步骤 2：创建 AWS Firewall Manager 默认管理员帐户。

2. 在导航窗格中，选择 “切换到 AWS WAF 经典版”。
3. 在 AWS WAF 经典版导航窗格中，选择规则组。
4. 选择要编辑的规则组。
5. 选择 编辑规则组。
6. 要添加规则，请执行以下步骤：

   a. 选择一个规则，然后选择 将规则添加到规则组。选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。有关选项的更多信息，请参阅AWS WAF 经典版的工作原理。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. 选择更新。

7. 要删除规则，请执行以下步骤：

   a. 选择要删除的规则旁的 X。重复操作以从规则组中删除更多规则。

   b. 选择更新。

开始使用 AWS Firewall ManagerAWS WAF 经典规则启用

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

您可以使用 AWS Firewall Manager 启用 AWS WAF 规则、 AWS WAF 经典规则、 AWS Shield Advanced 保护和 Amazon VPC 安全组。每一项的设置步骤略有不同。

- 要使用最新版本的 Firewall Manager 启用规则 AWS WAF，请不要使用本主题。请按照AWS Firewall ManagerAWS WAF 策略入门中的步骤操作。
- 要使用 Firewall Manager 启用 AWS Shield Advanced 保护，请按照中的步骤操作AWS Firewall ManagerAWS Shield Advanced 策略入门。
- 若要使用 Firewall Manager 启用 Amazon VPC 安全组，请按照 开始使用 A AWS Firewall Manager mazon VPC 安全组策略 中的步骤操作。

要使用 Firewall Manager 启用 AWS WAF 经典规则，请按顺序执行以下步骤。

主题

步骤 1：完成先决条件

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行步骤 2：创建规则之前，请完成所有先决条件。

步骤 2：创建规则

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

在此步骤中，您将使用 C AWS WAF lassic 创建规则。如果您已经有要使用的 AWS WAF 经典规则 AWS Firewall Manager，请跳过此步骤并转至步骤 3：创建规则组。

> **Note**
>
> 使用 AWS WAF 经典版控制台创建规则。

创建 AWS WAF 经典规则（控制台）

- 创建您的规则，然后将您的条件添加到规则。有关更多信息，请参阅 创建规则并添加条件。

您现在已准备好转到步骤 3：创建规则组。

步骤 3：创建规则组

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

规则组是一系列规则，用于定义在满足特定的一组条件时要执行的操作。您可以使用中的托管规则组 AWS Marketplace，也可以创建自己的规则组。有关托管规则组的信息，请参阅AWS Marketplace 规则组。

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. AWS Management Console 使用您在先决条件中设置的 AWS Firewall Manager 管理员帐户登录，然后在上打开 Firewall Manager 控制台https://console.aws.amazon.com/wafv2/fms。
2. 在导航窗格中，选择 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 关闭。
4. 选择 创建策略。

   对于 策略类型，选择 AWS WAF Classic。
5. 选择创建 AWS Firewall Manager 策略并添加新规则组。
6. 选择一个 AWS 区域，然后选择下一步。
7. 由于您已创建规则，因此无需创建条件。选择下一步。
8. 由于您已创建规则，因此无需创建规则。选择下一步。
9. 选择 创建规则组。
10. 对于 名称，输入一个易于理解的名称。
11. 输入 C AWS WAF lassic 将创建并与规则组关联的 CloudWatch 指标的名称。该名称只能包含字母数字字符（A-Z、a-z、0-9）或以下特殊字符：_-!"#`+*},./。且不能包含空格。
12. 选择规则，然后选择 添加规则。规则具有一项操作设置，可让您选择是允许、阻止符合规则条件的请求还是对这些请求进行计数。在本教程中，请选择 计数。重复添加规则，直到您已将所需的所有规则添加到规则组。
13. 选择 创建。

您现在已准备好转到步骤 4：创建并应用 AWS Firewall ManagerAWS WAF 经典策略。

步骤 4：创建并应用 AWS Firewall ManagerAWS WAF 经典策略

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

创建规则组后，即可创建 AWS Firewall Manager AWS WAF 策略。Firewall Manager AWS WAF 策略包含要应用于资源的规则组。

创建 Firewall Manager AWS WAF 策略（控制台）

1. 在您创建规则组（上一个过程步骤 3：创建规则组中的最后一步）后，控制台会显示 规则组摘要 页面。选择下一步。
2. 对于 名称，输入一个易于理解的名称。
3. 对于 策略类型，选择 WAF。
4. 对于区域，选择一个 AWS 区域。要保护 Amazon CloudFront 资源，请选择 “全球”。

   要保护多个区域中的资源（ CloudFront 资源除外），必须为每个区域创建单独的 Firewall Manager 策略。
5. 选择要添加的规则组，然后选择 添加规则组。
6. 一个策略有两个可能的操作：由规则组设置的操作 和 计数。如果您要测试策略和规则组，请将操作设置为 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 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 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 计数。
7. 选择下一步。
8. 如果您希望仅在策略中包含特定账户，或者仅从策略中排除特定账户，请选择 选择要在此策略中包含/排除的账户 (可选)。选择 仅在此策略中包含这些账户 或 仅从此策略中排除这些账户。您只能选择一个选项。选择 添加。选择要包含或排除的账号，然后选择 确定。

> **Note**
>
> 如果您不选择此选项，Firewall Manager 在 AWS Organizations中将策略应用于您组织中的所有账户。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。

9. 选择要保护的资源的类型。
10. 如果您只想保护带特定标签的资源，或者排除带特定标签的资源，请选择 使用标签来包含/排除资源，输入标签，然后选择 包含 或 排除。您只能选择一个选项。

    如果您输入了多个标签 (以逗号分隔)，并且某个资源带有任一这些标签，则会将该资源视为匹配项。

    有关标签的更多信息，请参阅使用标签编辑器。
11. 选择 创建此策略并将其应用于现有资源和新资源。

    此选项在组织中的每个适用账户中创建一个 Web ACL AWS Organizations，并将该 Web ACL 与账户中的指定资源相关联。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，如果您选择创建策略但不将策略应用于现有资源或新资源，则 Firewall Manager 会在组织内的每个适用账户中创建一个 Web ACL，但不会将 Web ACL 应用于任何资源。您稍后必须将策略应用于资源。
12. 在默认设置中保留对 替换现有关联 Web ACL 的选择。

    选择此选项后，Firewall Manager 会从范围内资源中删除所有现有 Web ACL 关联，然后再将新策略的 Web ACL 与资源关联。
13. 选择下一步。
14. 查看新策略。要进行任何更改，请选择 编辑。若您满意所创建的策略，请选择 创建策略。

教程：使用分层规则创建 AWS Firewall Manager策略

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

使用 AWS Firewall Manager，您可以创建和应用包含分层规则的 AWS WAF 经典保护策略。也就是说，您可以集中创建和实施某些规则，但将特定于账户的规则的创建和维护委派给其他人。您可以监控集中应用（常见）的规则，以防止意外删除或误操作，从而确保一致地应用它们。特定于账户的规则可根据各个团队的需求添加进一步的保护。

> **Note**
>
> 在的最新版本中 AWS WAF，此功能是内置的，不需要任何特殊处理。如果您尚未使用 AWS WAF Classic，请改用最新版本。请参阅 为创建 AWS Firewall Manager 策略 AWS WAF。

以下教程介绍如何创建一组分层的保护规则。

主题

步骤 1：指定 Firewall Manager 管理员账户

要使用 AWS Firewall Manager，您必须将组织中的一个帐户指定为 Firewall Manager 管理员帐户。该账户可以是管理账户，也可以是该组织中的成员账户。

您可以使用 Firewall Manager 管理员账户来创建一组通用规则，以便应用于组织中的其他账户。组织中的其他账户无法更改这些集中应用的规则。

要将账户指定为 Firewall Manager 管理员账户并完成使用 Firewall Manager 的其他先决条件，请参阅 AWS Firewall Manager 先决条件 中的说明。如果您已经完成了先决条件，则可以跳到本教程的步骤 2。

在本教程中，我们将管理员账户称为 **`Firewall-Administrator-Account`**。

步骤 2：使用 Firewall Manager 管理员账户创建规则组

接下来，使用 **Firewall-Administrator-Account** 创建规则组。此规则组包含您将应用于由您在下一步中创建的策略控制的所有成员账户的通用规则。仅 **Firewall-Administrator-Account** 可以对这些规则和容器规则组进行更改。

在本教程中，我们将此容器规则组称为 **Common-Rule-Group**。

要创建规则组，请参阅创建 AWS WAF 经典规则组中的说明。请记得在遵循这些说明时使用您的 Firewall Manager 管理员账户 (**Firewall-Administrator-Account**) 登录控制台。

步骤 3：创建 Firewall Manager 策略并附加通用规则组

使用 **Firewall-Administrator-Account**，创建 Firewall Manager 策略 在创建此策略时，您必须执行以下操作：

- 将 **Common-Rule-Group** 添加到新策略。
- 在组织中包含您希望 **Common-Rule-Group** 应用到的所有账户。
- 添加您希望 **Common-Rule-Group** 应用到的所有资源。

有关创建策略的说明，请参阅创建 AWS Firewall Manager 策略。

这将在每个指定的账户中创建一个 Web ACL，并将 **Common-Rule-Group** 添加到每个这些 Web ACL 中。创建策略后，此 Web ACL 和通用规则将部署到所有指定的账户。

在本教程中，我们将此 Web ACL 称为 **Administrator-Created-ACL**。现在，组织的每个指定成员账户中都存在唯一的 **Administrator-Created-ACL**。

步骤 4：添加特定于账户的规则

组织中的每个成员账户现在都可以将自己的特定于账户的规则添加到其账户中存在的 **Administrator-Created-ACL**。已有的通用规则以及针对账户的新规则**Administrator-Created-ACL**继续适用。 AWS WAF 根据规则在 Web ACL 中的显示顺序检查 Web 请求。这适用于 **Administrator-Created-ACL** 和特定于账户的规则。

要向 **Administrator-Created-ACL** 中添加规则，请参阅 编辑 Web ACL。

结论

您现在拥有一个 Web ACL，其中包含由 Firewall Manager 管理员账户管理的通用规则以及每个成员账户维护的特定于账户的规则。

每个账户中的 **Administrator-Created-ACL** 都引用单个 **Common-Rule-Group**。因此，Firewall Manager 管理员账户在未来对 **Common-Rule-Group** 进行的更改将立即在每个成员账户中生效。

成员账户无法更改或删除 **Common-Rule-Group** 中的通用规则。

特定于账户的规则不影响其他账户。

记录 Web ACL 流量信息

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

> **Note**
>
> 您不能使用 Amazon Security Lake 收集 AWS WAF 经典数据。

您可以启用日志记录，以获取有关 Web ACL 对流量进行分析的详细信息。日志中包含的信息包括 AWS WAF Classic 从您的 AWS 资源收到请求的时间、有关该请求的详细信息以及每个请求匹配的规则的操作。

要开始使用，您需要设置 Amazon Kinesis Data Firehose。在这个过程中，您需要选择用于存储日志的目标。接下来，选择您要启用日志记录的 Web ACL。启用日志记录后，通过消防水管将日志 AWS WAF 传送到您的存储目的地。

有关如何创建 Amazon Kinesis Data Firehose 以及如何查看存储的日志的信息，请参阅什么是亚马逊数据 Firehose？ 要了解 Kinesis Data Firehose 配置所需的权限，请参阅 使用 Amazon Kinesis Data Firehose 控制访问。

您必须拥有以下权限才能成功启用日志记录：

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

有关服务相关角色以及 `iam:CreateServiceLinkedRole` 权限的更多信息，请参阅在 Classic 中使用服务相关角色 AWS WAF。

为 Web ACL 启用日志记录

1. 使用aws-waf-logs前缀 “-” 开头的名称创建 Amazon Kinesis Data Firehose 例如，。`aws-waf-logs-us-east-2-analytics`使用 PUT 源，在您执行操作的区域中创建 Data Firehose。如果您要为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）创建消防水带。有关更多信息，请参阅创建 Amazon Data Firehose 传输流。

   > **Important**
   >
   > 请勿选择 `Kinesis stream` 作为源。
   > 一个 AWS WAF 经典日志相当于一个 Firehose 记录。如果您通常每秒收到 10,000 个请求并启用完整日志，则应在 Firehose 中设置每秒 10,000 条记录。如果您未正确配置 Firehose， AWS WAF Classic 将不会记录所有日志。有关更多信息，请参阅 Amazon Kinesis Data Firehose 限额。

2. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。

3. 在导航窗格中，选择 Web ACL。
4. 选择您要启用日志记录的 Web ACL 名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
5. 在 日志记录 选项卡上，选择 启用日志记录。
6. 选择您在第一步中创建的 Kinesis Data Firehose。您必须选择以 “aws-waf-logs-” 开头的消防水带。
7. （可选）如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 添加。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 `REDACTED`。例如，如果您编辑 cookie 字段，则日志中的 cookie 字段将为 `REDACTED`。
8. 选择启用日志记录。

> **Note**
>
> 成功启用日志记录后，AWS WAF Classic 将创建一个服务关联角色，该角色具有将日志写入亚马逊 Kinesis Data Firehose 的必要权限。有关更多信息，请参阅 在 Classic 中使用服务相关角色 AWS WAF。

禁用 Web ACL 的日志记录

1. 在导航窗格中，选择 Web ACL。
2. 选择您要禁用日志记录的 Web ACL 名称。然后将打开一个页面，其右侧窗格会显示 Web ACL 的详细信息。
3. 在 日志记录 选项卡上，选择 禁用日志记录。
4. 在对话框中，选择 禁用日志记录。

Example 示例日志


```
{

 "timestamp":1533689070589,
 "formatVersion":1,
 "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
 "terminatingRuleId":"Default_Action",
 "terminatingRuleType":"REGULAR",
 "action":"ALLOW",
 "httpSourceName":"CF",
 "httpSourceId":"i-123",
 "ruleGroupList":[
                         {
                          "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                          "terminatingRule":null,
                          "nonTerminatingMatchingRules":[
                                                          {"action" : "COUNT",
                                                          "ruleId" :
 "4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                         ],
                          "excludedRules":               [
```

```
                                                                {"exclusionType" :
 "EXCLUDED_AS_COUNT",
                                                                 "ruleId" :
 "5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                               ]
                          }
                         ],

 "rateBasedRuleList":[
                              {
                               "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                               "limitKey":"IP",
                               "maxRateAllowed":100

                              },
                              {
                               "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                               "limitKey":"IP",
                               "maxRateAllowed":100
                               }
                               ],

 "nonTerminatingMatchingRules":[
                                       {"action" : "COUNT",

                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                      ],

 "httpRequest":{
                       "clientIp":"192.10.23.23",

                       "country":"US",

                       "headers":[

                                  {
                                   "name":"Host",
                                   "value":"127.0.0.1:1989"
                                  },
                                  {
                                   "name":"User-Agent",
                                   "value":"curl/7.51.2"
```

```
                                    },
                                    {
                                     "name":"Accept",
                                     "value":"*/*"
                                    }
                                  ],
                        "uri":"REDACTED",
                        "args":"usernam=abc",
                        "httpVersion":"HTTP/1.1",
                        "httpMethod":"GET",
                        "requestId":"cloud front Request id"
                        }
}
```

下面是对这些日志中列出的各个项的说明：

时间戳

时间戳，以毫秒为单位。

formatVersion

日志的格式版本。

webaclId

Web ACL 的 GUID。

terminatingRuleId

终止请求的规则的 ID。如果没有任何情况会终止请求，则值为 `Default_Action`。

terminatingRuleType

终止请求的规则的类型。可能的值：RATE_BASED、REGULAR 和 GROUP。

action

操作。终止规则的可能值为：ALLOW 和 BLOCK。COUNT 不是终止规则的有效值。

terminatingRuleMatch详情

有关与请求匹配的终止规则的详细信息。终止规则具有针对 Web 请求结束检查过程的操作。终止规则的可能操作是 ALLOW 和 BLOCK。这仅适用于 SQL 注入和跨站点脚本 (XSS) 匹配规则语句。与所有用于检查多个事物的规则语句一样， AWS WAF 对第一个匹配应用操作并停止检查 Web 请求。除了日志中报告的威胁之外，具有终止操作的 Web 请求还可能包含其他威胁。

httpSourceName

请求的源。可能的值：CF（如果来源是亚马逊 CloudFront）、APIGW（如果来源是 Amazon API Gateway）和 ALB（如果来源是 Application Load Balancer）。

httpSourceId

源 ID。此字段显示关联的亚马逊 CloudFront 分配的 ID、API Gateway 的 REST API 或应用程序负载均衡器的名称。

ruleGroupList

对此请求进行操作的规则组的列表。在前面的代码示例中，只有一个。

ruleGroupId

规则组的 ID。如果规则阻止了请求，则 `ruleGroupID` 的 ID 与 `terminatingRuleId` 的 ID 相同。

terminatingRule

规则组中终止了请求的规则。如果这是非空值，它还会包含 ruleid 和 action。在这种情况下，操作将始终为 BLOCK。

nonTerminatingMatching规则

规则组中与请求匹配的规则列表。这些规则将始终为 COUNT 规则（匹配的非终止规则）。

操作（nonTerminatingMatching规则组）

它将始终为 COUNT（匹配的非终止规则）。

规则 ID（规则组）nonTerminatingMatching

规则组中与请求匹配并且为非终止规则的 ID。即 COUNT 规则。

excludedRules

规则组中您排除的规则的列表。这些规则的操作设置为 COUNT。

exclusionType（excludedRules 组）

一种类型，指示排除的规则具有操作 COUNT。

ruleId（excludedRules 组）

规则组中排除的规则的 ID。

rateBasedRule清单

对请求执行操作的基于速率的规则列表。

rateBasedRule我是

作用于请求的基于速率的规则的 ID。如果这已终止请求，则 `rateBasedRuleId` 的 ID 与 `terminatingRuleId` 的 ID 相同。

limitKey

AWS WAF 用于确定请求是否可能来自单一来源并因此受到速率监控的字段。可能的值：IP。

maxRateAllowed

在五分钟内允许的最大请求数，具有与 `limitKey` 所指定的字段相同的值。如果请求数超过，`maxRateAllowed`并且还满足了规则中指定的其他谓词，则会 AWS WAF 触发为此规则指定的操作。

httpRequest

关于请求的元数据。

clientIp

发送请求的客户端的 IP。

country

请求的源国家/地区。 AWS WAF 如果无法确定原产国，则会将此字段设置为-。

标头

标头的列表。

uri

请求的 URI。上述代码示例演示在编辑了此字段时应具有的值。

args

查询字符串。

httpVersion

HTTP 版本。

httpMethod

请求中的 HTTP 方法。

requestId

请求的 ID。

列出根据基于速率的规则而阻止的 IP 地址

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF Classic 提供了被基于速率的规则屏蔽的 IP 地址列表。

查看根据基于速率的规则阻止的地址

1. 登录 AWS Management Console 并打开 AWS WAF 控制台，网址为 https://console.aws.amazon.com/wafv2/。

   如果您在导航窗格中看到 “切换到 AWS WAF 经典版”，请将其选中。
2. 在导航窗格中，选择规则。
3. 在 Name 列中，选择一个基于速率的规则。

   列表显示该规则当前阻止的 IP 地址。

AWS WAF 经典版如何与 Amazon CloudFront 功能配合使用

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

创建 Web ACL 时，可以指定希望 Cl AWS WAF assic 检查的一个或多个 CloudFront 发行版。AWS WAF Classic 开始根据您在 Web ACL 中确定的条件允许、阻止或计算针对这些分配的 Web 请求。 CloudFront 提供了一些增强 AWS WAF 经典版功能的功能。本章介绍几种您可以配置的方法，CloudFront 以使Classic CloudFront 和 AWS WAF Classic更好地协同工作。

主题

在 CloudFront 自定义错误页面上使用 AWS WAF 经典版

当 AWS WAF Classic 根据您指定的条件阻止 Web 请求时，它会将 HTTP 状态码 403（禁止）返回到 CloudFront。接下来，将该状态码 CloudFront 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（可能使用与网站其余部分相同的格式），则可以配置 CloudFront 为向查看者返回包含自定义错误消息的对象（例如 HTML 文件）。

> **Note**
>
> CloudFront 无法区分您的源站返回的 HTTP 状态码 403 和 Cl AWS WAF assic 在请求被阻止时返回的 HTTP 状态码 403。这意味着，您无法根据 HTTP 状态代码 403 的不同原因返回不同的自定义错误页面。

有关 CloudFront 自定义错误页面的更多信息，请参阅 Amazon CloudFront 开发者指南中的自定义错误响应。

将 AWS WAF Classic 与 CloudFront用于在您自己的 HTTP 服务器上运行的应用程序

当您将 AWS WAF Classic 与配合使用时 CloudFront，您可以保护在任何 HTTP 网络服务器上运行的应用程序，无论是在亚马逊弹性计算云 (Amazon EC2) 中运行的网络服务器，还是您私下管理的网络服务器。您也可以配置 CloudFront 为要求在 CloudFront和您自己的 Web 服务器之间以及查看者和 CloudFront之间使用 HTTPS。

需要在 CloudFront 和你自己的网络服务器之间使用 HTTPS

要要求在 CloudFront 和您自己的网络服务器之间使用 HTTPS，您可以使用 CloudFront 自定义源功能，并为特定来源配置源协议策略和源域名设置。在您的 CloudFront 配置中，您可以指定服务器的 DNS 名称以及从源中获取对象时 CloudFront 要使用的端口和协议。您还应确保自定义源服务器上的 SSL/TLS 证书与您已配置的源域名匹配。在以外使用自己的 HTTP Web 服务器时 AWS，必须使用由受信任的第三方证书颁发机构 (CA) 签名的证书，例如 Comodo 或 Symante DigiCert c。有关要求在 CloudFront和您自己的网络服务器之间进行通信时需要 HTTPS 的更多信息，请参阅《亚马逊 CloudFront 开发者指南》中的 “需要使用 HTTPS 才能 CloudFront 与您的自定义源进行通信” 主题。

需要在查看器和之间使用 HTTPS CloudFront

要要求在查看者和之间使用 HTTPS CloudFront，您可以更改 CloudFront分配中一个或多个缓存行为的查看者协议策略。有关在观看者和之间使用 HTTPS 的更多信息 CloudFront，请参阅 Amazon CloudFront 开发者指南 CloudFront中的 “观看者之间需要使用 HTTPS 才能进行通信” 主题。您也可以带上自己的 SSL 证书，这样观众就可以使用自己的域名（例如 https://www.mysite.com）通过 HTTPS 连接到您的 CloudFront 发行版。有关更多信息，请参阅 Amazon CloudFront 开发者指南中的配置备用域名和 HTTPS 主题。

选择 CloudFront响应的 HTTP 方法

创建 Amazon CloudFront 网络分配时，您可以选择要 CloudFront 处理的 HTTP 方法并将其转发到您的来源。可从以下选项中进行选择：

- GET，HEAD — 你 CloudFront 只能使用从原点获取对象或获取对象标题。
- GE@@ T、H EAD、OPTIONS — 您 CloudFront 只能使用从您的来源获取对象、获取对象标头或检索源服务器支持的选项列表。
- GET、HEAD、OPTIONS、PUT、POST、PAT CH、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题。此外，您可以执行其他 POST 操作，例如从 Web 表格提交数据。

您还可以使用 AWS WAF 经典字符串匹配条件来允许或阻止基于 HTTP 方法的请求，如中所述使用字符串匹配条件。如果要使用 CloudFront 支持的方法组合，例如GET和HEAD，则无需将 Cl AWS WAF assic 配置为阻止使用其他方法的请求。如果要允许组合 CloudFront 不支持的方法，例如GETHEAD、和，则可以配置 CloudFront 为响应所有方法P0ST，然后使用 Cl AWS WAF assic 来阻止使用其他方法的请求。

有关选择 CloudFront 响应方法的更多信息，请参阅《Amazon CloudFront 开发者指南》中 “您在创建或更新 Web 分配时指定的值” 主题中的 “允许的 HTTP 方法”。

AWS WAF 经典版中的安全性

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 C AWS WAF lassic 的合规性计划，请参阅按合规性计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

本文档可帮助您了解在使用 Cl AWS WAF assic 时如何应用分担责任模型。以下主题向您介绍如何配置 AWS WAF Classic 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS WAF Classic 资源。

主题

AWS WAF 经典版中的数据保护

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS 分担责任模型分适用于 C AWS WAF lassic 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API 或 AWS SDK AWS 服务 使用 C AWS WAF lassic 或其他版本时。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

AWS WAF 经典实体（例如 Web ACL、规则和条件）采用静态加密，但某些无法加密的地区除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

删除 AWS WAF 经典资源

您可以删除在 C AWS WAF lassic 中创建的资源。请参阅以下各节中每种资源类型的指南。

- 删除 Web ACL
- 在 AWS WAF 经典规则组中添加和删除规则
- 删除规则

C AWS WAF lassic 的身份和访问管理

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 AWS WAF 经典资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- AWS WAF 经典版如何与 IAM 配合使用
- AWS WAF Classic 的基于身份的策略示例
- 对 AWS WAF 经典身份和访问进行故障排除
- 在 Classic 中使用服务相关角色 AWS WAF

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 C AWS WAF lassic 中所做的工作。

服务用户-如果您使用 AWS WAF Classic 服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多 AWS WAF 经典功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AWS WAF Classic 中的特征，请参阅 对 AWS WAF 经典身份和访问进行故障排除。

服务管理员-如果您负责公司的 AWS WAF Classic 资源，则可能拥有对 C AWS WAF lassic 的完全访问权限。您的工作是确定您的服务用户应访问哪些 AWS WAF 经典功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 C AWS WAF lassic 结合使用，请参阅AWS WAF 经典版如何与 IAM 配合使用。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 C AWS WAF lassic 的访问权限。要查看您可以在 IAM 中使用的基于身份的 AWS WAF 经典策略示例，请参阅。AWS WAF Classic 的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（ MFA ）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根

用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon QLDB 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS WAF 经典版如何与 IAM 配合使用

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。

有关的最新版本 AWS WAF，请参阅AWS WAF。

在使用 IAM 管理 AWS WAF 经典版访问权限之前，请先了解哪些可用于 CI AWS WAF assic 的 IAM 功能。

您可以在 C AWS WAF lassic 中使用的 IAM 功能

IAM 功能	AWS WAF 经典支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	支持
策略条件键（特定于服务）	支持
ACL	否
ABAC（策略中的标签）	部分
临时凭证	支持
转发访问会话（FAS）	支持
服务角色	支持
服务相关角色	支持

要全面了解 AWS WAF Classic 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

经典版基于身份的策略 AWS WAF

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

要查看基于身份的 AWS WAF 经典策略的示例，请参阅。AWS WAF Classic 的基于身份的策略示例

Classic 中 AWS WAF 基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

C AWS WAF lassic 的策略操作

支持策略操作	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AWS WAF 经典操作列表，请参阅《服务授权参考》中的 “由地区定义的操作” AWS WAF和 “由 AWS WAF 区域定义的操作”。

AWS WAF Classic 中的策略操作在操作前使用以下前缀：

```
waf
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要在 AWS WAF Classic 中指定所有以开头的操作`List`，请包括以下操作：

```
"Action": "waf:List*"
```

要查看基于身份的 AWS WAF 经典策略的示例，请参阅。AWS WAF Classic 的基于身份的策略示例

C AWS WAF lassic 的策略资源

支持策略资源	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 AWS WAF 经典资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 “由区域定义的资源” AWS WAF和 “由 AWS WAF 区域定义的资源”。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅由区域定义的操作 AWS WAF和由区域定义的 AWS WAF 操作。要允许或拒绝访问部分 AWS WAF 经典资源，请在策略的`resource`元素中包含该资源的 ARN。

在 AWS WAF Classic 中，资源是 Web ACL 和规则。 AWS WAF Classic 还支持字节匹配、IP 匹配和大小限制等条件。

这些资源和条件关联有唯一 Amazon 资源名称 (ARN)，如下表所示。

AWS WAF 控制台中的名称	AWS WAF SDK/CLI 中的名称	ARN 格式
Web ACL	WebACL	arn:aws:waf:: *account*:*webacl*/*ID*
规则	Rule	arn:aws:waf:: *account*:*rule*/*ID*
字符串匹配条件	ByteMatchSet	arn:aws:waf:: *account*:*bytematchset* /*ID*
SQL 注入匹配条件	SqlInjectionMatchSet	arn:aws:waf:: *account*:*sqlinjectionset* /*ID*
大小约束条件	SizeConstraintSet	arn:aws:waf:: *account*:*sizeconstraintset* /*ID*
IP 匹配条件	IPSet	arn:aws:waf:: *account*:*ipset*/*ID*
跨站点脚本匹配条件	XssMatchSet	arn:aws:waf:: *account*:*xssmatchset* /*ID*

要允许或拒绝访问部分 AWS WAF 经典资源，请在策略的`resource`元素中包含该资源的 ARN。C AWS WAF lassic 的 ARN 格式如下：

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

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

- *##*：您的 ID AWS 账户。您必须指定值。
- *##*： AWS WAF 经典资源的类型。
- *ID*： AWS WAF 经典资源的 ID，或通配符 (*)，表示与指定资源关联的指定类型的所有资源。 AWS 账户

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

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

AWS WAF 经典版的策略条件密钥

支持特定于服务的策略条件键	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS WAF 经典条件键列表，请参阅《服务授权参考》中的条件密钥 AWS WAF和AWS WAF区域定义的资源。要了解您可以使用哪些操作和资源使用条件键，请参阅区域定义的操作 AWS WAF和由 AWS WAF区域定义的操作。

要查看基于身份的 AWS WAF 经典策略的示例，请参阅。AWS WAF Classic 的基于身份的策略示例

经典版中的 AWS WAF ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 搭配经典版 AWS WAF

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）和许多 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 Cl AWS WAF assic 中使用临时证书

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以

用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

AWS WAF 标准版的转发访问会话

支持转发访问会话 (FAS)	支持

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AWS WAF Classic 的服务角色

支持服务角色	支持

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 AWS WAF Classic 功能。仅当 AWS WAF Classic 提供相关指导时，才可编辑服务角色。

Classic 的 AWS WAF 服务相关角色

支持服务相关角色	支持

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 AWS WAF Classic 服务相关角色的详细信息，请参阅在 Classic 中使用服务相关角色 AWS WAF。

AWS WAF Classic 的基于身份的策略示例

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

默认情况下，用户和角色无权创建或修改 AWS WAF Classic 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关 C AWS WAF lassic 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 “区域” 中的操作、资源和条件键以及 AWS WAF 区域的操作、资源和条件键。 AWS WAF

主题

- 策略最佳实践
- 使用 AWS WAF 经典版控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 AWS WAF 经典资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略 或 工作职能的AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy 语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 AWS WAF 经典版控制台

要访问 AWS WAF Classic 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 AWS WAF Classic 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

可以访问和使用 AWS 控制台的用户也可以访问 AWS WAF 经典版控制台。无需额外权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

对 AWS WAF 经典身份和访问进行故障排除

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

使用以下信息来帮助您诊断和修复在使用 C AWS WAF lassic 和 IAM 时可能遇到的常见问题。

主题

我无权在 C AWS WAF lassic 中执行任何操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `waf:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `waf:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到错误消息，提示您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 AWS WAF Classic。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 AWS WAF Classic 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AWS WAF 经典版资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 AWS WAF Classic 是否支持这些功能，请参阅AWS WAF 经典版如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

在 Classic 中使用服务相关角色 AWS WAF

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF 经典用户 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色类型，直接关联到 CI AWS WAF assic。服务相关角色由 AWS WAF Classic 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可以更轻松地设置 AWS WAF Classic，因为您不必手动添加必要的权限。 AWS WAF Classic 定义了其服务相关角色的权限，除非另有定义，否则只有 AWS WAF Classic 可以担任其角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这样可以保护您的 AWS WAF 经典资源，因为您不能无意中删除访问这些资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

AWS WAF Classic 的服务相关角色权限

AWS WAF Classic 使用以下服务相关角色：

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic 使用这些与服务相关的角色将日志写入 Amazon Data Firehose。只有在启用登录功能后才会使用这些角色 AWS WAF。有关更多信息，请参阅 记录 Web ACL 流量信息。

`AWSServiceRoleForWAFLogging` 和 `AWSServiceRoleForWAFRegionalLogging` 服务相关角色（分别）信任以下服务以代入该角色：

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

角色的权限策略允许 AWS WAF Classic 对指定资源完成以下操作：

- 操作：`firehose:PutRecord`firehose:PutRecordBatch在 Amazon Data 上，Firehose 的数据流资源名称以 “aws-waf-logs-” 开头。例如，`aws-waf-logs-us-east-2-analytics`。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS WAF Classic 创建服务相关角色

您无需手动创建服务相关角色。当您在上启用 Classi AWS WAF c 登录 AWS Management Console，或者在 AWS WAF 经典 CLI 或经 AWS WAF 典 API 中`PutLoggingConfiguration`发出请求时，CI AWS WAF assic 会为您创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。启用 AWS WAF Classic 日志记录后， AWS WAF Classic 会再次为您创建服务相关角色。

编辑 AWS WAF Classic 的服务相关角色

AWS WAF Classic 不允许您编辑`AWSServiceRoleForWAFLogging`和`AWSServiceRoleForWAFRegionalLogging`服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除客户端 AWS WAF Classic 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时，C AWS WAF lassic 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除**`AWSServiceRoleForWAFLogging`**和使用的 AWS WAF 经典资源**`AWSServiceRoleForWAFRegionalLogging`**

1. 在 AWS WAF Classic 控制台上，删除每个 Web ACL 的日志记录。有关更多信息，请参阅 记录 Web ACL 流量信息。
2. 使用 API 或 CLI，为已启用日志记录的每个 Web ACL 提交 `DeleteLoggingConfiguration` 请求。有关更多信息，请参阅 AWS WAF Classic API 参考。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 `AWSServiceRoleForWAFLogging` 和 `AWSServiceRoleForWAFRegionalLogging` 服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

AWS WAF Classic 服务相关角色的受支持区域

AWS WAF Classic 支持在以下内容 AWS 区域中使用服务相关角色。

区域名称	区域标识	AWS WAF 经典版 Support
美国东部（弗吉尼亚州北部）	us-east-1	支持
美国东部（俄亥俄州）	us-east-2	支持
美国西部（北加利福尼亚）	us-west-1	支持
US West（Oregon）	us-west-2	支持
亚太地区（孟买）	ap-south-1	支持
亚太地区（大阪）	ap-northeast-3	支持
亚太地区（首尔）	ap-northeast-2	支持
亚太地区（新加坡）	ap-southeast-1	支持
亚太地区（悉尼）	ap-southeast-2	支持
亚太地区（东京)	ap-northeast-1	支持
加拿大（中部）	ca-central-1	支持
欧洲地区（法兰克福）	eu-central-1	支持
欧洲地区（爱尔兰）	eu-west-1	支持
欧洲地区（伦敦）	eu-west-2	支持
欧洲地区（巴黎）	eu-west-3	支持
南美洲（圣保罗）	sa-east-1	支持

在 AWS WAF 经典版中进行日志记录和监控

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

监控是维护 CI AWS WAF assic 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控您的 AWS WAF 经典资源和响应潜在事件的工具：

亚马逊 CloudWatch 警报

使用 CloudWatch 警报，您可以监视您指定的时间段内的单个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 AWS Auto Scaling 政策 CloudWatch 发送通知。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

AWS CloudTrail 日志

CloudTrail 提供用户、角色或 AWS 服务在 C AWS WAF lassic 中执行的操作的记录。使用收集的信息 CloudTrail，您可以确定向 C AWS WAF lassic 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。有关更多信息，请参阅 使用 记录 AWS CloudTrail API 调用。

AWS WAF 经典版合规性验证

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

  > **Note**
  >
  > 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。

- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS WAF 经典版中的韧性

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS WAF 经典版中的基础设施安全

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

作为一项托管服务， AWS WAF Classic 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 AWS WAF Classic。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

AWS WAF 经典配额

> **Note**
>
> 这是 AWS WAF Classic 文档。只有在 2019 年 11 月 AWS WAF 之前创建了 AWS WAF 资源（如规则和 Web ACL），并且尚未将其迁移到最新版本时，才应使用此版本。要迁移您的资源，请参阅将您的 AWS WAF 经典资源迁移到 AWS WAF。
> 有关的最新版本 AWS WAF，请参阅AWS WAF。

AWS WAF Classic 受以下配额限制（以前称为限制）。

AWS WAF Classic 对每个区域每个账户的实体数量有默认配额。您可以请求提高这些限额。

资源	每个区域每个账户的默认限额
Web ACL	50
规则	100
R ate-based-rules	5
每区域每账户的条件数	对于除正则表达式匹配和地理匹配之外的所有条件，每种条件类型为 100 个。例如，100 个大小限制条件和 100 个 IP 匹配条件。有关正则表达式和地理匹配条件，请参阅下表。

资源	每个区域每个账户的默认限额
每秒请求数	每个 web ACL 25,000 个*

*此配额仅适用于 Application Load Balancer 上的 AWS WAF Classic。C AWS WAF lassic 版的每秒请求数 (RPS) 配额与《CloudFront 开发者指南》中描述 CloudFront 的 RPS 配额支持相同。CloudFront

AWS WAF 经典实体的以下配额无法更改。

资源	每区域每账户的限额
每个 Web ACL 的规则组数	2：1 个客户创建的规则组和 1 个 AWS Marketplace 规则组
每个 Web ACL 的规则数	10
每个规则的条件数	10
每个 IP 匹配条件的 IP 地址范围数（以 CIDR 表示法显示）	10000 一次最多可更新 1,000 个地址。API 调用 `UpdateIPSet` 一次最多可接受 1,000 个地址。
根据基于速率的规则而阻止的 IP 地址	10000
每 5 分钟周期内基于速率规则的最小速率限制	100
每个跨站点脚本匹配条件的筛选条件数	10

资源	每区域每账户的限额
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 标头名称中的字符数，当您将 AWS WAF Classic 配置为检查 Web 请求中的标头是否有指定值时	40
在字符串匹配条件中，您希望 C AWS WAF lassic 搜索的值中的字符数	50
正则表达式匹配条件	10
在正则表达式匹配条件中，您希望 C AWS WAF lassic 在模式中搜索的字符数	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
模式集数	5
地理匹配条件	50
每个地理匹配条件的地理位置	50

AWS WAF Classic 对每个地区的每个账户的通话量有以下固定配额。这些配额适用于通过任何可用方式（包括控制台、CLI、REST API 和软件开发工具包）对服务的总调用。 AWS CloudFormation无法更改这些限额。

调用类型	每区域每账户的限额
调用 `AssociateWebACL` 的最大次数	每 2 秒 1 个请求
调用 `DisassociateWebACL` 的最大次数	每 2 秒 1 个请求
调用 `GetWebACLForResource` 的最大次数	每秒 1 个请求

调用类型	每区域每账户的限额
调用 ListResourcesForWebACL 的最大次数	每秒 1 个请求
调用 CreateWebACLMigrationStack 的最大次数	每秒 1 个请求
调用 GetChangeToken 的最大次数	每秒 10 个请求
调用 GetChangeTokenStatus 的最大次数	每秒 1 个请求
对任何单个 List 操作的最大调用次数（如果未为其定义其他限额）	每秒 5 个请求
对任何单个 Create、Put、Get 或 Update 操作的最大调用次数（如果未为其定义其他限额）	每秒 1 个请求

AWS Shield

针对分布式拒绝服务 (DDoS) 攻击的防护对于面向互联网的应用程序至关重要。在此基础上构建应用程序时 AWS，可以利用 AWS 提供的保护措施，无需支付额外费用。此外，您还可以使用 AWS Shield Advanced 托管威胁防护服务，通过其他 DDoS 检测、缓解和响应功能来改善您的安全状况。

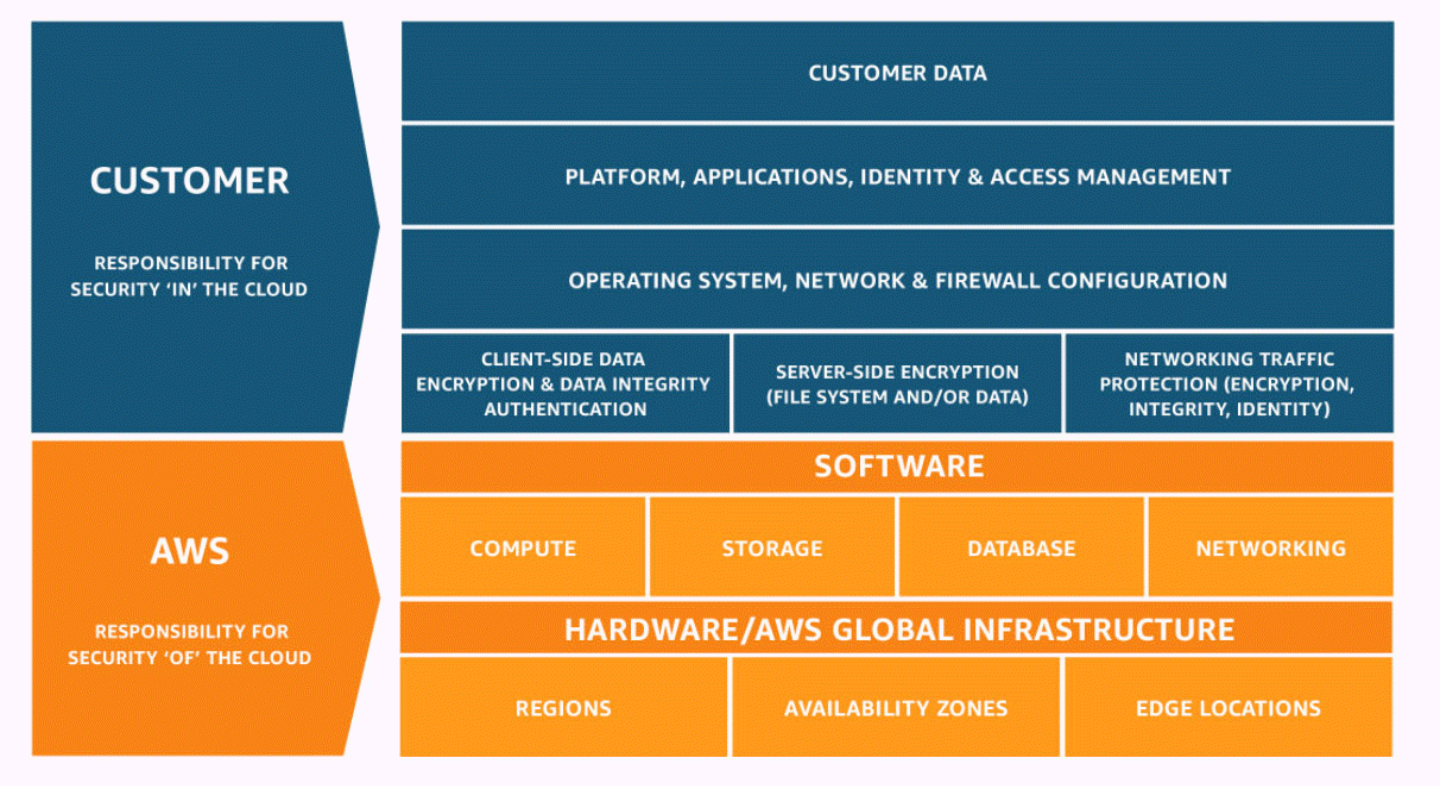
AWS 致力于为您提供工具、最佳实践和服务，以帮助确保高可用性、安全性和弹性，以防御互联网上的不良行为者。本指南旨在帮助 IT 决策者和安全工程师了解如何使用 Shield 和 Shield Advanced 来更好地保护其应用程序，使其免受 DDoS 攻击和其他外部威胁。

当你在其上构建应用程序时 AWS，你会获得自动保护， AWS 抵御常见的容量 DDoS 攻击向量，例如 UDP 反射攻击和 TCP SYN 洪水。您可以利用这些保护措施来设计和配置 DDoS 弹性架构， AWS 从而确保运行的应用程序的可用性。

本指南提供的建议可以帮助您设计、创建和配置应用程序架构，以实现 DDoS 弹性。当应用程序受到更大规模的 DDoS 攻击和更广泛的 DDoS 攻击向量时，遵守本指南中提供的最佳实践，则其可以从改进的可用性连续性中获益。此外，本指南还向您展示了如何使用 Shield Advanced 为您的关键应用程序实现优化的 DDoS 保护状态。其中包括您已保证为客户提供一定可用性的应用程序，以及在 DDoS 事件 AWS 期间需要运营支持的应用程序。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Shield Advanced 的合规性计划，请参阅合规性计划范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。



AWS Shield 和 Shield Advanced 的工作原

AWS Shield Standard 并针对网络和传输层（第 3 层和第 4 层）以及应用层（第 7 层）的 AWS 资源 AWS Shield Advanced 提供针对分布式拒绝服务 (DDoS) 攻击的保护。DDoS 攻击是一种攻击，在这种攻击中，多个受感染的系统试图向目标充斥流量。DDoS 攻击会阻止合法终端用户访问目标服务，并可能导致目标服务因流量过大而崩溃。

AWS Shield 提供针对各种已知的 DDoS 攻击向量和未修补攻击向量的保护。Shield 检测和缓解旨在提供针对威胁的覆盖范围，即使服务在检测时并未明确知道这些威胁。Shield Standard 是自动提供的，使用 AWS时不收取额外费用。

Shield 检测到的攻击类别包括：

- 网络容量攻击（第 3 层）：这是基础设施层攻击向量的子类别。这些向量试图使目标网络或资源的容量饱和，拒绝向合法用户提供服务。
- 网络协议攻击（第 4 层）：这是基础设施层攻击向量的子类别。这些向量滥用协议来拒绝向目标资源提供服务。网络协议攻击的一个常见示例是 TCP SYN 泛洪，它会耗尽服务器、负载均衡器或防火墙等资源的连接状态。网络协议攻击也可以是容量攻击。例如，较大的 TCP SYN 泛洪可能旨在使网络容量饱和，同时还会耗尽目标资源或中间资源的状态。

- 应用程序层攻击（第 7 层）：此类攻击向量试图通过向应用程序充斥对目标有效的查询（如 Web 请求泛洪）来拒绝向合法用户提供服务。

目录

AWS Shield Standard 概述

AWS Shield 是一项托管威胁防护服务，可保护应用程序的外围环境。外围是来自 AWS 网络外部的应用程序流量的第一个入口点。

要确定您的应用程序边界在哪里，请考虑用户如何从互联网访问您的应用程序。如果第一个入口点位于某个 AWS 区域，则应用程序边界就是您的亚马逊虚拟私有云 (VPC) VPC。如果用户通过 Amazon Route 53 定向到您的应用程序，并首先使用 Amazon CloudFront 或（或）访问该应用程序 AWS Global Accelerator，则应用程序边界将从 AWS 网络边缘开始。

Shield 为所有运行的应用程序提供 DDoS 检测和缓解优势 AWS，但是您在设计应用程序架构时做出的决策将影响您的 DDoS 弹性水平。DDoS 弹性是指您的应用程序在攻击期间继续在预期参数内运行的能力。

所有 AWS 客户均可享受Shield Standard的自动保护，无需额外付费。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 Shield Standard 有助于保护所有 AWS 客户，但您可以通过 Amazon Route 53 托管区域、亚马逊 CloudFront 分发和 AWS Global Accelerator 标准加速器获得特别的好处。这些资源可获得全面的可用性保护，抵御所有已知的网络和传输层攻击。

AWS Shield Advanced 概述

AWS Shield Advanced 是一项托管服务，可帮助您保护应用程序免受外部威胁，例如 DDoS 攻击、容量机器人和漏洞利用企图。要获得更高级别的攻击防护，您可以订购 AWS Shield Advanced。

当您订阅 Shield Advanced 并为您的资源添加保护时，Shield Advanced 会为这些资源提供扩展的 DDoS 攻击保护。根据您的架构和配置选择，您从 Shield Advanced 获得的保护可能会有所不同。使用本指南中的信息使用 Shield Advanced 构建和保护弹性应用程序，并在需要专家帮助时上报。

Shield 高级版订阅和 AWS WAF 费用

您的 Shield Advanced 订阅可支付使用标准 AWS WAF 功能来保护您使用 Shield Advanced 保护的资源的费用。Shield Advanced 保护所涵盖的标准 AWS WAF 费用包括每个 Web ACL 的费用、每条规则的费用以及每百万个 Web 请求检查的基本价格，最多 1,500 个 WCU，不超过默认主体尺寸。

启用 Shield Advanced 自动应用层 DDoS 缓解会向你的 Web ACL 中添加一个使用 150 个 Web ACL 容量单位 (WCU) 的规则组。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解、Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。

你对 Shield Advanced 的 AWS WAF 订阅不包括使用你无法使用 Shield Advanced 保护的资源。它也不包括受保护资源的任何额外非标准 AWS WAF 成本。非标准 AWS WAF 成本的示例包括 Bot Control、CAPTCHA规则操作、使用超过 1,500 个 WCU 的 Web ACL 以及检查超出默认正文大小的请求正文。完整列表在 AWS WAF 定价页面上提供。

有关完整信息和定价示例，请参阅 Shield 定价和 AWS WAF 定价。

Shield Advanced 订阅账单

如果您是 AWS 渠道经销商，请与您的客户团队联系以获取信息和指导。此账单信息适用于非 AWS 渠道经销商的客户。

对于所有其他订阅和计费指南，则适用以下订阅和计费指南：

- 对于属于 AWS Organizations 组织成员的账户，无论付款人账户本身是否已订阅，都要从该组织的付款人账户中扣除 Shield Advanced 订阅 AWS 费用。
- 当您订阅属于同一个AWS Organizations 整合账单账户系列的多个账户时，该系列中所有已订阅的账户适用一个订阅价格。组织必须拥有其所有 AWS 账户 和所有资源。
- 当您为多个组织订阅多个账户时，如果您拥有所有组织、账户和资源，您可以用一笔订阅费支付所有组织、账户和资源的费用。请联系您的客户经理或 AWS 支持人员，申请免除其中一个组织以外的所有组织的 AWS Shield Advanced 订阅费用。

有关定价信息和示例的详细信息，请参阅 AWS Shield 定价。

主题

AWS Shield Advanced 受保护的资源

> **Note**
>
> 只有你在 Shield Advanced 中明确指定的资源或通过 Shield Advanced 策略保护的资源才会启用 AWS Firewall Manager Shield 高级保护。Shield Advanced 不会自动保护您的资源。

您可以使用 Shield Advanced 对以下资源类型进行高级监控和保护：

- 亚马逊 CloudFront 配送。为了 CloudFront 持续部署，Shield Advanced 可以保护与受保护的主发行版关联的所有暂存分发。
- Amazon Route 53 托管区。
- AWS Global Accelerator 标准加速器。
- Amazon EC2 弹性 IP 地址 Shield Advanced 可保护与受保护的弹性 IP 地址关联的资源。
- Amazon EC2 实例，通过 Amazon EC2 弹性 IP 地址的关联。
- 以下弹性负载均衡（ELB）负载均衡器：
  - 应用程序负载均衡器。

- 经典负载均衡器。
- 网络负载均衡器，通过与 Amazon EC2 弹性 IP 地址的关联。

有关这些资源类型保护的更多信息，请参阅 AWS Shield Advanced 按资源类型划分的保护。

AWS Shield Advanced 功能和选项

AWS Shield Advanced 订阅包括以下功能和选项。它们补充了您已经获得的 DDoS 检测和缓解功能。AWS

- AWS WAF 集成 — Shield Advanced 使用 AWS WAF Web ACL、规则和规则组作为其应用层保护的一部分。有关的更多信息 AWS WAF，请参阅如何 AWS WAF 运作。

  > **Note**
  >
  > 您的 Shield Advanced 订阅可支付使用标准 AWS WAF 功能来保护您使用 Shield Advanced 保护的资源的费用。Shield Advanced 保护所涵盖的标准 AWS WAF 费用包括每个 Web ACL 的费用、每条规则的费用以及每百万个 Web 请求检查的基本价格，最多 1,500 个 WCU，不超过默认主体尺寸。
  >
  > 启用 Shield Advanced 自动应用层 DDoS 缓解会向你的 Web ACL 中添加一个使用 150 个 Web ACL 容量单位 (WCU) 的规则组。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解、Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。
  >
  > 你对 Shield Advanced 的 AWS WAF 订阅不包括使用你无法使用 Shield Advanced 保护的资源。它也不包括受保护资源的任何额外非标准 AWS WAF 成本。非标准 AWS WAF 成本的示例包括 Bot Control、CAPTCHA规则操作、使用超过 1,500 个 WCU 的 Web ACL 以及检查超出默认正文大小的请求正文。完整列表在 AWS WAF 定价页面上提供。
  >
  > 有关完整信息和定价示例，请参阅 Shield 定价和 AWS WAF 定价。

- 应用程序层 DDoS 自动缓解：您可以将 Shield Advanced 配置为自动响应，以缓解对受保护资源的应用程序层（第 7 层）攻击。通过自动缓解，Shield Advanced 对来自已知 DDoS 来源的请求强制执行 AWS WAF 速率限制，并自动添加和管理自定义 AWS WAF 保护以应对检测到的 DDoS 攻击。您可以配置自动缓解以计算或阻止作为攻击一部分的 Web 请求。

  有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

- 运行状况检测：您可以将 Amazon Route 53 运行状况检查与 Shield Advanced 结合使用，为事件检测和缓解提供信息。Health checks 会根据您的规格监控您的应用程序，在满足您的规格时报告运行

状况正常，不符合规格时报告运行状况不佳。在 Shield Advanced 中使用运行状况检查有助于防止误报，并在受保护的资源状况不佳时更快地进行检测和缓解。您可以对除 Route 53 托管区域之外的任何资源类型使用运行状况检测。Shield Advanced 主动交互仅适用于启用了运行状况检测的资源。

有关更多信息，请参阅 使用运行状况检查进行基于运行状况的检测。

- 保护组：您可以使用保护组来创建受保护资源的逻辑分组，以增强对整个组的检测和缓解。您可以定义保护组成员资格的条件，以便自动包括新受保护的资源。受保护资源可归属于多个保护组。

  有关更多信息，请参阅 AWS Shield Advanced 保护小组。

- 增强对 DDoS 事件和攻击的可见性：Shield Advanced 允许您访问高级的实时指标和报告，从而全面了解受保护 AWS 资源的事件和攻击。您可以通过 Shield Advanced API 和控制台以及亚马逊 CloudWatch 指标访问这些信息。

  有关更多信息，请参阅 对 DDoS 事件的可见性。

- 通过 AWS Firewall Manager集中管理 Shield Advanced 保护：您可以使用 Firewall Manager 自动对您的新账户和资源应用 Shield Advanced 保护，并将 AWS WAF 规则部署到您的 Web ACL。Firewall Manager Shield Advanced 保护策略包含在内，Shield Advanced 客户无需额外付费。您还可以使用带有 Amazon Simple Notification Service (SNS) 主题或 AWS Security Hub的 Firewall Manager 为您的账户集中管理 Shield Advanced 监控活动或。

  有关使用 Firewall Manager 管理 Shield Advanced 保护的更多信息，请参阅 AWS Firewall Manager 和 AWS Shield Advanced 政策。有关 Firewall Manager 定价的更多信息，请参阅 AWS Firewall Manager 定价。

- AWS Shield Response Team (SRT) — SRT 在保护 AWS亚马逊及其子公司方面拥有丰富的经验。作为 AWS Shield Advanced 客户，在影响应用程序可用性的 DDoS 攻击期间，您可以随时联系 SRT 寻求帮助。您还可以使用 SRT 为您的资源创建和管理自定义缓解措施。要使用 SRT 的服务，您还必须订阅 Business Support Plan或企业支持计划。

  有关更多信息，请参阅 Shield 响应小组 (SRT) 支持。

- 主动参与：通过主动参与，如果您与受保护资源关联的 Amazon Route 53 运行状况检查在 Shield Advanced 检测到的事件中显示状况不佳，则 Shield 响应团队 (SRT) 会直接与您联系。这样一来，当您的应用程序可用性可能受到疑似攻击影响时，您可以更快地与专家联系。

  有关更多信息，请参阅 配置主动参与。

- 成本保护机会 — Shield Advanced 提供了一些成本保护，可抵御因针对受保护资源的 DDoS 攻击而导致 AWS 账单激增。这可能包括对 Shield Advanced 数据传出 (DTO) 使用费峰值的保障。Shield Advanced 以 Shield Advanced 服务积分的形式提供任何成本保护。

有关更多信息，请参阅 申请积分 AWS Shield Advanced。

决定是否订阅 AWS Shield Advanced 和应用其他保护

请查看本节中的场景，以帮助决定哪些账户应订阅 AWS Shield Advanced 以及在何处应用其他保护。使用 Shield Advanced，您只需为整合账单账户下创建的所有账户支付月度订阅费，外加根据传出的数据量 GB 计算的使用费。有关 Shield Advanced 定价的信息，请参阅 AWS Shield Advanced 定价。

要使用 Shield Advanced 保护应用程序及其资源，您需要将管理该应用程序的账户订阅到 Shield Advanced，然后为应用程序的资源添加保护。有关订阅账户和保护资源的信息，请参阅 入门 AWS Shield Advanced。

Shield 高级版订阅和 AWS WAF 费用

您的 Shield Advanced 订阅可支付使用标准 AWS WAF 功能来保护您使用 Shield Advanced 保护的资源的费用。Shield Advanced 保护所涵盖的标准 AWS WAF 费用包括每个 Web ACL 的费用、每条规则的费用以及每百万个 Web 请求检查的基本价格，最多 1,500 个 WCU，不超过默认主体尺寸。

启用 Shield Advanced 自动应用层 DDoS 缓解会向你的 Web ACL 中添加一个使用 150 个 Web ACL 容量单位 (WCU) 的规则组。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解、Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。

你对 Shield Advanced 的 AWS WAF 订阅不包括使用你无法使用 Shield Advanced 保护的资源。它也不包括受保护资源的任何额外非标准 AWS WAF 成本。非标准 AWS WAF 成本的示例包括机器人控制、CAPTCHA规则操作、使用超过 1,500 个 WCU 的 Web ACL 以及检查超出默认正文大小的请求正文。完整列表在 AWS WAF 定价页面上提供。

有关完整信息和定价示例，请参阅 Shield 定价和 AWS WAF 定价。

Shield Advanced 订阅账单

如果您是 AWS 渠道经销商，请咨询您的客户团队以获取信息和指导。此账单信息适用于非 AWS 渠道经销商的客户。

对于所有其他订阅和计费指南，则适用以下订阅和计费指南：

- 对于属于 AWS Organizations 组织成员的账户，无论付款人账户本身是否已订阅，都要从该组织的付款人账户中扣除 Shield Advanced 订阅 AWS 费用。

- 当您订阅属于同一个AWS Organizations 整合账单账户系列的多个账户时，该系列中所有已订阅的账户适用一个订阅价格。组织必须拥有其所有 AWS 账户 和所有资源。
- 当您为多个组织订阅多个账户时，如果您拥有所有组织、账户和资源，您可以用一笔订阅费支付所有组织、账户和资源的费用。请联系您的客户经理或 AWS 支持人员，申请免除其中一个组织以外的所有组织的 AWS Shield Advanced 订阅费用。

有关定价信息和示例的详细信息，请参阅 AWS Shield 定价。

确定要保护的应用程序

考虑为需要以下任何一项的应用程序实施 Shield Advanced 保护：

- 保证应用程序用户的可用性。
- 如果应用程序受到 DDoS 攻击的影响，可以快速联系 DDoS 缓解专家。
- 意识到应用程序可能受 AWS 到 DDoS 攻击的影响，并向您的安全或运营团队发出攻击通知 AWS 并升级到您的安全或运营团队。
- 云成本的可预测性，包括 DDoS 攻击何时影响您的 AWS 服务使用。

如果应用程序或其资源需要上述任何一项，请考虑为相关账户创建订阅。

确定要保护的资源

对于每个订阅的账户，可以考虑为每个具有以下任一特征的资源添加 Shield Advanced 保护：

- 该资源为互联网上的外部用户提供服务。
- 该资源暴露在互联网上，也是关键应用程序的一部分。考虑每一个暴露的资源，无论您是否打算让互联网上的用户访问这些资源。
- 该资源受到 AWS WAF Web ACL 的保护。

要了解有关为资源创建和管理保护措施的更多信息，请参阅 中的资源保护 AWS Shield Advanced

此外，请按照本指南中的建议进行操作，以帮助确保您的应用程序能够实现 DDoS 弹性，并正确配置 Shield Advanced 的功能以获得最佳保护。

DDoS 攻击示例

AWS Shield Advanced 提供针对多种类型攻击的扩展保护。

以下列表描述了一些常见的攻击类型：

用户数据报协议 (UDP) 反射攻击

在 UDP 反射攻击中，攻击者能够仿冒请求来源，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，并阻止合法最终用户访问所需资源。

TCP SYN 泛洪

TCP 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 TCP SYN 数据包。服务器将返回确认，客户端将返回自己的确认，完成三次握手。在 TCP SYN 泛洪中，永远不会返回第三个确认，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 查询洪水中，攻击者使用多个 DNS 查询耗尽 DNS 服务器的资源。 AWS Shield Advanced 可以帮助抵御对 Route 53 DNS 服务器的 DNS 查询洪水攻击。

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。

如何 AWS Shield 检测事件

AWS 为 AWS 网络和个别 AWS 服务运行服务级别检测系统，以确保它们在 DDoS 攻击期间保持可用。此外，资源级检测系统会监控每个单独的 AWS 资源，以确保流向该资源的流量保持在预期参数之内。这种组合通过应用缓解措施来保护目标 AWS 资源和 AWS 服务，这些缓解措施可以丢弃已知的错误数据包，突出显示潜在的恶意流量，并优先考虑来自最终用户的流量。

检测到的事件显示在您的 Shield Advanced 事件摘要、攻击详情和 Amazon CloudWatch 指标中，要么作为 DDoS 攻击向量的名称，`Volumetric`要么就好像评估基于流量而不是签名一样。有关该`DDoSDetected` CloudWatch指标中可用的攻击向量维度的更多信息，请参阅 AWS Shield Advanced 指标

主题

- 基础设施层威胁的检测逻辑

- 应用程序层威胁检测逻辑
- 应用程序中多个资源的检测逻辑

基础设施层威胁的检测逻辑

用于保护目标 AWS 资源免受基础设施层（第 3 层和第 4 层）中 DDoS 攻击的检测逻辑取决于资源类型以及是否使用 AWS Shield Advanced保护资源。

检测亚马逊 CloudFront 和亚马逊 53 号公路

当您使用 CloudFront 和 Route 53 为 Web 应用程序提供服务时，该应用程序的所有数据包都将由完全内联的 DDoS 缓解系统进行检查，该系统不会引入任何可观察到的延迟。实时缓解了针对 CloudFront 分布和 Route 53 托管区域的 DDoS 攻击。无论您是否使用 AWS Shield Advanced，这些保护措施都适用。

尽可能遵循使用 CloudFront 和 Route 53 作为 Web 应用程序入口点的最佳实践，以最快地检测和缓解 DDoS 事件。

检测 AWS Global Accelerator 和区域服务

资源级检测可保护 AWS Global Accelerator 标准加速器和在 AWS 区域中启动的资源，例如经典负载均衡器、应用程序负载均衡器和弹性 IP 地址 (EIP)。监控到这些资源类型的流量上升情况，可能表明存在需要缓解的 DDoS 攻击。每分钟都会评估每种 AWS 资源的流量。如果资源流量增加，则会执行其他检查以测量该资源的容量。

Shield 会执行以下标准检查：

- Amazon Elastic Compute Cloud (Amazon EC2) 实例、附加到Amazon EC2 实例的 EIP：Shield 会从受保护资源检索容量。容量取决于目标的实例类型、实例大小和其他因素，例如实例是否使用增强联网。
- 经典负载均衡器和应用程序负载均衡器：Shield 从目标负载均衡器节点检索容量。
- 连接到网络负载均衡器的 EIP：Shield 从目标负载均衡器检索容量。容量与目标负载均衡器的组配置无关。
- AWS Global Accelerator 标准加速器 — Shield 根据端点配置检索容量。

这些评估跨网络流量的多个维度进行，例如端口和协议。如果超过目标资源的容量，Shield 会实施 DDoS 缓解措施。Shield 采取的缓解措施将减少 DDoS 流量，但可能无法将其消除。如果在与已知的

DDoS 攻击向量一致的流量维度上超过资源容量的一小部分，Shield 也可以采取缓解措施。Shield 将这种缓解设置为有限生存时间 (TTL)，只要攻击仍在继续，它就会延长该缓解措施。

> **Note**
>
> Shield 采取的缓解措施将减少 DDoS 流量，但可能无法将其消除。您可以使用诸如 AWS Network Firewall 或主机防火墙之类的解决方案来增强 Shield，iptables以防止您的应用程序处理对您的应用程序无效或不是由合法最终用户生成的流量。

Shield Advanced 保护在现有的 Shield 检测活动中增加了以下内容：

- 降低检测阈值：Shield Advanced 将缓解措施设置为计算容量的一半。这可以更快地缓解上升速度较慢的攻击，并缓解体量特征较为模糊的攻击。
- 间歇性攻击防护：Shield Advanced 根据攻击的频率和持续时间，将缓解的生存时间 (TTL) 以指数形式递增。当资源经常成为攻击目标以及攻击发生在短时间内时，这可以延长缓解措施的持续时间。
- 运行状况检测：将 Route 53 运行状况检查与 Shield Advanced 受保护的资源关联时，将在检测逻辑中使用运行状况检查的状态。在检测到的事件中，如果运行状况检查显示状况正常，Shield Advanced 需要进一步确信该事件是攻击，才会采取缓解措施。相反，如果运行状况检查显示状况不佳，Shield Advanced 可能会在确信之前就采取缓解措施。此功能有助于避免误报，并且可以更快地对影响应用程序的攻击做出反应。有关使用 Shield Advanced 进行运行状况检查的信息，请参阅 使用运行状况检查进行基于运行状况的检测。

应用程序层威胁检测逻辑

AWS Shield Advanced 为受保护的 Amazon CloudFront 分配和应用程序负载均衡器提供 Web 应用程序层检测。使用 Shield Advanced 保护这些资源类型时，可以将 AWS WAF Web ACL 与保护关联起来，以启用 Web 应用程序层检测。Shield Advanced 使用关联的 Web ACL 的请求数据，并为您的应用程序构建流量基准。Web 应用程序层检测依赖于 Shield Advanced 和 AWS WAF。要详细了解应用层保护，包括将 AWS WAF Web ACL 与 Shield Advanced 受保护的资源相关联，请参阅AWS Shield Advanced 应用层（第 7 层）保护。

对于 Web 应用程序层检测，Shield Advanced 会监控应用程序流量，并将其与历史基线进行比较，以查找异常情况。这种监控涵盖了总流量和流量构成。在 DDoS 攻击期间，我们预计流量的数量和组成都会发生变化，而 Shield Advanced 需要这两者都出现统计意义上的显著偏差才能宣布事件发生。

Shield Advanced 根据历史时间窗口进行测量。这种方法可以减少因流量的合理变化或符合预期模式的流量变化（如每天同一时间的促销活动）而产生的误报。

> **Note**
>
> 让 Shield Advanced 有时间建立代表正常、合法流量模式的基准，从而避免在 Shield Advanced 保护中出现误报。当你将 Web ACL 与受保护的资源关联时，Shield Advanced 开始收集其基准信息。在任何可能导致网络流量异常模式的计划事件发生前至少 24 小时将 Web ACL 与您的受保护资源关联。Shield Advanced Web 应用程序层检测在观察到 30 天正常流量时最为准确。

Shield Advanced 检测事件所花费的时间受其观察到的流量变化程度的影响。对于较小的流量变化，Shield Advanced 会进行较长时间的流量观测，以确定事件的发生。对于较大的流量变化，Shield Advanced 可以更快地检测和报告事件。

Web ACL 中基于速率的规则，无论是您添加的还是由 Shield Advanced 自动应用层缓解功能添加的，都可以在攻击达到可检测级别之前对其进行缓解。有关自动应用层 DDoS 缓解的更多信息，请参阅Shield Advanced 应用程序层 DDoS 自动缓解。

> **Note**
>
> 您可以设计您的应用程序，使其能够根据流量或负载的增加进行扩展，从而帮助确保它不会受到较小的请求泛滥的影响。使用 Shield Advanced，您的受保护资源将受到成本保护。这有助于防止因 DDoS 攻击而导致云账单意外增加。要了解有关 Shield Advanced 成本保护的更多信息，请参阅 申请积分 AWS Shield Advanced。

应用程序中多个资源的检测逻辑

您可以使用 AWS Shield Advanced 保护组来创建属于同一应用程序的受保护资源的集合。您可以选择在保护组中放置哪些受保护的资源，也可以指明应将相同类型的所有资源视为一个组。例如，您可以创建一个由所有应用程序负载均衡器组成的组。创建保护组时，Shield Advanced 检测会聚合组内受保护资源的所有流量。如果您有许多资源，每个资源都有少量流量，但聚合量很大，则此功能非常有用。对于在受保护资源之间传输流量的蓝绿部署，您也可以使用保护组来保留应用程序基准。

您可以选择通过以下一种方式聚合保护组中的流量：

- 总计：此聚合将合并保护组中所有资源间的流量。您可以使用此聚合来确保新创建的资源具有现有基准并降低检测敏感度，这有助于防止误报。
- 平均值：此聚合使用保护组中所有流量的平均值。您可以将此聚合用于资源间流量均匀的应用程序，例如负载均衡器。

- 最大：该聚合使用保护组中任何资源的最高流量。当一个保护组中有多个应用程序层时，您可以使用此聚合。例如，您的保护组可能包括 CloudFront 分配、其应用程序负载均衡器来源和应用程序负载均衡器的 Amazon EC2 实例目标。

对于针对多个面向互联网的弹性 IP 或 AWS Global Accelerator 标准加速器的攻击，您还可以使用保护组来提高 Shield Advanced 设置缓解措施的速度。当保护组中的一个资源成为目标时，Shield Advanced 会建立对该组中其他资源的信心。这会使 Shield Advanced 检测处于警戒状态，并可以缩短创建额外缓解措施所需的时间。

要详细了解保护组，请参阅 AWS Shield Advanced 保护小组。

如何 AWS Shield 缓解事件

保护应用程序的缓解逻辑可能因应用程序架构而异。当您使用 Amazon CloudFront 和 Amazon Route 53 保护网络应用程序时，您将受益于特定于 Web 和 DNS 用例的缓解措施，这些缓解措施可以保护服务的所有流量。当您的应用程序的入口点是在某个 AWS 区域中运行的资源时，缓解逻辑会因服务、资源类型和您的使用情况而异 AWS Shield Advanced。

AWS DDoS 缓解系统由 Shield 工程师开发，它们与 AWS 服务紧密集成。工程师会考虑架构的各个方面，例如目标资源的容量和运行状况。Shield 工程师持续监控 DDoS 缓解系统的功效和性能，并能够在发现或预计到新威胁时快速做出响应。

您可以设计您的应用程序，使其能够根据流量或负载的增加进行扩展，从而帮助确保它不会受到较小的请求泛洪的影响。如果您使用 Shield Advanced 来保护您的资源，则可以防止由于 DDoS 攻击而造成的云账单意外增加。

基础设施缓解

对于基础设施层攻击， AWS Shield DDoS 缓解系统存在于 AWS 网络边界和边 AWS 缘位置。在整个 AWS 基础架构中放置多个级别的安全控制 defense-in-depth 可为您的云应用程序提供支持。

Shield 在所有来自互联网的入口点维护 DDoS 缓解系统。当 Shield 检测到 DDoS 攻击时，对于每个入口点，它都会通过位于相同位置的 DDoS 缓解系统重新路由流量。这不会带来任何可观察到的额外延迟，并且在所有 AWS 区域和所有边缘位置提供了超过 TeraBits 每秒 100 (Tbps) 的缓解能力。Shield 可以保护您的资源可用性，而无需将流量重新路由到外部或远程清理中心，这可能会增加延迟。

- 在 AWS 网络边界，对于任何 AWS 服务或资源，DDoS 缓解系统可以缓解来自互联网的基础设施层攻击。当 Shield Response Team (SRT) 的工程师发出信号时，系统会执行缓解措施。
- 在 AWS 边缘位置，DDoS 缓解系统会持续检查转发到亚马逊 CloudFront 分配和 Amazon Route 53 托管区域的每个数据包，无论其来源如何。必要时，系统会应用专为 Web 和 DNS 流量设计的

缓解措施。使用 Amazon CloudFront 和 Amazon Route 53 保护您的网络应用程序的另一个好处是，DDoS 攻击可以立即缓解，而无需从 Shield 检测中发出信号。

应用程序层缓解措施

Shield Advanced 为启用了 Shield Advanced 保护的亚马逊 CloudFront 分配和应用程序负载均衡器提供 Web 应用程序层缓解措施。启用保护后，可以将 AWS WAF Web ACL 与资源关联，以启用 Web 应用程序层检测。此外，您可以选择启用自动应用程序层缓解，这将指示 Shield Advanced 在 DDoS 攻击期间为您管理保护。

Shield 仅为针对已启用 Shield Advanced 和自动应用层缓解的资源的应用层攻击提供自定义缓解措施。通过自动缓解，Shield Advanced 对来自已知 DDoS 来源的请求强制执行 AWS WAF 速率限制，并自动添加和管理自定义 AWS WAF 保护以应对检测到的 DDoS 攻击。有关此类缓解措施的详细信息，请参阅 Shield Advanced 如何管理自动缓解。

Web ACL 中基于速率的规则，无论是您添加的还是由 Shield Advanced 自动应用层缓解功能添加的，都可以在攻击达到可检测级别之前对其进行缓解。有关检测的更多信息，请参阅应用程序层威胁检测逻辑。

缓解功能

AWS Shield DDoS 缓解的主要功能如下：

- 数据包验证：可确保每个被检查的数据包都符合预期的结构，并且对其协议有效。支持的协议验证包括 IP、TCP（包括标头和选项）、UDP、ICMP、DNS 和 NTP。
- 访问控制列表（ACL）和整形器：ACL 根据特定属性评估流量，要么丢弃匹配的流量，要么将其映射到整形器。整形器限制匹配流量的数据包速率，丢弃多余的数据包以容纳到达目的地的容量。AWS Shield 检测和 Shield Response Team (SRT) 工程师可以为预期流量提供专用的速率分配，并对属性与已知 DDoS 攻击向量匹配的流量进行更严格的速率分配。ACL 可以匹配的属性包括端口、协议、TCP 标志、目标地址、来源国家和数据包负载中的任意模式。
- 怀疑评分：这利用 Shield 对预期流量的了解来对每个数据包进行分数。与已知良好流量模式更接近的数据包会被赋予较低的可疑分数。观察已知的不良流量属性可能会增加数据包的可疑分数。当需要对数据包进行速率限制时，Shield 会先丢弃可疑分数较高的数据包。这有助于 Shield 缓解已知和未修补的 DDoS 攻击，同时避免误报。
- TCP SYN 代理：它通过发送 TCP SYN Cookie 来挑战新连接，然后再允许它们传递到受保护的服务，从而防止 TCP SYN 泛洪。Shield DDoS 缓解措施提供的 TCP SYN 代理是无状态的，这使其能够在不达到状态耗尽的情况下缓解已知最大的 TCP SYN 泛洪攻击。这是通过与 AWS 服务集成以移

交连接状态来实现的，而不是在客户端和受保护的服务之间维护持续的代理。TCP SYN 代理目前在亚马逊 CloudFront 和亚马逊 Route 53 上可用。

- 速率分布：这会根据流向受保护资源的流量的入口模式不断调整每个位置的整形器值。这样可以防止对可能无法均匀进入 AWS 网络的客户流量进行速率限制。

AWS Shield CloudFront 和 Route 53 的缓解逻辑

Shield DDoS 缓解措施会持续检查 53 号公路 CloudFront 的流量。这些服务在全球分布的 AWS 边缘网络上运行，使您可以广泛访问Shield的DDoS缓解能力，并通过更接近最终用户的基础设施交付应用程序。

- CloudFront— Shield DDoS 缓解措施仅允许对网络应用程序有效的流量通过该服务。这可以自动防范许多常见的 DDoS 向量，例如 UDP 反射攻击。

  CloudFront 保持与应用程序来源的持续连接，通过与 Shield TCP SYN 代理功能集成，TCP SYN 洪水会自动缓解，传输层安全 (TLS) 在边缘终止。这些组合功能可确保您的应用程序源仅接收格式正确的 Web 请求，并保护其免受低层 DDoS 攻击、连接泛洪和 TLS 滥用的侵害。

  CloudFront 结合使用 DNS 流量方向和任播路由。这些技术通过缓解靠近源头的攻击，提供故障隔离以及确保访问容量以缓解已知最大规模的攻击，从而提高应用程序的弹性。
- Route 53：Shield 缓解措施仅允许有效的 DNS 请求到达服务。Shield 使用可疑评分来缓解 DNS 查询泛洪，该评分会优先考虑已知良好的查询，并降低包含可疑或已知 DDoS 攻击属性的查询的优先级。

  Route 53 使用随机分片为每个托管区域（包括 IPv4 和 IPv6）提供一组唯一的四个解析器 IP 地址。每个 IP 地址对应于 Route 53 位置的不同子集。每个位置子集都由权威 DNS 服务器组成，这些服务器仅与任何其他子集中的基础设施部分重叠。这样可以确保如果用户查询因任何原因失败，则在重试时将成功提供该查询。

  Route 53 使用任播路由，根据网络邻近程度，将 DNS 查询定向到最近的边缘站点。任播还将 DDoS 流量分散到许多边缘站点，从而防止攻击集中在单个位置。

除了缓解速度外， CloudFront 53号公路还为Shield的全球分布容量提供了广泛的访问权限。要利用这些功能，请将这些服务用作动态或静态 Web 应用程序的入口点。

要了解有关使用 CloudFront 和 Route 53 保护 Web 应用程序的更多信息，请参阅如何使用亚马逊 CloudFront 和 Amazon Route 53 帮助保护动态 Web 应用程序免受 DDoS 攻击。要了解有关 Route 53 故障隔离的更多信息，请参阅全局故障隔离案例研究。

AWS ShieldAWS 区域的缓解逻辑

在 AWS 区域中启动的资源受到 Shield 资源级检测放置的 AWS Shield DDoS 缓解系统的保护。区域资源包括弹性 IP (EIP)、经典负载均衡器和应用程序负载均衡器。

在设置缓解措施之前，Shield 会识别目标资源及其容量。Shield 使用容量来确定其缓解措施应允许转发到资源的最大总流量。访问控制列表（ACL）和缓解措施中的其他整形器可能会减少某些流量的允许流量，例如与已知的 DDoS 攻击向量匹配或预计不会出现大量流量的流量。这进一步限制了缓解措施允许进行 UDP 反射攻击或具有 TCP SYN 或 FIN 标志的 TCP 流量所允许的流量。

Shield 会根据每种资源类型确定容量和缓解措施。

- 对于 Amazon EC2 实例或附加到 Amazon EC2 实例的 EIP，Shield 会根据实例类型和其他实例属性（例如该实例是否启用了增强联网功能）来计算容量。
- 对于应用程序负载均衡器或经典负载均衡器，Shield 会单独计算负载均衡器中每个目标节点的容量。这些资源的 DDoS 攻击缓解措施结合了 Shield DDoS 缓解措施和负载均衡器的自动扩展。当 Shield Response Team 对应用程序负载均衡器或经典负载均衡器资源进行攻击时，作为一项额外的保护措施，他们可能会加速扩展。
- Shield 根据底层 AWS 基础设施的可用容量计算某些 AWS 资源的容量。这些资源类型包括网络负载均衡器 (NLB) 和通过网关负载均衡器或路由流量的资源。 AWS Network Firewall

> **Note**
>
> 通过连接受 Shield Advanced 保护的 EIP 来保护您的网络负载均衡器。您可以与 SRT 合作，根据底层应用程序的预期流量和容量构建自定义缓解措施。

当 Shield 设置缓解措施时，Shield 在缓解逻辑中定义的初始速率限制将平等地应用于每个 Shield DDoS 缓解系统。例如，如果 Shield 将缓解措施设定为每秒 100,000 个数据包 (pps) 的限制，则它最初将允许在每个位置使用 100,000 pps。然后，Shield 会持续汇总缓解指标以确定实际流量比率，并使用该比率来调整每个位置的速率限制。这样可以防止误报，并确保缓解措施不会过于宽松。

AWS ShieldAWS Global Accelerator 标准加速器的缓解逻辑

Shield Advanced 缓解措施将只允许有效的流量到达 Global Accelerator 标准加速器的侦听器端点。标准加速器在全球范围内部署，它们为您提供 IP 地址，您可以使用这些地址将流量路由到任何 AWS 地区的 AWS 资源。Shield 为缓解全局加速器而实施的速率限制基于标准加速器将流量路由到的资源容

量。当总流量超过确定的速率时，以及已知的 DDoS 向量超过该速率的一小部分时，Shield 会采取缓解措施。

配置标准加速器时，您需要为每个 AWS 区域定义端点组，您将在其中为应用程序路由流量。当 Shield 设置缓解措施时，它会计算每个端点组的容量，并相应地更新每个 Shield DDoS 缓解系统的速率限制。根据Shield对流量将如何从互联网路由到您的 AWS 资源的假设，每个位置的费率各不相同。端点组的容量计算方法是组中的资源数量乘以组中任何资源的最低容量。Shield 会定期重新计算应用程序的容量，并根据需要更新速率限制。

> **Note**
>
> 使用流量拨号来更改定向到端点组的流量百分比不会改变 Shield 计算速率限制或向其 DDoS 缓解系统分配速率限制的方式。如果您使用流量拨号，请将您的端点组配置为在资源类型和数量方面相互镜像。这有助于确保 Shield 计算出的容量代表为您的应用程序提供流量的资源。

有关全局加速器中的端点组和流量拨号的更多信息，请参阅 AWS Global Accelerator 标准加速器中的端点组。

AWS Shield Advanced 弹性 IP 的缓解逻辑

当你使用保护弹性 IP (EIP) 时 AWS Shield Advanced，Shield Advanced 会增强 Shield 在 DDoS 事件期间采取的缓解措施。Shield Advanced DDoS 缓解系统会复制与 EIP 关联的公有子网的网络 ACL (NACL) 配置。例如，如果您的 NACL 配置为阻止所有 UDP 流量，Shield Advanced 会将该规则合并到 Shield 放置的缓解措施中。

这项附加功能可以帮助您避免由于流量对您的应用程序无效而导致的可用性风险。您还可以使用 NACL 来阻止单个源 IP 地址或源 IP 地址 CIDR 范围。对于非分布式的 DDoS 攻击，这可能是一个有用的缓解工具。它还允许您轻松管理自己的允许列表或屏蔽不应与您的应用程序通信的 IP 地址，而无需依赖 AWS 工程师的干预。

AWS Shield Advanced Web 应用程序的缓解逻辑

AWS Shield Advanced AWS WAF 用于缓解 Web 应用程序层攻击。 AWS WAF 包含在 Shield Advanced 中，无需额外付费。

标准应用程序层保护

使用 Shield Advanced 保护亚马逊 CloudFront 分配或应用程序负载均衡器时，如果尚未关联 AWS WAF 网络 ACL，则可以使用 Shield Advanced 将网络 ACL 与受保护的资源相关联。如果您尚未配置

Web ACL，则可以使用 Shield Advanced 控制台向导创建一个，然后向其添加基于速率的规则。基于速率的规则限制了每个 IP 地址每五分钟时间窗口的请求数，从而提供了防止 Web 应用程序层请求泛洪的基本保护。您可以配置速率，起始速率低至 100。有关更多信息，请参阅 Shield 高级应用层 AWS WAF Web ACL 和基于速率的规则。

您也可以使用该 AWS WAF 服务来管理 Web ACL。通过 AWS WAF，您可以扩展 Web ACL 配置以执行诸如检查特定 Web 请求组件的字符串匹配或模式、添加自定义请求和响应处理以及与请求源的地理位置进行匹配等操作。有关 AWS WAF 规则的更多信息，请参阅AWS WAF 规则。

自动应用程序层缓解

要增强保护，请启用 Shield Advanced 自动应用程序层缓解。使用此选项，Shield Advanced 会为来自已知 DDoS 来源的请求维护 AWS WAF 速率限制规则，并为检测到的 DDoS 攻击提供自定义缓解措施。

当 Shield Advanced 检测到针对受保护资源的攻击时，它会尝试识别攻击特征，将攻击流量与流向应用程序的正常流量隔离开来。Shield Advanced 会根据受到攻击的资源以及与同一 Web ACL 关联的任何其他资源的历史流量模式评估已识别的攻击特征。

如果 Shield Advanced 确定攻击特征码仅隔离 DDoS 攻击中涉及的流量，则它会在关联的 Web ACL 中的 AWS WAF 规则中实施签名。您可以指示 Shield Advanced 设置缓解措施，这些缓解措施只计算与之匹配的流量，或者阻止流量，您可以随时更改设置。当 Shield Advanced 确定不再需要其缓解规则时，它会将其从 Web ACL 中删除。有关应用程序层事件缓解的更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

有关 Shield Advanced 应用程序层缓解的更多信息，请参阅 AWS Shield Advanced 应用层（第 7 层）保护。

基本 DDoS 弹性架构示例

DDoS 弹性是指您的应用程序架构能够抵御分布式拒绝服务 (DDoS) 攻击，同时继续为合法的最终用户提供服务。高弹性的应用程序可以在攻击期间保持可用，且错误或延迟等性能指标受到的影响最小。本节展示了一些常见的示例架构，并描述了如何使用 AWS 和 Shield Advanced 提供的 DDoS 检测和缓解功能来提高其 DDoS 弹性。

本节中的示例架构重点介绍可为您部署的应用程序提供最大 DDoS 弹性优势的 AWS 服务。重点介绍的服务具有以下优势：

- 访问全球分布的网络容量 — Amazon 和 Ama CloudFront zon Route 53 服务为您提供跨 AWS 全球边缘网络的互联网访问和 DDoS 缓解能力。 AWS Global Accelerator这对于缓解规模可能达到 TB

的较大容量攻击非常有用。您可以在任何 AWS 地区运行您的应用程序，并使用这些服务来保护合法用户的可用性并优化性能。

- 针对 Web 应用程序层 DDoS 攻击向量的防护：最好结合使用应用程序扩展和 Web 应用程序防火墙 (WAF) 来缓解 Web 应用程序层 DDoS 攻击。Shield Advanced 使用来自的 Web 请求检查日志 AWS WAF 来检测异常情况，这些异常可以自动缓解，也可以通过与 AWS 盾牌响应小组 (SRT) 合作来缓解。可通过部署的 AWS WAF 基于速率的规则以及 Shield Advanced 自动应用程序层 DDoS 缓解来实现自动缓解。

除了查看这些示例外，还要查看并遵循 DDoS 弹性AWS 最佳实践中适用的最佳实践。

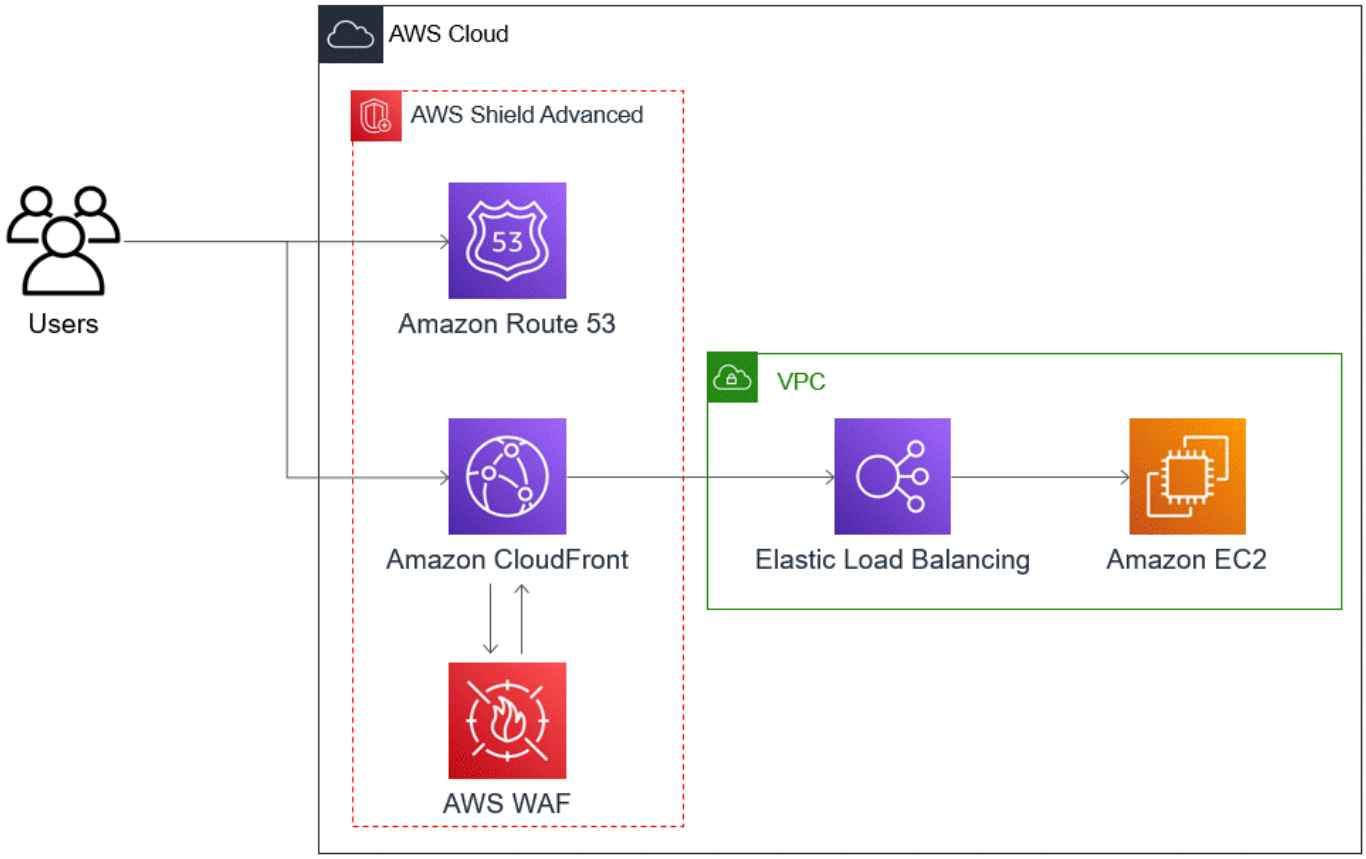
常见 Web 应用程序的 DDoS 弹性示例

您可以在任何 AWS 区域构建 Web 应用程序，并通过该区域 AWS 提供的检测和缓解功能获得自动 DDoS 保护。

此示例适用于使用经典负载均衡器、应用程序负载均衡器、网络负载均衡器、 AWS Marketplace 解决方案或您自己的代理层等资源将用户路由到 Web 应用程序的架构。您可以通过在这些网络应用程序资源和您的用户之间插入 Amazon Route 53 托管区域、Amazon CloudFront 分配和 AWS WAF 网络 ACL 来提高 DDoS 弹性。这些插入可以混淆应用程序来源，在离最终用户更近的地方提供请求，并检测和缓解应用程序层请求泛洪。使用 CloudFront 和 Route 53 向用户提供静态或动态内容的应用程序受到集成的完全内联 DDoS 缓解系统的保护，该系统可以实时缓解基础设施层的攻击。

这些架构改进到位后，您可以使用 Shield Advanced 保护您的 Route 53 托管区域和 CloudFront 分布。保护 CloudFront 分发时，Shield Advanced 会提示您关联 AWS WAF Web ACL 并为其创建基于速率的规则，并允许您选择启用自动应用层 DDoS 缓解或主动参与。主动参与和应用程序层 DDoS 自动缓解使用您与资源关联的 Route 53 运行状况检查。要了解有关这些选项的更多信息，请参阅中的资源保护 AWS Shield Advanced。

以下参考图描绘了这种 Web 应用程序的 DDoS 弹性架构。



这种方法为您的 Web 应用程序带来的好处有：

- 针对经常使用的基础设施层（第 3 层和第 4 层）进行 DDoS 攻击防护，无检测延迟。此外，如果资源经常成为攻击目标，Shield Advanced 会将缓解措施放置更长时间。Shield Advanced 还使用从 Web ACL (NACL) 推断出的应用程序环境，以进一步阻止上游不需要的流量。这样可以将故障隔离在更靠近其来源的地方，从而最大限度地减少对合法用户的影响。
- 针对 TCP SYN 泛洪的防护。与 CloudFront Route 53 集成的 DDoS 缓解系统 AWS Global Accelerator 提供了 TCP SYN 代理功能，可以挑战新的连接尝试，并且仅为合法用户提供服务。
- 针对 DNS 应用程序层攻击的防护，因为 Route 53 负责提供权威的 DNS 响应。
- 针对 Web 应用程序层请求泛洪的防护。当源 IP 发送的请求超出规则允许的数量时，您在 AWS WAF Web ACL 中配置的基于速率的规则会阻止它们。
- 如果您选择启用此选项，则可为您的 CloudFront 发行版自动缓解应用层 DDoS。通过自动 DDoS 缓解功能，Shield Advanced 在发行版的关联 AWS WAF Web ACL 中维护了一条基于速率的规则，该规则限制了来自已知 DDoS 来源的请求量。此外，当 Shield Advanced 检测到影响应用程序运行状况的事件时，它会自动在 Web ACL 中创建、测试和管理缓解规则。

- 与 Shield 响应小组 (SRT) 主动交互（如果您选择启用此选项）。当 Shield Advanced 检测到影响应用程序运行状况的事件时，SRT 会做出响应，并使用您提供的联系信息主动与您的安全或运营团队互动。SRT 会分析您的流量模式，并可以更新您的 AWS WAF 规则以阻止攻击。

TCP 和 UDP 应用程序的 DDoS 弹性示例

此示例显示了使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例或弹性 IP (EIP) 地址的 AWS 区域内的 TCP 和 UDP 应用程序的 DDoS 弹性架构。

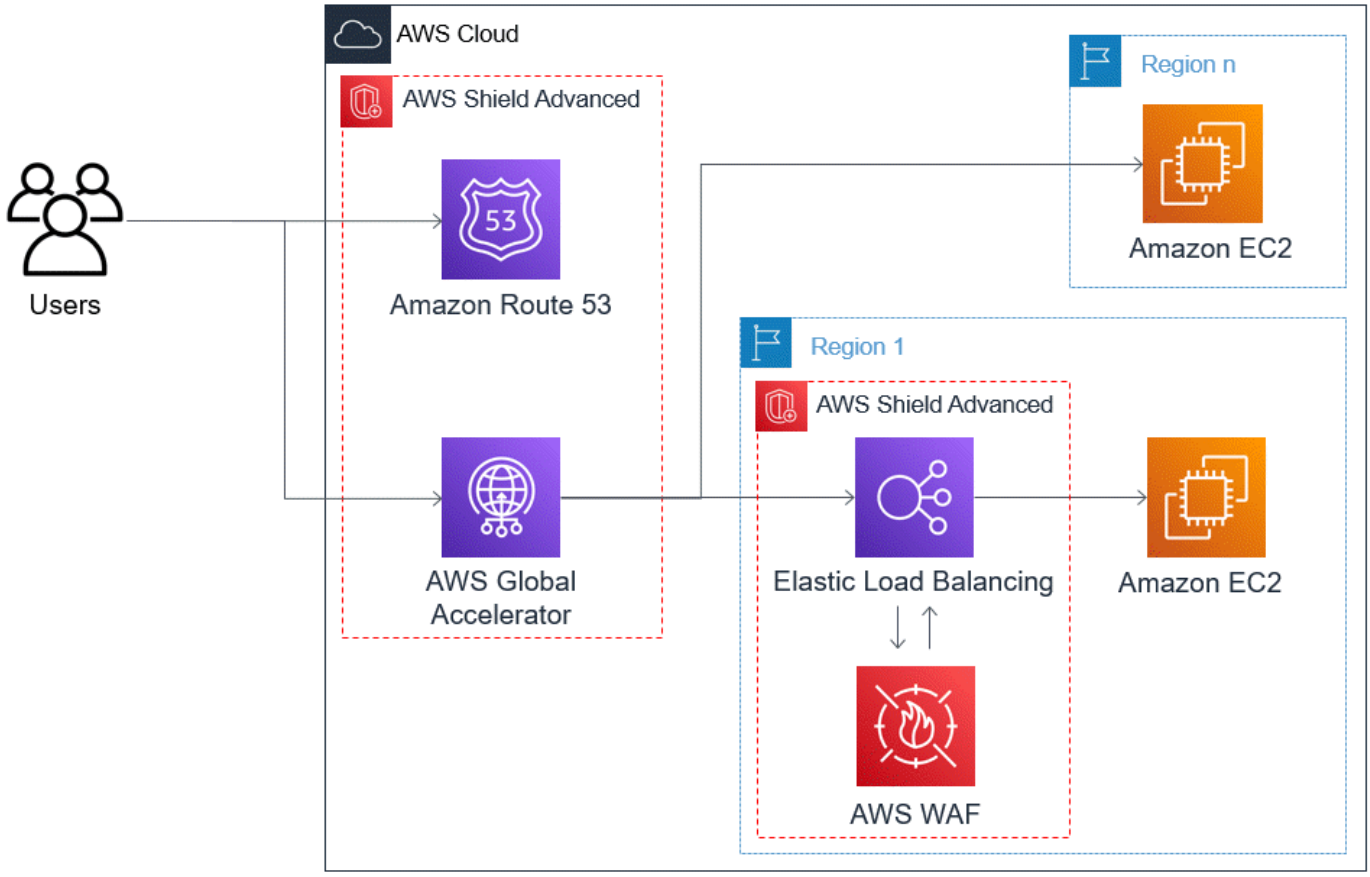
您可以按照此通用示例来提高以下应用程序类型的 DDoS 弹性：

- TCP 或 UDP 应用程序。例如，用于游戏、物联网和 IP 语音的应用程序。
- 需要静态 IP 地址或使用 Amazon CloudFront 不支持的协议的 Web 应用程序。例如，您的应用程序可能需要用户可以添加到其防火墙允许列表的 IP 地址，而这些地址不会被任何其他 AWS 客户使用。

您可以通过引入 Amazon Route 53 和 AWS Global Accelerator来提高这些应用程序类型的 DDoS 弹性。这些服务可以将用户路由到您的应用程序，并且可以为您的应用程序提供通过 AWS 全局边缘网络进行任播路由的静态 IP 地址。Global Accelerator 标准加速器可以将用户延迟缩短多达 60%。如果您有 Web 应用程序，则可以通过在应用程序负载均衡器上运行该应用程序，然后使用 Web ACL 保护应用程序负载均衡器来检测和缓解 AWS WAF Web 应用程序层请求洪水。

构建应用程序后，使用 Shield Advanced 保护您的 Route 53 托管区域、Global Accelerator 标准加速器和任何应用程序负载均衡器。保护应用程序负载均衡器时，可以关联 AWS WAF Web ACL 并为其创建基于速率的规则。通过关联新的或现有的 Route 53 运行状况检查，您可以为 Global Accelerator 标准加速器和应用程序负载均衡器配置与 SRT 的主动互动。要了解有关这些选项的更多信息，请参阅 中的资源保护 AWS Shield Advanced。

以下参考图描绘了 TCP 和 UDP 应用程序的 DDoS 弹性架构示例。



这种方法为您的应用程序带来的好处有：

- 针对已知最大的基础设施层（第 3 层和第 4 层）DDoS 攻击的防护。如果攻击量导致上游的拥塞 AWS，则故障将在离其来源更近的地方隔离，并最大限度地减少对合法用户的影响。
- 针对 DNS 应用程序层攻击的防护，因为 Route 53 负责提供权威的 DNS 响应。
- 如果您有 Web 应用程序，则此方法可以防止 Web 应用程序层请求泛洪。您在 AWS WAF Web ACL 中配置的基于速率的规则会阻止源 IP，因为它们发送的请求超出了规则允许的数量。
- 与 Shield 响应小组 (SRT) 主动交互，如果您选择为符合条件的资源启用此选项。当 Shield Advanced 检测到影响应用程序运行状况的事件时，SRT 会做出响应，并使用您提供的联系信息主动与您的安全或运营团队互动。

Shield Advanced 用例示例

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将其他服务与 Shield Advanced 结合使用以提供最佳保护。以下是如何使用 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 保护亚马逊 CloudFront 分发和应用程序负载均衡器	Elastic Load Balancing 文档、亚马逊 CloudFront 文档
保护基于 TCP 的应用程序免受 DDoS 攻击	Shield Advanced 保护 AWS Global Accelerator 标准加速器；连接到弹性 IP 地址	AWS Global Accelerator 文档，Elastic Load Balancing 文档
保护基于 UDP 的游戏服务器免受 DDoS 攻击	Shield Advanced，用于保护附加到弹性 IP 地址的 Amazon EC2 实例	Amazon Elastic Compute Cloud 文档

例如，如果您使用 Shield Advanced 来保护弹性 IP 地址，Shield Advanced 会保护与其关联的任何资源。攻击期间，Shield Advanced 会自动将您的网络 ACL 部署到网络边界。 AWS 当您的网络 ACL 位于网络边界时，Shield Advanced 可以提供保护以防范更大的 DDoS 事件。通常情况下，网络 ACL 会应用到您 AmazonVPC 中的 Amazon EC2 实例附近。网络 ACL 只能缓解您的 Amazon VPC 和实例可以处理的攻击。如果连接到您的 Amazon EC2 实例的网络接口可以处理高达 10 Gbps，那么超过 10 Gbps 的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。

入门 AWS Shield Advanced

本教程将引导你开始 AWS Shield Advanced 使用 Shield Advanced 控制台。

> **Note**
>
> Shield Advanced 需要订阅，但 AWS Shield Standard 不需要。Shield Standard 提供的保护对所有 AWS 客户都是免费的。

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。有关 Shield Advanced 的更多信息，请参阅 AWS Shield Advanced 概述。

AWS 技术社区发布了一个使用基础架构即代码 (IaC) 工具 AWS CloudFormation 和 Terraform 配置 Shield Advanced 的自动流程示例。如果您的账户属于某个组织， AWS Organizations 并且您要保护除了 Amazon Route 53 或之外的任何资源类型，则可以使用 AWS Firewall Manager 此解决方案 AWS Global Accelerator。要探索此选项，请参阅 aws-samples /- aws-shield-advanced-one click-deployment 中的代码库和一键部署 Shield Advanced 中的教程。

> **Note**
>
> 在分布式拒绝服务 (DDoS) 事件发生之前，请务必完全配置 Shield Advanced。完成配置以帮助确保您的应用程序受到保护，并且在应用程序受到 DDoS 攻击影响时您已准备好做出响应。

按顺序执行以下步骤，开始使用 Shield Advanced。

目录

订阅 AWS Shield Advanced

你必须为每个 AWS 账户 想要保护的物品订阅 Shield Advanced。您无需订阅 Shield Standard。

Shield Advanced 订阅账单

如果您是 AWS 渠道经销商，请咨询您的客户团队以获取信息和指导。此账单信息适用于非 AWS 渠道经销商的客户。

对于所有其他订阅和计费指南，则适用以下订阅和计费指南：

- 对于属于 AWS Organizations 组织成员的账户，无论付款人账户本身是否已订阅，都要从该组织的付款人账户中扣除 Shield Advanced 订阅 AWS 费用。
- 当您订阅属于同一个AWS Organizations 整合账单账户系列的多个账户时，该系列中所有已订阅的账户适用一个订阅价格。组织必须拥有其所有 AWS 账户 和所有资源。
- 当您为多个组织订阅多个账户时，如果您拥有所有组织、账户和资源，您可以用一笔订阅费支付所有组织、账户和资源的费用。请联系您的客户经理或 AWS 支持人员，申请免除其中一个组织以外的所有组织的 AWS Shield Advanced 订阅费用。

有关定价信息和示例的详细信息，请参阅 AWS Shield 定价。

通过以下方式简化订阅 AWS Firewall Manager

如果您的账户属于某个组织，我们建议您尽可能使用 AWS Firewall Manager 进行自动订阅并为该组织提供自动保护。Firewall Manager 支持除了 Amazon Route 53 和 AWS Global Accelerator之外的所有受保护资源类型。如需使用 Firewall Manager，请参阅 AWS Firewall Manager 和 AWS Firewall ManagerAWS Shield Advanced 策略入门。

如果不使用 Firewall Manager，请针对每个需要保护资源的账户，使用以下步骤进行订阅和添加保护。

要订阅账户 AWS Shield Advanced

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航栏中，选择开始。选择订阅 Shield Advanced。
3. 在订阅 Shield Advanced 页面中，阅读协议的每个条款，然后选中所有复选框以表示您接受这些条款。对于整合账单系列中的账户，您必须同意每个账户的条款。

> **Important**
>
> 订阅后，如需取消订阅，您必须联系 AWS Support。

要禁用订阅的自动续订，您必须使用 Shield API 操作UpdateSubscription或 CLI 命令更新订阅。

选择订阅 Shield Advanced。这将使您的账户订阅 Shield Advanced 并激活该服务。

您的账户已订阅。继续执行以下步骤，使用 Shield Advanced 保护您账户的资源。

> **Note**
>
> Shield Advanced 不会在您订阅后自动保护您的资源。您必须指定希望 Shield Advanced 保护的资源，并配置保护。

添加资源以保护和配置保护

Shield Advanced 仅保护您通过 Shield Advanced 或在 Firewall Manager Shield Advanced 策略中指定的资源。它不会自动保护订阅账户的资源。

如果您使用 AWS Firewall Manager Shield Advanced 策略进行保护，则无需执行此步骤。您可以使用要保护的资源类型来配置策略，Firewall Manager 会自动为策略范围内的资源添加保护。

如果您不使用 Firewall Manager，请为每个需要保护资源的账户执行以下步骤。

使用 Shield Advanced 选择要保护的资源

1. 从先前步骤的订阅确认页面，或者从受保护的资源或概述页面中选择添加要保护的资源。
2. 在选择要使用 Shield Advanced 保护的资源页面的指定区域和资源类型中，提供要保护的资源的区域和资源类型规格。您可以通过选择所有区域来保护多个区域中的资源，也可以通过选择全局将选择范围缩小到全局资源。您可以取消选择任何不想保护的资源类型。有关您的资源类型保护的信息，请参阅 AWS Shield Advanced 按资源类型划分的保护。
3. 选择加载资源。Shield Advanced 会使用符合您条件的 AWS 资源填充选择资源部分。
4. 在选择资源 部分，您可以通过在资源列表中输入要搜索的字符串来筛选资源列表。

   选择要保护的资源。
5. 在标签部分，如果要为正在创建的 Shield Advanced 保护添加标签，请指定这些标签。有关标记 AWS 资源的信息，请参阅使用标签编辑器。

6. 选择使用 Shield Advanced 保护。这为资源增加了 Shield Advanced 保护。

继续浏览控制台向导屏幕，完成资源保护的配置。

主题

- 使用以下方法配置应用层（第 7 层）DDoS 保护 AWS WAF
- 为您的保护配置运行状况检测
- 配置通知和警报
- 查看并完成您的保护配置

使用以下方法配置应用层（第 7 层）DDoS 保护 AWS WAF

为了保护应用层资源，Shield Advanced 使用带有基于速率的规则的 AWS WAF Web ACL 作为起点。AWS WAF 是一个 Web 应用程序防火墙，允许您监控转发到应用层资源的 HTTP 和 HTTPS 请求，并允许您根据请求的特征控制对内容的访问权限。基于速率的规则根据您的请求聚合条件限制流量，从而为您的应用程序提供基本的 DDoS 保护。有关更多信息，请参阅 如何 AWS WAF 运作 和 基于速率的规则语句。

您还可以选择启用 Shield Advanced 自动应用层 DDoS 缓解功能，以允许来自已知 DDoS 源的 Shield Advanced 速率限制请求，并自动为您提供特定于事件的保护。

> **Important**
>
> 如果您通过 AWS Firewall Manager 使用 Shield Advanced 策略来管理 Shield 高级保护，则无法在此处管理应用层保护。必须在 Firewall Manager Shield Advanced 策略中对其进行管理。

Shield 高级版订阅和 AWS WAF 费用

您的 Shield Advanced 订阅可支付使用标准 AWS WAF 功能来保护您使用 Shield Advanced 保护的资源的费用。Shield Advanced 保护所涵盖的标准 AWS WAF 费用包括每个 Web ACL 的费用、每条规则的费用以及每百万个 Web 请求检查的基本价格，最多 1,500 个 WCU，不超过默认主体尺寸。

启用 Shield Advanced 自动应用层 DDoS 缓解会向你的 Web ACL 中添加一个使用 150 个 Web ACL 容量单位 (WCU) 的规则组。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解、Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。

你对 Shield Advanced 的 AWS WAF 订阅不包括使用你无法使用 Shield Advanced 保护的资源。它也不包括受保护资源的任何额外非标准 AWS WAF 成本。非标准 AWS WAF 成本的示例包括 Bot Control、CAPTCHA规则操作、使用超过 1,500 个 WCU 的 Web ACL 以及检查超出默认正文大小的请求正文。完整列表在 AWS WAF 定价页面上提供。

有关完整信息和定价示例，请参阅 Shield 定价和 AWS WAF 定价。

为某个区域配置第 7 层 DDoS 保护

Shield Advanced 允许您选择性地为所选资源所在的每个区域配置第 7 层 DDoS 缓解措施。如果您要在多个区域添加保护，则向导将引导您完成每个区域的以下步骤。

1. 配置第 7 层 DDoS 保护页面列出了所有尚未与 Web ACL 关联的资源。对于每个资源，您可以选择现有 Web ACL，活着创建一个新的 Web ACL。对于任何已经关联的 Web ACL 的资源，您可以先通过取消关联当前的 Web ACL 来更改 Web ACL。 AWS WAF有关更多信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

   对于还没有基于速率的规则的 Web ACL，配置向导会提示您添加一个规则。当 IP 地址发送大量请求时，基于速率的规则会限制来自这些地址的流量。基于速率的规则有助于保护您的应用程序免受 Web 请求泛洪的侵害，并可以提供有关流量突然激增的警报，提示您可能存在 DDoS 攻击。选择添加速率限制规则，然后提供速率限制和规则操作，将基于速率的规则添加到 Web ACL。您可以通过在 Web ACL 中配置其他保护 AWS WAF。

   有关在 Shield Advanced 保护中使用 Web ACL 和基于速率的规则（包括基于速率的规则的其他配置选项）的信息，请参阅 Shield 高级应用层 AWS WAF Web ACL 和基于速率的规则。

2. 对于自动应用层 DDoS 缓解，如果您想让 Shield Advanced 自动缓解针对您的应用层资源的 DDoS 攻击，请选择 “启用”，然后选择希望 Shield Advanced 在其自定义 AWS WAF 规则中使用的规则操作。此设置适用于您在向导会话中管理的资源的所有 Web ACL。

   通过自动应用层 DDoS 缓解，Shield Advanced 在资源的 AWS WAF Web ACL 中维护了基于速率的规则，该规则限制了来自已知 DDoS 来源的请求量。此外，Shield Advanced 将当前流量模式与历史流量基线进行比较，以检测可能表明 DDoS 攻击的偏差。当 Shield Advanced 检测到 DDoS 攻击时，它会通过创建、评估和部署自定义 AWS WAF 规则来做出响应。您可以指定自定义规则是计数还是代表您阻止攻击。

   > **Note**
   >
   > 自动应用层 DDoS 缓解仅适用于使用最新版本 AWS WAF (v2) 创建的 Web ACL。

有关 Shield Advanced 自动应用层 DDoS 缓解的更多信息，包括使用此功能的注意事项和最佳实践，请参阅。Shield Advanced 应用程序层 DDoS 自动缓解

3. 选择下一步。控制台向导将进入运行状况检测页面。

为您的保护配置运行状况检测

将 Shield Advanced 配置为使用基于生命值的检测来提高攻击检测和缓解的响应能力和准确性。配置良好的运行状况检查对于准确检测事件至关重要。您可以为除 Route 53 托管区域之外的任何资源类型配置基于运行状况的检测。

要使用基于运行状况的检测，请在 Route 53 中为您的资源定义运行状况检查，然后将运行状况检查与您的 Shield Advanced 保护关联起来。您配置的运行状况检查必须准确反映资源的运行状况，这一点很重要。有关配置运行状况检查以与 Shield Advanced 配合使用的信息和示例，请参阅 使用运行状况检查进行基于运行状况的检测。

Shield Response Team (SRT) 的主动参与支持需要进行运行状况检查。有关主动参与的信息，请参阅配置主动参与。

> **Note**
>
> 将运行状况检查与 Shield Advanced 保护关联时，必须报告运行状况正常。

配置运行状况检测

1. 在 关联运行状况检查 下，选择要与保护关联的运行状况检查的 ID。

   > **Note**
   >
   > 如果您没有看到所需的运行状况检查，请转到 Route 53 控制台并验证运行状况检查及其 ID。有关信息，请参阅创建和更新运行状况检查。

2. 选择下一步。控制台向导进入警报和通知页面。

配置通知和警报

您可以选择为检测到的亚马逊 CloudWatch 警报和基于速率的规则活动配置亚马逊简单通知服务通知。当 Shield 在受保护的资源上检测到事件或超过基于速率的规则中配置的速率限制时，您可以使用它们来接收通知。

有关 Shield 高级 CloudWatch 指标的信息，请参阅AWS Shield Advanced 指标。有关 Amazon SNS 的信息，请参阅 Amazon Simple Notification Service 开发人员指南。

配置通知和警报

1. 选择要通知的 Amazon SNS 主题。您可以为所有受保护的资源和基于速率的规则使用单个 Amazon SNS 主题，也可以选择针对您的组织定制的不同主题。例如，您可以为负责一组特定资源的事件响应的每个团队创建一个 SNS 主题。
2. 选择下一步。控制台向导进入资源保护查看页面。

查看并完成您的保护配置

查看和配置您的设置

1. 在查看和配置 DDoS 缓解和可见性页面中，查看您的设置。要进行修改，请在要修改的区域中选择编辑。系统会带您返回到控制台向导中的关联页面。进行更改，然后在后续页面中选择下一步，直到返回到查看并配置 DDoS 缓解和可见性页面。
2. 选择完成配置。受保护的资源页面列出了您新近受保护的资源。

配置 AWS SRT 支持

Shield Response Team (SRT) 是专门研究 DDoS 事件响应的安全工程师团队。您可以选择添加权限，允许 SRT 在 DDoS 事件期间代表您管理资源。此外，您还可以对 SRT 进行配置，以便在检测到事件期间，如果与受保护资源相关的 Route 53 运行状况检查显示运行状况不佳，SRT 会主动与您联系。这两项新增的保护功能均可更快地响应 DDoS 事件。

> **Note**
>
> 要使用 Shield Response Team (SRT) 的服务，您必须订阅 Business Support 计划或企业支持计划。

SRT 可以在应用程序层事件期间监控 AWS WAF 请求数据和日志，以识别异常流量。他们可以帮助制定自定义 AWS WAF 规则，以减少违规流量来源。根据需要，SRT 可能会提出架构建议，以帮助您更好地将资源与 AWS 建议保持一致。

有关 SRT 的更多信息，请参阅 Shield 响应小组 (SRT) 支持。

授予使用 SRT 的权限

1. 在 AWS Shield 控制台概述页面的配置 AWS SRT 支持下，选择编辑 SRT 访问权限。编辑 AWS Shield 响应小组 (SRT) 访问页面打开。
2. 对于 SRT 访问设置，请选择以下选项之一：
   - 不要授予 SRT 访问我的账户的权限 – Shield 会删除您之前授予 SRT 访问您的账户和资源的任何权限。
   - 为 SRT 创建一个访问我的账户的新角色 – Shield 创建一个代表 SRT 的服务主体的角色 `drt.shield.amazonaws.com`，并将托管策略 `AWSShieldDRTAccessPolicy` 附加到该主体。托管策略允许 SRT 代表您拨 AWS WAF 打 API 调用和访问您的 AWS WAF 日志。 AWS Shield Advanced 有关托管策略的更多信息，请参阅AWS 托管策略：AWSShieldDRTAccessPolicy。
   - 选择一个现有角色让 SRT 访问我的账户 — 对于此选项，您必须按如下方式修改 AWS Identity and Access Management (IAM) 中角色的配置：
     - 将托管策略 `AWSShieldDRTAccessPolicy` 附加到角色。此托管策略允许 SRT 代表您拨 AWS WAF 打 API 调用并访问您的 AWS WAF 日志。 AWS Shield Advanced 有关托管策略的更多信息，请参阅AWS 托管策略： AWSShieldDRTAccessPolicy。有关如何将托管策略附加到角色的信息，请参阅附加和分离 IAM 策略。
     - 修改角色以信任 `drt.shield.amazonaws.com` 服务主体。这是代表 SRT 的服务主体。有关更多信息，请参阅 IAM JSON 策略元素：主体。
3. 选择 保存 以保存您的更改。

有关授予 SRT 访问您的保护措施和数据的更多信息，请参阅 配置 Shield 响应小组 (SRT) 的访问权限。

启用 SRT 主动参与

1. 在 AWS Shield 控制台概述页面的主动互动和联系人下方的联系人区域中，选择编辑。

   在编辑联系人页面中，提供您希望 SRT 主动联系的人员的联系信息。

如果您提供了多个联系人，请在备注中说明应分别在什么情况下与每个联系人联系。包括主要和次要联系人名称，并提供每位联系人的可用时间和时区。

联系人备注示例：

- 这是一条全天候值班热线。请与作出回应的分析师合作，他们会转接相应人员。
- 如果热线在 5 分钟内没有响应，请与我联系。

2. 选择 保存。

概述页面反映了已更新的联系信息。

3. 选择编辑主动互动功能，选择启用，然后选择保存以启用主动互动。

有关主动参与的更多信息，请参阅 配置主动参与。

在中创建 DDoS 仪表板 CloudWatch 并设置警报 CloudWatch

您可以使用亚马逊监控潜在的 DDoS 活动 CloudWatch，亚马逊会从 Shield Advanced 收集原始数据，并将其处理为可读的近乎实时的指标。您可以使用中的统计信息 CloudWatch 来了解您的 Web 应用程序或服务的性能。有关使用的更多信息 CloudWatch，请参阅《Amazon CloudWatch 用户指南》CloudWatch中的内容。

- 有关创建 CloudWatch 仪表板的说明，请参阅使用 Amazon 进行监控 CloudWatch。
- 有关可添加到控制面板的 Shield Advanced 指标的说明，请参阅 AWS Shield Advanced 指标。

Shield Advanced 在 DDoS 事件期间报告资源指标的频率要高于没有事件进行时的频率。 CloudWatch Shield Advanced 在活动期间每分钟报告一次指标，然后在活动结束后立即报告一次。在没有事件的情况下，Shield Advanced 会每天报告一次分配给指定资源的指标。此定期报告可保持指标处于活动状态，并可在您的自定义 CloudWatch 警报中使用。

Shield Advanced 入门教程到此结束。要充分利用您选择的保护功能，请继续探索 Shield Advanced 的功能和选项。首先，请熟悉在 对 DDoS 事件的可见性 和 响应 DDoS 事件 查看和响应事件的选项。

Shield 响应小组 (SRT) 支持

Shield 响应小组 (SRT) 为 Shield Advanced 客户提供额外支持。SRT 是专门研究 DDoS 事件响应的安全工程师团队。作为对 AWS Support 计划的额外支持，您可以直接与 SRT 合作，将他们的专业知识应用到事件响应工作流程中。有关选项的信息以及配置指导，请参阅以下主题。

> **Note**
>
> 要使用 Shield Response Team (SRT) 的服务，您必须订阅 Business Support 计划或企业支持计划。

SRT 支持活动

与 SRT 合作的主要目标是保护应用程序的可用性和性能。根据 DDoS 事件类型和应用程序架构，SRT 可能会执行以下一项或多项操作：

- AWS WAF 日志分析和规则-对于使用 AWS WAF Web ACL 的资源，SRT 可以分析您的 AWS WAF 日志，以识别应用程序 Web 请求中的攻击特征。在参与期间，经您批准后，SRT 可以对您的 Web ACL 进行更改，以阻止所发现的攻击。
- 构建自定义网络缓解措施：SRT 可以为您编写针对基础设施层攻击的自定义缓解措施。SRT 可以与您合作，了解应用程序的预期流量，阻止意外流量，并优化每秒数据包速率限制。有关更多信息，请参阅 使用 Shield 响应小组 (SRT) 配置自定义缓解措施。
- 网络流量工程 — SRT 与 AWS 网络团队密切合作，保护 Shield Advanced 客户。必要时， AWS 可以更改互联网流量到达 AWS 网络的方式，以便为您的应用程序分配更多的缓解容量。
- 架构建议 — SRT 可能会确定，攻击的最佳缓解措施需要更改架构以更好地与 AWS 最佳实践保持一致，他们将有助于支持您实施这些实践。有关信息，请参阅 实现 DDoS 弹性的AWS 最佳实践。

主题

配置 Shield 响应小组 (SRT) 的访问权限

您可以授权 Shield 响应小组 (SRT) 代表您采取行动、访问您的 AWS WAF 日志并调用 AWS Shield Advanced 和 AWS WAF API 来管理保护。在应用层 DDoS 事件期间，SRT 可以监控 AWS WAF 请求以识别异常流量，并帮助制定自定义 AWS WAF 规则以缓解违规流量来源。

此外，您可以向 SRT 授予访问您存储在 Amazon S3 存储桶中的其他数据的权限，例如来自应用程序负载均衡器 CloudFront、Amazon 或第三方来源的数据包捕获或日志。

> **Note**
>
> 要使用 Shield Response Team (SRT) 的服务，您必须订阅 Business Support 计划或企业支持计划。

管理 SRT 的权限

1. 在 AWS Shield 控制台概述页面的配置 AWS SRT 支持下，选择编辑 SRT 访问权限。编辑 AWS Shield 响应小组 (SRT) 访问页面打开。
2. 对于 SRT 访问设置，请选择以下选项之一：
   - 不要授予 SRT 访问我的账户的权限 – Shield 会删除您之前授予 SRT 访问您的账户和资源的任何权限。
   - 为 SRT 创建一个访问我的账户的新角色 – Shield 创建一个代表 SRT 的服务主体的角色 `drt.shield.amazonaws.com`，并将托管策略 `AWSShieldDRTAccessPolicy` 附加到该主体。托管策略允许 SRT 代表您拨 AWS WAF 打 API 调用和访问您的 AWS WAF 日志。 AWS Shield Advanced 有关托管策略的更多信息，请参阅AWS 托管策略：AWSShieldDRTAccessPolicy。
   - 选择一个现有角色让 SRT 访问我的账户 — 对于此选项，您必须按如下方式修改 AWS Identity and Access Management (IAM) 中角色的配置：
     - 将托管策略 `AWSShieldDRTAccessPolicy` 附加到角色。此托管策略允许 SRT 代表您拨 AWS WAF 打 API 调用并访问您的 AWS WAF 日志。 AWS Shield Advanced 有关托管策略的更多信息，请参阅AWS 托管策略： AWSShieldDRTAccessPolicy。有关如何将托管策略附加到角色的信息，请参阅附加和分离 IAM 策略。
     - 修改角色以信任 `drt.shield.amazonaws.com` 服务主体。这是代表 SRT 的服务主体。有关更多信息，请参阅 IAM JSON 策略元素：主体。
3. 对于（可选）：授予 SRT 访问 Amazon S3 存储桶的权限，如果您需要共享 AWS WAF Web ACL 日志中没有的数据，请进行此配置。例如，Application Load Balancer 访问 CloudFront 日志、Amazon 日志或来自第三方来源的日志。

> **Note**
>
> 您无需为 AWS WAF Web ACL 日志执行此操作。当您授予账户访问权限时，SRT 将获得访问权限。

a. 根据以下准则配置 Amazon S3 存储桶：

- 存储桶的位置必须与您在之前的步骤 AWS Shield Response Team (SRT) 访问权限中授予 SRT 一般访问权限的存储桶位置相同 AWS 账户 。
- 存储桶可以是纯文本，也可以采用 SSE-S3 加密。有关 Amazon S3 SSE-S3 加密的更多信息，请参阅《Amazon S3 用户指南》中的使用具有 Amazon S3 托管式加密密钥的服务器端加密 (SSE-S3) 保护数据。

  SRT 无法查看或处理存储在使用存储在 AWS Key Management Service ()AWS KMS中的密钥加密的存储桶中的日志。

b. 在 Shield Advanced（可选）：授予 SRT 访问 Amazon S3 存储桶的权限部分，对于存储您的数据或日志的每个 Amazon S3 存储桶，输入存储桶的名称并选择添加存储桶。您最多可以添加 10 个存储桶。

   这将授予 SRT 对每个存储桶的以下权限：`s3:GetBucketLocation`、`s3:GetObject` 和 `s3:ListBucket`。

   如果您想授予 SRT 访问超过 10 个存储桶的权限，则可以编辑其他存储桶策略并手动授予此处列出的 SRT 权限。

   下面是一个策略列表示例。

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
    ]
}
```

4. 选择 保存 以保存您的更改。

您也可以通过 API 对 SRT 进行授权，方法是创建 IAM 角色，将策略附加 AWSShieldDRTAccessPolicy 到该角色，然后将该角色传递给操作 AssociatedRrole。

配置主动参与

通过主动参与，当您的应用程序的可用性或性能因可能的攻击而受到影响时，Shield Response Team (SRT) 会直接与您联系。我们推荐使用这种参与模式，因为这样 SRT 可以进行最快的响应，甚至在与您建立联系之前就开始故障排除。

针对弹性 IP 地址和 AWS Global Accelerator 标准加速器上的网络层和传输层事件，以及 Amazon CloudFront 分配和应用程序负载均衡器上的 Web 请求洪流，均可主动参与。主动参与仅适用于具有关联 Amazon Route 53 运行状况检查的 Shield Advanced 资源保护。有关管理和使用运行状况检查问题的详细信息，请参阅 使用运行状况检查进行基于运行状况的检测。

在 Shield Advanced 检测到的事件中，SRT 会使用您的健康检查状态来确定该事件是否符合主动参与的条件。如果是，SRT 将根据您在主动参与配置中提供的联系指南与您联系。

您最多可以配置十个联系人以进行主动参与，还可以提供备注来指导 SRT 与您联系。在活动期间，您的主动参与联系人应该可以与 SRT 进行互动。如果您没有全天候运营中心，则可以提供寻呼机联系人，并在联系人备注中注明该联系人偏好。

主动参与要求您执行以下操作：

- 您必须订购 Business Support 计划或企业支持计划。
- 您必须将 Amazon Route 53 运行状况检查与您想要通过主动参进行保护的任何资源相关联。SRT 使用您的运行状况检查的状态来帮助确定事件是否需要主动参与，因此您的运行状况检查必须准确反映受保护资源的状态。有关更多信息和指导，请参阅 使用运行状况检查进行基于运行状况的检测。
- 对于关联了 AWS WAF Web ACL 的资源，必须使用 AWS WAF (v2) 创建 Web ACL，这是的最新版本。 AWS WAF
- 您必须至少提供一位联系人，以便 SRT 在活动期间进行主动参与。保持完整且最新的联系信息。

启用 SRT 主动参与

1. 在 AWS Shield 控制台概述页面的主动互动和联系人下方的联系人区域中，选择编辑。

   在编辑联系人页面中，提供您希望 SRT 主动联系的人员的联系信息。

如果您提供了多个联系人，请在备注中说明应分别在什么情况下与每个联系人联系。包括主要和次要联系人名称，并提供每位联系人的可用时间和时区。

联系人备注示例：

- 这是一条全天候值班热线。请与作出回应的分析师合作，他们会转接相应人员。
- 如果热线在 5 分钟内没有响应，请与我联系。

2. 选择 保存。

概述页面反映了已更新的联系信息。

3. 选择编辑主动互动功能，选择启用，然后选择保存以启用主动互动。

联系 Shield 响应小组 (SRT)

您可以通过以下方式联系 Shield 响应小组 (SRT)：

支持案例

您可以在 AWS 支持中心控制台中的 AWS Shield 下方打开案例。

有关创建支持案例的指导，请参阅 AWS Support Center。

根据您的情况选择严重级别并提供您的联系方式。在描述中，提供尽可能详细的信息。提供有关您认为可能受影响的任何受保护资源以及最终用户体验的当前状态的信息。例如，如果用户体验变差或应用程序的某些部分当前无法可用，请提供该信息。

- 对于可疑的 DDoS 攻击 – 如果应用程序的可用性或性能当前受到可能的 DDoS 攻击的影响，请选择以下严重级别和联系方式：
  - 对于严重级别，请选择支持计划可用的最高严重级别：
    - 对于业务支持，该级别为生产系统停机：< 1 小时。
    - 对于企业支持，该级别为关键业务系统停机：< 15 分钟。
  - 对于联系选项，请选择电话或聊天，然后提供您的详细信息。使用实时联系方式可提供最快的响应。

主动联系

通过 AWS Shield Advanced 主动参与，如果与您的受保护资源关联的 Amazon Route 53 运行状况检查在检测到的事件期间变得不正常，SRT 会直接与您联系。有关此选项的更多信息，请参阅 配置主动参与。

使用 Shield 响应小组 (SRT) 配置自定义缓解措施

对于您的弹性 IP (EIP) 和 AWS Global Accelerator 标准加速器，您可以与 Shield 响应小组 (SRT) 合作配置自定义缓解措施。如果您知道在实施缓解措施时应强制执行的特定逻辑，则这一操作很有帮助。例如，您可能希望仅允许来自某些国家/地区的流量，强制执行特定的速率限制，配置可选验证，禁止分段，或者只允许与数据包有效载荷中特定模式匹配的流量。

常见自定义缓解措施示例：

- 模式匹配：如果您运营的服务与客户端应用程序交互，则可以选择匹配这些应用程序特有的已知模式。例如，您可能经营游戏或通信服务，要求最终用户安装您分配的特定软件。您可以在应用程序发送给您的服务的每个数据包中加入一个幻数字。您最多可以匹配 128 字节（单独或连续）的未分段 TCP 或 UDP 数据包有效负载和标头。匹配可以用十六进制表示法表示，即从数据包有效载荷开始的特定偏移量，或已知值之后的动态偏移量。例如，缓解措施可以查找字节 `0x01`，然后期望 `0x12345678` 为接下来的四个字节。
- 特定于 DNS：如果您使用诸如 Global Accelerator 或 Amazon Elastic Compute Cloud (Amazon EC2) 之类的服务运营自己的权威 DNS 服务，则可以请求自定义缓解措施来验证数据包以确保它们是有效的 DNS 查询，并应用可疑评分来评估特定于 DNS 流量的属性。

要询问如何与 SRT 合作构建自定义缓解措施，请在 AWS Shield下方创建支持案例。要了解有关创建 AWS Support 案例的更多信息，请参阅入门 AWS Support。

中的资源保护 AWS Shield Advanced

您可以为资源添加和配置 AWS Shield Advanced 保护。您可以管理单个资源的保护，也可以将受保护的资源分组归入逻辑集合，以便更好地管理事件。您还可以使用跟踪对您的 Shield 高级保护的更改 AWS Config。

主题

- AWS Shield Advanced 按资源类型划分的保护
- AWS Shield Advanced 应用层（第 7 层）保护
- 使用运行状况检查进行基于运行状况的检测
- 在中管理资源保护 AWS Shield Advanced

- AWS Shield Advanced 保护小组
- 在中跟踪资源保护的变化 AWS Config

AWS Shield Advanced 按资源类型划分的保护

Shield Advanced 可保护网络和传输层（第 3 层和第 4 层）以及应用层（第 7 层）中的 AWS 资源。您可以直接保护某些资源，也可以通过与受保护的资源关联来保护其他资源。Shield Advanced 支持 IPv4，但是不支持 IPv6。

此部分提供有关每种资源类型的 Shield Advanced 保护的信息。

> **Note**
>
> Shield Advanced 仅保护您在 Shield Advanced 中或通过 AWS Firewall Manager Shield Advanced 策略指定的资源。它不会自动保护您的资源。

您可以使用 Shield Advanced 对以下资源类型进行高级监控和保护：

- 亚马逊 CloudFront 配送。为了 CloudFront 持续部署，Shield Advanced 可以保护与受保护的主发行版关联的所有暂存分发。
- Amazon Route 53 托管区。
- AWS Global Accelerator 标准加速器。
- Amazon EC2 弹性 IP 地址 Shield Advanced 可保护与受保护的弹性 IP 地址关联的资源。
- Amazon EC2 实例，通过 Amazon EC2 弹性 IP 地址的关联。
- 以下弹性负载均衡（ELB）负载均衡器：
  - 应用程序负载均衡器。
  - 经典负载均衡器。
  - 网络负载均衡器，通过与 Amazon EC2 弹性 IP 地址的关联。

您无法使用 Shield Advanced 来保护任何其他资源类型。例如，您无法保护 AWS Global Accelerator 自定义路由加速器或网关负载均衡器。

针对每个 AWS 账户，每种资源类型最多可监控和保护 1,000 个资源。例如，在一个账户中，您可以保护 1,000 个 Amazon EC2 弹性 IP 地址、1,000 个 CloudFront 分配和 1,000 个应用程序负载均衡

器。您可以通过服务限额控制台请求增加使用 Shield Advanced 可以保护的资源数量，网址为 https://console.aws.amazon.com/servicequotas/。

使用 Shield Advanced 保护 Amazon EC2 实例和网络负载均衡器

您可以保护 Amazon EC2 实例和网络负载均衡器，方法是先将这些资源附加到弹性 IP 地址，然后在 Shield Advanced 中保护弹性 IP 地址。

当您保护弹性 IP 地址时，Shield Advanced 会识别和保护它们所连接的资源。Shield Advanced 会自动识别附加到弹性 IP 地址的资源类型，并对该资源应用适当的检测和缓解措施。这包括配置特定于该弹性 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，请参阅下述指南：Amazon Elastic Compute Cloud 文档或 弹性负载均衡文档。

攻击期间，Shield Advanced 会自动将您的网络 ACL 部署到网络边界。 AWS 当您的网络 ACL 位于网络边界时，Shield Advanced 可以提供保护以防范更大的 DDoS 事件。通常情况下，网络 ACL 会应用到您 AmazonVPC 中的 Amazon EC2 实例附近。网络 ACL 只能缓解您的 Amazon VPC 和实例可以处理的攻击。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。

某些扩展工具（例如 AWS Elastic Beanstalk）不允许您将弹性 IP 地址自动附加到 Network Load Balancer。对于这些情况，您需要手动附加弹性 IP 地址。

AWS Shield Advanced 应用层（第 7 层）保护

要使用 Shield Advanced 保护您的应用程序层资源，首先要将 AWS WAF Web ACL 与资源关联，然后向其添加一个或多个基于速率的规则。此外，您还可以启用应用程序层 DDoS 自动缓解措施，这会让 Shield Advanced 自动代表您创建和管理 Web ACL 规则，以响应 DDoS 攻击。

当您使用 Shield Advanced 保护应用程序层资源时，Shield Advanced 会分析一段时间内的流量以建立和维护基准。Shield Advanced 使用这些基准来检测可能表明 DDoS 攻击的流量模式中的异常。Shield Advanced 检测到攻击的时间点取决于 Shield Advanced 在攻击之前能够观察到的流量以及您用于 Web 应用程序的架构。可能影响 Shield Advanced 行为的架构变化包括您使用的实例类型、实例大小以及实例类型是否支持增强联网。您还可以将 Shield Advanced 配置为自动缓解应用程序层攻击。

Shield 高级版订阅和 AWS WAF 费用

您的 Shield Advanced 订阅可支付使用标准 AWS WAF 功能来保护您使用 Shield Advanced 保护的资源的费用。Shield Advanced 保护所涵盖的标准 AWS WAF 费用包括每个 Web ACL 的费用、每条规则的费用以及每百万个 Web 请求检查的基本价格，最多 1,500 个 WCU，不超过默认主体尺寸。

启用 Shield Advanced 自动应用层 DDoS 缓解会向你的 Web ACL 中添加一个使用 150 个 Web ACL 容量单位 (WCU) 的规则组。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解、Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。

你对 Shield Advanced 的 AWS WAF 订阅不包括使用你无法使用 Shield Advanced 保护的资源。它也不包括受保护资源的任何额外非标准 AWS WAF 成本。非标准 AWS WAF 成本的示例包括机器人控制、CAPTCHA规则操作、使用超过 1,500 个 WCU 的 Web ACL 以及检查超出默认正文大小的请求正文。完整列表在 AWS WAF 定价页面上提供。

有关完整信息和定价示例，请参阅 Shield 定价和 AWS WAF 定价。

主题

检测和缓解

本节介绍影响 Shield Advanced 检测和缓解应用层事件的因素。

运行状况检查

Health 检查可以准确报告应用程序的整体运行状况，从而为 Shield Advanced 提供有关您的应用程序正在经历的流量状况的信息。当您的应用程序报告运行状况不佳时，Shield Advanced 需要更少的指向潜在攻击的信息，如果您的应用程序报告运行正常，则需要更多的攻击证据。

配置运行状况检查非常重要，这样它们才能准确地报告应用程序的运行状况。有关更多信息和指导，请参阅 使用运行状况检查进行基于运行状况的检测。

流量基线

流量基线为 Shield Advanced 提供了有关您的应用程序正常流量特征的信息。Shield Advanced 使用这些基准来识别您的应用程序何时未收到正常流量。，因此它可以通知您，并根据配置开始设计和测试缓解选项来抵御潜在的攻击。有关 Shield Advanced 如何使用流量基准检测潜在事件的更多信息，请参阅概述部分应用程序层威胁检测逻辑。

Shield Advanced 根据与受保护资源关联的 Web ACL 提供的信息创建其基准。Web ACL 必须与资源关联至少 24 小时至 30 天，Shield Advanced 才能可靠地确定应用程序的基准。所需时间从您关联 Web ACL 时开始，无论是通过 Shield Advanced 还是通过 AWS WAF。

有关使用 Web ACL 和 Shield 高级应用层保护的更多信息，请参阅Shield 高级应用层 AWS WAF Web ACL 和基于速率的规则。

基于速率的规则

基于速率的规则可以帮助缓解攻击。它们还可以掩盖攻击，方法是在攻击成为足够大的问题以至于出现在正常流量基线或运行状况检查状态报告中的问题之前对其进行缓解。

当你使用 Shield Advanced 保护应用程序资源时，我们建议在你的 Web ACL 中使用基于速率的规则。尽管它们的缓解措施可以掩盖潜在的攻击，但它们是宝贵的第一道防线，有助于确保您的应用程序可供合法客户使用。基于速率的规则检测到的流量和速率限制在您的 AWS WAF 指标中可见。

除了您自己的基于速率的规则外，如果您启用自动应用层 DDoS 缓解，Shield Advanced 还会在您的 Web ACL 中添加一个用于缓解攻击的规则组。在此规则组中，Shield Advanced 始终采用基于速率的规则，该规则限制了来自已知是 DDoS 攻击来源的 IP 地址的请求量。Shield Advanced 规则缓解的流量指标无法供您查看。

有关基于费率的规则的更多信息，请参阅基于速率的规则语句。有关 Shield Advanced 用于自动缓解应用层 DDoS 的基于速率的规则的信息，请参阅。Shield Advanced 规则组

有关 Shield Advanced 和 AWS WAF 指标的更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

Shield 高级应用层 AWS WAF Web ACL 和基于速率的规则

要使用 Shield Advanced 保护应用层资源，首先要将 AWS WAF Web ACL 与该资源关联。 AWS WAF 是一种 Web 应用程序防火墙，允许您监控转发到应用层资源的 HTTP 和 HTTPS 请求，并允许您根据请求的特征控制对内容的访问权限。您可以配置 Web ACL，根据请求的来源、查询字符串和 Cookie 的内容以及来自单个 IP 地址的请求速率等因素来监控和管理请求。要进行 Shield Advanced 保护，您至少要将 Web ACL 与基于速率的规则相关联，该规则限制了每个 IP 地址的请求速率。

如果关联的 Web ACL 没有定义基于速率的规则，Shield Advanced 会提示您定义至少一个规则。当来自源 IP 的流量超过您定义的阈值时，基于速率的规则会自动阻止这些流量。它们有助于保护您的应用程序免受 Web 请求泛洪的侵害，并可以提供有关流量突然激增的警报，提示您可能存在 DDoS 攻击。

> **Note**
>
> 基于速率的规则可以非常快速地响应该规则所监控的流量峰值。因此，基于速率的规则不仅可以防止攻击，还可以防止通过Shield Advanced检测检测到潜在的攻击。这种权衡有利于预防，而不是完全了解攻击模式。我们建议使用基于速率的规则作为抵御攻击的第一道防线。

设置好 Web ACL 后，如果发生 DDoS 攻击，您可以通过在 Web ACL 中添加和管理规则来采取缓解措施。您可以在 Shield Response Team 的帮助下直接执行此操作，也可以通过应用程序层 DDoS 自动缓解措施来自动执行此操作。

> **Important**
>
> 如果您还使用自动应用层 DDoS 缓解，请参阅管理 Web ACL 的最佳实践，网址为使用自动缓解的最佳实践。

基于速率的默认规则行为

当您使用默认配置的基于速率的规则时， AWS WAF 会定期评估前 5 分钟时间段内的流量。 AWS WAF 阻止来自超过规则阈值的任何 IP 地址的请求，直到请求速率降至可接受的水平。通过 Shield Advanced 配置基于速率的规则时，请将其速率阈值配置为一个大于您在任何五分钟时间窗口内预期来自任何一个源 IP 的正常流量速率的值。

您可能希望在 Web ACL 中使用多个基于速率的规则。例如，您可以为所有具有高阈值的流量设置一个基于速率的规则，外加一个或多个其他规则，这些规则配置为与您的 Web 应用程序的选定部分相匹配且阈值较低。例如，您可以对阈值较低的 URI `/login.html` 进行匹配，以减少对登录页面的滥用行为。

您可以将基于速率的规则配置为使用不同的评估时间窗口，并按多个请求组件（例如标头值、标签和查询参数）聚合请求。有关更多信息，请参阅 基于速率的规则语句。

有关更多信息和指导，请参阅安全博客文章《三个最重要的 AWS WAF 基于费率的规则》。

通过以下方式扩展了配置选项 AWS WAF

Shield Advanced 控制台允许您添加基于速率的规则，并使用基本的默认设置对其进行配置。您可以通过管理基于费率的规则来定义其他配置选项。 AWS WAF例如，您可以将规则配置为根据转发的 IP 地址、查询字符串和标签等密钥聚合请求。您还可以在规则中添加范围缩小语句，从评估和速率限制中筛选出一些请求。有关更多信息，请参阅 基于速率的规则语句。有关使用 AWS WAF 管理 Web 请求监控和管理规则的信息，请参阅创建 Web ACL。

Shield Advanced 应用程序层 DDoS 自动缓解

您可以将 Shield Advanced 配置为自动响应，通过计算或阻止作为攻击一部分的 Web 请求来缓解针对受保护应用程序层资源的应用程序层（第 7 层）攻击。此选项是您通过Shield Advanced添加的应用层保护的补充，该保护具有 AWS WAF Web ACL和您自己的基于速率的规则。

当为资源启用自动缓解时，Shield Advanced 会在资源的关联 Web ACL 中维护一个规则组，在这里，它代表资源管理缓解规则。该规则组包含一个基于速率的规则，用于跟踪来自已知为 DDoS 攻击来源的 IP 地址的请求量。

此外，Shield Advanced 将当前流量模式与历史流量基线进行比较，以检测可能表明 DDoS 攻击的偏差。Shield Advanced 通过在规则组中创建、评估和部署其他自定义 AWS WAF 规则来响应检测到的 DDoS 攻击。

目录

使用自动缓解的注意事项

以下列表描述了 Shield Advanced 应用程序层 DDoS 自动缓解的注意事项，并描述了您可能需要采取的应对措施。

- 自动应用层 DDoS 缓解仅适用于使用最新版本 AWS WAF (v2) 创建的 Web ACL。
- Shield Advanced 需要时间来建立应用程序的正常、历史流量的基准，它利用该基准来检测攻击流量并将其与正常流量隔离开来，从而缓解攻击流量。从将 Web ACL 与受保护的应用程序资源关联起，建立基准的时间介于 24 小时到 30 天之间。有关流量基线的更多信息，请参阅检测和缓解。

- 启用自动应用层 DDoS 缓解会将一个规则组添加到您的 Web ACL 中，该规则组使用 150 个 Web ACL 容量单位 (WCU)。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。有关更多信息，请参阅 Shield Advanced 规则组 和 AWS WAF 网络 ACL 容量单位 (WCU)。
- Shield 高级规则组生成 AWS WAF 指标，但无法查看。这与您在 Web ACL 中使用但不拥有的任何其他规则组相同，例如 AWS 托管规则规则组。有关 AWS WAF 指标的更多信息，请参阅AWS WAF 指标和维度。有关此 Shield 高级保护选项的信息，请参阅Shield Advanced 应用程序层 DDoS 自动缓解。
- 对于保护多个资源的 Web ACL，自动缓解仅部署不会对任何受保护资源产生负面影响的自定义缓解措施。
- 从 DDoS 攻击开始到 Shield Advanced 放置自定义自动缓解规则的时间间隔因每个事件而异。某些 DDoS 攻击可能会在部署自定义规则之前结束。当缓解措施已经到位时，可能会发生其他攻击，因此可能会从该事件开始就通过这些规则来缓解。此外，Web ACL 和 Shield Advanced 规则组中基于速率的规则可能会在攻击流量被检测为可能的事件之前对其进行缓解。
- 对于通过内容分发网络 (CDN)（例如 Ama CloudFront zon）接收任何流量的应用程序负载均衡器，Shield Advanced 针对这些应用程序负载均衡器资源的应用程序层自动缓解能力将降低。Shield Advanced 使用客户端流量属性来识别攻击流量并将其从正常流量中隔离到您的应用程序，而 CDN 可能不会保留或转发原始客户端流量属性。如果您使用 CloudFront，我们建议您在 CloudFront 发行版上启用自动缓解功能。
- 应用程序层 DDoS 自动缓解不会与保护组交互。您可以为保护组中的资源启用自动缓解，但是 Shield Advanced 不会根据保护组的调查发现自动应用攻击缓解措施。Shield Advanced 会对单个资源进行自动攻击缓解。

使用自动缓解的最佳实践

使用自动缓解时，请遵守本节中提供的指导。

一般保护管理

在规划和实施自动缓解保护时，请遵循以下指南。

- 通过 Shield Advanced 管理所有自动缓解保护，或者如果你使用 AWS Firewall Manager 管理你的 Shield Advanced 自动缓解设置，也可以通过 Firewall Manager 管理所有自动缓解保护。在管理这些保护时，请勿将 Shield Advanced 和 Firewall Manager 混用。
- 对于相似的资源，使用相同的 Web ACL 和保护设置进行管理；对于不同的资源，使用不同的 Web ACL 进行管理。当 Shield Advanced 缓解对受保护资源的 DDoS 攻击时，它会为与该资源关联的 Web ACL 定义规则，然后针对与 Web ACL 相关联的所有资源流量来测试规则。只有在规则不会对

任何相关资源产生负面影响的情况下，Shield Advanced 才会应用这些规则。有关更多信息，请参阅 Shield Advanced 如何管理自动缓解。

- 对于所有互联网流量都通过 Amazon 分配代理的应用程序负载均衡器，仅在 CloudFront分配上启用自动缓解功能。 CloudFront该 CloudFront 发行版将始终拥有最多的原始流量属性，Shield Advanced 利用这些属性来缓解攻击。

检测和缓解优化

请遵循以下指导方针，优化自动缓解措施为受保护资源提供的保护。有关应用层检测和缓解的概述，请参阅检测和缓解。

- 为受保护的资源配置运行状况检查，并使用这些检查在 Shield Advanced 防护中启用基于生命值的检测。有关操作指南，请参阅 使用运行状况检查进行基于运行状况的检测。
- 在 Shield Advanced 为正常的历史流量建立基准之前，在Count模式下启用自动缓解。Shield Advanced 需要 24 小时到 30 天的时间来建立基准。

  建立正常流量模式的基线需要满足以下条件：

  - Web ACL 与受保护资源的关联。您可以 AWS WAF 直接使用关联您的 Web ACL，也可以在启用 Shield 高级应用层保护并指定要使用的 Web ACL 时让 Shield Advanced 将其关联。
  - 正常流量流向受保护的应用程序。如果您的应用程序没有正常流量，例如在应用程序启动之前，或者如果它长时间缺乏生产流量，则无法收集历史数据。

Web ACL 管理

请遵循以下指导方针，管理用于自动缓解的 Web ACL。

- 如果您需要替换与受保护资源关联的 Web ACL，请按顺序进行以下更改：

  1. 在 Shield Advanced 中，禁用自动缓解。
  2. 在中 AWS WAF，取消关联旧的 Web ACL 并关联新的 Web ACL。
  3. 在 Shield Advanced 中，启用自动缓解。

  Shield Advanced 不会自动将自动缓解措施从旧的 Web ACL 转移到新的 Web ACL。
- 请勿从 Web ACL 中删除任何名称以开头的 `ShieldMitigationRuleGroup` 规则组规则。如果您确实删除了此规则组，则会禁用 Shield Advanced 为与 Web ACL 关联的每个资源提供的自动缓解保护。此外，Shield Advanced 可能需要一些时间才能收到更改通知并更新其设置。在此期间，Shield Advanced 控制台页面所提供的信息是不准确的。

有关规则组的更多信息，请参阅 Shield Advanced 规则组。

- 请勿修改名称以 ShieldMitigationRuleGroup 开头的规则组规则的名称。该操作可能会干扰 Shield Advanced 自动缓解通过 Web ACL 提供的保护。
- 创建规则和规则组时，请勿使用以 ShieldMitigationRuleGroup 开头的名称。Shield Advanced 使用此字符串来管理您的自动缓解措施。
- 在管理 Web ACL 规则时，请勿将优先级设置为 10,000,000。Shield Advanced 在添加自动缓解规则组规则时会将该优先级设置分配给该规则。
- 在Web ACL 的规则中保持 ShieldMitigationRuleGroup 规则的优先顺序，使其根据您的需要运行。Shield Advanced 为 Web ACL 添加规则组规则，优先级为 10,000,000，这样它将在其他规则之后运行。如果您使用 AWS WAF 控制台向导来管理 Web ACL，请在向 Web ACL 添加规则后根据需要调整优先级设置。
- 如果您 AWS CloudFormation 使用管理 Web ACL，则无需管理ShieldMitigationRuleGroup规则组规则。按照 AWS CloudFormation 与自动应用层 DDoS 缓解配合使用 中的指导进行操作。

启用自动缓解所需的配置

您可以启用 Shield Advanced 自动缓解作为资源应用程序层 DDoS 保护的一部分。有关在控制台上执行此操作的信息，请参阅 配置应用程序层 DDoS 保护。

自动缓解功能要求您执行以下操作：

- 将 Web ACL 与资源关联：这是任何 Shield Advanced 应用程序层保护所必需的。您可以对多个资源使用相同的 Web ACL。我们建议仅对流量相似的资源执行此操作。有关 Web ACL 的信息，包括将其用于多种资源的要求，请参阅 如何 AWS WAF 运作。
- 启用和配置 Shield Advanced 应用程序层 DDoS 自动缓解：启用此功能后，您可以指定是希望 Shield Advanced 自动阻止还是计算其确定为 DDoS 攻击一部分的网络请求。Shield Advanced 将规则组添加到关联的 Web ACL 中，并使用它来动态管理其对资源上的 DDoS 攻击的响应。有关规则操作选项的信息，请参阅 规则操作。
- （可选，但建议设置）在 Web ACL 中添加基于速率的规则：默认情况下，基于速率的规则可防止任何单个 IP 地址在短时间内发送过多请求，从而为您的资源提供防御 DDoS 攻击的基本保护。有关基于速率的规则（包括自定义请求聚合选项和示例）的信息，请参阅 基于速率的规则语句。

Shield Advanced 如何管理自动缓解

本节中的主题介绍了 Shield Advanced 如何处理应用程序层 DDoS 自动缓解的配置更改，以及启用自动缓解后如何处理 DDoS 攻击。

主题

在启用自动缓解时发生的情况

启用自动缓解后，Shield Advanced 会执行以下操作：

- 根据需要添加规则组以供 Shield Advanced 使用 — 如果您与资源关联的 AWS WAF Web ACL 还没有专门用于自动缓解应用层 DDoS 的 AWS WAF 规则组规则，Shield Advanced 会添加一条规则组规则。

  规则组规则的名称以 `ShieldMitigationRuleGroup` 开头。该规则组始终包含一个名为 `ShieldKnownOffenderIPRateBasedRule` 的基于速率的规则，用于限制来自已知为 DDoS 攻击来源的 IP 地址的请求量。有关 Shield Advanced 规则组和引用它的 Web ACL 规则的其他详细信息，请参阅 Shield Advanced 规则组。
- 开始响应针对资源的 DDoS 攻击：Shield Advanced 会自动响应受保护资源的 DDoS 攻击。除了始终存在的基于速率的规则外，Shield Advanced 还使用其规则组来部署缓解 DDoS 攻击的自定义 AWS WAF 规则。Shield Advanced 会根据您的应用程序和应用程序遇到的攻击量身定制这些规则，并在部署之前根据该资源的历史流量对其进行测试。

Shield Advanced 在您用于自动缓解的任何 Web ACL 中使用单个规则组规则。如果 Shield Advanced 已经为另一个受保护资源添加了规则组，则不会向 Web ACL 添加另一个规则组。

应用程序层 DDoS 的自动缓解取决于是否存在用于缓解攻击的规则组。如果出于任何原因将规则组从 AWS WAF Web ACL 中删除，则删除规则组将禁用与该 Web ACL 关联的所有资源的自动缓解措施。

Shield Advanced 如何通过自动缓解来响应 DDoS 攻击

当您在受保护的资源上启用了自动缓解时，Shield Advanced 规则组中基于速率的规则 `ShieldKnownOffenderIPRateBasedRule` 会自动响应来自已知 DDoS 来源的提升流量。此速率限制可以快速应用，能起到抵御攻击的前线防御作用。

当 Shield Advanced 检测到攻击时，它会执行下列操作：

1. 尝试识别攻击签名，该特征码将攻击流量与发送到您的应用程序的正常流量隔离开来。目标是制定高质量的 DDoS 缓解规则，这些规则放置后仅影响攻击流量，不会影响应用程序的正常流量。
2. 根据受到攻击的资源以及与相同 Web ACL 关联的任何其他资源的历史流量模式，评估已识别的攻击特征。Shield Advanced 会在部署任何规则以响应事件之前执行此操作。

   根据评估结果，Shield Advanced 执行以下操作之一：

   - 如果 Shield Advanced 确定攻击签名仅隔离 DDoS 攻击所涉及的流量，则它将在 Web ACL 的 Shield Advanced 缓解规则组中的 AWS WAF 规则中实施签名。Shield Advanced 为这些规则提供了您为资源自动缓解配置的操作设置，可以是 Count 或 Block。
   - 否则，Shield Advanced 不会提供缓解措施。

在整个攻击过程中，Shield Advanced 会发送与基本 Shield Advanced 应用程序层保护相同的通知并提供相同的事件信息。您可以在 Shield Advanced 事件控制台中查看有关事件和 DDoS 攻击的信息，以及任何针对攻击的 Shield Advanced 缓解措施的信息。有关信息，请参阅 对 DDoS 事件的可见性。

如果您已将自动缓解配置为使用 Block 规则操作，并且 Shield Advanced 部署的缓解规则发生误报，则可以将规则操作更改为 Count。有关如何执行此操作的信息，请参阅 更改用于应用程序层 DDoS 自动缓解的操作。

Shield Advanced 如何管理规则操作设置

您可以将自动缓解的规则操作设置为 Block 或 Count。

当您更改受保护资源的自动缓解规则操作设置时，Shield Advanced 会更新该资源的所有规则设置。它会更新 Shield Advanced 规则组中资源当前存在的任何规则，并在创建新规则时使用新的操作设置。

对于使用相同 Web ACL 的资源，如果指定不同的操作，Shield Advanced 将使用规则组基于速率的规则 `ShieldKnownOffenderIPRateBasedRule` 的 Block 操作设置。Shield Advanced 代表特定的受保护资源创建和管理规则组中的其他规则，并使用您为该资源指定的操作设置。Web ACL 中的 Shield Advanced 规则组中的所有规则都应用于所有相关资源的 Web 流量。

更改操作设置可能需要几秒钟进行传播。在此期间，某些使用规则组的位置会显示旧设置，而另一些会显示新设置。

您可以在控制台的事件页面和应用程序层配置页面更改自动缓解配置的规则操作设置。有关事件的更多信息，请参阅 响应 DDoS 事件。有关配置文件的更多信息，请参阅配置应用程序层 DDoS 保护。

攻击消退后 Shield Advanced 如何管理缓解措施

当 Shield Advanced 确定不再需要为特定攻击部署的缓解规则时，它会将其从 Shield Advanced 缓解规则组中删除。

攻击结束并不意味着取消缓解规则。Shield Advanced 会监控它在您的受保护资源上检测到的攻击模式。它可以保持针对首次发生攻击时部署的规则，以主动防御带有特定特征的攻击再次发生。根据需要，Shield Advanced 会延长遵守规则的时间窗口。这样，Shield Advanced 就可以在使用特定特征码的重复攻击影响您的受保护资源之前缓解这些攻击。

Shield Advanced 永远不会删除基于速率的规则 `ShieldKnownOffenderIPRateBasedRule`，该规则限制来自已知为 DDoS 攻击来源的 IP 地址的请求量。

在禁用自动缓解时发生的情况

当您为资源禁用自动缓解时，Shield Advanced 会执行以下操作：

- 停止自动响应 DDoS 攻击：Shield Advanced 停止对该资源的自动响应活动。
- 从 Shield Advanced 规则组中移除不需要的规则：如果 Shield Advanced 代表受保护资源维护其托管规则组中的任何规则，则会将其删除。
- 如果已不再使用 Shield Advanced 规则组，则将其删除：如果您与该资源关联的 Web ACL 未与任何其他启用了自动缓解的资源相关联，Shield Advanced 将从 Web ACL 中删除其规则组规则。

Shield Advanced 规则组

Shield Advanced 使用规则组中它拥有和为您管理的规则来管理自动缓解活动。Shield Advanced 在 Web ACL 中引用具有与受保护资源关联的规则的规则组。

Web ACL 中的规则组规则

您的 Web ACL 中的 Shield Advanced 规则组规则具有下列属性：

- 名称 – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*

- Web ACL 容量单位 (WCU) 数：150。这些 WCU 会计入您的 Web ACL 中的 WCU 使用量。

Shield Advanced 在你的 Web ACL 中创建此规则，优先级设置为 10,000,000，这样它就可以在 Web ACL 中的其他规则和规则组之后运行。 AWS WAF 从 up 的最低数字优先级设置开始运行 Web ACL 中的规则。在管理 Web ACL 期间，此优先级设置可能会发生变化。

除了 Web ACL 中的规则组使用的 WCU 之外，自动缓解功能不会消耗您账户中的任何其他 AWS WAF 资源。例如，Shield Advanced 规则组不算作您账户的规则组之一。有关中的账户限制的信息 AWS WAF，请参阅AWS WAF 配额。

规则组中的规则

在引用的 Shield Advanced 规则组中，Shield Advanced 维护一个基于速率的规则 `ShieldKnownOffenderIPRateBasedRule`，该规则限制来自已知为 DDoS 攻击来源的 IP 地址的请求量。此规则是抵御任何攻击的第一道防线，因为它始终存在于规则组中，并且不依赖对流量模式的分析来遏制攻击。与规则组中的其他规则一样，此规则的操作设置为您为自动缓解选择的操作。有关基于速率的规则的更多信息，请参阅 基于速率的规则语句。

> **Note**
>
> 基于速率的规则的`ShieldKnownOffenderIPRateBasedRule`运行独立于 Shield Advanced 事件检测。启用自动缓解功能后，此规则会限制已知是 DDoS 攻击来源的 IP 地址。对于这些 IP 地址，规则的速率限制可以防止攻击，还可以防止攻击出现在 Shield Advanced 检测信息中。这种权衡有利于预防，而不是完全了解攻击模式。

除了上述基于速率的永久规则外，该规则组还包含 Shield Advanced 当前用于缓解 DDoS 攻击的所有规则。Shield Advanced 根据需要添加、修改和删除这些规则。有关信息，请参阅 Shield Advanced 如何管理自动缓解。

指标

规则组生成 AWS WAF 指标，但由于此规则组归Shield Advanced所有，因此无法查看这些指标。有关更多信息，请参阅 AWS WAF 指标和维度。

管理应用程序层 DDoS 自动缓解

使用本节中的指南来管理您的应用程序层 DDoS 自动缓解配置。有关自动缓解的工作原理的信息，请参阅前面的主题。

> **Note**
>
> 请遵循中描述的最佳实践使用自动缓解的最佳实践。

主题

查看资源的应用程序层 DDoS 自动缓解配置

您可以在受保护资源页面和各个保护页面中查看资源的应用程序层 DDoS 自动缓解配置。

要查看应用程序层 DDoS 自动缓解配置

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。在受保护资源列表中，应用程序层 DDoS 自动缓解列表示是否启用了自动缓解，如果已启用，则显示 Shield Advanced 将在缓解中使用的操作。

   您也可以选择任何应用程序层资源，以查看该资源保护页面上列出的相同信息。

启用和禁用应用程序层 DDoS 自动缓解

以下过程介绍如何对受保护资源启用或禁用自动响应。

为单个资源启用或禁用应用程序层 DDoS 自动缓解

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护选项卡中，选择要为其启用自动缓解功能的应用程序层资源。资源的保护页面打开。
4. 在保护组页面上，选择编辑。

5. 在为全局资源配置第 7 层 DDoS 缓解（可选）页面中，对于应用程序层 DDoS 自动缓解，选择要用于自动缓解的选项。控制台上的选项如下：

   - 保留当前设置：不对受保护资源的自动缓解设置进行任何更改。
   - 启用：为受保护的资源启用自动缓解。选择此选项时，还要选择要在 Web ACL 规则中使用自动缓解措施的规则操作。有关规则操作设置的信息，请参阅 规则操作。

     如果您的受保护资源还没有正常应用程序流量的历史记录，请在Count模式下启用自动缓解功能，直到 Shield Advanced 可以建立基准。当您将 Web ACL 与受保护的资源关联时，Shield Advanced 会开始收集其基准信息，并且可能需要 24 小时到 30 天才能建立正常流量的良好基准。
   - 禁用：禁用受保护资源的自动缓解。
6. 浏览其余页面，直到完成并保存配置。

在保护页面中，将更新资源的自动缓解设置。

更改用于应用程序层 DDoS 自动缓解的操作

您可以在控制台的多个位置更改 Shield Advanced 用于其应用程序层自动响应的操作：

- 自动缓解配置：在为资源配置自动缓解时更改操作。有关操作步骤，请参阅上一节 启用和禁用应用程序层 DDoS 自动缓解。
- 事件详细信息页面：当您在控制台中查看事件信息时，在活动详细信息页面中更改操作。有关信息，请参阅 AWS Shield Advanced 活动详情。

如果您有两个受保护资源共享一个 Web ACL，并且您将其中一个资源的操作设置为 Count，将另一个资源的操作设置为 Block，Shield Advanced 会将规则组的基于速率的规则 `ShieldKnown0ffenderIPRateBasedRule` 的操作设置为 Block。

AWS CloudFormation 与自动应用层 DDoS 缓解配合使用

了解如何使用 AWS CloudFormation 来管理您的防护和 AWS WAF Web ACL。

启用或禁用应用程序层 DDoS 自动缓解

您可以使用`AWS::Shield::Protection`资源通过 AWS CloudFormation启用和禁用自动应用层 DDoS 缓解。效果与通过控制台或任何其他界面启用或禁用该功能时的效果相同。有关 AWS CloudFormation 资源的信息，请参阅AWS CloudFormation 用户指南AWS::Shield::Protection中的。

管理与自动缓解配合使用的 Web ACL

Shield Advanced 使用受保护资源的 AWS WAF Web ACL 中的规则组规则管理受保护资源的自动缓解措施。通过 AWS WAF 控制台和 API，您将看到 Web ACL 规则中列出的规则，其名称以开头`ShieldMitigationRuleGroup`。该规则专用于您的应用程序层 DDoS 自动缓解，由 Shield Advanced 和 AWS WAF管理. 有关更多信息，请参阅 Shield Advanced 规则组 和 Shield Advanced 如何管理自动缓解。

如果您使用 AWS CloudFormation 管理网页 ACL，请不要将 Shield Advanced 规则组规则添加到您的 Web ACL 模板中。当您更新与自动缓解保护一起使用的 Web ACL 时， AWS WAF 会自动管理 Web ACL 中的规则组规则。

与您管理的其他 Web ACL 相比，您将看到以下区别： AWS CloudFormation

- AWS CloudFormation 不会报告使用 Shield Advanced 规则组规则的 Web ACL 的实际配置与没有规则的 Web ACL 模板之间的堆栈偏移状态存在任何偏差。Shield Advanced 规则不会出现在资源实际列表的偏移细节中。

  您将能够在从中检索的 Web ACL 列表中看到 Shield Advanced 规则组规则 AWS WAF，例如通过 AWS WAF 控制台或 AWS WAF API。
- 如果您修改堆栈中的 Web ACL 模板， AWS WAF Shield Advanced 会在更新后的 Web ACL 中自动维护 Shield Advanced 自动缓解规则。Shield Advanced 提供的自动缓解保护不会因您对 Web ACL 的更新而中断。

不要在你的 AWS CloudFormation 网页 ACL 模板中管理 Shield Advanced 规则。Web ACL 模板不应列出 Shield Advanced 规则。请在 使用自动缓解的最佳实践 按照 Web ACL 管理的最佳实践进行操作。

使用运行状况检查进行基于运行状况的检测

您可以将 Shield Advanced 配置为使用运行状况检测，以提高攻击检测和缓解的响应能力和准确性。您可以将此选项用于除 Route 53 托管区域之外的任何资源类型。

要配置运行状况检测，您可以在 Route 53 中为资源定义运行状况检查，验证其报告运行状况是否正常，然后将其与您的 Shield Advanced 保护相关联。有关 Route 53 运行状况检查的信息，请参阅《Amazon Route 53 开发人员指南》中的 Amazon Route 53 如何检查资源的运行状况以及创建、更新和删除运行状况检查。

> **Note**
>
> Shield Response Team (SRT) 的主动参与支持需要进行运行状况检查。有关主动参与的信息，请参阅 配置主动参与。

运行状况检查根据您定义的要求衡量资源的运行状况。运行状况检查状态为 Shield Advanced 检测机制提供了重要输入，使它们对特定应用程序的当前状态更加敏感。

您可以为除 Route 53 托管区域之外的任何资源类型启用运行状况检测。

- 网络和传输层（第 3 层/第 4 层）资源：运行状况检测可提高网络负载均衡器、弹性 IP 地址和全局加速器标准加速器的网络层和传输层事件检测和缓解的准确性。当您使用 Shield Advanced 保护这些资源类型时，Shield Advanced 可以缓解较小的攻击，更快地缓解攻击，即使流量在应用程序的容量之内。

  添加运行状况检测后，如果关联的运行状况检查显示状况不佳，Shield Advanced 可采用更低的阈值，以更快的速度实施缓解措施。
- 应用程序层（第 7 层）资源 — 基于运行状况的检测提高了 CloudFront分布和应用程序负载均衡器的 Web 请求洪水检测的准确性。使用 Shield Advanced 保护这些资源类型时，根据请求特征，当流量出现统计意义上的显著偏差并与流量模式的显著变化相结合时，您就会收到 Web 请求泛洪检测警报。

  采用运行状况检测后，如果关联的 Route 53 运行状况检查显示状况不佳，则 Shield Advanced 可以就较小的偏差发出警报，并且可以更快地报告事件。相反，如果关联的 Route 53 运行状况检查显示状况正常，Shield Advanced 需要较大的偏差才会发出警报。

目录

- 运行状况检查示例
  - 亚马逊配 CloudFront 送
  - 负载均衡器
  - Amazon EC2 弹性 IP 地址（EIP）

使用 Shield Advanced 进行运行状况检查的最佳实践

在 Shield Advanced 中创建和使用运行状况检查时，请遵循本节中的最佳实践。

- 通过确定要监控的基础架构组件来规划运行状况检查。请考虑以下运行状况检查的资源类型：
  - 关键资源。
  - 任何您想在 Shield Advanced 检测和缓解中获得更高敏感度的资源。
  - 您希望 Shield Advanced 主动与您联系的资源。运行状况检查将为主动参与提供状态信息。

  您可能想要监控的资源示例包括亚马逊 CloudFront分配、面向互联网的负载均衡器和 Amazon EC2 实例。
- 使用尽可能少的通知来定义能够准确反映应用程序来源运行状况的运行状况检查。
  - 编写运行状况检查，这样只有当您的应用程序不可用或无法在可接受的参数范围内运行时，它们才会处于不健康状态。您负责根据应用程序的特定要求定义和维护运行状况检查。
  - 尽可能少地使用运行状况检查，同时仍能准确报告应用程序的运行状况。例如，来自应用程序多个区域的多个警报都报告了相同的问题，这可能会增加响应活动的运营费用，而不会增加信息价值。
  - 使用计算的运行状况检查，使用亚马逊 CloudWatch 指标的组合来监控应用程序的运行状况。例如，您可以根据应用程序服务器的延迟及其 5XX 错误率来计算组合运行状况，这表明原始服务器未完成请求。
  - 根据需要创建自己的应用程序运行状况指标并将其发布到 CloudWatch 自定义指标，并将其用于计算的运行状况检查。
- 实施和管理您的运行状况检查，以改善检测并减少不必要的维护活动。
  - 在将运行状况检查与 Shield Advanced 保护关联之前，请确保其处于正常状态。关联报告运行状况不佳的运行状况检查可能会影响受保护资源的 Shield Advanced 检测机制。
  - 让您的运行状况检查可用于 Shield Advanced。不要删除您在 Route 53 中用于 Shield Advanced 保护的运行状况检查。
  - 仅使用暂存和测试环境来测试您的运行状况检查。仅为需要生产级性能和可用性的环境维护运行状况检查关联。不要在 Shield Advanced 中为暂存和测试环境维护运行状况检查关联。

常用于运行状况检查的指标

本部分列出了运行状况检查中常用的亚马逊 CloudWatch 指标，这些指标用于衡量分布式拒绝服务 (DDoS) 事件期间的应用程序运行状况。有关每种资源类型的 CloudWatch 指标的完整信息，请参阅表格后面的列表。

主题

用于监控应用程序运行状况的指标

资源	指标	描述
Route 53	HealthCheckStatus	运行状况检查端点的状态。
CloudFront	5xxErrorRate	HTTP 状态代码为 5XX 的所有请求的百分比。这表示正在影响应用程序的攻击。
应用程序负载均衡器	HTTPCode_ELB_5XX_Count	负载均衡器生成的 HTTP 5xx 客户端错误代码的数量。
应用程序负载均衡器	RejectedConnectionCount	由于负载均衡器达到连接数上限被拒绝的链接的数量。
应用程序负载均衡器	TargetConnectionErrorCount	负载均衡器和目标之间连接建立不成功的次数。
应用程序负载均衡器	TargetResponseTime	请求离开负载均衡器直至收到来自目标的响应所用的时间（以秒为单位）。
应用程序负载均衡器	UnHealthyHostCount	被视为未正常运行的目标数量。
Amazon EC2	CPUUtilization	当前正在使用的已分配 EC2 计算单位的百分率。

每种资源类型的 Amazon CloudWatch 指标

有关受保护资源可用指标的更多信息，请参阅资源指南中的以下部分：

- 亚马逊 Route 53 — 使用亚马逊 Route 53 运行状况检查和亚马逊 Route 53 开发者指南 CloudWatch 中的亚马逊监控您的资源。
- 亚马逊 CloudFront -《亚马逊 CloudFront 开发者指南》 CloudWatch中的 “ CloudFront 使用亚马逊监控”。
- Application Load Balancer —《应用程序负载均衡器用户指南》中应用程序负载均衡器的 CloudWatch 指标。
- Network Load Balancer — 网络负载均衡器用户指南中您的网络负载均衡器的CloudWatch 指标。
- AWS Global Accelerator — AWS Global Accelerator在《 AWS Global Accelerator 开发者指南》中 CloudWatch 搭配使用 Amazon。
- 亚马逊 ElasticCompute Cloud — 在 https://docs.aws.amazon.com/ AWSEC 2/l UserGuide atest/ / 中列出您的实例的可用 CloudWatch 指标。
- Amazon EC2 Auto Scaling — Amazon EC2 A uto Scaling 用户指南中针对自动扩展组和实例的监控 CloudWatch 指标。

管理运行状况检查关联

如果运行状况检查仅在您的应用程序运行在可接受的参数范围内时才报告运行状况正常，而仅在运行状况不佳时才报告运行状况不佳，那么使用 Shield Advanced 的运行状况检查将使您受益最大。使用本节中的指导在 Shield Advanced 中管理您的运行状况检查关联。

> **Note**
>
> Shield Advanced 不会自动管理您的运行状况检查。

使用 Shield Advanced 进行运行状况检查需要满足以下条件：

- 将运行状况检查与 Shield Advanced 保护关联时，运行状况检查必须报告运行状况正常。
- 运行状况检查必须与受保护资源的运行状况相关。您负责定义和维护运行状况检查，以根据应用程序的特定要求准确报告应用程序的运行状况。
- 运行状况检查必须保持可用状态，以供 Shield Advanced 保护使用。不要删除您在 Route 53 中用于 Shield Advanced 保护的运行状况检查。

主题

将运行状况检查与您的资源相关联

以下过程显示如何将 Amazon Route 53 运行状况检查与受保护资源相关联。

> **Note**
>
> 在将运行状况检查与 Shield Advanced 保护关联之前，请确保其处于正常状态。有关信息，请参阅《Amazon Route 53 开发人员指南》中的监控运行状况检查状态和获取通知。

关联运行状况检查

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护选项卡上，选择要与运行状况检查关联的资源。
4. 选择配置保护。
5. 选择下一步，直到进入配置基于运行状况检查的 DDoS 检测（可选）页面。
6. 在 关联运行状况检查 下，选择要与保护关联的运行状况检查的 ID。

   > **Note**
   >
   > 如果您没有看到所需的运行状况检查，请转到 Route 53 控制台并验证运行状况检查及其 ID。有关信息，请参阅创建和更新运行状况检查。

7. 浏览其余页面，直到完成配置。在保护页面上，将列出您更新的资源运行状况检查关联。
8. 在保护页面上，检查您新关联的运行状况检查是否报告正常。

   当运行状况检查报告运行状况不佳时，您无法成功开始在 Shield Advanced 中使用运行状况检查。这样做会导致 Shield Advanced 在非常低的阈值下检测到误报，还可能对 Shield Response Team (SRT) 为资源提供主动参与的能力产生负面影响。

如果新关联的运行状况检查报告运行状况不佳，请执行以下操作：

a. 在 Shield Advanced 中取消运行状况检查与您的保护的关联。
b. 在 Amazon Route 53 中重新查看您的运行状况检查规范，并验证您的整体应用程序性能和可用性。
c. 如果您的应用程序在运行状况正常的参数范围内运行，并且运行状况检查报告运行状况正常，请再次尝试在 Shield Advanced 中关联运行状况检查。

当您建立了新的运行状况检查关联并在 Shield Advanced 中报告运行状况正常后，运行状况检查关联程序即告完成。

取消运行状况检查与资源的关联

以下过程说明如何解除 Amazon Route 53 运行状况检查与受保护资源的关联。

取消运行状况检查的关联

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护选项卡上，选择要取消与运行状况检查关联的资源。
4. 选择配置保护。
5. 选择下一步，直到进入配置基于运行状况检查的 DDoS 检测（可选）页面。
6. 在关联运行状况检查下，选择列为 - 的空选项。
7. 浏览其余页面，直到完成配置。

在保护页面上，您的资源的运行状况检查字段设置为 -，表示没有运行状况检查关联。

运行状况检查关联状态

您可以在 AWS WAF 和 Shield 控制台的受保护资源页面和每个资源的详细信息页面上查看与保护相关的运行状况检查的状态。

- 正常：运行状况检查可用且报告运行状况正常。
- 不佳：运行状况检查可用且报告运行状况不佳。
- 不可用：运行状况检查对 Shield Advanced 不可用。

解决不可用运行状况检查

创建并使用新的运行状况检查。在运行状况检查在 Shield Advanced 中处于不可用状态后，不要再次尝试关联该检查。

有关执行这些步骤的详细指导，请参阅前面的主题。

1. 在 Shield Advanced 中，取消运行状况检查与资源的关联。
2. 在 Route 53 中，为资源创建新的运行状况检查并记下其 ID。有关信息，请参阅《Amazon Route 53 开发人员指南》中的创建和更新运行状况检查。
3. 在 Shield Advanced 中，将新的运行状况检查与资源关联。

运行状况检查示例

本节显示了可以在计算的运行状况检查中使用的运行状况检查示例。计算后的运行状况检查使用多个单独的运行状况检查来确定组合状态。每项运行状况检查的状态取决于终端节点的运行状况或 Amazon CloudWatch 指标的状态。您可以将运行状况检查合并到计算的运行状况检查，然后配置计算运行状况检查，根据单个运行状况检查的合并运行状况检查来报告运行状况。根据您对应用程序性能和可用性的要求，调整计算运行状况检查的敏感度。

有关计算的运行状况检查的信息，请参阅 Amazon Route 53 开发人员指南中的监控其他运行状况检查（计算出的运行状况检查）。有关更多信息，请参阅博客文章 Route 53 改进：计算运行状况检查和延迟检查。

主题

- 亚马逊配 CloudFront 送
- 负载均衡器
- Amazon EC2 弹性 IP 地址（EIP）

亚马逊配 CloudFront 送

以下示例描述了可以组合为 CloudFront 分配的计算运行状况检查的运行状况检查：

- 通过为提供动态内容的分发上的路径指定域名来监控端点。运行状况响应将包括 HTTP 响应代码 2XX 和 3XX。
- 监控正在测量 CloudFront 源站健康状况的 CloudWatch 警报的状态。例如，您可以维护有关 Application Load Balancer 指标的 CloudWatch 警报`TargetResponseTime`，并创建反映警报状态

的运行状况检查。当从请求离开负载均衡器到负载均衡器收到来自目标的响应之间的响应时间超过警报中配置的阈值时，运行状况检查可能不佳。

- 监控警报的状态，该 CloudWatch 警报衡量响应的 HTTP 状态代码为 5xx 的请求的百分比。如果 CloudFront 分布的 5xx 错误率高于 CloudWatch 警报中定义的阈值，则此运行状况检查的状态将切换为不健康。

负载均衡器

以下示例描述了可用于应用程序负载均衡器、网络负载均衡器或全局加速器标准加速器的计算运行状况检查的运行状况检查。

- 监控警报的状态，该 CloudWatch 警报测量客户端与负载均衡器建立的新连接的数量。您可以将平均新连接数的警报阈值设置为比每天的平均值高出一定程度。每种资源类型的指标如下：
  - 应用程序负载均衡器：`NewConnectionCount`
  - 网络负载均衡器：`ActiveFlowCount`
  - 全局加速器：`NewFlowCount`
- 对于 Application Load Balancer 和 Network Load Balancer，监控 CloudWatch 警报的状态，该警报用于衡量被认为运行状况良好的负载均衡器数量。您可以在可用区或负载均衡器所需的最低运行状况主机数上设置警报阈值。负载均衡器资源的可用指标如下：
  - 应用程序负载均衡器：`HealthyHostCount`
  - 网络负载均衡器：`HealthyHostCount`
- 对于 Application Load Balancer，监控 CloudWatch 警报的状态，该警报用于测量负载均衡器目标生成的 HTTP 5xx 响应代码数量。对于应用程序负载均衡器，您可以使用指标 `HTTPCode_Target_5XX_Count`，并根据负载均衡器所有 5XX 错误的总和来设置警报阈值。

Amazon EC2 弹性 IP 地址（EIP）

以下运行状况检查示例可以合并到针对 Amazon EC2 弹性 IP 地址的计算运行状况检查中：

- 为弹性 IP 地址指定 IP 地址，监控端点。只要能够与 IP 地址后面的资源建立 TCP 连接，运行状况检查就会保持正常状态。
- 监控警报的状态，该 CloudWatch 警报用于衡量实例上当前正在使用的已分配 Amazon EC2 计算单元的百分比。您可以使用 Amazon EC2 指标 `CPUUtilization`，并根据您认为的应用程序 CPU 高利用率（如 90%）来设置警报阈值。

在中管理资源保护 AWS Shield Advanced

使用本节中的指南为您的资源管理 Shield Advanced 保护。

> **Note**
>
> Shield Advanced 仅保护你在 Shield Advanced 中或通过 Shi AWS Firewall Manager eld Advanced 策略指定的资源。它不会自动保护您的资源。

如果您使用的是 AWS Firewall Manager Shield Advanced 策略，则无需管理针对该政策范围内的资源的保护。Firewall Manager 会根据策略配置自动管理对策略范围内的账户和资源的保护。有关更多信息，请参阅 AWS Shield Advanced 政策。

主题

- 为 AWS 资源添加 AWS Shield Advanced 保护
- 配置 AWS Shield Advanced 保护
- 移除对 AWS 资源的 AWS Shield Advanced 保护

为 AWS 资源添加 AWS Shield Advanced 保护

按照本节中的指导，为一个或多个资源添加 Shield Advanced 保护。

为 AWS 资源添加保护

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在导航窗格中， AWS Shield 选择受保护的资源。
3. 选择添加要保护的资源。
4. 在选择要使用 Shield Advanced 保护的资源页面的指定区域和资源类型中，提供要保护的资源的区域和资源类型规格。您可以通过选择所有区域来保护多个区域中的资源，也可以通过选择全局将选择范围缩小到全局资源。您可以取消选择任何不想保护的资源类型。有关您的资源类型保护的信息，请参阅 AWS Shield Advanced 按资源类型划分的保护。
5. 选择加载资源。Shield Advanced 会使用符合您条件的 AWS 资源填充选择资源部分。
6. 在选择资源 部分，您可以通过在资源列表中输入要搜索的字符串来筛选资源列表。

选择要保护的资源。

7. 在标签部分，如果要为正在创建的 Shield Advanced 保护添加标签，请指定这些标签。有关标记 AWS 资源的信息，请参阅使用标签编辑器。
8. 选择使用 Shield Advanced 保护。这为资源增加了 Shield Advanced 保护。

配置 AWS Shield Advanced 保护

您可以随时更改 AWS Shield Advanced 保护设置。为此，您可以查看所选的保护选项，并修改需要更改的设置。

管理受保护资源

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护选项卡中，选择要保护资源。
4. 选择所需的配置保护和资源规格选项。
5. 浏览每个资源保护选项，根据需要进行更改。

配置应用程序层 DDoS 保护

为了防范对 Amazon CloudFront 和 Application Load Balancer 资源的攻击，您可以添加 AWS WAF 网页 ACL 并添加基于速率的规则。有关此问题的信息，请参阅 Shield 高级应用层 AWS WAF Web ACL 和基于速率的规则。

您还可以启用 Shield Advanced 应用程序层 DDoS 自动缓解配合使用。有关 AWS WAF 工作原理的信息，请参阅AWS WAF。有关自动缓解功能的信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

> **Important**
>
> 如果您通过 AWS Firewall Manager 使用 Shield Advanced 策略来管理 Shield 高级保护，则无法在此处管理应用层保护。对于所有其他资源，我们建议至少为每个资源关联一个 Web ACL，即使该 Web ACL 不包含任何规则。

> **Note**
>
> 当您为资源启用应用程序层 DDoS 自动缓解时，如果需要，该操作会自动向您的账户添加服务相关角色，从而为 Shield Advanced 提供管理 Web ACL 保护所需的权限。有关信息，请参阅使用 Shield Advance 的服务相关角色。

配置应用程序层 DDoS 保护

1. 在配置第 7 层 DDoS 保护页面中，如果资源尚未与 Web ACL 关联，则可以选择现有的 Web ACL 或创建自己的网络 ACL。

   要创建 Web ACL，请执行以下操作：

   a. 选择 创建 Web ACL。

   b. 输入名称。Web ACL 在创建之后无法更改名称。

   c. 选择 创建。

   > **Note**
   >
   > 如果资源已与一个 Web ACL关联，则不能更改为其他 Web ACL。如果要更改 Web ACL，您必须先从资源中删除关联的 Web ACL。有关更多信息，请参阅 将 Web ACL 与资源关联或取消关联 AWS。

2. 如果 Web ACL 未定义基于速率的规则，则可以选择添加速率限制规则，然后执行以下步骤来添加规则：

   a. 输入名称。

   b. 输入速率限制。这是在对 IP 地址应用基于速率的规则操作之前，在任何 5 分钟内允许来自任何单个 IP 地址的最大请求数。当来自该 IP 地址的请求低于限制时，该操作将停止。

   c. 将规则操作设置为在 IP 地址的请求计数超过限制时对 IP 的请求进行计数或阻止。规则操作的应用和删除可能会在 IP 地址请求速率更改一两分钟后生效。

   d. 选择 添加规则。

3. 对于应用程序层 DDoS 攻击自动缓解，请选择是否希望 Shield Advanced 代表您自动缓解 DDoS 攻击，如下所示：

- 要启用自动缓解，请选择 “启用”，然后选择希望 Shield Advanced 在其自定义规则中使用的规则操作。 AWS WAF 您的选择是 Count 和 Block。有关这些 AWS WAF 规则操作的信息，请参阅规则操作。有关 Shield Advanced 如何管理此操作设置的信息，请参阅 Shield Advanced 如何管理规则操作设置。
- 要禁用自动缓解，请选择禁用。
- 要使您管理的资源的自动缓解设置保持不变，请保留默认选项保持当前设置。

有关 Shield Advanced 应用程序层 DDoS 自动缓解的更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

4. 选择下一步。

创建警报和通知

以下过程说明如何管理受保护资源的 CloudWatch 警报。

> **Note**
>
> CloudWatch 会产生额外费用。有关 CloudWatch 定价，请参阅 Amazon CloudWatch 定价。

创建警报和通知

1. 在保护页面创建警报和通知（可选）中，为要接收的警报和通知配置 SNS 主题。对于不想接收通知的资源，请选择 无主题。可以添加一个 Amazon SNS 主题，也可以创建一个新的主题。
2. 要创建 Amazon SNS 主题，请执行以下步骤：
   a. 从下拉列表中，选择创建 SNS 主题。
   b. 输入主题名称。
   c. 可选择输入 Amazon SNS 消息将发送到的电子邮件地址，然后选择添加电子邮件地址。可以输入多个。
   d. 选择 创建。
3. 选择下一步。

移除对 AWS 资源的 AWS Shield Advanced 保护

您可以随时取消对任何 AWS 资源的 AWS Shield Advanced 保护。

> **Important**
>
> 删除 AWS 资源并不会从中移除该资源 AWS Shield Advanced。您还必须从中移除对资源的保护 AWS Shield Advanced，如本过程所述。

移除对 AWS 资源的 AWS Shield Advanced 保护

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护选项卡中，选择要删除其保护的资源。
4. 选择删除保护。
   - 如果您为保护配置了 Amazon CloudWatch 警报，则可以选择删除警报和保护。如果您选择此时不删除警报，则可以在以后使用 CloudWatch 控制台将其删除。

> **Note**
>
> 对于配置了 Amazon Route 53 运行状况检查的保护，如果稍后再次添加保护，则保护仍会包括该运行状况检查。

前面的步骤取消了对特定 AWS 资源的 AWS Shield Advanced 保护。他们不会取消您的 AWS Shield Advanced 订阅。您将继续为该服务付费。有关您的 AWS Shield Advanced 订阅的信息，请联系AWS Support 中心。

从 Shield 高级保护中移除 CloudWatch 警报

要从 Shield 高级防护中移除 CloudWatch 警报，请执行以下任一操作：

- 删除保护，如移除对 AWS 资源的 AWS Shield Advanced 保护中所述。确保选中 同时删除相关的 DDoSDetection 警报 旁边的复选框。

- 使用 CloudWatch 控制台删除警报。要删除的警报的名称以 DDoS DetectedAlarmForProtection 开头。

AWS Shield Advanced 保护小组

使用保护组创建受保护资源的逻辑集合，并将其保护作为一个组进行管理。有关管理资源保护的信息，请参阅 配置 AWS Shield Advanced 保护。

> **Note**
>
> 应用程序层 DDoS 自动缓解不会与保护组交互。您可以为保护组中的资源启用自动缓解，但是 Shield Advanced 不会根据保护组的调查发现自动应用攻击缓解措施。Shield Advanced 会对单个资源进行自动攻击缓解。

AWS Shield Advanced 保护组通过将多个受保护资源视为一个单元，为您提供了一种自助服务方式，可以自定义检测和缓解的范围。资源分组可以带来许多好处。

- 提高检测的准确性。
- 减少不可操作的事件通知。
- 扩大缓解措施的覆盖范围，将事件期间也可能受到影响的受保护资源包括在内。
- 加快缓解多个相似目标攻击的时间。
- 促进对新创建的受保护资源的自动保护。

在蓝/绿交换等情况下，保护组可以帮助减少误报，在这种情况下，资源在接近零负载和满载之间交替出现。另一种情况是，您在保持群组成员共享的负载水平的同时频繁创建和删除资源。对于此类情况，监控单个资源可能会导致误报，而监控资源组的运行状况则不会导致误报。

您可以将保护组配置为包括所有受保护的资源、特定资源类型的所有资源或单独指定的资源。满足保护组条件的新受保护资源将自动包含在您的保护组中。受保护资源可归属于多个保护组。

管理 AWS Shield Advanced 保护组

使用本节中的指导来管理您的保护组配置。

创建 Shield Advanced 保护组

创建保护组

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 选择保护组选项卡，然后选择创建保护组。
4. 在创建保护组页面中，为您的组提供一个名称。您将使用此名称来标识受保护资源列表中的群组。在创建保护组后，您无法更改其名称。
5. 在保护分组条件中，选择您希望 Shield Advanced 用来标识要包含在组中的受保护资源的条件。根据您选择的条件进行其他选择。
6. 对于聚合，选择希望 Shield Advanced 如何合并群组的资源数据，以检测、缓解和报告事件。
   - 总计：使用整个群组的总流量。对于大多数情况，这是一个很好的选择。例如，可手动或自动扩展的 Amazon EC2 实例的弹性 IP 地址。
   - 均值：使用整个群组的平均流量。对于统一共享流量的资源，这是一个很好的选择。例如，加速器和负载均衡器。
   - 最大：使用每个资源的最大流量。这对于不共享流量的资源以及以非统一方式共享流量的资源很有用。示例包括用于 CloudFront 分配的 Amazon CloudFront 分配和来源资源。
7. 选择保存以保存您的保护组并返回到受保护资源页面。

在 Shield 事件页面中，您可以查看保护组的事件，并深入查看该组中受保护资源的其他信息。

更新 Shield Advanced 保护组

更新保护组

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护组选项卡中，选中要修改的保护组旁边的复选框。
4. 在保护组页面上，选择编辑。对保护组设置进行更改。
5. 选择 保存 以保存您的更改。

删除 Shield Advanced 保护组

删除保护组

1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择受保护的资源。
3. 在保护组选项卡中，选中要删除的保护组旁边的复选框。
4. 在保护组的页面中，选择删除并确认操作。

在中跟踪资源保护的变化 AWS Config

您可以使用记录对资源 AWS Shield Advanced 保护的更改 AWS Config。然后，您可以使用此信息来维护配置更改历史记录以进行审核和故障排除。

要记录保护更改，请 AWS Config 为要跟踪的每个资源启用该选项。有关更多信息，请参阅《AWS Config 开发人员指南》中的 AWS Config入门

您必须 AWS Config 为 AWS 区域 包含跟踪资源的每个资源启用。您可以 AWS Config 手动启用，也可以在《AWS CloudFormation 用户指南》的 “AWS CloudFormation StackSets 示例 AWS CloudFormation 模板 AWS Config” 中使用 “启用” 模板。

如果您启用 AWS Config，则会按AWS Config 定价页面上的详细信息向您收费。

> **Note**
>
> 如果您已经 AWS Config 启用了必要的区域和资源，则无需执行任何操作。 AWS Config 有关资源保护更改的日志开始自动填充。

启用后 AWS Config，使用 AWS Config 控制台中的美国东部（弗吉尼亚北部）区域查看 AWS Shield Advanced 全球资源的配置更改历史记录。

通过 AWS Config 控制台查看美国东部（弗吉尼亚北部）、美国东部（俄亥俄州）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、欧洲（爱尔兰）、欧洲（法兰克福）、亚太地区（东京）和亚太地区（悉尼）地区的 AWS Shield Advanced 区域资源的变更历史记录。

对 DDoS 事件的可见性

AWS Shield 提供对以下类别的事件和事件活动的可见性：

- 全局：所有客户都可以访问过去两周全局威胁活动的汇总视图。您可以在控制台的 “入门” 和 “全球威胁” AWS Shield 控制面板页面下看到此信息。有关更多信息，请参阅 AWS Shield 全球活动和账户活动。
- 账户：所有客户都可以访问其账户上一年度的事件摘要。您可以在 AWS Shield 控制台的 “入门” 页面下看到此信息。有关更多信息，请参阅 AWS Shield 全球活动和账户活动。

当您订阅 Shield Advanced 并为您的资源添加保护时，您可以访问有关受保护资源的事件和 DDoS 攻击的其他信息：

- 受保护资源上的事件 — Shield Advanced 通过 AWS Shield 控制台的 “事件” 页面提供每个事件的详细信息。有关更多信息，请参阅 AWS Shield Advanced 事件。
- 受保护资源的事件指标 — Shield Advanced 会发布其保护的所有资源的检测、缓解和主要贡献者 Amazon CloudWatch 指标。您可以使用这些指标来配置 CloudWatch 仪表板和警报。有关更多信息，请参阅 AWS Shield Advanced 指标。
- 受保护资源的跨账户事件可见性 — 如果您使用 AWS Firewall Manager 管理您的 Shield Advanced 防护，则可以通过将 Firewall Manager 与 AWS Security Hub结合使用来启用跨多个帐户的保护可见性。有关更多信息，请参阅 所有账户内的事件可见性。

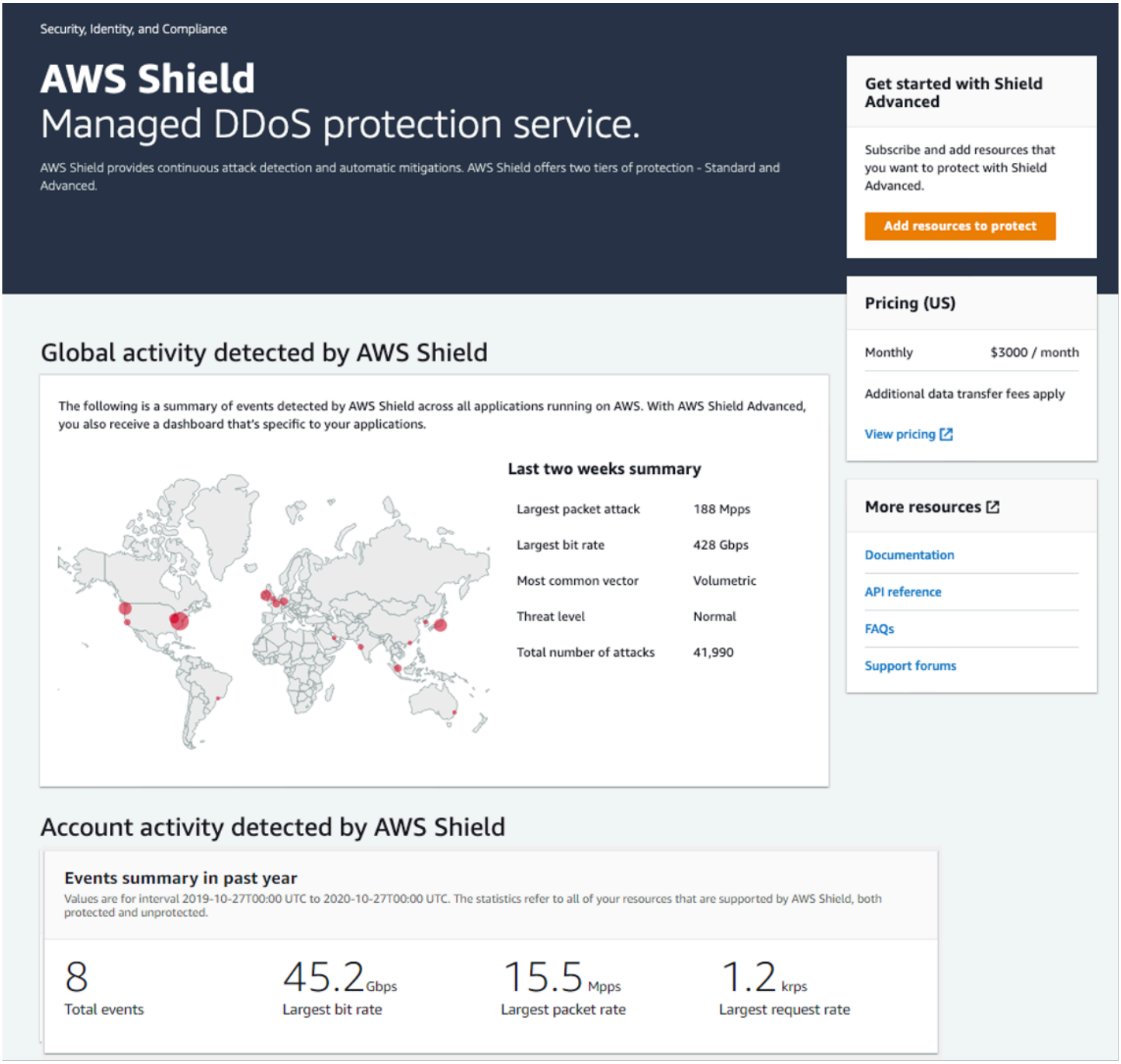
如果您为应用层保护启用自动应用层 DDoS 缓解，

主题

AWS Shield 全球活动和账户活动

您可以在控制台的 “入门” 和 “全球威胁 AWS Shield 控制面板” 页面中访问全球威胁活动的汇总视图和每个账户的事件摘要。

以下屏幕截图显示一个开始使用页面示例。



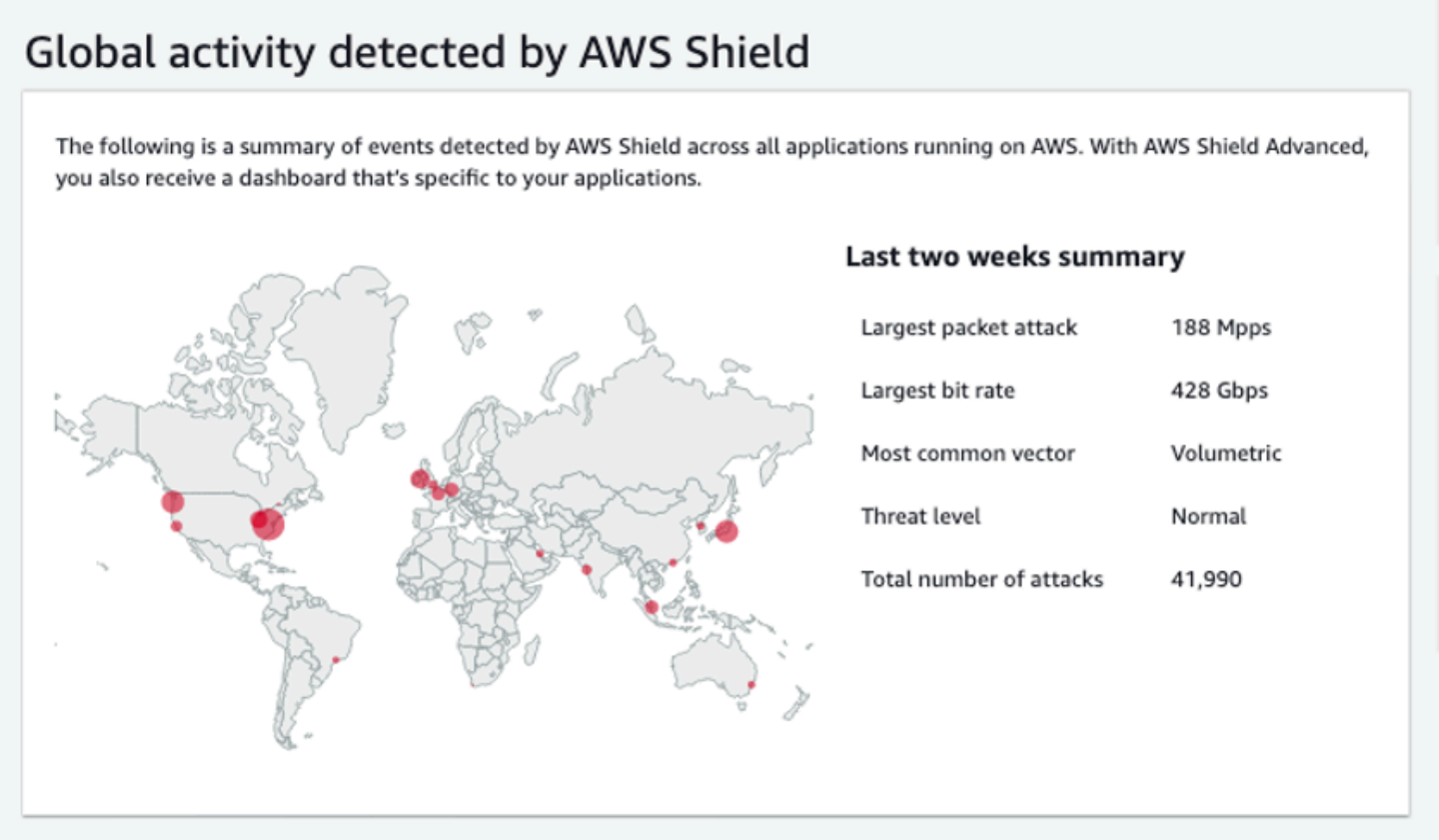
访问控制 AWS Shield 台

- 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。

您无需订阅 Shield Advanced 即可访问全局活动和账户活动摘要信息。

全局活动

此信息可通过控制台的 “全球威胁” AWS Shield 控制面板和 “入门” 页面获得。以下屏幕截图显示了全局活动窗格的一个示例。



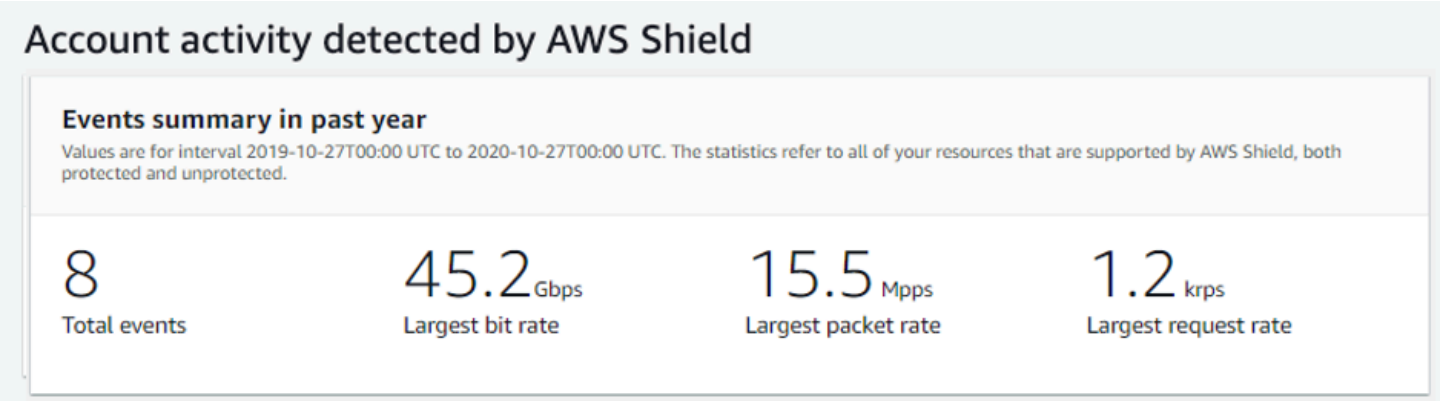
全球活动描述了在所有 AWS 客户中观察到的 DDoS 事件。每小时 AWS 更新一次，更新前两周的信息。在控制台窗格中，您可以看到按 AWS 区域划分并显示在世界热图上的结果。在地图旁边，Shield 显示摘要信息，例如最大数据包攻击、最大比特率、最常见矢量、攻击总数和威胁级别。威胁级别是对当前全局活动与 AWS 通常观察到的活动进行比较的评估。默认威胁级别值为正常。对于提升的 DDoS 活动， AWS 会自动将该值更新为高。

全局威胁控制面板还提供时间序列指标，使您能够在持续时间之间进行更改。要查看重大 DDoS 攻击的历史记录，您可以自定义控制面板，查看从过去一天到最近两周的视图。时间序列指标提供了在您选择的时间窗口内为正在运行的应用程序检测到的所有事件的最大比特率、数据包速率或请求速率的视图。 AWS Shield AWS

账户活动

此信息可在 AWS Shield 控制台的 “入门” 页面中找到。

以下屏幕截图显示了账户活动窗格的一个示例。



账户活动描述了 Shield 为您的资源检测到的符合 Shield Advanced 保护条件的 DDoS 事件。每天，Shield 都会为截至前一天 00:00 UTC 的年度创建摘要指标，然后显示事件总数、最大比特率、最大数据包速率和最大请求速率。

- 事件总数指标反映了 Shield 每次在发往您的应用程序的流量中观察到的可疑属性。可疑属性可能包括高于正常水平的流量、与应用程序的历史配置文件不匹配的流量，或者与 Shield 为有效应用程序流量定义的启发式方法不匹配的流量。
- 每种资源都有最大比特率和最大数据包速率统计信息。
- 最大的请求率统计数据仅适用于具有关联 AWS WAF Web ACL 的 Amazon CloudFront 分配和应用程序负载均衡器。

> **Note**
>
> 您还可以通过 AWS Shield API 操作访问账户级别的事件摘要DescribeAttackStatistics。

AWS Shield Advanced 事件

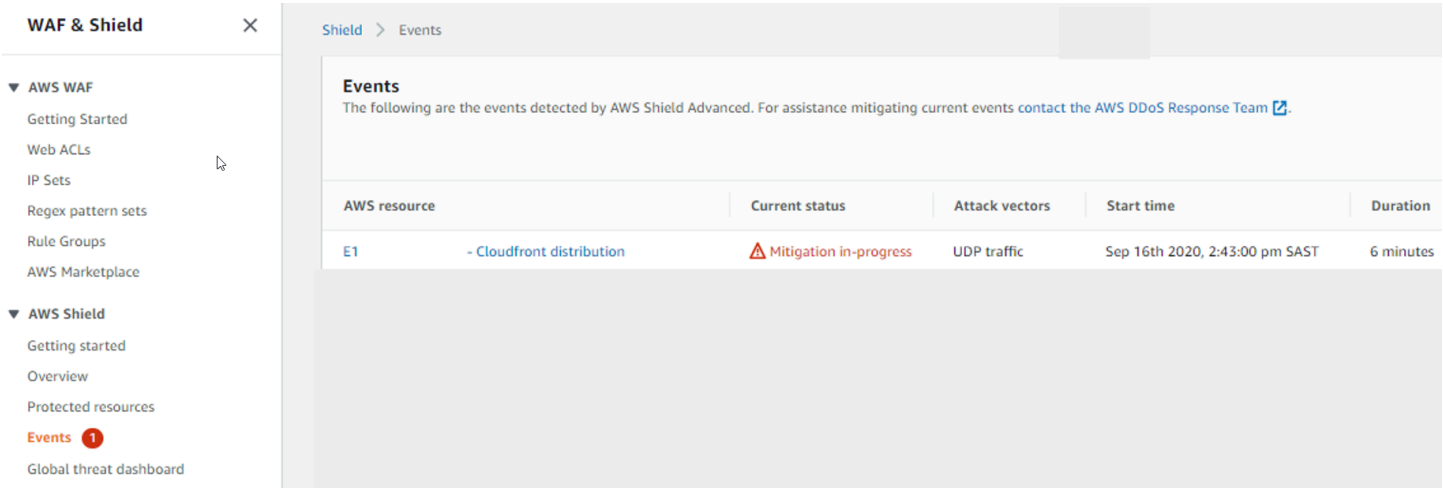
当您订阅 Shield Advanced 并保护您的资源时，您就可以访问资源的其他可见性功能。其中包括对 Shield Advanced 检测到的事件的近实时通知，以及有关检测到的事件和缓解措施的其他信息。

> **Note**
>
> 你在 Shield Advanced 控制台中的事件信息基于 Shield Advanced 的指标。有关 Shield 高级指标的信息，请参阅 AWS Shield Advanced 指标

AWS Shield 从多个维度评估流向受保护资源的流量。当检测到异常时，Shield Advanced 会为每个受影响的资源创建一个单独的事件。

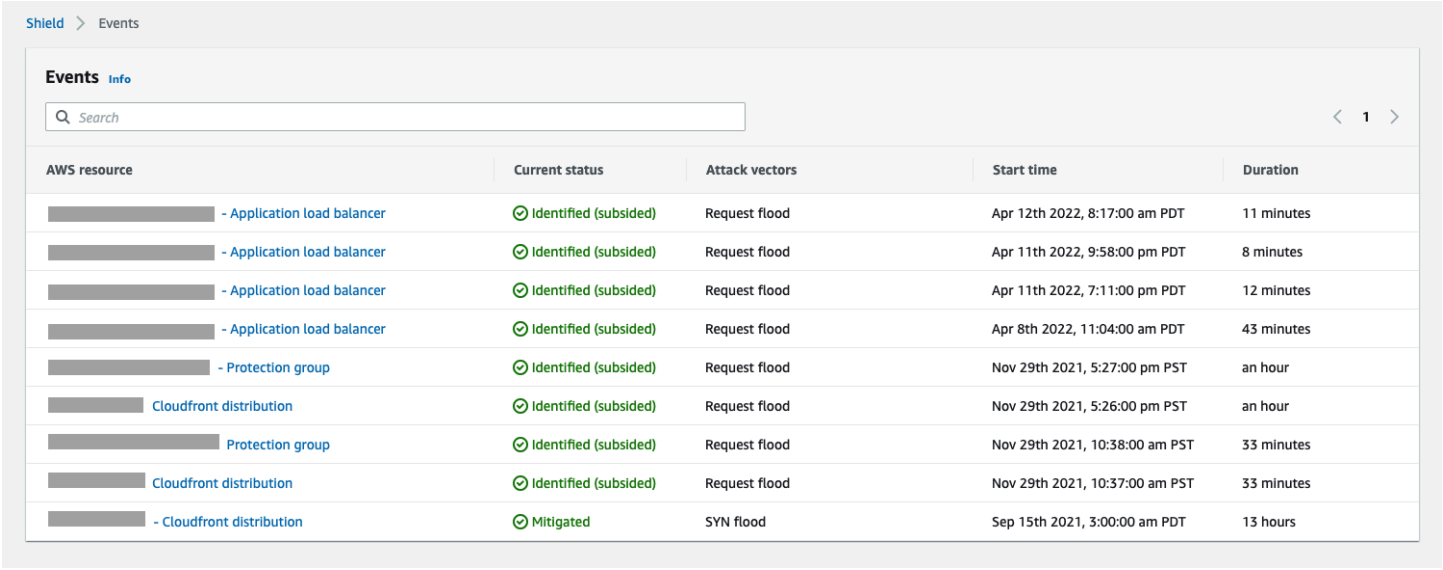
您可以通过 Shield 控制台的事件页面访问事件摘要和详细信息。顶级事件页面概述了当前和过去的事件。

以下屏幕截图显示了一个事件页面示例，其中有一个正在进行的事件。左侧导航窗格中也会标记此活跃事件。



Shield Advanced 还可能自动缓解攻击，具体取决于流量类型和您配置的保护措施。这些缓解措施可以保护您的资源免于承受超额流量或与已知 DDoS 攻击特征相匹配的流量。

以下屏幕截图显示了一个事件列表示例，其中所有事件均已由 Shield Advanced 缓解或自行消退。



在活动开始前保护您的资源

在资源遭受 DDoS 攻击之前，使用 Shield Advanced 在接收正常预期流量时对其进行保护，从而提高事件检测的准确性。

为了准确报告受保护资源的事件，Shield Advanced 必须首先为其建立预期流量模式的基准。

- Shield Advanced 会在资源受到保护至少 15 分钟后报告基础设施层事件。
- Shield Advanced 会在资源受到保护至少 24 小时后报告资源的 Web 应用程序层事件。在 Shield Advanced 观察到预期流量 30 天后，应用程序层事件的检测精度最高。

在 AWS Shield 控制台中访问事件信息

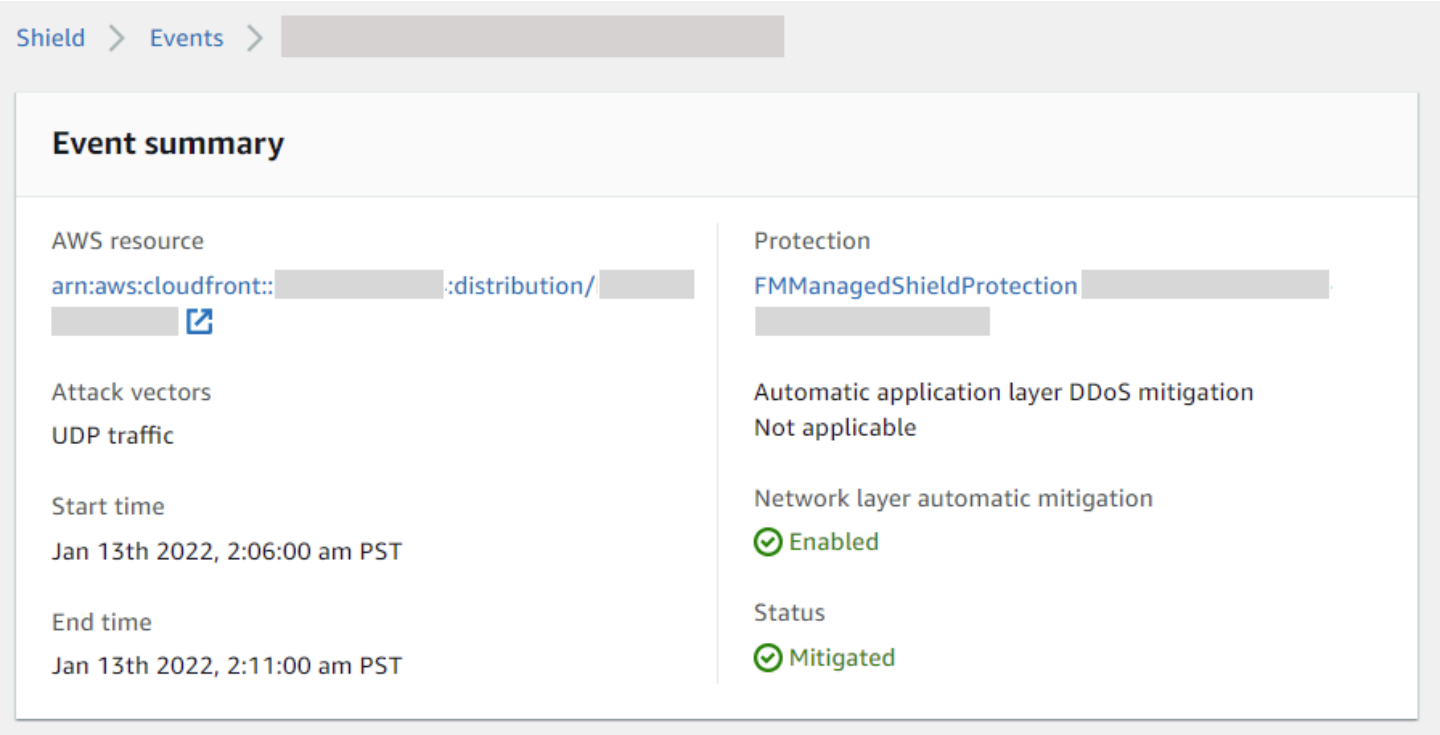
1. 登录 AWS Management Console 并打开 AWS WAF & Shield 控制台，网址为 https://console.aws.amazon.com/wafv2/。
2. 在 AWS Shield 导航窗格中，选择事件。控制台显示事件页面。
3. 在事件页面中，您可以选择列表中的任何事件，以查看该事件的其他摘要信息和详细信息。

主题

AWS Shield Advanced 活动摘要

您可以在活动的控制台页面中查看活动的摘要和详细信息。要打开活动页面，请从 “活动” 页面列表中选择其 AWS 资源名称。

以下屏幕截图显示了网络层事件的示例事件摘要。



活动页面摘要信息包含以下内容：

- 当前状态：表示事件状态以及 Shield Advanced 对事件采取的操作的值。状态值适用于基础设施层（第 3 层或第 4 层）和应用程序层（第 7 层）事件。
  - 已识别（进行中）和已识别（已消退）：表明 Shield Advanced 检测到了事件，但到目前为止尚未对其采取任何行动。已识别（消退）表示 Shield 检测到的可疑流量在没有干预的情况下停止活动。
  - 正在进行缓解和已缓解：表明 Shield Advanced 检测到事件并已对其采取措施。当目标资源是 Amazon CloudFront 分配或 Amazon Route 53 托管区域（它们有自己的自动内联缓解措施）时，也可以使用缓解措施。
- 攻击向量：DDoS 攻击向量，例如 TCP SYN 泛洪和请求泛洪等 Shield Advanced检测启发式方法。这些可能是 DDoS 攻击的迹象。
- 开始时间：检测到第一个异常流量数据点的日期和时间。
- 持续时间或结束时间：表示从事件开始时间到 Shield Advanced 观察到的最后一个异常数据点之间的时间间隔。在活动进行期间，这些值将继续增加。
- 保护：命名与资源关联的 Shield Advanced 保护，并提供指向其保护页面的链接。这可在单个活动的页面上找到。

- 应用程序层 DDoS 自动缓解：用于应用程序层保护，以指示是否为资源启用了 Shield Advanced 应用程序层 DDoS 自动缓解。如果已启用，则会提供访问和管理配置的链接。这可在单个活动的页面上找到。
- 网络层自动缓解：表示资源在网络层是否具有自动缓解功能。如果资源具有网络层组件，则它将启用该组件。该信息可在单个活动的页面上找到。

对于经常成为攻击目标的资源，Shield 可能会在过剩流量消退后保留缓解措施，以防止事件再次发生。

> **Note**
>
> 您还可以通过 AWS Shield API 操作访问受保护资源的事件摘要ListAttacks。

AWS Shield Advanced 活动详情

您可以在事件控制台页面的底部查看有关事件检测、缓解和主要贡献者的详细信息。此部分可能包括合法流量和潜在有害流量的组合，可能既代表传递到受保护资源的流量，也代表被 Shield 缓解措施阻止的流量。

- 检测和缓解：提供有关观察到的事件以及针对该事件采取的任何缓解措施的信息。有关事件缓解的信息，请参阅 响应 DDoS 事件。
- 排名靠前的贡献者：对活动中涉及的流量进行分类，并列出 Shield 为每个类别确定的主要流量来源。对于应用层事件，请使用排名靠前的贡献者信息来大致了解事件的性质，但要使用 AWS WAF 日志来做出安全决策。有关更多信息，请参阅下面的部分。

你在 Shield Advanced 控制台中的事件信息基于 Shield Advanced 的指标。有关 Shield 高级指标的信息，请参阅 AWS Shield Advanced 指标

Amazon CloudFront 或 Amazon Route 53 资源的缓解指标不包括在内，因为这些服务受缓解系统的保护，该系统始终处于启用状态，不需要对单个资源进行缓解。

详细信息部分根据信息是针对基础设施层还是应用程序层事件而有所不同。

应用程序层事件详细信息

您可以在事件控制台页面的底部查看有关应用程序层事件的检测、缓解和主要贡献者的详细信息。此部分可能包括合法流量和潜在有害流量的组合，可能既代表传递到受保护资源的流量，也可能代表被 Shield Advanced 缓解措施屏蔽的流量。

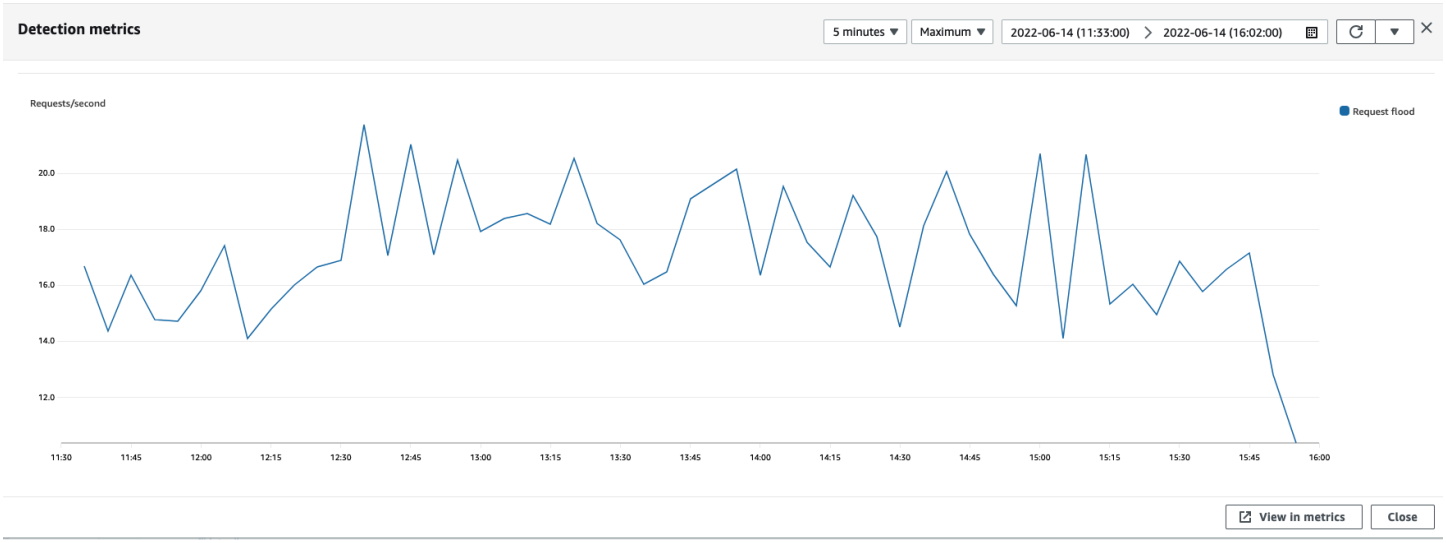
缓解详细信息适用于 Web ACL 中与资源关联的所有规则，包括专门为响应攻击而部署的规则和在 Web ACL 中定义的基于速率的规则。如果您为应用程序启用自动应用层 DDoS 缓解，则缓解指标将包括这些额外规则的指标。有关这些应用层保护的信息，请参阅AWS Shield Advanced 应用层（第 7 层）保护。

检测和缓解

对于应用层（第 7 层）事件，“检测和缓解” 选项卡显示基于从 AWS WAF 日志中获取的信息的检测指标。缓解指标基于关联 Web ACL 中的 AWS WAF 规则，这些规则配置为阻止不需要的流量。

对于亚马逊 CloudFront 分配，您可以将 Shield Advanced 配置为自动为您应用缓解措施。对于任何应用程序层资源，您都可以选择在 Web ACL 中定义自己的缓解规则，也可以向 Shield 响应小组 (SRT) 请求帮助。有关这些选项的信息，请参阅 响应 DDoS 事件。

以下屏幕截图显示了应用程序层事件的检测指标示例，该事件在数小时后消退。



在缓解规则生效之前消退的事件流量不会显示在缓解指标中。这可能会导致检测图中显示的 Web 请求流量与缓解图表中显示的允许和阻止指标之间存在差异。

排名靠前的贡献者

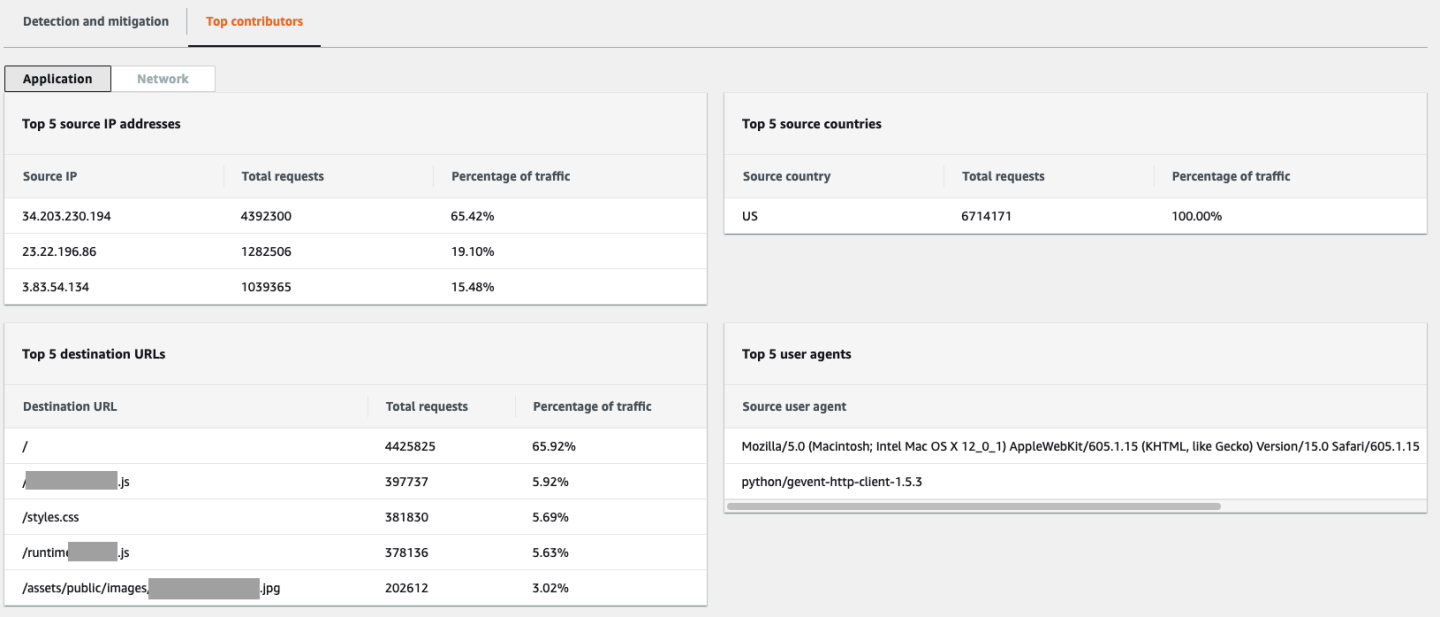
应用层事件的热门贡献者选项卡显示 Shield 根据检索到的 AWS WAF 日志为该事件确定的前 5 个贡献者。Shield 按来源 IP、来源国家和目标 URL 等维度对排名靠前的贡献者的信息进行分类。

> **Note**
>
> 要获得有关导致应用层事件的流量的最准确信息，请使用日 AWS WAF 志。

Shield 应用程序层排名靠前的贡献者信息应仅用于大致了解攻击的性质，不要据此做出安全决策。对于应用层事件， AWS WAF 日志是了解攻击的起因者和制定缓解策略的最佳信息来源。

Shield 贡献率最高的信息并不总是能完全反映 AWS WAF 日志中的数据。在摄取日志时，Shield 优先考虑减少对系统性能的影响，而不是从日志中检索完整的数据集。这可能会导致 Shield 可用于分析的数据的粒度丢失。在大多数情况下，大多数信息都是可用的，但是对于任何攻击，排名靠前的贡献者数据都可能在一定程度上存在偏差。

以下屏幕截图显示了应用程序层事件的排名靠前的贡献者选项卡示例。



贡献者信息基于对合法流量和潜在有害流量的请求。数据量较大的事件和请求源分布不高的事件更有可能具有可识别的排名靠前的贡献者。显著分布式攻击可能有多种来源，因此很难确定攻击的主要贡献者。如果 Shield Advanced 未识别出特定类别的重要贡献者，则会将数据显示为不可用。

基础设施层事件详细信息

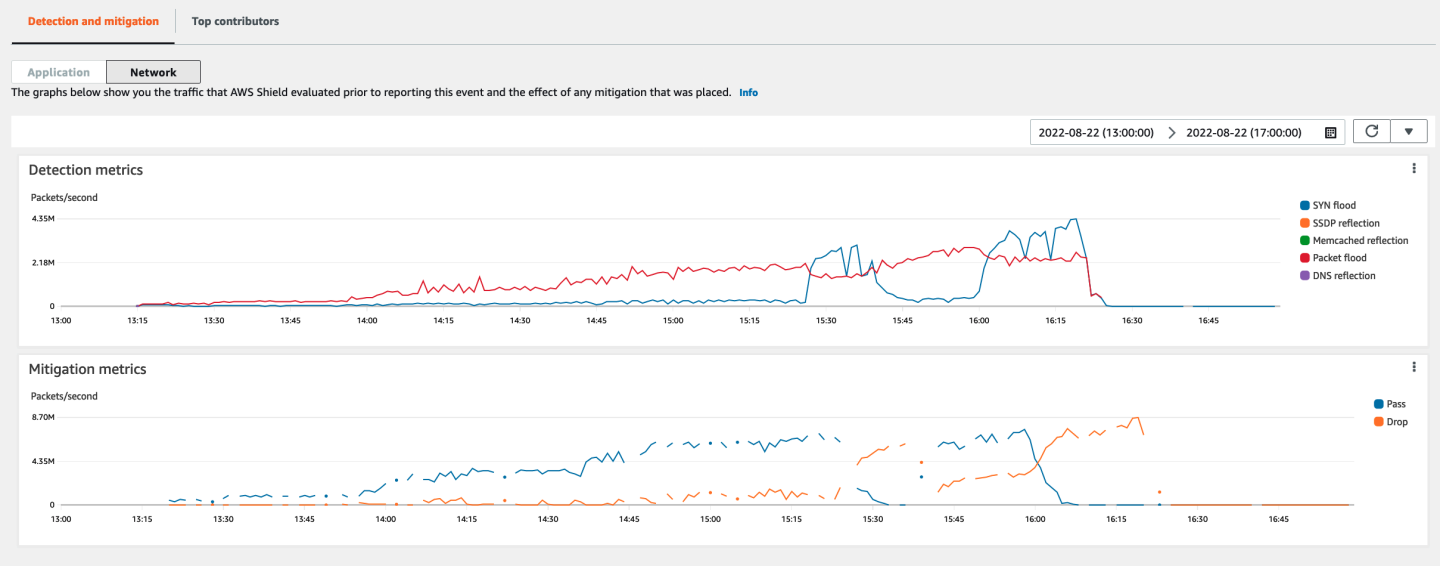
您可以在事件控制台页面的底部查看有关基础设施层事件的检测、缓解和主要贡献者的详细信息。此部分可能包括合法流量和潜在有害流量的组合，可能既代表传递到受保护资源的流量，也代表被 Shield 缓解措施阻止的流量。

检测和缓解

对于基础设施层（第 3 层或第 4 层）事件，检测和缓解选项卡显示基于采样网络流的检测指标和基于缓解系统观察到的流量的缓解指标。缓解指标可以更精确地衡量进入您的资源的流量。

Shield 会自动为受保护的资源类型创建缓解措施：弹性 IP (EIP)、Classic Load Balancer (CLB)、应用程序负载均衡器 (ALB) 和 AWS Global Accelerator 标准加速器。EIP 地址和 AWS Global Accelerator 标准加速器的缓解指标表示通过和丢弃的数据包数量。

以下屏幕截图显示了基础设施层事件的检测和缓解选项卡示例。

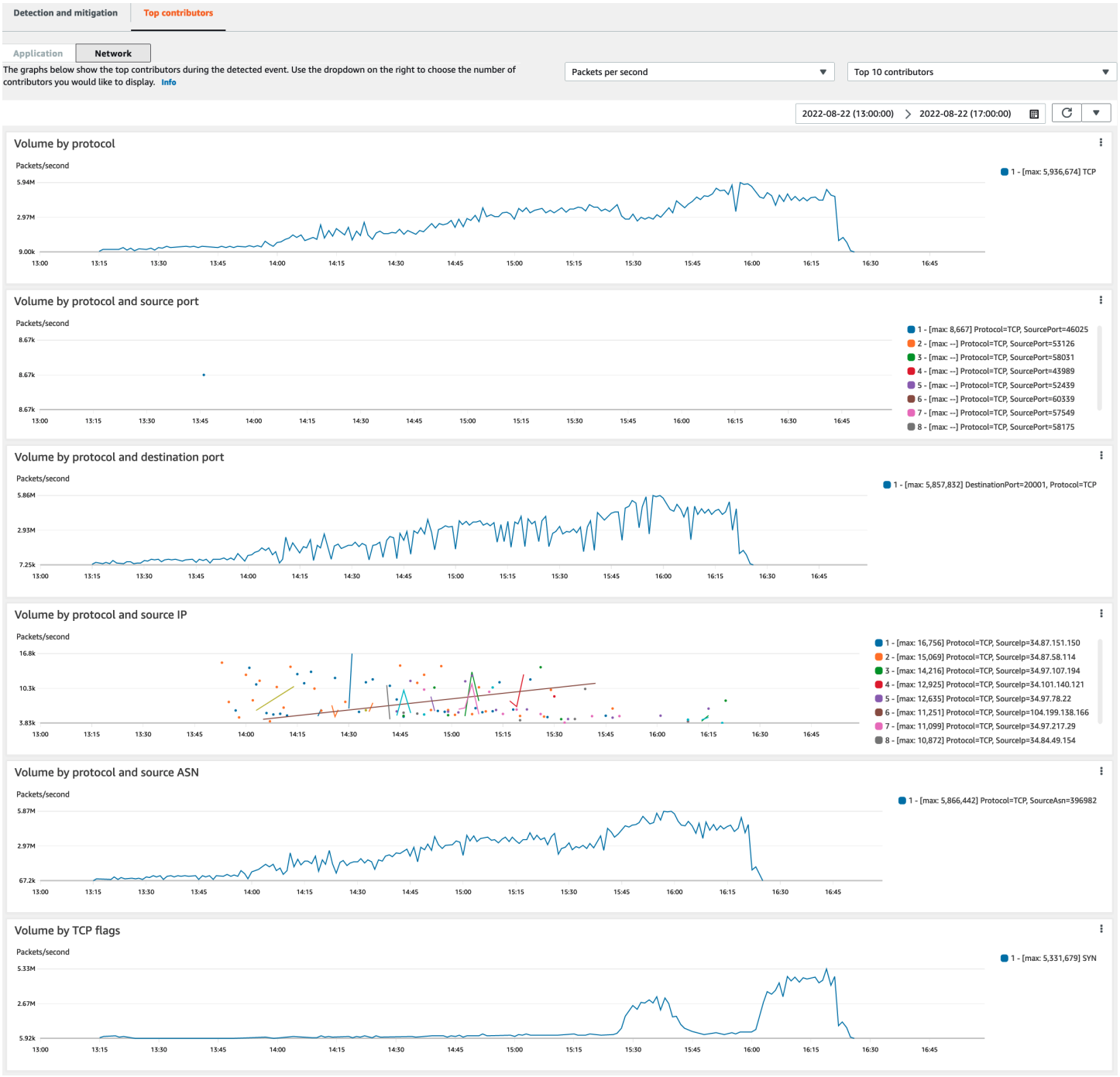


在 Shield 实施缓解措施之前消退的事件流量不包含在缓解指标中。这可能会导致检测图中显示的流量与缓解图表中显示的通过和丢弃指标之间存在差异。

排名靠前的贡献者

基础设施层事件的排名靠前的贡献者选项卡列出了多个流量维度上最多 100 个排名靠前的贡献者的指标。详细信息包括可以识别出至少五个重要流量来源在任何维度的网络图层属性。流量来源的示例包括源 IP 和源 ASN。

以下屏幕截图显示了基础架构层事件的排名靠前的贡献者选项卡示例。



贡献者指标基于对合法流量和潜在有害流量的采样网络流量。数据量较大的事件和流量来源不高度分布的事件更有可能具有可识别的最大贡献者。显著分布式攻击可能有多种来源，因此很难确定攻击的主要贡献者。如果 Shield 未识别出特定指标或类别的任何重要贡献者，则会将数据显示为不可用。

在基础设施层 DDoS 攻击中，流量来源可能会被欺骗或反射。欺骗源是攻击者故意伪造的。反射源是检测到的流量的真正来源，但它不是攻击的自愿参与者。例如，攻击者可能会将攻击从互联网上通常合

法的服务中反射出来，从而向目标生成大量的放大流量。在这种情况下，源信息可能有效，但它不是攻击的实际来源。这些因素可能会限制基于数据包标头的阻止源的缓解技术的可行性。

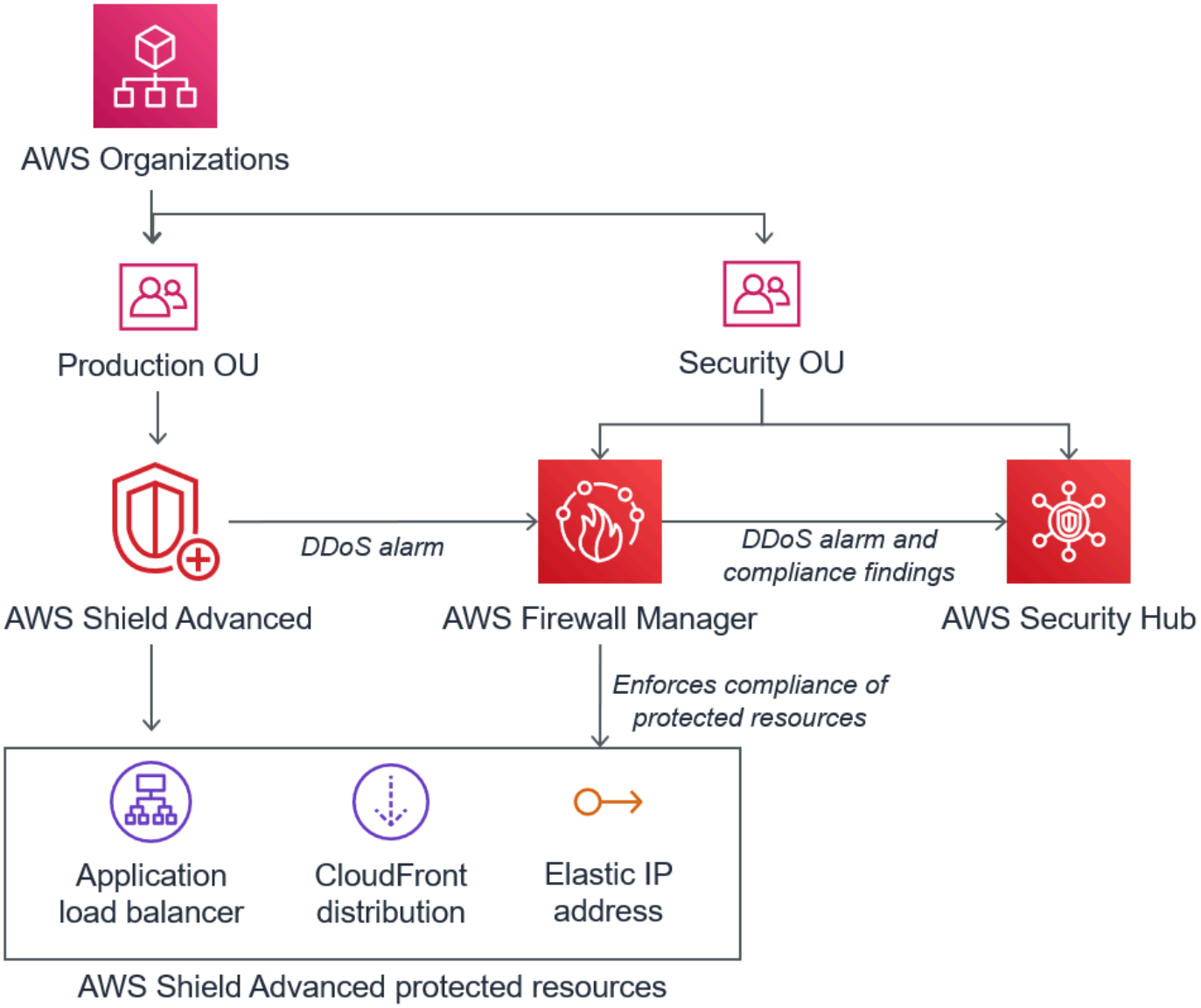
所有账户内的事件可见性

您可以使用 AWS Firewall Manager 和 AWS Security Hub 来管理和监控多个账户中的 AWS Shield Advanced 受保护资源。

借助 Firewall Manager，您可以创建 Shield Advanced 安全策略，用于报告和强制所有账户的 DDoS 保护合规。Firewall Manager 会监控您的受保护资源，包括为属于 Shield Advanced 策略范围的新资源添加保护。

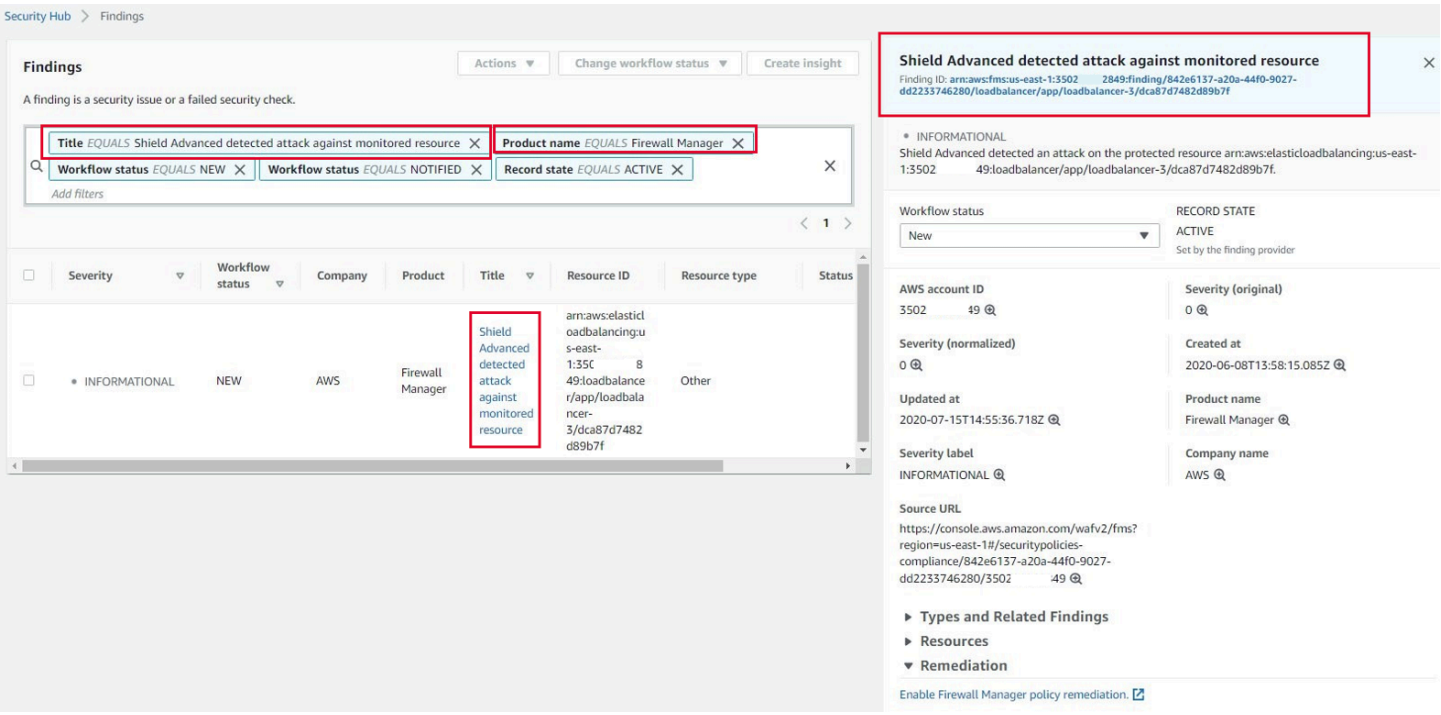
当防火墙管理器识别出不符合你的 Shield Advanced 安全策略的资源时，你可以将 Firewall Manager 与 AWS Security Hub 集成，获得一个控制面板，用于报告 Shield Advanced 和 Firewall Manager 合规性发现检测到的 DDoS 事件。

下图描绘了使用 Firewall Manager 和 Security Hub 监控 Shield Advanced 受保护资源的典型架构。



将 Firewall Manager 与 Security Hub 集成后，您可以在一个地方查看安全性调查发现，以及您运行的应用程序的其他警报和合规状态信息 AWS。

以下屏幕截图突出显示了当您进行此类集成时，您可以在 Security Hub 控制台中看到的 Shield Advanced 事件的信息。



要了解如何将 Firewall Manager 和 Security Hub 与 Shield Advanced 集成，以便在受保护的账户中集中监控事件和合规性，请参阅 AWS 安全博客为 DDoS 事件设置集中监控并自动修复不合规的资源。

响应 DDoS 事件

AWS 自动缓解网络和传输层（第 3 层和第 4 层）分布式拒绝服务 (DDoS) 攻击。如果您使用 Shield Advanced 来保护您的 Amazon EC2 实例，则在攻击期间，Shield Advanced 会自动将您的 Amazon VPC 网络 ACL 部署到 AWS 网络边界。这使得 Shield Advanced 能够针对较大的 DDoS 事件提供保护。有关网络 ACL 的更多信息，请参阅网络 ACL。

对于应用层（第 7 层）DDoS 攻击， AWS 尝试检测并通过 CloudWatch 警报通知 AWS Shield Advanced 客户。默认情况下，它不会自动应用缓解措施，以避免无意中阻止有效的用户流量。

对于应用程序层（第 7 层）资源，您可以使用以下选项来响应攻击。

- 提供您自己的缓解措施：您可以自行调查和缓解攻击。有关信息，请参阅 手动缓解应用程序层 DDoS 攻击。
- 联系支持人员：如果您是 Shield Advanced 客户，可以联系 AWS Support 中心寻求缓解方面的帮助。重大和紧急案例将直接转给 DDoS 专家。有关信息，请参阅 在应用程序层 DDoS 攻击期间联系支持中心。

此外，在攻击发生之前，您可以主动启用以下缓解选项：

- 对亚马逊 CloudFront 分发进行自动缓解 — 使用此选项，Shield Advanced 可以在您的网络 ACL 中为您定义和管理缓解规则。有关应用程序层自动缓解的信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。
- 主动参与 — 当 AWS Shield Advanced 检测到针对您的一个应用程序的大型应用程序层攻击时，SRT 可以主动与您联系。SRT 会筛选 DDoS 事件并创建 AWS WAF 缓解操作。SRT 会与您联系，并且经您同意，可以适用 AWS WAF 规则。有关此选项的更多信息，请参阅 配置主动参与。

在应用程序层 DDoS 攻击期间联系支持中心

如果您是 AWS Shield Advanced 客户，可以联系AWS Support 中心寻求缓解方面的帮助。重大和紧急案例将直接转给 DDoS 专家。因此 AWS Shield Advanced，复杂的案例可以上报给在保护 AWS Amazon.com 及其子公司方面拥有丰富经验的 AWS Shield 响应小组 (SRT)。有关 SRT 的更多信息，请参阅 Shield 响应小组 (SRT) 支持。

要获得 Shield 响应小组 (SRT) 支持，请联系 AWS Support 中心。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。

选择以下选项：

- 案例类型：技术支持
- 服务：分布式拒绝服务 (DDoS)
- 类别：入境至 AWS
- 严重性： 选择适当的选项

在与我们的代表讨论时，请说明您是可能遭受 DDoS 攻击的 AWS Shield Advanced 客户。我们的代表会将您的电话转给适当的 DDoS 专家。如果您使用分布式拒绝服务攻击 (DDoS) 服务类型通过 AWS Support 中心 开立案例，则可以通过聊天或电话直接与 DDoS 专家交流。DDoS 支持工程师可以帮助您识别攻击、推荐 AWS 架构改进建议，并就如何使用缓解 DDoS 攻击的 AWS 服务提供指导。

对于应用程序层攻击，SRT 可以帮助您分析可疑活动。如果您为资源启用了自动缓解功能，SRT 可以审查 Shield Advanced 自动针对攻击采取的缓解措施。无论如何，SRT 可以帮助您审查和缓解问题。SRT 建议的缓解措施通常要求 SRT 在您的账户中创建或更新 AWS WAF 网络访问控制列表 (Web ACL)。要完成这项工作，SRT 需要首先获得您的许可。

> **Important**
>
> 我们建议在启用过程中 AWS Shield Advanced，按照中的步骤主动配置 Shield 响应小组 (SRT) 的访问权限向 SRT 提供他们在攻击期间为您提供帮助所需的权限。提前提供授权有助于防止在实际发生攻击时耽误问题的解决。

SRT 可帮助您筛选 DDoS 攻击，以识别攻击签名和模式。经您同意，SRT 会创建并部署 AWS WAF 规则来缓解攻击。

您也可以在可能的攻击前或在攻击期间联系 SRT，以便审查缓解措施并开发和部署自定义缓解措施。例如，如果您正在运行一个 Web 应用程序且只需打开端口 80 和 443，您可以与 SRT 一起预先配置一个 Web ACL，只“允许”打开端口 80 和 443。

您在账户级别授权和联系 SRT。也就是说，如果您在 Firewall Manager Shield Advanced 策略中使用 Shield Advanced，则必须由账户所有者（而不是 Firewall Manager 管理员）联系 SRT 寻求支持。Firewall Manager 管理员只能为他们拥有的账户联系 SRT。

手动缓解应用程序层 DDoS 攻击

如果您确定资源的事件页面中的活动代表 DDoS 攻击，则可以在 Web ACL 中创建自己的 AWS WAF 规则来缓解攻击。如果您不是 Shield Advanced 客户，这是唯一可用的选项。 AWS WAF 包含 AWS Shield Advanced 在内，无需支付额外费用。有关在 Web ACL 中创建规则的更多信息，请参阅 AWS WAF Web 访问控制列表 (Web ACL)。

如果您使用 AWS Firewall Manager，则可以将您的 AWS WAF 规则添加到 Firewall Manager AWS WAF 策略中。

手动缓解潜在的应用程序层 DDoS 攻击

1. 在 Web ACL 中创建符合异常行为的标准的规则语句。首先，将它们配置为对匹配请求进行计数。有关配置 Web ACL 和规则语句的信息，请参阅 Web ACL 规则和规则组评估 和 测试和调整您的 AWS WAF 保护措施。

   > **Note**
   >
   > 请务必先使用规则操作 Count 而不是 Block 来测试您的规则。在您认为新规则能确定正确的请求后，便可以修改规则以阻止这些请求。

2. 监控请求计数以确定是否要阻止匹配的请求。如果请求量仍然异常高，并且您确信自己的规则正在捕获导致大量流量的请求，请更改 Web ACL 中的规则以阻止这些请求。
3. 继续监控事件页面，确保您的流量按您期望的方式进行处理。

AWS 提供了预配置的模板以帮助您快速入门。这些模板包含一组 AWS WAF 规则，您可以自定义这些规则并使用这些规则来阻止常见的基于 Web 的攻击。有关更多信息，请参阅 AWS WAF 安全自动化。

申请积分 AWS Shield Advanced

如果您订阅了 DDoS 攻击，该攻击会增加盾牌高级保护资源的利用率，则可以申请 Shield Advanced 高级版服务积分，以支付与使用率提高相关的费用，前提是盾牌高级版无法缓解该费用。 AWS Shield Advanced

> **Note**
>
> 您只能将通过此流程获得的任何积分用于 Shield Advanced 的使用。Shield Advanced 积分不可与其他服务一起使用。

积分仅适用于以下类型的费用：

- Shield Advanced 数据传出
- 亚马逊 CloudFront HTTP/HTTPS 请求
- CloudFront 数据传出
- Amazon Route 53 查询
- AWS Global Accelerator 标准加速器数据传输
- 应用程序负载均衡器的负载均衡器容量单位
- 受保护的 Amazon Elastic Compute Cloud (Amazon EC2) 实例的成本，这些实例是为应对攻击而通过自动扩缩策略创建的

申请积分的先决条件

要获得获得积分的资格，您必须攻击开始之前完成以下操作：

- 为要申请积分的资源添加了 Shield Advanced 保护。攻击期间添加的受保护资源不适用成本保护。

> **Note**
>
> 在你的上启用 Shield Advanced AWS 账户 不会自动为单个资源启用 Shield 高级保护。

有关如何使用 Shield Advanced 保护 AWS 资源的更多信息，请参阅为 AWS 资源添加 AWS Shield Advanced 保护。

- 对于适用 CloudFront 且受 Application Load Balancer 保护的资源，您必须已关联 AWS WAF Web ACL，并在Block模式下在 Web ACL 中实现基于速率的规则。有关 AWS WAF 基于速率的规则的更多信息，请参阅 基于速率的规则语句。有关如何将 Web ACL 与 AWS 资源关联的信息，请参阅AWS WAF Web 访问控制列表 (Web ACL)。
- 您必须在实现 DDoS 弹性的AWS 最佳实践中实施适当的最佳实践，才能使应用程序在 DDoS 攻击期间最大限度地降低成本。

如何申请积分

要获得积分资格，您必须在攻击发生的账单月份之后的 15 天内立即提交积分申请。

要申请积分，请通过 AWS Support 中心提交账单案例。您的请求应包括以下内容：

- 主题行中的词语“DDoS Concession”
- 您申请积分的每项事件或可用性中断的日期和时间
- 受影响的 AWS 服务和特定资源

在您提交请求后， AWS Shield 响应小组 (SRT) 将验证是否发生了 DDoS 攻击，如果发生了，则验证是否有任何受保护的资源可以吸收 DDoS 攻击。如果 AWS 确定受保护的资源已扩展以吸收 DDoS 攻击，则 AWS 将为 AWS 确定由 DDoS 攻击引起的那部分流量发放积分。服务抵扣金额有效期为 12 个月。

您使用 AWS Shield 服务的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

> **Note**
>
> 本节为你使用 AWS Shield 服务及其 AWS 资源（例如 Shield Advanced 保护）提供标准 AWS 安全指南。
> 有关使用 Shield 和 Shield Advanced 保护 AWS 资源的信息，请参阅 AWS Shield 指南的其余部分。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Shield 的合规性计划，请参阅合规性计划范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Shield 时应用责任共担模式。以下主题说明如何配置 Shield 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Shield 资源。

主题

- Shield 中的数据保护
- 的身份和访问管理 AWS Shield
- Shield 中的日志记录和监控
- Shield 的合规性验证
- Shield 中的故障恢复能力
- AWS Shield中的基础设施安全性

Shield 中的数据保护

分 AWS 担责任模型适用于中的数据保护 AWS Shield。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括你使用控制台、API 或 AWS 软件开发工具包 AWS 服务 使用 Shield 或其他软件时。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

Shield 实体（如保护）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

的身份和访问管理 AWS Shield

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Shield 资源的人员。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- AWS 的托管策略 AWS Shield
- 对 AWS Shield 身份和访问进行故障排除
- 使用 Shield Advance 的服务相关角色

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Shield 中所做的工作。

服务用户：如果使用 Shield 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Shield 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Shield 中的功能，请参阅 对 AWS Shield 身份和访问进行故障排除。

服务管理员：如果您在公司负责管理 Shield 资源，则您可能具有 Shield 的完全访问权限。您有责任确定您的服务用户应访问哪些 Shield 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Shield 搭配使用的更多信息，请参阅 如何 AWS Shield 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解有关如何编写策略以管理对 Shield 的访问权限的详细信息。要查看您可在 IAM 中使用的 Shield 基于身份的策略示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon QLDB 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Shield 与 IAM 配合使用

在使用 IAM 管理对 Shield 的访问之前，您应该了解哪些 IAM 功能可用于 Shield。

您可以搭配使用的 IAM 功能 AWS Shield

IAM 功能	Shield 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	支持
策略条件键（特定于服务）	支持
ACL	否
ABAC（策略中的标签）	部分
临时凭证	支持
转发访问会话（FAS）	支持
服务角色	支持
服务相关角色	支持

要全面了解 Shield 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Shield 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

要查看 Shield 基于身份的策略的示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

Shield 内基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Shield 的策略操作

支持策略操作	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Shield 操作的列表，请参阅服务授权参考》中的 AWS Shield定义的操作。

Shield 中的策略操作在操作前使用以下前缀：

```
shield
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要在 Shield 中指定以 `List` 开头的所有操作，包括以下操作：

```
"Action": "shield:List*"
```

要查看 Shield 基于身份的策略的示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

Shield 的策略资源

支持策略资源	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Shield 的资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 AWS Shield定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Shield定义的操作。要允许或拒绝对 Shield 资源子集的访问权限，请在策略的 `resource` 元素中包含资源的 ARN。

在中 AWS Shield，资源是保护和攻击。这些资源具有关联的唯一 Amazon 资源名称 (ARN)，如下表所示。

AWS Shield 控制台中的名称	AWS Shield SDK/CLI 中的名称	ARN 格式	
事件或攻击	`AttackDetail`	`arn:aws:shield:: account:attack/ID`	
保护	`Protection`	`arn:aws:shield:: account:protection/ ID`	

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

```
arn:partition:shield::account:resource/ID
```

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

- *##*：您的 ID AWS 账户。您必须指定值。
- *resource*：资源的类型，`attack` 或 `protection`。
- *ID*：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` 的所有保护：

```
arn:aws:shield::111122223333:protection/*
```

Shield 资源的 ARN 具有以下格式：

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

有关 ARN 的信息，请参阅 Amazon Web Services 一般参考中的 Amazon 资源名称 (ARN)。

以下列出了特定于 wafv2 资源 ARN 的要求：

- ##：对于用于保护亚马逊 CloudFront 分配的 Shield 资源，请将其设置为us-east-1。否则，请将其设置为您正在使用受保护区域资源的区域。
- s@@ co pe：将范围设置为，以便global在 Amazon CloudFront 配送中使用或regional与 AWS WAF 支持的任何区域资源一起使用。区域资源是 Amazon API Gateway REST API、应用程序负载均衡器、 AWS AppSync GraphQL API、Amazon Cognito 用户池、服务和 AWS 已验证访问实 AWS App Runner 例。
- ####：指定下述值之一：对于事件或攻击，指定 attack；或者对于保护，指定 protection。
- ####：指定您为 Shield 资源提供的名称，或指定通配符 (*) 以表示满足 ARN 中其他规格的所有资源。您必须指定资源名称和资源 ID，或者为两者指定通配符。
- resource-id：指定 Shield 资源的 ID，或指定通配符 (*) 以表示满足 ARN 中其他规格的所有资源。您必须指定资源名称和资源 ID，或者为两者指定通配符。

例如，以下 ARN 指定区域 us-west-1 中具有账户 111122223333 的区域作用域的所有 Web ACL：

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

以下 ARN 为区域 us-east-1 中的账户 111122223333 指定了名为 MyIPManagementRuleGroup 全局范围规则组：

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

要查看 Shield 基于身份的策略的示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

Shield 的策略条件键

支持特定于服务的策略条件键	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Shield 条件键的列表，请参阅服务授权参考中的 AWS Shield的条件键。要了解可以使用条件键的操作和资源，请参阅由定义的操作 AWS Shield。

要查看 Shield 基于身份的策略的示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

Shield 中的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

带 Shield 的 ABAC

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证用于 Shield

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Shield 的转发访问会话

支持转发访问会话 (FAS)	支持

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Shield的服务角色

支持服务角色	支持

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Shield 的功能。仅当 Shield 提供相关指导时才编辑服务角色。

Shield 的服务相关角色

支持服务相关角色	支持

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 Shield 服务相关角色的详细信息，请参阅 使用 Shield Advance 的服务相关角色。

适用于 AWS Shield的基于身份的策略示例

默认情况下，用户和角色没有创建或修改 Shield 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关 Shield 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考中的 AWS Shield的操作、资源和条件键。

主题

- 策略最佳实践
- 使用 Shield 控制台
- 允许用户查看他们自己的权限
- 授予对您的 Shield Advanced 保护的读取权限
- 授予对 Shield 的只读访问权限 CloudFront，以及 CloudWatch

- 授予对 Shield 的完全访问权限 CloudFront，以及 CloudWatch

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Shield 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略 或 工作职能的AWS 托管式策略。
- 应用最低权限 – 在使用 IAM policy 设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM policy 中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM policy，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM policy 语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 Shield 控制台

要访问 AWS Shield 控制台，您必须拥有一组最低权限。这些权限必须允许您在中列出和查看有关 Shield 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

可以访问和使用 AWS 控制台的用户也可以访问 AWS Shield 控制台。无需额外权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授予对您的 Shield Advanced 保护的读取权限

AWS Shield 允许跨账户资源访问，但不允许您创建跨账户资源保护。您只能为拥有这些资源的账户中的资源创建保护。

以下示例策略授予对所有资源执行 shield:ListProtections 操作的权限。Shield 不支持使用某些 API 操作的资源 ARN (也称为资源级权限) 标识特定资源，因此应指定通配符 (*)。这仅允许访问您可以通过操作 ListProtections 检索的资源。

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

授予对 Shield 的只读访问权限 CloudFront，以及 CloudWatch

以下政策向用户授予对 Shield 和相关资源（包括亚马逊 CloudFront 资源和亚马逊 CloudWatch 指标）的只读访问权限。这对于需要权限才能查看 Shield 防护和攻击中的设置以及监控其中的指标的用户很有用 CloudWatch。这些用户无法创建、更新或删除 Shield 资源：

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
```

```
                "globalaccelerator:DescribeAccelerator"
            ],
            "Resource": [
                "arn:aws:elasticloadbalancing:*:*:*",
                "arn:aws:cloudfront::*:*",
                "arn:aws:route53:::hostedzone/*",
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldReadOnly",
            "Effect": "Allow",
            "Action": [
                "shield:List*",
                "shield:Describe*",
                "shield:Get*"
            ],
            "Resource": "*"
        }
    ]
}
```

授予对 Shield 的完全访问权限 CloudFront，以及 CloudWatch

以下政策允许用户执行任何 Shield 操作、对 CloudFront Web 分发执行任何操作以及监控中的指标和请求示例 CloudWatch。它对作为 Shield 管理员的用户十分有用：

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
```

```
                "cloudwatch:List*",
                "cloudfront:GetDistribution*",
                "globalaccelerator:ListAccelerators",
                "globalaccelerator:DescribeAccelerator"
            ],
            "Resource": [
                "arn:aws:elasticloadbalancing:*:*:*",
                "arn:aws:cloudfront::*:*",
                "arn:aws:route53:::hostedzone/*",
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldFullAccess",
            "Effect": "Allow",
            "Action": [
                "shield:*"
            ],
            "Resource": "*"
        }
    ]
}
```

强烈建议您为拥有管理权限的用户配置 Multi-Factor Authentication (MFA)。有关更多信息，请参阅 IAM 用户指南中的在 AWS中使用多重身份验证（MFA）设备。

AWS 的托管策略 AWS Shield

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： AWSShieldDRTAccessPolicy

AWS Shield 当您授予 Shield 响应小组 (SRT) 代表您采取行动的权限时，将使用此托管策略。此政策授予 SRT 对您的 AWS 账户的有限访问权限，以帮助在高严重性事件期间缓解 DDoS 攻击。此政策允许 SRT 管理您的 AWS WAF 规则和 Shield Advanced 保护并访问您的 AWS WAF 日志。

有关授予 SRT 代表您进行操作的权限的信息，请参阅 配置 Shield 响应小组 (SRT) 的访问权限。

有关此策略的详细信息，请参阅 IAM 控制台AWSShieldDRTAccessPolicy中的。

AWS 托管策略： AWSShieldServiceRolePolicy

当您启用应用程序层 DDoS 自动缓解时，Shield Advanced 会使用此托管策略来设置管理账户资源所需的权限。此策略允许 Shield Advanced 在您与受保护资源关联的 Web ACL 中创建和应用 AWS WAF 规则和规则组，以自动响应 DDoS 攻击。

您无法附加 AWSShieldServiceRolePolicy 到您的 IAM 实体。Shield 将此策略附加到服务相关角色 `AWSServiceRoleForAWSShield`，以允许 Shield 代表您执行操作。

当您启用应用程序层 DDoS 自动缓解时，Shield Advanced 允许使用此策略。有关使用该策略的更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

有关使用此策略的服务相关角色 AWSServiceRoleForAWSShield 的信息，请参阅 使用 Shield Advance 的服务相关角色

有关此策略的详细信息，请参阅 IAM 控制台AWSShieldServiceRolePolicy中的。

Shield 对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来对 Shield AWS 托管政策的更新的详细信息。有关此页面更改的自动提示，请订阅 Shield 文档历史记录页面上的 RSS 源，网址是 文档历史记录。

Policy	更改的说明	Date
`AWSShieldServiceRolePolicy`	添加此策略是为了向 Shield Advanced 提供应用程序层 DDoS 自动缓解功能所需的权限。有关此功能的信息，请参	2021 年 12 月 1 日

Policy	更改的说明	Date
此政策允许 Shield 访问和管理 AWS 资源，以便代表您自动响应应用层 DDoS 攻击。 IAM 控制台中的详细信息：AWSShieldServiceRolePolicy 服务相关角色 `AWSServiceRoleForAWSShield` 使用该策略。有关信息，请参阅 使用 Shield Advance 的服务相关角色。	阅 Shield Advanced 应用程序层 DDoS 自动缓解。	
Shield 已开启跟踪更改	Shield 开始跟踪其 AWS 托管策略的变更。	2021 年 3 月 3 日

对 AWS Shield 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Shield 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Shield 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我的 AWS 账户 Shield 资源

我无权在 Shield 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `shield:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 shield:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Shield。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Shield 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 AWS 账户 Shield 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Shield 是否支持这些功能，请参阅 如何 AWS Shield 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

使用 Shield Advance 的服务相关角色

AWS Shield Advanced 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Shield Advanced 直接相关。服务相关角色由 Shield Advanced 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Shield Advanced，因为您不必手动添加必要的权限。Shield Advanced 定义其服务相关角色的权限，除非另外定义，否则只有 Shield Advanced 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务相关角色。这将保护您的 Shield Advanced 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

Shield Advanced 的服务相关角色权限

Shield Advanced 使用名为AWSServiceRoleForAWSShield的服务相关角色。此角色允许 Shield Advanced 访问和管理 AWS 资源，以便代表您自动响应应用层 DDoS 攻击。有关此函数的更多信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

AWSServiceRoleForAWSShield 服务相关角色信任以下服务来代入该角色：

- `shield.amazonaws.com`

名为的角色权限策略 AWSShieldServiceRolePolicy 允许 Shield Advanced 对所有 AWS 资源完成以下操作：

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

当允许对所有 AWS 资源执行操作时，这在策略中显示为"Resource": "*"。这仅意味着服务相关角色可以对该操作支持的所有 AWS 资源执行每项指明的操作。例如，只有 wafv2 Web ACL 资源支持操作 wafv2:GetWebACL。

Shield Advanced 仅对已启用应用程序层保护功能的受保护资源以及与这些受保护资源关联的 Web ACL 进行资源级 API 调用。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Shield Advance 创建服务相关角色

您无需手动创建服务相关角色。当您为、或 AWS API 中的资源启用自动应用层 DDoS 缓解时 AWS Management Console，Shield Advanced 会为您创建服务相关角色。 AWS CLI

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您为某个资源启用 DDoS 的自动缓解时，Shield Advanced 将再次为您创建服务相关角色。

为 Shield Advance 编辑服务相关角色

Shield Advanced 不允许你编辑 AWSServiceRoleForAWSShield 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

为 Shield Advance 删除服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 在您尝试删除资源时，如果 Shield Advanced 正在使用该角色，删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除使用的 Shield Advanced 资源 AWSServiceRoleForAWSShield

对于配置了应用程序层 DDoS 保护的所有资源，请禁用应用程序层 DDoS 自动缓解。有关控制台说明，请参阅 配置应用程序层 DDoS 保护。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAWSShield服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

Shield Advanced 服务相关角色支持的区域

Shield Advanced 支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Shield Advanced 端点和限额。

Shield 中的日志记录和监控

监控是维护 Shield 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控您的 Shield 资源和响应潜在事件的工具：

亚马逊 CloudWatch 警报

使用 CloudWatch 警报，您可以监视您指定的时间段内的单个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 AWS Auto Scaling 政策 CloudWatch 发送通知。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

AWS CloudTrail 日志

CloudTrail 提供用户、角色或 AWS 服务在 Shield 中采取的操作的记录。使用收集的信息 CloudTrail，您可以确定向 Shield 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。有关更多信息，请参阅 使用 记录 AWS CloudTrail API 调用。

Shield 的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Shield 中的故障恢复能力

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS Shield中的基础设施安全性

作为一项托管服务 AWS Shield ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Shield。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

AWS Shield Advanced 配额

AWS Shield Advanced 对每个区域的实体数量有默认配额。您可以请求提高这些限额。

资源	默认限额
每个账户为其 AWS Shield Advanced 提供保护的每种资源类型的最大受保护资源数量。	1000
每个账户的保护组的最大数量。	100
您可以专门包含在保护组中的单个受保护资源的最大数量。在 API 中，这适用于您在将保护组 `Pattern` 设置为 `ARBITRARY` 时指定的 `Members`。在控制台中，这适用于您为保护分组从受保护资源中选择选择的资源。	1000

AWS Firewall Manager

AWS Firewall Manager 简化您跨多个账户和资源的管理和维护任务，以实现各种保护，包括 AWS WAF Amazon VPC 安全组和网络 ACL 以及 Amazon Route 53 Resolver DNS 防火墙。 AWS Shield Advanced AWS Network Firewall使用 Firewall Manager 一次设置好保护措施，该服务就会自动将其应用于您的账户和资源，即使添加新资源和账户时也是如此。

Firewall Manager 提供了以下优势：

- 有助于跨账户保护资源
- 有助于保护特定类型的所有资源，例如所有 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
- 允许您订阅 AWS Organizations 组织中的所有成员账户 AWS Shield Advanced，并自动订阅加入该组织的新范围内的账户
- 允许您将安全组规则应用到 AWS Organizations 组织中的所有成员账户或特定账户子集，并自动将这些规则应用到新加入组织的范围内账户
- 允许您使用自己的规则，或从中购买托管规则 AWS Marketplace

如果要保护整个组织而不是少数特定账户和资源，或者经常添加要保护的新资源，Firewall Manager 尤其有用。Firewall Manager 还可对整个组织的 DDoS 攻击进行集中监控。

主题

AWS Firewall Manager 定价

产生的 AWS Firewall Manager 费用适用于基础服务，例如 AWS WAF 和 AWS Config。有关更多信息，请参阅 AWS Firewall Manager 定价。

AWS Firewall Manager 先决条件

本主题向您展示如何做好管理准备 AWS Firewall Manager。您可以使用一个 Firewall Manager 管理员账户在 中 AWS Organizations中管理组织的所有 Firewall Manager 安全策略。除非另有说明，否则请使用您将用作 Firewall Manager 管理员的账户执行先决步骤。

在首次使用 Firewall Manager 之前，请按顺序执行以下步骤。

主题

步骤 1：加入并配置 AWS Organizations

要使用 Firewall Manager，您的账户必须是您要使用 Firewall Manager 策略的 AWS Organizations 服务中的组织成员。

> **Note**
>
> 有关 Organizations 的信息，请参阅 AWS Organizations 用户指南。

建立所需的成员 AWS Organizations 资格和配置

1. 在“组织”中选择一个账户作为该组织的 Firewall Manager 管理员。
2. 如果您选择的账户还不是该组织的成员，请将其加入。按照邀请加入您的组织中的指导 AWS 账户进行操作。

3. 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，请遵循启用组织中的所有功能中的指导。

步骤 2：创建 AWS Firewall Manager 默认管理员帐户

此过程使用您在上一步中选择和配置的账户和组织。

只有组织的管理账户可以作为 Firewall Manager 默认管理员账户。您创建的第一个管理员账户是默认管理员账户。默认管理员账户可以管理第三方防火墙，并且具有完整的管理范围。设置默认管理员帐户时，Firewall Manager 会自动将其设置为防火墙管理器的 AWS Organizations 委派管理员。这样，Firewall Manager 就可以访问组织单位 (OU)。您可以使用 OU 来指定 Firewall Manager 策略作用域。有关设置策略作用域的更多信息，请参阅 创建 AWS Firewall Manager 策略 下针对各个策略类型的指南。有关 Organizations 和管理账户的更多信息，请参阅管理组织中的 AWS 账户。

组织管理账户的必要设置

组织管理账户必须具有以下设置才能将组织加入 Firewall Manager 并创建默认管理员：

- 它必须是您要在 AWS Organizations 其中应用 Firewall Manager 策略的组织的成员。

设置默认管理员账户（控制台）

1. AWS Management Console 使用现有 AWS Organizations 管理帐户登录 Firewall Manager。
2. 通过以下网址打开 Firewall Manager 控制台：https://console.aws.amazon.com/wafv2/fmsv2。
3. 在导航窗格中，选择 设置。
4. 键入 AWS 您选择用作 Firewall Manager 管理员的帐户的帐户 ID。

> **Note**
>
> 默认管理员具有完全管理范围。完全管理范围意味着此账户可以将策略应用于组织内的所有账户和组织单位 (OU)，在所有区域采取行动，并管理所有 Firewall Manager 策略类型。

5. 选择创建管理员账户以创建该账户。

有关管理 Firewall Manager 管理员账户的更多信息，请参阅 与 AWS Firewall Manager 管理员合作。

步骤 3：启用 AWS Config

要使用 Firewall Manager，必须启用 AWS Config。

> **Note**
>
> 根据 AWS Config 定价，您的 AWS Config 设置会产生费用。有关更多信息，请参阅入门 AWS Config。

> **Note**
>
> 为了让 Firewall Manager 监控策略合规性， AWS Config 必须持续记录受保护资源的配置更改。在您的 AWS Config 配置中，必须将录制频率设置为 “连续”，这是默认设置。

为 Firewall AWS Config Manager 启用

1. AWS Config 为每个 AWS Organizations 成员帐户启用，包括 Firewall Manager 管理员帐户。有关更多信息，请参阅入门 AWS Config。
2. AWS Config 为 AWS 区域 包含您要保护的资源的每个资源启用该选项。您可以 AWS Config 手动启用，也可以使用AWS CloudFormation StackSets 示例 AWS CloudFormation 模板中的 “启用 AWS Config” 模板。

   如果您不想 AWS Config 为所有资源启用，则必须根据所使用的 Firewall Manager 策略类型启用以下选项：

   - WAF 策略 — 为资源类型启用配置： CloudFront 分发、Application Load Balancer（从列表中选择 ElasticLoadBalancingV2）、API Gateway、WAF WebACL、WAF 区域 WebACL 和 Wafv2 WebACL 和 Wafv2 WebACL。 AWS Config 要启用保护 CloudFront 分配，您必须位于美国东部（弗吉尼亚北部）区域。其他地区没有 CloudFront 选项。
   - Shield 策略 — 为 Shield Protection、Protection、 ShieldRegional Application Load Balancer、EC2 EIP、WAF WebACL、WAF 区域 WebACL 和 Wafv2 WebACL 等资源类型启用配置。
   - 安全组策略 — 为 EC2 SecurityGroup、EC2 实例和 EC2 资源类型启用 Config NetworkInterface。
   - 网络 ACL 策略 — 为 Amazon EC2 子网和 Amazon EC2 网络 ACL 的资源类型启用 Config。

- N@@ etwork Firewall 策略 — 为资源类型 NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup、EC2 VPC、EC2 InternetGateway RouteTable、EC2 和 EC2 子网启用配置。
- DNS 防火墙策略：为 EC2 VPC 资源类型启用“配置”。
- 第三方防火墙策略 — 为 Amazon EC2 VPC、亚马逊 EC2、亚马逊 EC2、Amazon EC InternetGateway 2 RouteTable 子网和亚马逊 EC2 vpcendPoint 资源类型启用配置。

> **Note**
>
> 如果您将 AWS Config 记录器配置为使用自定义 IAM 角色，则需要确保 IAM 策略具有记录 Firewall Manager 策略所需的资源类型的适当权限。如果没有适当的权限，则可能无法记录所需的资源，这会使 Firewall Manager 无法正确保护您的资源。Firewall Manager 无法查看这些权限错误配置。有关将 IAM 与配合使用的信息 AWS Config，请参阅适用于 IAM 的信息 AWS Config。

步骤 4：对于第三方策略，请在 AWS Marketplace 中订阅并配置第三方设置

要开始使用 Firewall Manager 第三方防火墙策略，请完成以下先决条件。

Fortigate 云原生防火墙 (CNF) 即服务策略先决条件

使用 Fortigate CNF for Firewall Manager

1. 在 Marketplace 上订阅 F ortigate 云原生防火墙 (CNF) 即服务服务。 AWS
2. 首先，在 Fortigate CNF 产品门户网站上注册租户。然后在 Fortigate CNF 产品门户网站上的租户下添加您的 Firewall Manager 管理员账户。有关更多信息，请参阅 Fortigate CNF 文档。

有关使用 Fortigate CNF 策略的信息，请参阅 Fortigate 云原生防火墙 (CNF) 即服务策略。

Palo Alto Networks 云下一代防火墙策略先决条件

要使用 Palo Alto Networks Cloud NGFW for Firewall Manager

1. 在 Marketplace 上订阅 Palo Alto Networks Cloud 下一代防火墙即用即付服务。 AWS
2. 完成 “部署帕洛阿尔托网络云 NGFW” 中列出的帕洛阿尔托网络云 NGFW 部署步骤， AWS Firewall Manager主题见帕洛阿尔托网络云下一代防火墙部署指南。 AWS AWS

有关如何使用 Palo Alto Networks Cloud NGFW 策略的信息，请参阅 Palo Alto Networks Cloud NGFW 策略。

步骤 5：针对 Network Firewall 和 DNS 防火墙策略，启用资源共享

要管理 Firewall Manager 网络防火墙和 DNS 防火墙策略，必须启用与 AWS Organizations 中的共享 AWS Resource Access Manager。启用该功能后，Firewall Manager 可以在您创建这些策略类型时跨账户地部署保护。

要启用与 AWS Organizations 中的共享 AWS Resource Access Manager

- 按照 AWS Resource Access Manager 用户指南中启用与 AWS Organizations共享的指导进行操作。

如果您在资源共享方面遇到问题，请参阅 Network Firewall 和 DNS 防火墙策略的资源共享 中的指南。

步骤 6： AWS Firewall Manager 在默认禁用的区域中使用

要在默认禁用的区域中使用 Firewall Manager，必须同时为 AWS 组织的管理帐户和 Firewall Manager 的默认管理员帐户启用该区域。有关默认禁用区域以及如何启用这些区域的信息，请参阅 AWS 一般参考中的管理 AWS 区域。

启用或禁用区域

- 对于组织管理账户和 Firewall Manager 默认管理员账户，请按照 AWS 一般参考中启用区域的指导进行操作。

完成这些步骤后，您可以配置 Firewall Manager 以开始保护您的资源。有关更多信息，请参阅 AWS Firewall ManagerAWS WAF 策略入门。

与 AWS Firewall Manager 管理员合作

使用后， AWS Firewall Manager 您可以有一个或多个管理员来管理您组织的防火墙资源。如果要在组织中使用多个 Firewall Manager 管理员，则可以对每个管理员应用管理范围条件来定义他们可以管理的资源。这使您可以灵活地在组织中使用不同的管理员角色，并帮助您保持最低权限访问的原则。例如，您可以让一个管理员管理组织的一套组织单位 (OU)，而委托另一个管理员仅管理特定的 Firewall Manager 策略类型。有关 Organizations 和管理账户的更多信息，请参阅管理组织中的 AWS 账户。

有关每个组织可以拥有的最大管理员人数，请参阅 AWS Firewall Manager 配额

开始使用 Firewall Manager 管理员

开始使用 Firewall Manager 管理员之前，您必须先完成 AWS Firewall Manager 先决条件 中列出的先决条件。在先决条件中，您将 AWS Organizations 组织加入防火墙管理器，并为防火墙管理器创建默认管理员帐户。默认管理员账户可以管理第三方防火墙，并且具有完整的管理范围。

管理范围

管理范围定义了 Firewall Manager 管理员可以管理的资源。 AWS Organizations 管理帐户将组织登录到 Firewall Manager 后，该管理帐户可以创建具有不同管理范围的其他防火墙管理器管理员。 AWS Organizations 管理帐户可以授予管理员全部或受限的管理范围。完全范围为管理员提供了对上述所有资源类型的完全访问权限。受限范围是指仅向上述资源的子集授予管理权限。我们建议您仅向管理员授予他们履行其角色职责所需的权限。您可以将以下管理范围条件的任意组合应用于管理员：

- 您组织中管理员可以对其应用策略的账户或 OU。
- 管理员可以在其中执行操作的区域。
- 管理员可以管理的 Firewall Manager 策略类型。

管理员角色

Firewall Manager 中有两种类型的管理员角色：默认管理员和Firewall Manager 管理员。

- 默认管理员：当组织的管理账户在完成操作的同时将组织加入Firewall Manager时，会创建一个 Firewall Manager 的默认管理员账户AWS Firewall Manager 先决条件。默认管理员可以管理第三方防火墙并具有完整的管理范围，但如果您选择拥有多个管理员，则默认管理员与其他管理员处于同等级别。
- Firewall Manager 管理员：Firewall Manager 管理员可以管理 AWS Organizations 管理账户在其管理范围配置中为他们指定的资源。有关每个组织可以拥有的最大管理员人数，请参阅 AWS Firewall Manager 配额。在创建 Firewall Manager 管理员帐户后，该服务会检查该帐户是否已经是组织内防火墙管理器的授权管理员。 AWS Organizations 如果不是，Firewall Manager 会调用 Organizations，将该账户设置为 Firewall Manager 的委托管理员。有关 Organizations 委托管理员的信息，请参阅 AWS Organizations 用户指南中的AWS Organizations 术语和概念。

现有管理员

如果您是 Firewall Manager 的现有客户，并且已经设置了管理员，则该现有管理员将是 Firewall Manager 的默认管理员。您的现有流程不应受到任何影响。如果要添加更多管理员，可以按照本章中的步骤进行操作。

创建、更新和撤销 Firewall Manager 管理员账户

以下主题中的过程介绍了如何创建、更新和撤销 Firewall Manager 管理员账户。只有组织的管理账户才能创建和更新 Firewall Manager 管理员账户。只有个人 Firewall Manager 管理员才能撤消自己的管理员账户。

创建 Firewall Manager 管理员账户

以下过程介绍了如何使用 Firewall Manager 控制台创建 Firewall Manager 管理员账户。

创建 Firewall Manager 管理员账户

1. AWS Management Console 使用现有 AWS Organizations 管理帐户登录 Firewall Manager。
2. 通过以下网址打开 Firewall Manager 控制台：https://console.aws.amazon.com/wafv2/fmsv2。
3. 在导航窗格中，选择 设置。
4. 选择创建管理员账户。
5. 在详细信息窗格中，为 AWS 账户 ID 键入要添加为 Firewall Manager 管理员的成员账户的 AWS ID。
6. 对于管理范围，请选择下列选项之一：

   - 全部：管理员能够将策略应用于组织内的所有账户和组织单位 (OU)，在所有区域采取行动，并应用除第三方防火墙之外的所有 Firewall Manager 策略类型。只有默认管理员才能创建和管理第三方防火墙。向管理员授予此级别的权限时要谨慎行事。本着最低权限的精神，我们建议只授予管理员履行其职责所需的权限。
   - 受限：如果应用受限范围，则在配置管理范围中配置账户和组织单位、地区以及账户可以管理的策略类型。

     对于账户和组织单位，请按以下方式选择选项：
     - 如果要将策略应用于组织中的所有账户或组织单位，请选择 “包括我的 AWS 组织下的所有帐户”。
     - 如果您只想将策略应用于特定账户或特定 AWS Organizations 组织单位 (OU) 中的账户，请选择 “仅包括指定的账户和组织单位”，然后添加要包括的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
     - 如果要将策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

对于区域，选择以下选项之一：

- 如果要允许管理员在所有可用区域中执行操作，请选择包括所有区域。
- 如果您希望管理员仅在特定区域执行操作，请选择仅包括指定的区域，然后指定要包括的区域。

> **Note**
>
> 要包括默认禁用的区域，您必须同时为 AWS Organizations 组织管理账户和默认管理账户启用该区域。有关为账户启用区域的信息，请参阅 Amazon Web Services 一般参考 中的启用区域。

对于策略类型，请按以下方式选择选项：

- 如果要允许管理员管理所有策略类型，请选择包括所有策略类型。
- 如果您希望管理员仅管理特定的策略类型，请选择仅包括指定的策略类型，然后指定要包括的策略类型。

7. 选择创建管理员账户以创建管理员账户。创建后，Firewall Manager 会打电话 AWS Organizations 查看管理员是否已经是您组织的委托管理员。否则，Firewall Manager 会将该账户指定为委托管理员。有关 Organizations 中的委派管理员的信息，请参阅 AWS Organizations 用户指南中的 AWS Organizations 术语和概念。

如果您应用受限管理范围，Firewall Manager 会根据您的设置自动评估任何新资源。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将该账户包含在管理范围内。

更新 Firewall Manager 管理员账户

以下过程介绍了如何使用 Firewall Manager 控制台更新 Firewall Manager 管理员账户。

> **Note**
>
> 要更新管理员的作用域以包括默认禁用的区域，您必须为 AWS Organizations 组织管理账户和默认管理账户启用该区域。有关为账户启用区域的信息，请参阅 Amazon Web Services 一般参考 中的启用区域。

设置管理员账户（控制台）

1. AWS Management Console 使用现有 AWS Organizations 管理帐户登录 Firewall Manager。
2. 通过以下网址打开 Firewall Manager 控制台：https://console.aws.amazon.com/wafv2/fmsv2。
3. 在导航窗格中，选择 设置。
4. 在 Firewall Manager 管理员表中，选择要更新的账户。
5. 选择编辑以更改管理员账户的详细信息。您不能更改账户 ID。
6. 选择 保存 以保存您的更改。

创建管理员账户

以下过程介绍了如何撤销 Firewall Manager 管理员账户。如果您是默认管理员，则必须先撤消组织中的所有 Firewall Manager 管理员账户，然后才能撤消自己的账户。要撤销管理员账户，请按以下过程操作

撤销管理员账户（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。
2. 在导航窗格中，选择 Settings（设置）。
3. 在管理员账户窗格中，选择撤消管理员账户以撤消您的账户。

> **Important**
>
> 当您从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。

更改默认管理员账户

您只能指定组织中的一个账户作为 Firewall Manager 的默认管理员账户。默认管理员账户遵循先入后出的原则。要指定不同的默认管理员账户，每个管理员账户必须先撤消自己的账户。然后，现有默认管理员可以撤消自己的账户，这也将使组织脱离 Firewall Manager。当管理员撤销其账户时，由该账户创建的所有 Firewall Manager 策略都将删除。要指定新的默认管理员帐户，则必须使用 AWS Organizations 管理帐户登录 Firewall Manager 以指定新的管理员帐户。要更改组织的默认管理员账户，请执行以下步骤。

更改默认管理员账户

1. AWS Management Console 使用现有 AWS Organizations 管理帐户登录 Firewall Manager。
2. 通过以下网址打开 Firewall Manager 控制台：https://console.aws.amazon.com/wafv2/fmsv2。
3. 在导航窗格中，选择 设置。
4. 键入您选择用作 Firewall Manager 管理员账户的 ID。

> **Note**
>
> 该账户获得了跨组织内的所有账户创建和管理 Firewall Manager 策略的权限。

5. 选择创建管理员账户。
6. 键入您选择用作 Firewall Manager 管理员的帐户的 AWS ID。

> **Note**
>
> 此账户具有完全的管理范围。完全管理范围意味着此账户可以将策略应用于组织内的所有账户和组织单位 (OU)，在所有区域采取行动，并管理所有 Firewall Manager 策略类型。

7. 选择创建管理员账户以创建默认管理员账户。

取消管理员账户更改的资格

对管理员账户进行某些更改可能会取消其保留管理员账户的资格。

本节介绍可能取消管理员帐户资格的更改，以及 Firewall Manager 如何 AWS 处理这些更改。

账号已从组织中移除 AWS Organizations

如果 AWS Firewall Manager 管理员帐户已从中的组织中删除 AWS Organizations，则该帐户将无法再管理该组织的策略。Firewall Manager 执行以下任一操作：

- 没有策略的账户：如果 Firewall Manager 管理员账户没有 Firewall Manager 策略，Firewall Manager 会撤消管理员账户。
- 使用防火墙管理器策略的帐户-如果防火墙管理器管理员帐户具有防火墙管理器策略，Firewall Manager 将在 AWS 销售客户代表的帮助下发送一封电子邮件通知您情况并提供您可以采取的选项。

账户已关闭

如果您关闭了 AWS Firewall Manager 管理员使用的帐户， AWS 并且 Firewall Manager 会按以下方式处理关闭操作：

- AWS 从 Firewall Manager 撤消帐户的管理员访问权限，Firewall Manager 会停用管理员帐户管理的所有策略。这些策略提供的保护将在整个组织中停止。
- AWS 自管理员帐户关闭生效之日起，将 Firewall Manager 的策略数据保留 90 天。在这 90 天内，您可以重新打开已关闭的账户。
  - 如果您在 90 天内重新打开已关闭的帐户，则会将该帐户重新 AWS 分配为 Firewall Manager 管理员并恢复该帐户的防火墙管理器策略数据。
  - 否则，在 90 天期限结束时，将 AWS 永久删除该帐户的所有 Firewall Manager 策略数据。

AWS Firewall Manager 策略入门

您可以使用 AWS Firewall Manager 来启用多种不同类型的安全策略。进行设置的步骤对于每一项略有不同。

主题

AWS Firewall ManagerAWS WAF 策略入门

AWS Firewall Manager 要使用在整个组织中启用 AWS WAF 规则，请按顺序执行以下步骤。

主题

步骤 1：完成先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行步骤 2：创建并应用 AWS WAF 策略之前，请先满足所有先决条件。

步骤 2：创建并应用 AWS WAF 策略

Firewall Manager AWS WAF 策略包含要应用于资源的规则组。Firewall Manager 会在您应用策略的每个账户中创建一个 Firewall Manager Web ACL。除了您在此处定义的规则组之外，各个客户经理还可以向生成的 Web ACL 中添加规则和规则组。有关 Firewall Manager AWS WAF 策略的信息，请参见AWS WAF 政策。

创建 Firewall Manager AWS WAF 策略（控制台）

AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

1. 在导航窗格中，选择 安全策略。
2. 选择 创建策略。
3. 对于 策略类型，选择 AWS WAF。
4. 对于区域，选择一个 AWS 区域。要保护 Amazon 的 CloudFront配送，请选择 “全球”。

   要保护多个区域（ CloudFront 分布除外）中的资源，必须为每个区域创建单独的 Firewall Manager 策略。
5. 选择下一步。
6. 对于策略名称，请键入策略的描述性名称。Firewall Manager 在其管理的 Web ACL 的名称中包含策略名称。Web ACL 名称中包括 `FMManagedWebACLV2-`，后接您在此处输入的策略名称、`-`，以及 Web ACL 创建时间戳（以 UTC 毫秒为单位）。例如，`FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。

> **Important**
>
> Web ACL 名称在创建后无法更改。如果您更新策略的名称，Firewall Manager 将不会更新关联的 Web ACL 名称。要让 Firewall Manager 创建具有不同名称的 Web ACL，您必须创建新的策略。

7. 在 策略规则 下的 最先运行的规则组 中，选择 添加规则组。展开 AWS 托管规则组。对于 核心规则集，切换 添加到 Web ACL。对于 AWS 已知不良输入，请切换添加到 Web ACL。选择 添加规则。

   对于 最后运行的规则组，请选择 添加规则组。展开 AWS 托管规则组，对于 Amazon IP 声誉列表，切换添加到 Web ACL。选择 添加规则。

   在 “第一个规则组” 下，选择 “核心规则集”，然后选择 “向下移动”。 AWS WAF 先根据AWS 已知的错误输入规则组评估 Web 请求，然后再根据核心规则集进行评估。

   如果需要，您也可以使用 AWS WAF 控制台创建自己的 AWS WAF 规则组。您创建的任何规则组都将显示在描述策略：添加规则组页面的您的规则组下。

   您通过 Firewall Manager 管理的第一个和最后一个 AWS WAF 规则组的名称分别以`PREFMManaged-`或`POSTFMManaged-`开头，后跟防火墙管理器策略名称和规则组创建时间戳（以 UTC 毫秒为单位）。例如，`PREFMManaged-MyWAFPolicyName-1621880555123`。
8. 将 Web ACL 的默认操作保留为 允许。
9. 将 策略操作 保留为默认状态，以便不会自动修复不合规的资源。您随后可以更改此选项。
10. 选择下一步。
11. 对于 策略范围，您可以提供用于标识要应用策略的资源的账户、资源类型和标签设置。在本教程中，请保留 AWS 账户 和资源的默认设置，然后选择一种或多种资源类型。
12. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
13. 选择下一步。
14. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。

15. 选择下一步。
16. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。
17. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

第 3 步：清除

为了避免产生不必要的费用，请删除任何非必要的策略和资源。

删除策略 (控制台)

1. 在 AWS Firewall Manager 策略 页面上，选择策略名称旁边的单选按钮，然后选择删除。
2. 在 删除 确认框中，选择 删除所有策略资源，然后再次选择 删除。

   AWS WAF 移除该策略及其在您的账户中创建的所有关联资源，例如 Web ACL。更改可能需要几分钟才能传播到所有账户。

AWS Firewall ManagerAWS Shield Advanced 策略入门

您可以使用 AWS Firewall Manager 在整个组织中启用 AWS Shield Advanced 保护。

> **Important**
>
> Firewall Manager 不支持 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保护这些资源，则不能使用 Firewall Manager 策略。而是应按照为 AWS 资源添加 AWS Shield Advanced 保护中的说明操作。

要使用 Firewall Manager 来启用 Shield Advanced 保护，请按顺序执行以下步骤。

主题

步骤 1：完成先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行步骤 2：创建并应用 Shield Advanced 策略之前，请完成所有先决条件。

步骤 2：创建并应用 Shield Advanced 策略

完成先决条件后，您可以创建 AWS Firewall Manager Shield Advanced 策略。Firewall Manager Shield Advanced 策略包含您要使用 Shield Advanced 保护的账户和资源。

> **Important**
>
> Firewall Manager 不支持 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保护这些资源，则不能使用 Firewall Manager 策略。而是应按照为 AWS 资源添加 AWS Shield Advanced 保护中的说明操作。

创建 Firewall Manager Shield Advanced 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，选择 Shield Advanced。

要创建 Shield Advanced 策略，您的 Firewall Manager 必须订阅 Shield Advanced。如果您尚未订阅，则会提示您订阅。有关订阅成本的更多信息，请参阅 AWS Shield Advanced 定价。

> **Note**
>
> 您无需为每个会员账户手动订阅 Shield Advanced。Firewall Manager 在创建策略时会为您执行此操作。每个账户都必须继续订阅 Firewall Manager 和 Shield Advanced，才能继续保护账户中的资源。

5. 对于区域，选择一个 AWS 区域。要保护 Amazon CloudFront 资源，请选择 “全球”。

   要保护多个区域中的资源（ CloudFront 资源除外），必须为每个区域创建单独的 Firewall Manager 策略。
6. 选择下一步。
7. 对于名称，请键入策略的描述性名称。
8. （仅全局区域）仅对于全局区域策略，您可以选择是否要管理 Shield Advanced 应用程序层 DDoS 自动缓解。在本教程中，将此选项保留为默认设置忽略。
9. 对于策略操作，请选择不会自动修复的选项。
10. 选择下一步。
11. AWS 账户 本政策适用于允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 包括我的组织下的所有账户。
12. 选择要保护的资源的类型。

    Firewall Manager 不支持 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保护这些资源，则不能使用 Firewall Manager 策略。否则，请按照 为 AWS 资源添加 AWS Shield Advanced 保护 提供的 Shield Advanced 的指导进行操作。
13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
14. 选择下一步。
15. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。

16. 选择下一步。
17. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。
18. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

继续步骤 3：（可选）向 Shield Response Team (SRT) 授权。

步骤 3：（可选）向 Shield Response Team (SRT) 授权

的好处之一 AWS Shield Advanced 是来自Shield响应小组（SRT）的支持。当您遇到潜在 DDoS 攻击时，您可以联系 AWS Support 中心。如有必要，支持中心会将您的问题上报至 SRT。SRT 可以帮助您分析可疑的活动，并帮助您缓解问题。这种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 ACL。SRT 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，但团队需要您的授权才能这样做。我们建议在设置过程中 AWS Shield Advanced，主动向 SRT 提供所需的授权。提前提供授权有助于防止在实际发生攻击时耽误问题的解决。

您在账户级别授权和联系 SRT。也就是说，账户所有者（而不是 Firewall Manager 管理员）必须执行以下步骤来授权 SRT 以缓解潜在的攻击。Firewall Manager 管理员只能为他们拥有的账户授权 SRT。同样，只有账户所有者可以联系 SRT 以获得支持。

> **Note**
>
> 要使用 SRT 的服务，您必须订阅 Business Support Plan或企业支持计划。

要授权 SRT 代表您缓解潜在的攻击，请按照 Shield 响应小组 (SRT) 支持 中的步骤操作。您可以随时使用相同的步骤更改 SRT 访问权限和权限。

继续步骤 4：配置亚马逊 SNS 通知和亚马逊警报 CloudWatch 。

步骤 4：配置亚马逊 SNS 通知和亚马逊警报 CloudWatch

您可以继续执行此步骤，无需配置 Amazon SNS 通知或 CloudWatch 警报。但是，配置这些警报和通知可以显著提高您对可能的 DDoS 事件的可见性。

您可以使用 Amazon SNS 监控受保护的资源以了解是否存在潜在的 DDoS 活动。要接收可能攻击的通知，请为每个区域创建一个 Amazon SNS 主题。

在 Firewall Manager（控制台）创建 Amazon SNS 主题

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中的 AWS FMS 下，选择 设置。
3. 选择 创建新主题。
4. 输入主题名称。
5. 输入 Amazon SNS 消息将发送到的电子邮件地址，然后选择添加电子邮件地址。
6. 选择 更新 SNS 配置。

配置 Amazon CloudWatch 警报

Shield Advanced 记录了您可以监控的检测、缓解和主要贡献者指标。 CloudWatch 有关更多信息，请参阅AWS Shield Advanced 指标。 CloudWatch 会产生额外费用。有关 CloudWatch 定价，请参阅Amazon CloudWatch 定价。

要创建 CloudWatch 警报，请按照使用 Amazon CloudWatch 警报中的说明进行操作。默认情况下，Shield Advanced 会配置 CloudWatch 为在出现潜在 DDoS 事件的一个指标后提醒您。如果需要，您可以使用CloudWatch 控制台更改此设置，使其仅在检测到多个指标后提醒您。

> **Note**
>
> 除了警报外，您还可以使用 CloudWatch 仪表板来监控潜在的 DDoS 活动。此控制面板可从 CloudWatch 收集原始数据，并将数据处理为易读的近乎实时的指标。您可以使用 Amazon

中的统计数据 CloudWatch 来了解您的 Web 应用程序或服务的性能。有关更多信息，请参阅《Amazon CloudWatch 用户指南》 CloudWatch中的内容。
有关创建 CloudWatch 仪表板的说明，请参阅使用 Amazon 进行监控 CloudWatch。有关您可以添加到控制面板的 Shield Advanced 指标的信息，请参阅 AWS Shield Advanced 指标。

完成 Shield Advanced 配置后，请熟悉在 对 DDoS 事件的可见性 查看事件的选项。

开始使用 A AWS Firewall Manager mazon VPC 安全组策略

AWS Firewall Manager 要使用在您的组织中启用 Amazon VPC 安全组，请按顺序执行以下步骤。

主题

步骤 1：完成先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行步骤 2：创建在您策略中使用的安全组之前，请完成所有先决条件。

步骤 2：创建在您策略中使用的安全组

在此步骤中，您将创建一个安全组，您可以使用 Firewall Manager 在组织中应用该安全组。

> **Note**
>
> 在本教程中，您不将安全组策略应用到组织中的资源。您仅仅创建策略，并查看将策略的安全组应用到资源时会发生什么情况。您可以通过在策略上禁用自动修复来执行此操作。

如果您已经定义了通用安全组，请跳过此步骤并转到步骤 3：创建和应用通用安全组策略。

创建在 Firewall Manager 通用安全组策略中使用的安全组

- 按照 Amazon VPC 用户指南中您的 VPC 安全组下的指导，创建一个可以应用于组织中所有账户和资源的安全组。

有关安全组规则选项的信息，请参阅安全组规则参考。

您现在已准备好转到步骤 3：创建和应用通用安全组策略。

步骤 3：创建和应用通用安全组策略

完成先决条件后，您可以创建 AWS Firewall Manager 通用的安全组策略。通用安全组策略为您的整个 AWS 组织提供集中控制的安全组。它还定义了安全组适用的 AWS 账户 和资源。除了通用安全组策略之外，Firewall Manager 还支持内容审核安全组策略（用于管理组织中正在使用的安全组规则），以及使用情况审核安全组策略（用于管理未使用和多余的安全组）。有关更多信息，请参阅 安全组策略。

对于本教程，您将创建通用安全组策略并将其操作设置为不自动修复。这使您能够在不对 AWS 组织进行更改的情况下查看该政策会产生什么影响。

创建 Firewall Manager 通用安全组策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 如果您未满足先决条件，控制台会显示有关如何解决任何问题的说明。按照说明操作，然后返回此步骤以创建通用安全组策略。
4. 选择 创建策略。
5. 对于 策略类型，选择 安全组。
6. 对于 安全组策略类型，选择 通用安全组。
7. 对于区域，选择一个 AWS 区域。
8. 选择下一步。
9. 对于策略名称，请键入策略的描述性名称。
10. 策略规则 选项允许您选择如何应用和维护此策略中的安全组。在本教程中，不要选中这些选项。

11. 选择 添加主安全组，选择您为本教程创建的安全组，然后选择 添加安全组。
12. 对于 策略操作，请选择 确定不符合策略规则的资源，但不自动修复。
13. 选择下一步。
14. AWS 账户 受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 包括我的组织下的所有账户。
15. 对于资源类型，根据您为 AWS 组织定义的资源选择一个或多个类型。
16. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
17. 选择下一步。
18. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
19. 选择下一步。
20. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。
21. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息
22. 在探索完成后，如果您不希望保留为本教程创建的策略，请依次选择策略名称、删除、清除此策略创建的资源，最后选择 删除。

有关 Firewall Manager 安全组策略的更多信息，请参阅 安全组策略。

开始使用 A AWS Firewall Manager mazon VPC 网络 ACL 策略

AWS Firewall Manager 要使用在整个组织中启用网络 ACL，请按顺序执行本节中的步骤。

有关网络 ACL 的信息，请参阅 Amazon VPC 用户指南中的使用网络 ACL 控制子网流量。

主题

步骤 1：完成先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行步骤 2：创建网络 ACL 策略之前，请完成所有先决条件。

步骤 2：创建网络 ACL 策略

完成先决条件后，您可以创建 Firewall Manager 网络 ACL 策略。网络 ACL 策略为您的整个 AWS 组织提供集中控制的网络 ACL 定义。它还定义了网络 ACL 适用的 AWS 账户 和子网。

有关 Firewall Manager 网络 ACL 策略的信息，请参见网络 ACL 策略。

有关 Firewall Manager 网络 ACL 策略的一般信息，请参见网络 ACL 策略。

> **Note**
>
> 在本教程中，您不会将网络 ACL 策略应用于组织中的子网。您只需创建策略并查看将策略的网络 ACL 应用于子网后会发生什么。您可以通过在策略上禁用自动修复来执行此操作。

创建 Firewall Manager 网络 ACL 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。

3. 如果您未满足先决条件，控制台会显示有关如何解决任何问题的说明。按照说明进行操作，然后返回到此步骤，创建网络 ACL 策略。
4. 选择 创建策略。
5. 对于区域，选择一个 AWS 区域。
6. 对于策略类型，选择网络 ACL。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 对于网络 ACL 策略规则，定义入站和出站流量的第一个和最后一个规则。

   您在 Firewall Manager 中定义网络 ACL 规则的方式与通过 Amazon VPC 定义网络访问控制规则的方式类似。唯一的区别是，您无需自己分配规则编号，而是分配每组规则的运行顺序，然后 Firewall Manager 在保存策略时为您分配编号。您最多可以定义 5 条入站规则，以任意方式划分为第一个和最后一个，并且最多可以定义 5 个出站规则。

   有关指定网络 ACL 规则的指南，请参阅 Amazon VPC 用户指南中的添加和删除网络 ACL 规则。

   您在 Firewall Manager 策略中定义的规则指定了网络 ACL 必须符合网络 ACL 策略的最低规则配置。例如，网络 ACL 的入站规则不能与策略兼容，除非它们以策略的入站优先规则开头，其顺序与策略中指定的顺序相同。有关更多信息，请参阅 网络 ACL 策略。
10. 对于 策略操作，请选择 确定不符合策略规则的资源，但不自动修复。
11. 选择下一步。
12. AWS 账户 受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 包括我的组织下的所有账户。

    网络 ACL 策略的资源类型始终为子网。
13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
14. 选择下一步。
15. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
16. 选择下一步。

17. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要做出的更改。

18. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

19. 在探索完成后，如果您不希望保留为本教程创建的策略，请依次选择策略名称、删除、清除此策略创建的资源，最后选择删除。

有关 Firewall Manager 网络 ACL 策略的更多信息，请参阅网络 ACL 策略。

AWS Firewall ManagerAWS Network Firewall 策略入门

AWS Firewall Manager 要使用在组织中启用 AWS Network Firewall 防火墙，请按顺序执行以下步骤。有关 Firewall Manager Network Firewall 策略的信息，请参阅 AWS Network Firewall 政策。

主题

- 步骤 1：完成一般先决条件
- 步骤 2：创建要在策略中使用的 Network Firewall 规则组
- 步骤 3：创建和应用 Network Firewall 策略

步骤 1：完成一般先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 2：创建要在策略中使用的 Network Firewall 规则组

要学习本教程，您应该熟悉 AWS Network Firewall 并知道如何配置其规则组和防火墙策略。

您必须在 Network Firewall 中至少有一个要用于 AWS Firewall Manager 策略的规则组。如果您尚未在 Network Firewall 中创建规则组，请立即创建。有关使用 Network Firewall 的信息，请参阅 AWS Network Firewall 开发人员指南。

步骤 3：创建和应用 Network Firewall 策略

完成先决条件后，您将创建一个 AWS Firewall Manager Network Firewall 策略。Network Firewall 策略为您的整个 AWS 组织提供集中控制的 AWS Network Firewall 防火墙。它还定义了防火墙适用的 AWS 账户 和资源。

有关 Firewall Manager 如何管理 Network Firewall 策略的更多信息，请参阅 AWS Network Firewall 政策。

创建 Firewall Manager Network Firewall 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 如果您未满足先决条件，控制台会显示有关如何解决任何问题的说明。按照说明操作，然后返回此步骤以创建 Network Firewall 策略。
4. 选择创建安全策略。
5. 对于 策略类型，选择 AWS Network Firewall。
6. 对于区域，选择一个 AWS 区域。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 策略配置允许您定义防火墙策略。这与您在 AWS Network Firewall 控制台中使用的过程相同。您可以添加要在策略中使用的规则组，并提供默认的无状态操作。在本教程中，配置此策略的过程和在 Network Firewall 中配置防火墙策略的过程一样。

   > **Note**
   >
   > Network Fire AWS Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不自动修复的选项。

10. 选择下一步。
11. 对于防火墙端点，请选择多个防火墙端点。此选项可为您的防火墙提供高可用性。创建策略时，Firewall Manager 会在每个您要保护公有子网的可用区中创建一个防火墙子网。
12. 对于 AWS Network Firewall 路由配置，请选择监控，让 Firewall Manager 监控您的 VPC 是否存在路由配置违规行为，并通过补救建议提醒您，以帮助您使路由合规。或者，如果您不想让 Firewall Manager 监控您的路由配置并接收这些警报，请选择关闭。

> **Note**
>
> 监控为您提供有关由于路由配置错误而导致的不合规资源的详细信息，并建议通过 Firewall Manager `GetViolationDetails` API 采取补救措施。例如，如果流量未通过策略创建的防火墙端点进行路由，则 Network Firewall 会发出警报。

> **Warning**
>
> 如果您选择监控，则将来无法将该策略更改为关闭。为此，您必须创建新的策略。

13. 对于流量类型，选择添加到防火墙策略以通过互联网网关进行流量路由。
14. AWS 账户 受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 包括我的组织下的所有账户。

    Network Firewall 策略的资源类型始终是 VPC。
15. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
16. 选择下一步。
17. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
18. 选择下一步。
19. 查看新的政策设置，然后返回需要进行任何调整的页面。

进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。

20. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

21. 在探索完成后，如果您不希望保留为本教程创建的策略，请依次选择策略名称、删除、清除此策略创建的资源，最后选择删除。

有关 Firewall Manager Network Firewall 策略的更多信息，请参阅 AWS Network Firewall 政策。

AWS Firewall Manager DNS 防火墙策略入门

AWS Firewall Manager 要使用在您的组织中启用 Amazon Route 53 解析器 DNS 防火墙，请按顺序执行以下步骤。有关 Firewall Manager DNS 防火墙策略的信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

主题

步骤 1：完成一般先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 2：创建要在策略中使用的 DNS 防火墙规则组

要学习本教程，您应该熟悉 Amazon Route 53 Resolver DNS 防火墙，并且了解如何配置其规则组。

您必须在 DNS 防火墙中至少有一个要用于 AWS Firewall Manager 策略的规则组。如果您尚未在 DNS 防火墙中创建规则组，请立即创建。有关使用 DNS 防火墙的信息，请参阅 Amazon Route 53 开发人员指南中的 Amazon Route 53 Resolver DNS 防火墙。

步骤 3：创建和应用 DNS 防火墙策略

完成先决条件后，您可以创建 AWS Firewall Manager DNS 防火墙策略。DNS 防火墙策略为您的整个 AWS 组织提供了一组集中控制的 DNS 防火墙规则组关联。它还定义了防火墙适用的 AWS 账户 和资源。

有关 Firewall Manager 如何管理您的 DNS 防火墙规则组关联的更多信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

创建 Firewall Manager DNS 防火墙策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。
2. 在导航窗格中，选择 安全策略。
3. 如果您未满足先决条件，控制台会显示有关如何解决任何问题的说明。按照说明操作，然后返回此步骤以创建 DNS 防火墙策略。
4. 选择创建安全策略。
5. 对于策略类型，请选择 Amazon Route 53 Resolver DNS 防火墙。
6. 对于区域，选择一个 AWS 区域。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 策略配置允许您定义要通过 Firewall Manager 管理的 DNS 防火墙规则组关联。添加要在策略中使用的规则组。您可以定义一个关联来先评估您的 VPC，然后再定义一个关联进行评估。在本教程中，根据需要添加一两个规则组关联。
10. 选择下一步。
11. AWS 账户 受此政策影响允许您通过指定要包含或排除的账户来缩小策略的范围。对于本教程，选择 包括我的组织下的所有账户。

    DNS 防火墙策略的资源类型始终是 VPC。
12. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

13. 选择下一步。
14. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
15. 选择下一步。
16. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要做出的更改。
17. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息
18. 在探索完成后，如果您不希望保留为本教程创建的策略，请依次选择策略名称、删除、清除此策略创建的资源，最后选择删除。

有关 Firewall Manager DNS 防火墙策略的更多信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

AWS Firewall Manager Palo Alto Networks Cloud 下一代防火墙策略入门

AWS Firewall Manager 要使用启用 Palo Alto Networks Cloud 下一代防火墙 (NGFW) 策略，请按顺序执行以下步骤。有关 Palo Alto Networks Cloud NGFW 策略的信息，请参阅 Palo Alto Networks Cloud NGFW 策略。

主题

- 步骤 1：完成一般先决条件
- 步骤 2：完成 Palo Alto Networks Cloud NGFW 策略先决条件
- 步骤 3：创建并应用 Palo Alto Networks Cloud NGFW 策略

步骤 1：完成一般先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 2：完成 Palo Alto Networks Cloud NGFW 策略先决条件

要使用 Palo Alto Networks Cloud NGFW 策略，您还必须完成几个额外的强制性步骤。Palo Alto Networks 云下一代防火墙策略先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 3：创建并应用 Palo Alto Networks Cloud NGFW 策略

完成先决条件后，您将创建 AWS Firewall Manager Palo Alto Networks Cloud NGFW 策略。

有关 Palo Alto Networks Cloud NGFW 的 Firewall Manager 策略的更多信息，请参阅 Palo Alto Networks Cloud NGFW 策略。

要为 Palo Alto Networks Cloud NGFW（控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，请选择 Palo Alto Networks Cloud NGFW。如果你还没有在 Marketplace 上订阅 Palo Alto N AWS etworks Cloud NGFW 服务，则需要先订阅。要在 AWS Marketplace 上订阅，请选择 “查看 AWS 商城详情”。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定了 Firewall Manager 如何管理策略的端点。采用分布式模式，Firewall Manager 在策略作用域内的每个 VPC 中维护防火墙端点。在集中式模式下，Firewall Manager 在检查 VPC 中维护单个端点。
6. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 在策略配置中，选择要与此策略关联的 Palo Alto Networks Cloud NGFW 防火墙策略。Palo Alto Networks Cloud NGFW 防火墙策略列表包含与您的 Palo Alto Networks Cloud NGFW 租户关联

的所有 Palo Alto Networks Cloud NGFW 防火墙策略。有关创建和管理 Palo Alto Networks Cloud NGFW 防火墙策略的信息，请参阅 Deplo y Palo Alto Networks Cloud NGFW 的 NGFW 部署指南中的 AWS Firewall Manager主题。 AWS AWS

10. 对于 Palo Alto Networks Cloud NGFW 日志记录——可选，可以选择为你的策略选择要记录的 Palo Alto Networks Cloud NGFW 日志类型。有关 Palo Alto Networks Cloud NGFW 日志类型的信息，请参阅《帕洛阿尔托网络云 NGFW 部署指南》 AWS中的 “为帕洛阿尔托网络云 NGFW 配置日志记录”。 AWS

    对于日志记录目标，指定 Firewall Manager 何时应写入日志。

11. 选择下一步。

12. 在配置第三方防火墙端点下，根据创建防火墙端点的部署模型（分布式部署模型或集中式部署模型）执行以下操作之一：

    - 如果您为此策略使用分布式部署模型，请在可用区下选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
    - 如果您使用此策略的集中式部署模型，请在检查 VPC 配置下的 AWS Firewall Manager 端点配置中输入检查 VPC 所有者的 AWS 账户 ID 和检查 VPC 的 VPC ID。
        - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。

13. 选择下一步。

14. 对于策略作用域，在 AWS 账户 本策略适用于下，选择以下选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

Network Firewall 策略的资源类型是 VPC。

15. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

16. 对于授予跨账户存取权限，请选择下载 AWS CloudFormation 模板。这将下载一个可用于创建 AWS CloudFormation 堆栈的 AWS CloudFormation 模板。此堆栈创建了一个 AWS Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户管理帕洛阿尔托网络云 NGFW 资源的权限。有关堆栈的信息，请参阅 AWS CloudFormation 用户指南中的使用堆栈。
17. 选择下一步。
18. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
19. 选择下一步。
20. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。

21. 若您满意所创建的策略，请选择 创建策略。

    AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

有关 Palo Alto Networks Cloud NGFW 的 Firewall Manager 策略的更多信息，请参阅 Palo Alto Networks Cloud NGFW 策略。

AWS Firewall Manager Fortigate CNF 政策入门

Fortigate 云原生防火墙 (CNF) 即服务是一项第三方防火墙服务，您可以将其用于您的策略。 AWS Firewall Manager 使用 Fortigate CNF for Firewall Manager，您可以在所有账户中创建和集中部署 Fortigate CNF 资源和策略集。 AWS AWS Firewall Manager 要使用启用 Fortigate CNF 策略，请按顺序执行以下步骤。有关 Fortigate CNF 策略 的更多信息，请参阅 Fortigate 云原生防火墙 (CNF) 即服务策略。

主题

步骤 1：完成一般先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 2：完成 Fortigate CNF 策略先决条件

要使用 Fortigate CNF 策略，您还必须完成其他强制性步骤。Fortigate 云原生防火墙 (CNF) 即服务策略先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

步骤 3：创建和应用 Fortigate CNF 策略

完成先决条件后，您可以创建 AWS Firewall Manager Fortigate CNF 策略。

有关 Fortigate CNF 的 Firewall Manager 策略的更多信息，请参阅 Fortigate 云原生防火墙 (CNF) 即服务策略。

创建适用于 Fortigate CNF 的 Firewall Manager 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

> **Note**
>
> 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，请选择 Fortigate CNF。如果你还没有在 Marketpl AWS ace 上订阅 Fortigate CNF 服务，则需要先订阅。要在 AWS Marketplace 上订阅，请选择 “查看 AWS 商城详情”。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定了 Firewall Manager 如何管理策略的端点。采用分布式模式，Firewall Manager 在策略作用域内的每个 VPC 中维护防火墙端点。在集中式模式下，Firewall Manager 在检查 VPC 中维护单个端点。
6. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择下一步。
8.
9. 在策略配置中，选择要与此策略关联的 Fortigate CNF 防火墙策略。Fortigate CNF 防火墙策略列表包含与您的 Fortigate CNF 租户关联的所有 Fortigate CNF 防火墙策略。有关创建和管理 Fortigate CNF 防火墙策略的信息，请参阅 Fortinet CNF 文档。
10. 选择下一步。
11. 在配置第三方防火墙端点下，根据创建防火墙端点的部署模型（分布式部署模型或集中式部署模型）执行以下操作之一：

    - 如果您为此策略使用分布式部署模型，请在可用区下选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
    - 如果您使用此策略的集中式部署模型，请在检查 VPC 配置下的 AWS Firewall Manager 端点配置中输入检查 VPC 所有者的 AWS 账户 ID 和检查 VPC 的 VPC ID。
      - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
12. 选择下一步。
13. 对于策略作用域，在 AWS 账户 本策略适用于下，选择以下选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。

- 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择“仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

Fortigate CNF 策略的资源类型是 VPC。

14. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

15. 对于授予跨账户存取权限，请选择下载 AWS CloudFormation 模板。这将下载一个可用于创建 AWS CloudFormation 堆栈的 AWS CloudFormation 模板。此堆栈创建了一个 AWS Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户管理 Fortigate CNF 资源的权限。有关堆栈的信息，请参阅 AWS CloudFormation 用户指南中的使用堆栈。要创建堆栈，您需要来自 Fortigate CNF 门户网站的账户 ID。
16. 选择下一步。
17. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
18. 选择下一步。
19. 查看新的政策设置，然后返回需要进行任何调整的页面。

    进行检查以确保 策略操作 设置为 确定不符合策略规则的资源，但不自动修复。这样，您就可以在启用策略之前查看策略将要进行的更改。

20. 若您满意所创建的策略，请选择 创建策略。

AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

有关 Firewall Manager Fortigate CNF 策略的更多信息，请参阅 Fortigate 云原生防火墙 (CNF) 即服务策略。

使用 AWS Firewall Manager 策略

AWS Firewall Manager 提供了以下类型的策略。对于每种策略类型，您可以定义：

- AWS WAF策略 — F irewall Manager 支持的策略 AWS WAF 和 AWS WAF 经典策略。对于这两个版本，您都可以定义哪些资源受策略保护。
  - AWS WAF 策略类型需要一组规则组在 Web ACL 中首先运行，最后一次运行。然后，在您应用 Web ACL 的账户中，账户所有者可以添加要在两组之间运行的规则和规则组。
  - AWS WAF 经典策略类型需要在 Web ACL 中运行单个规则组。
- Shield Advanced 策略 — 此策略类型会针对您指定的资源类型在整个组织中应用 Shield 高级保护。
- Amazon VPC 安全组策略 — 此策略类型使您可以控制整个组织中使用的安全组，并允许您在整个组织中强制执行一组基准规则。
- Amazon VPC 网络访问控制列表 (ACL) 策略 — 此策略类型使您可以控制整个组织中使用的网络 ACL，并允许您在整个组织中强制执行一组基准网络 ACL。
- Network Firewall 策略-此策略类型将 AWS Network Firewall 保护应用于您组织的 VPC。
- Amazon Route 53 Resolver DNS 防火墙策略 – 此策略将 DNS 防火墙保护应用于您组织的 VPC。
- 第三方防火墙策略-此策略类型应用第三方防火墙保护。第三方防火墙可以通过在 Marketplace 上的 AWS Marketplace 控制台AWS 订阅获得。
  - 帕洛阿尔托网络云下一代防火墙政策 — 此政策类型将帕洛阿尔托网络云下一代防火墙 (NGFW) 保护和帕洛阿尔托网络云下一代防火墙 (NGFW) 保护和帕洛阿尔托网络云 NGFW 规则堆栈应用于组织的 VPC。
  - Fortigate 云原生防火墙 (CNF) 即服务策略 — 此策略类型适用于 Fortigate 云原生防火墙 (CNF) 即服务保护。Fortigate CNF 是一种以云为中心的解决方案，可通过行业领先的高级威胁防护、智能 Web 应用程序防火墙 (WAF) 和 API 保护来阻止未修补的威胁并保护云基础架构。

Firewall Manager 策略特定于单独的策略类型。如果要跨账户实施多个策略类型，您可以创建多个策略。您可以为每种类型创建多个策略。

如果您向使用 AWS Organizations创建的组织添加新帐户，Firewall Manager 会自动将该策略应用于该账户中在该策略范围内的资源。

AWS Firewall Manager 策略的常规设置

AWS Firewall Manager 托管策略有一些常见的设置和行为。您可以对所有人指定名称并定义策略的范围，还可以使用资源标记来控制策略范围。您可以选择在不采取纠正措施的情况下查看不合规的账户和资源，也可以选择自动修复不合规资源。

有关策略范围的信息，请参阅 AWS Firewall Manager 政策范围。

创建 AWS Firewall Manager 策略

创建策略的步骤因策略类型而异。请确保使用适用于所需策略类型的过程。

> **Important**
>
> AWS Firewall Manager 不支持 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 保护这些资源，则不能使用 Firewall Manager 策略。而是应按照为 AWS 资源添加 AWS Shield Advanced 保护中的说明操作。

主题

- 为创建 AWS Firewall Manager 策略 AWS WAF
- 为 AWS WAF 经典版创建 AWS Firewall Manager 策略
- 为创建 AWS Firewall Manager 策略 AWS Shield Advanced
- 创建 AWS Firewall Manager 通用安全组策略
- 创建 AWS Firewall Manager 内容审核安全组策略
- 创建 AWS Firewall Manager 使用情况审核安全组策略
- 创建 AWS Firewall Manager 网络 ACL 策略
- 为创建 AWS Firewall Manager 策略 AWS Network Firewall
- 为 Amazon Route 53 解析器 DNS 防火墙创建 AWS Firewall Manager 策略
- 为 Palo Alto Networks Cloud AWS Firewall Manager 制定政策 NGFW
- 为 Fortigate 云原生防火墙 (CNF) 即服务创建 AWS Firewall Manager 策略

为创建 AWS Firewall Manager 策略 AWS WAF

在 Firewall Manager AWS WAF 策略中，您可以使用托管规则组，该 AWS 组由 AWS Marketplace 卖家为您创建和维护。您也可以创建和使用自己的规则组。有关规则组的更多信息，请参阅AWS WAF 规则组。

如果要使用自己的规则组，请在创建 Firewall Manager AWS WAF 策略之前创建这些规则组。有关操作指南，请参阅 管理您自己的规则组。要使用单个自定义规则，您必须定义自己的规则组，再在其中定义您的规则，然后在策略中使用该规则组。

有关 Firewall Manager AWS WAF 策略的信息，请参见AWS WAF 政策。

为 AWS WAF （控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 AWS WAF。
5. 对于区域，选择一个 AWS 区域。要保护 Amazon CloudFront 配送，请选择 “全球”。

   要保护多个区域（ CloudFront 分布除外）中的资源，必须为每个区域创建单独的 Firewall Manager 策略。
6. 选择下一步。
7. 对于策略名称，请键入策略的描述性名称。Firewall Manager 在其管理的 Web ACL 的名称中包含策略名称。Web ACL 名称中包括 `FMManagedWebACLV2-`，后接您在此处输入的策略名称、`-`，以及 Web ACL 创建时间戳（以 UTC 毫秒为单位）。例如，`FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。
8. 对于 Web 请求正文检查，可以选择更改正文大小限制。有关正文检查大小限制的信息，包括定价注意事项，请参阅AWS WAF 开发人员指南中的 管理车身检查的大小限制。

9. 在 “策略规则” 下，在 Web ACL 中添加 AWS WAF 要首先和最后评估的规则组。要使用 AWS WAF 托管规则组版本控制，请切换启用版本控制。各客户经理可以在最先运行的规则组和最后运行的规则组之间添加规则和规则组。有关在 Firewall Manager 策略中使用 AWS WAF 规则组的更多信息 AWS WAF，请参阅AWS WAF 政策。

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

   - 对于托管规则组，覆盖部分或全部规则的规则操作。如果您没有为规则定义覆盖操作，则评估将使用规则组中定义的规则操作。有关此选项的更多信息，请参阅 AWS WAF 开发人员指南中的规则组的操作覆盖选项。
   - 某些托管规则组要求您提供其他配置。请参阅您的托管规则组提供程序所提供的文档。有关 AWS 托管规则组的特定信息，请参阅AWS WAF 开发者指南AWS 的托管规则 AWS WAF中的。

   完成设置后，选择保存规则。

10. 设置 Web ACL 的默认操作。这是 AWS WAF 在 Web 请求与 Web ACL 中的任何规则都不匹配时采取的操作。您可以使用允许操作添加自定义标题，也可以为屏蔽操作添加自定义响应。有关默认 Web ACL 操作的更多信息，请参阅 Web ACL 默认操作。有关设置自定义 Web 请求和响应的信息，请参阅 AWS WAF中的自定义 Web 请求和响应。

11. 对于日志记录配置，选择启用日志记录以打开日志记录。日志记录提供了有关 Web ACL 对流量进行分析的详细信息。选择日志记录目标，然后选择您配置的日志记录目标。必须选择名称以 `aws-waf-logs-` 开头的日志记录目标。有关配置 AWS WAF 日志目标的信息，请参阅为 AWS WAF 策略配置日志记录。

12. （可选）如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 添加。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为 REDACTED。

13. （可选）如果您不想向日志发送所有请求，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个筛选器，选择添加筛选条件，然后选择您的筛选条件并指定是要保留还是删除符合条件的请求。添加完筛选条件后，如果需要，可以修改默认日志记录行为。有关更多信息，请参阅 AWS WAF 开发人员指南中的 Web ACL 日志记录配置。

14. 您可以定义令牌域列表，以便在受保护的应用程序之间实现令牌共享。当您使用 AWS WAF 欺诈控制账户接管预防 (ATP) 和 AWS WAF 机器人控制的 AWS 托管规则组时，令牌由和Challenge操作以及应用程序集成 SDK 使用。CAPTCHA

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

默认情况下，仅 AWS WAF 接受受保护资源域的令牌。如果您在此列表中添加令牌域，则 AWS WAF 接受列表中所有域和关联资源域的令牌。有关更多信息，请参阅 AWS WAF 开发人员指南中的 AWS WAF Web ACL 令牌域列表配置。

只有在编辑现有 Web ACL 时，才能更改 Web ACL 的验证码和挑战免疫时间。您可以在 Firewall Manager 策略详细信息页面下找到这些设置。有关这些设置的信息，请参阅时间戳过期：AWS WAF 代币免疫时间。如果您更新现有策略中的关联配置、验证码、挑战或令牌域列表设置，Firewall Manager 将使用新值覆盖您的本地 Web ACL。但是，如果您不更新策略的关联配置、验证码、挑战或令牌域列表设置，则本地 Web ACL 中的值将保持不变。有关此选项的更多信息，请参阅 AWS WAF 开发人员指南中的 CAPTCHA然后Challenge在 AWS WAF。

15. 在 Web ACL 管理下，如果您希望 Firewall Manager 管理未关联的 Web ACL，请启用管理未关联的 Web ACL。启用此选项后，只有当至少一个资源使用 Web ACL 时，Firewall Manager 才会在策略范围内的账户中创建 Web ACL。当某个账户在任何时候进入策略范围时，如果至少有一个资源将使用 Web ACL，则 Firewall Manager 会自动在该账户中创建一个 Web ACL。启用此选项后，Firewall Manager 会对您的账户中未关联的 Web ACL 进行一次性清理。清理过程可能需要数小时时间。如果资源在 Firewall Manager 创建 Web ACL 后离开策略范围，Firewall Manager 将取消该资源与 Web ACL 的关联，但不会清理未关联的 Web ACL。只有当您在策略中首次启用对未关联的 Web ACL 的管理时，Firewall Manager 才会清理未关联的 Web ACL。
16. 对于策略操作，如果要在组织中的每个适用账户内创建一个 Web ACL，但不将 Web ACL 应用于任何资源，请选择识别不符合策略规则的资源，但不进行自动修复，不要选择管理关联 Web ACL。您随后可以更改这些选项。

    若要自动将策略应用于现有的范围内资源，请选择 自动修复任何不合规的资源。如果禁用管理未关联的 Web ACL，则自动修复任何不合规资源选项会在组织内的每个适用账户中创建一个 Web ACL，并将该 Web ACL 与账户中的资源关联。如果启用管理未关联的 Web ACL，则自动修复任何不合规资源选项仅在拥有可与 Web ACL 关联的资源的账户中创建和关联 Web ACL。

    当您选择自动修复任何不符合要求的资源时，对于不由其他活动的 Firewall Manager 策略管理的 Web ACL，还可以选择删除 Web ACL 与范围内资源之间的现有关联。如果选择此选项，Firewall Manager 首先将策略的 Web ACL 与资源关联，然后删除之前的关联。如果某个资源与另一个由其他活动的 Firewall Manager 策略管理的 Web ACL 具有关联，则此选择不会影响该关联。
17. 选择下一步。
18. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。

- 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择“仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要将策略应用于除特定的一组账户或 AWS Organizations 组织单位 (OU) 之外的所有其他账户或组织单位，请选择 排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

19. 对于 资源类型，选择要保护的资源的类型。
20. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
21. 选择下一步。
22. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
23. 选择下一步。
24. 查看新的政策设置，然后返回需要进行任何调整的页面。

    若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

为 AWS WAF 经典版创建 AWS Firewall Manager 策略

为 AWS WAF 经典版创建 Firewall Manager 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 AWS WAF Classic。
5. 如果您已经创建了要添加到策略中的 AWS WAF 经典规则组，请选择创建 AWS Firewall Manager 策略并添加现有规则组。如果要创建新规则组，请选择创建 Firewall Manager 策略并添加新规则组。
6. 对于区域，选择一个 AWS 区域。要保护 Amazon CloudFront 资源，请选择 “全球”。

   要保护多个区域中的资源（ CloudFront 资源除外），必须为每个区域创建单独的 Firewall Manager 策略。
7. 选择下一步。
8. 如果您要创建规则组，请按照创建 AWS WAF 经典规则组中的说明操作。在创建规则组后，请继续执行以下步骤。
9. 输入策略名称。
10. 如果您要添加现有规则组，请使用下拉菜单选择要添加的规则组，然后选择 添加规则组。
11. 一个策略有两个可能的操作：由规则组设置的操作 和 计数。如果您要测试策略和规则组，请将操作设置为 计数。此操作会覆盖该策略中的规则组所指定的任何阻止 操作。即，如果将策略的操作设置为 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 由规则组设置的操作，则会使用规则组规则的操作。选择适当的操作。
12. 选择下一步。
13. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

- 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
- 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

  您只能选择其中一个选项。

  应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

14. 选择要保护的资源的类型。
15. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
16. 如果您要将策略自动应用于现有资源，请选择 创建此策略并将其应用于现有资源和新资源。

    此选项在 AWS 组织中的每个适用账户内创建一个 Web ACL，并将 Web ACL 与账户中的资源关联。此选项还将策略应用于符合上述条件 (资源类型和标签) 的所有新资源。或者，如果您选择 创建策略但不将策略应用于现有资源或新资源，则 Firewall Manager 会在组织内的每个适用账户中创建一个 Web ACL，但不会将 Web ACL 应用于任何资源。您稍后必须将策略应用于资源。选择适当的选项。
17. 对于 替换现有关联的 Web ACL，您可以选择删除当前为范围内资源定义的任何 Web ACL 关联，然后将它们替换为与您使用此策略创建的 Web ACL 之间的关联。默认情况下，Firewall Manager 不会在添加新的 Web ACL 关联之前删除现有的 Web ACL 关联。如果要删除现有关联，请选择此选项。
18. 选择下一步。

19. 查看新策略。要进行任何更改，请选择 编辑。若您满意所创建的策略，请选择 创建并应用策略。

为创建 AWS Firewall Manager 策略 AWS Shield Advanced

为 Shield Advanced（控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，选择 Shield Advanced。

   要创建 Shield Advanced 策略，您必须订阅 Shield Advanced。如果您尚未订阅，则会提示您订阅。有关订阅成本的更多信息，请参阅 AWS Shield Advanced 定价。
5. 对于区域，选择一个 AWS 区域。要保护 Amazon CloudFront 配送，请选择 “全球”。

   对于除全球以外的区域选项，要保护多个区域中的资源，必须为每个区域创建单独的 Firewall Manager 策略。
6. 选择下一步。
7. 对于名称，请键入策略的描述性名称。
8. 仅对于全球区域策略，您可以选择是否要管理 Shield Advanced 应用程序层 DDoS 自动缓解。有关 Shield Advanced 功能的信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

   您可以选择启用或禁用自动缓解，也可以选择忽略自动缓解。如果您选择忽略它，则 Firewall Manager 将完全不管理 Shield Advanced 保护的自动缓解。有关这些策略选项的详细信息，请参阅 自动应用程序层 DDoS 缓解。
9. 在 Web ACL 管理下，如果您希望 Firewall Manager 管理未关联的 Web ACL，请启用管理未关联的 Web ACL。启用此选项后，只有当至少一个资源使用 Web ACL 时，Firewall Manager 才会在策略范围内的账户中创建 Web ACL。当某个账户在任何时候进入策略范围时，如果至少有一个资源将使用 Web ACL，则 Firewall Manager 会自动在该账户中创建一个 Web ACL。启用此选项

后，Firewall Manager 会对您的账户中未关联的 Web ACL 进行一次性清理。清理过程可能需要数小时时间。如果资源在 Firewall Manager 创建 Web ACL 后离开策略范围，Firewall Manager 不会取消该资源与 Web ACL 的关联。要将 Web ACL 包含在一次性清理中，必须先手动取消资源与 Web ACL 的关联，然后启用管理未关联的 Web ACL。

10. 对于策略操作，建议使用不自动修复不合规资源的选项来创建策略。禁用自动修正后，可以在应用新策略之前对其进行评测。如果您对所做的更改满意，编辑策略并更改策略操作以启用自动修复。

    若要自动将策略应用于现有的范围内资源，请选择 自动修复任何不合规的资源。此选项对 AWS 组织内的每个适用账户和账户中的每个适用资源应用 Shield Advanced 保护。

    仅对于全球区域策略，如果您选择自动修复任何不合规的资源，则还可以选择让 Firewall Manager 自动将任何现有的经 AWS WAF 典 Web ACL 关联替换为使用最新版本 AWS WAF (v2) 创建的 Web ACL 的新关联。如果选择此选项，Firewall Manager 会删除与早期版本的 Web ACL 的关联，并使用最新版本的 Web ACL 创建新的关联，然后在任何还没有该策略的范围内账户中创建新的空 Web ACL。有关此选项的更多信息，请参阅 [将 AWS WAF 经典 Web ACL 替换为最新版本的 Web ACL]。

11. 选择下一步。

12. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将策略应用于组织中的所有账户，请保留默认选项包括我的 AWS 组织下的所有账户。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择“仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

    应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

13. 选择要保护的资源的类型。

Firewall Manager 不支持 Amazon Route 53 或 AWS Global Accelerator。如果您需要使用 Shield Advanced 来保护资源免受这些服务的侵害，则不能使用 Firewall Manager 策略。否则，请按照为 AWS 资源添加 AWS Shield Advanced 保护 提供的 Shield Advanced 的指导进行操作。

14. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

15. 选择下一步。

16. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。

17. 选择下一步。

18. 查看新的政策设置，然后返回需要进行任何调整的页面。

    若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

创建 AWS Firewall Manager 通用安全组策略

有关通用安全组策略的工作原理，请参阅 通用安全组策略。

创建通用安全组策略的前提是，您已在您的 Firewall Manager 管理员账户中创建了一个将用作策略主安全组的安全组。您可以通过 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 Amazon VPC 用户指南中的使用安全组。

创建 通用安全组策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

> **Note**
>
> 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 安全组。
5. 对于 安全组策略类型，选择 通用安全组。
6. 对于区域，选择一个 AWS 区域。
7. 选择下一步。
8. 对于 策略名称，输入一个友好名称。
9. 对于策略规则，请执行以下操作：

   a. 从规则选项中，选择要应用于安全组规则的限制以及策略范围内的资源。如果您选择将标签从主要安全组分发给由此策略创建的安全组，则还必须选择识别并报告由此策略创建的安全组何时变得不合规。

   > **Important**
   >
   > Firewall Manager 不会将 AWS 服务添加的系统标签分发到副本安全组中。系统标签以 `aws:` 为前缀。此外，如果现有安全组的标签与组织的标签策略存在冲突，Firewall Manager 将不会更新现有安全组的标签或创建新的安全组。有关标签策略的信息，请参阅《 AWS Organizations 用户指南》中的标签策略。

   如果您选择将安全组引用从主要安全组分发给由此策略创建的安全组，则仅当安全组引用在 Amazon VPC 中具有有效的对等连接时，Firewall Manager 才会分发安全组引用。有关此选项的信息，请参阅策略规则设置。

   b. 对于主安全组，选择添加安全组，然后选择要使用的安全组。Firewall Manager 在防火墙管理器管理员账户中填充来自所有 Amazon VPC 实例的安全组列表。

   默认情况下，每个策略的主安全组的最大数量为 3。有关该设置的信息，请参阅 AWS Firewall Manager 配额。

c. 对于 策略操作，建议使用不自动修复的选项来创建策略。这样，您就可以在应用新策略之前对其进行评测。如果您对所做的更改满意，编辑策略并更改策略操作以启用对不合规资源的自动修复。

10. 选择下一步。
11. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

    应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。
12. 对于 资源类型，选择要保护的资源的类型。

    如果您选择 EC2 实例，则可以选择在每个 Amazon EC2 实例中包含所有弹性网络接口，或者只在每个实例中包含默认接口。如果您在任何范围内的 Amazon EC2 实例中有多个弹性网络接口，则选择包含所有接口的选项可以允许 Firewall Manager 将策略应用于所有接口。启用自动修正后，如果 Firewall Manager 无法将策略应用于 Amazon EC2 实例中的所有弹性网络接口，则会将该实例标记为不合规。
13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

14. 对于 共享 VPC 资源，如果除了账户拥有的 VPC 外，您要将策略应用于共享 VPC 中的资源，请选择 包括共享 VPC 中的资源。
15. 选择下一步。
16. 查看策略设置，确保它们满足您的需求，然后选择 创建策略。

Firewall Manager 在范围内账户中包含的每个 Amazon VPC 实例中创建主要安全组的副本，不超过每个账户支持的 Amazon VPC 最大限额。Firewall Manager 将副本安全组与每个范围内账户的策略范围内的资源相关联。有关此策略工作方式的更多信息，请参阅通用安全组策略。

创建 AWS Firewall Manager 内容审核安全组策略

有关内容审核安全组策略的工作原理，请参阅 内容审核安全组策略。

对于某些内容审核策略设置，您必须提供一个审核安全组以供 Firewall Manager 用作模板。例如，您可能有一个审核安全组，其中包含您在任何安全组中都不允许的所有规则。必须先使用 Firewall Manager 管理员账户创建这些审核安全组，然后才能在策略中使用它们。您可以通过 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 Amazon VPC 用户指南中的使用安全组。

创建内容审核安全组策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 安全组。
5. 对于安全组策略类型，请选择安全组规则的审核和执行。
6. 对于区域，选择一个 AWS 区域。
7. 选择下一步。

8. 对于 策略名称，输入一个友好名称。
9. 对于策略规则，请选择要使用的托管或自定义策略规则选项。

   a. 对于配置托管审核策略规则，请执行以下操作：

      i. 在配置待审核的安全组规则中，选择要应用审核策略的安全组规则的类型。

      ii. 如果您想根据安全组中的协议、端口和 CIDR 范围设置执行诸如审核规则之类的操作，请选择审核过于宽松的安全组规则，然后选择所需的选项。

      对于选择规则允许所有流量，您可以提供自定义应用程序列表来指定要审核的应用程序。有关自定义应用程序列表以及如何在策略中使用它们的信息，请参阅 托管列表 和 使用托管列表。

      对于使用协议列表的选择，您可以使用现有列表，也可以创建新列表。有关协议列表以及如何在策略中使用这些列表的信息，请参阅 托管列表 和 使用托管列表。

      iii. 如果要根据他们对保留或非保留 CIDR 范围的访问权限来审核高风险，请选择审核高风险应用程序，然后选择所需的选项。

      以下选项相互排斥：只能访问保留 CIDR 范围的应用程序和允许访问非保留 CIDR 范围的应用程序。您可以在任何策略中最多选择其中一项。

      对于使用应用程序列表的选择，您可以使用现有列表，也可以创建新列表。有关应用程序列表以及如何在策略中使用它们的信息，请参阅 托管列表 和 使用托管列表。

      iv. 使用覆盖设置可以显式覆盖策略中的其他设置。您可以选择始终允许或始终拒绝特定的安全组规则，无论这些规则是否符合您为该策略设置的其他选项。

      对于此选项，您可以提供一个审核安全组作为允许的规则或拒绝的规则模板。对于审核安全组，选择添加审核安全组，然后选择要使用的安全组。Firewall Manager 会填充 Firewall Manager 管理员账户中所有 Amazon VPC 实例的审核安全组列表。策略的审核安全组的默认最大限额为 1。有关增加限额的信息，请参阅 AWS Firewall Manager 配额。

   b. 对于配置自定义策略规则，请执行以下操作：

      i. 从规则选项中选择仅允许审核安全组中定义的规则，或是拒绝所有规则。有关此选择的信息，请参阅 内容审核安全组策略。

      ii. 对于审核安全组，选择添加审核安全组，然后选择要使用的安全组。Firewall Manager 会填充 Firewall Manager 管理员账户中所有 Amazon VPC 实例的审核安全组列表。策略的

审核安全组的默认最大限额为 1。有关增加限额的信息，请参阅 AWS Firewall Manager 配额。

iii. 对于 Policy action (策略操作)，您必须使用不自动修复的选项来创建策略。这样，您就可以在应用新策略之前对其进行评测。如果您对所做的更改满意，编辑策略并更改策略操作以启用对不合规资源的自动修复。

10. 选择下一步。
11. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

    应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。
12. 对于资源类型，选择要保护的资源的类型。
13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
14. 选择下一步。
15. 查看策略设置，确保它们满足您的需求，然后选择 创建策略。

Firewall Manager 会根据您的策略规则设置将审核安全组与 AWS 组织内的安全组进行比较。您可以在策略控制台中查看 AWS Firewall Manager 策略状态。创建策略后，您可以对其进行编辑并启用自动修正，从而使您的审核安全组策略生效。有关此策略工作方式的更多信息，请参阅内容审核安全组策略。

创建 AWS Firewall Manager 使用情况审核安全组策略

有关使用情况审核安全组策略的工作原理，请参阅 使用情况审核安全组策略。

创建使用情况审核安全组策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 安全组。
5. 对于安全组策略类型，选择未关联和冗余安全组审核和清理。
6. 对于区域，选择一个 AWS 区域。
7. 选择下一步。
8. 对于 策略名称，输入一个友好名称。
9. 对于 策略规则，选择其中一个或全部两个可用选项。

   - 如果您选择此策略范围中的安全组必须至少由一个资源使用，Firewall Manager 将删除它认为未使用的任何安全组。启用此规则后，Firewall Manager 会在您保存策略时最后运行该规则。

     有关 Firewall Manager 如何确定使用情况和补救时间的详细信息，请参阅使用情况审核安全组策略。

> **Note**
>
> 使用此使用情况审计安全组策略类型时，请避免在短时间内对范围内安全组的关联状态进行多次更改。这样做可能会导致 Firewall Manager 错过相应的事件。

默认情况下，一旦安全组未被使用，Firewall Manager 就会将其视为不符合此策略规则。您可以选择指定安全组在被视为不合规之前可以处于未使用状态的分钟数，最长为 525,600 分钟（365 天）。您可以使用此设置让自己有时间将新的安全组与资源关联起来。

> **Important**
>
> 如果您指定的分钟数不是默认值 0，则必须在中启用间接关系 AWS Config。否则，您的使用情况审核安全组策略将无法按预期运行。有关间接关系的信息 AWS Config，请参阅《AWS Config 开发者指南》 AWS Config中的间接关系。

- 如果您选择此策略范围中的安全组必须唯一，则 Firewall Manager 将合并多余的安全组，因此仅有一个安全组与任意资源关联。如果您选择此规则，则 Firewall Manager 将在您保存策略时最先运行它。

10. 对于 策略操作，建议使用不自动修复的选项来创建策略。这样，您就可以在应用新策略之前对其进行评测。如果您对所做的更改满意，编辑策略并更改策略操作以启用对不合规资源的自动修复。
11. 选择下一步。
12. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

14. 选择下一步。

15. 如果您尚未将 Firewall Manager 管理员账户排除在策略范围之外，Firewall Manager 会提示您采取此项操作。这样，您将实现手动控制用于常用和审核安全组策略的 Firewall Manager 管理员账户中的安全组。在此对话框中选择您的选项。

16. 查看策略设置，确保它们满足您的需求，然后选择 创建策略。

如果您选择需要唯一的安全组，则 Firewall Manager 在各个范围内的 Amazon VPC 实例中扫描多余的安全组。然后，如果您选择要求每个安全组至少由一个资源使用，Firewall Manager 会扫描在规则中指定分钟内未使用的安全组。您可以在策略控制台中查看 AWS Firewall Manager 策略状态。有关此策略工作方式的更多信息，请参阅使用情况审核安全组策略。

创建 AWS Firewall Manager 网络 ACL 策略

有关网络 ACL 策略的工作原理的信息，请参阅网络 ACL 策略。

要创建网络 ACL 策略，您必须知道如何定义用于您的 Amazon VPC 子网的网络 ACL。有关信息，请参阅 Amazon VPC 用户指南中的使用网络 ACL 控制子网流量和使用网络 ACL。

创建网络 ACL 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

> **Note**
>
> 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，请选择网络 ACL。
5. 对于区域，选择一个 AWS 区域。
6. 选择下一步。
7. 对于策略名称，请键入策略的描述性名称。
8. 对于策略规则，请定义要始终在 Firewall Manager 为您管理的网络 ACL 中运行的规则。网络 ACL 监控和处理入站和出站流量，因此在您的策略中，您可以定义双向的规则。

   对于任一方向，您都要定义要始终先运行的规则和要始终最后运行的规则。在 Firewall Manager 管理的网络 ACL 中，账户所有者可以定义在第一条和最后一条规则之间运行的自定义规则。
9. 对于策略操作，如果您想识别不合规的子网和网络 ACL，但尚未采取任何更正措施，请选择 “识别不符合策略规则但不自动修复的资源”。您随后可以更改这些选项。

   相反，如果您想将策略自动应用于现有范围内子网，请选择自动修复任何不合规的资源。使用此选项，您还可以指定当策略规则的流量处理行为与网络 ACL 中的自定义规则冲突时是否强制修复。无论您是否强制修复，Firewall Manager 都会报告其合规性违规中存在冲突的规则。
10. 选择下一步。
11. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包含特定帐户，则 Firewall Manager 不会将该策略应用于任何不同的新帐户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

12. 对于资源类型，子网中的设置是固定的。
13. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
14. 选择下一步。
15. 查看策略设置，确保它们满足您的需求，然后选择 创建策略。

Firewall Manager 会根据您的设置创建策略并开始监视和管理范围内的网络 ACL。有关此策略工作方式的更多信息，请参阅网络 ACL 策略。

为创建 AWS Firewall Manager 策略 AWS Network Firewall

在 Firewall Manager Network Firewall 策略中，您可以使用您在 AWS Network Firewall中管理的规则组。有关管理规则组的信息，请参阅 Network Firewall 开发人员指南中的AWS Network Firewall 规则组。

有关 Firewall Manager Network Firewall 策略的信息，请参阅 AWS Network Firewall 政策。

为 AWS Network Firewall （控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

> **Note**
>
> 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于 策略类型，选择 AWS Network Firewall。
5. 在防火墙管理类型下，选择您希望 Firewall Manager 如何管理策略的防火墙。从以下选项中进行选择：

   - 分布式 – Firewall Manager 在策略范围内的每个 VPC 中创建和维护防火墙端点。
   - 集中式 – Firewall Manager 在单个检查 VPC 中创建和维护端点。
   - 导入现有防火墙 – Firewall Manager 使用资源集从 Network Firewall 导入现有防火墙。有关资源集的信息，请参阅 在 Firewall Manager 中使用资源集。
6. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。Firewall Manager 将策略名称包含在其创建的 Network Firewall 防火墙和防火墙策略的名称中。
9. 在AWS Network Firewall 策略配置中，像在 Network Firewall 中一样配置防火墙策略。添加您的无状态和有状态规则组，并指定策略的默认操作。您可以选择设置策略的状态规则评测顺序和默认操作以及日志记录配置。有关 Network Firewall 防火墙策略管理的信息，请参阅AWS Network Firewall 开发人员指南中的AWS Network Firewall 防火墙策略。

   在创建 Firewall Manager 网络防火墙策略时，Firewall Manager 会为范围内的账户创建防火墙策略。个人账户管理员可以向防火墙策略添加规则组，但他们无法更改您在此处提供的配置。
10. 选择下一步。
11. 根据在上一步中选择的防火墙管理类型，执行以下操作之一：

    - 如果您使用的是分布式防火墙管理类型，请在防火墙终端位置下的 AWS Firewall Manager 端点配置中，选择以下选项之一：
      - 自定义端点配置 – Firewall Manager 在您指定的可用区内为策略范围内的每个 VPC 创建防火墙。每个防火墙至少包含一个防火墙端点。
        - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
        - 如果要为 Firewall Manager 提供 CIDR 块以用于 VPC 中的防火墙子网，则它们必须全部为 /28 CIDR 块。每行输入一个块。如果省略这些地址，Firewall Manager 将从 VPC 中可用的 IP 地址中为您选择 IP 地址。

> **Note**
>
> Network Fire AWS Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不自动修复的选项。

- 自动配置端点 – Firewall Manager 会自动在可用区中创建防火墙端点，并在您的 VPC 中使用公有子网。
  - 对于防火墙端点配置，请指定 Firewall Manager 如何管理防火墙端点。为了获得高可用性，我们建议使用多个端点。
- 如果您使用的是集中式防火墙管理类型，请在检查 VPC 配置下的 AWS Firewall Manager 端点配置中，输入检查 VPC 所有者的 AWS 账户 ID 和检查 VPC 的 VPC ID。
  - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
  - 如果要为 Firewall Manager 提供 CIDR 块以用于 VPC 中的防火墙子网，则它们必须全部为 /28 CIDR 块。每行输入一个块。如果省略这些地址，Firewall Manager 将从 VPC 中可用的 IP 地址中为您选择 IP 地址。

> **Note**
>
> Network Fire AWS Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不自动修复的选项。

- 如果您使用的是导入现有防火墙防火墙管理类型，请在资源集中添加一个或多个资源集。资源集定义了您要在本策略中集中管理的组织账户所拥有的现有 Network Firewall 防火墙。要将资源集添加到策略中，必须先使用控制台或 PutResourceSetAPI 创建资源集。有关资源集的信息，请参阅 在 Firewall Manager 中使用资源集。有关从 Network Firewall 导入现有防火墙的更多信息，请参阅导入现有防火墙。

12. 选择下一步。
13. 如果您的策略使用分布式防火墙管理类型，请在路由管理下选择 Firewall Manager 是否监控必须通过相应防火墙端点路由的流量并发出警报。

> **Note**
>
> 如果您选择监控，则以后无法将该设置更改为关闭。监控将持续运行，直到您删除该策略。

14. 对于流量类型，可以选择性地添加为了进行防火墙检查而需要路由流量的流量端点。
15. 对于允许所需的跨可用区流量，如果您启用此选项，则对于没有自己防火墙端点的可用区，Firewall Manager 会将从可用区发送流量到外部进行检查的路由视为合 规路由。具有端点的可用区必须始终检查自己的流量。
16. 选择下一步。
17. 对于策略作用域，在 AWS 账户 本策略适用于下，选择以下选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

    应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。
18. Network Firewall 策略的资源类型是 VPC。
19. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
20. 选择下一步。
21. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
22. 选择下一步。
23. 查看新的政策设置，然后返回需要进行任何调整的页面。

若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

为 Amazon Route 53 解析器 DNS 防火墙创建 AWS Firewall Manager 策略

在 Firewall Manager DNS Firewall 策略中，您可以使用在 Amazon Route 53 Resolver DNS 防火墙中管理的规则组。有关管理规则组的信息，请参阅 Amazon Route 53 开发人员指南中的在 DNS 防火墙中管理规则组和规则。

有关 Firewall Manager DNS 防火墙策略的信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

为 Amazon Route 53 Resolver DNS 防火墙（控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，请选择 Amazon Route 53 Resolver DNS 防火墙。
5. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。
6. 选择下一步。
7. 对于策略名称，请键入策略的描述性名称。
8. 在策略配置中，在 VPC 的规则组关联中添加您希望 DNS Firewall 首先和最后评测的规则组。您最多可以向策略添加两个规则组。

   在创建 Firewall Manager DNS 防火墙策略时，Firewall Manager 会使用您提供的关联优先级为范围内的 VPC 和账户创建规则组关联。个人账户经理可以在您的第一个和最后一个关联之间添

加规则组关联，但他们无法更改您在此处定义的关联。有关更多信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

9. 选择 下一步。
10. 对于适用此策略的AWS 账户 ，请按以下方式选择选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

    您只能选择其中一个选项。

    应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。
11. DNS 防火墙策略的资源类型是 VPC。
12. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
13. 选择下一步。
14. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
15. 选择下一步。
16. 查看新的政策设置，然后返回需要进行任何调整的页面。

    若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分

钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

为 Palo Alto Networks Cloud AWS Firewall Manager 制定政策 NGFW

借助帕洛阿尔托网络云下一代防火墙（Palo Alto Networks Cloud NGFW）的防火墙管理器策略，您可以使用防火墙管理器部署帕洛阿尔托网络云下一代防火墙资源，并在所有账户中集中管理 NGFW 规则堆栈。 AWS

有关 Firewall Manager Palo Alto Networks Cloud NGFW 策略的信息，请参阅 Palo Alto Networks Cloud NGFW 策略。有关如何配置和管理适用于 Firewall Manager 的 Palo Alto Networks Cloud NGFW 的信息，请参阅 AWS文档中的 Palo Alto Networks Cloud NGFW。

先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

要为 Palo Alto Networks Cloud NGFW（控制台）创建 Firewall Manager 策略

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，请选择 Palo Alto Networks Cloud NGFW。如果你还没有在 Marketplace 上订阅 Palo Alto N AWS etworks Cloud NGFW 服务，则需要先订阅。要在 AWS Marketplace 上订阅，请选择 “查看 AWS 商城详情”。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定了 Firewall Manager 如何管理策略的端点。采用分布式模式，Firewall Manager 在策略作用域内的每个 VPC 中维护防火墙端点。在集中式模式下，Firewall Manager 在检查 VPC 中维护单个端点。

6. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。
7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 在策略配置中，选择要与此策略关联的 Palo Alto Networks Cloud NGFW 防火墙策略。Palo Alto Networks Cloud NGFW 防火墙策略列表包含与您的 Palo Alto Networks Cloud NGFW 租户关联的所有 Palo Alto Networks Cloud NGFW 防火墙策略。有关创建和管理 Palo Alto Networks Cloud NGFW 防火墙策略的信息，请参阅 Deplo y Palo Alto Networks Cloud NGFW 的 NGFW 部署指南中的 AWS Firewall Manager主题。 AWS AWS
10. 对于 Palo Alto Networks Cloud NGFW 日志记录——可选，可以选择为你的策略选择要记录的 Palo Alto Networks Cloud NGFW 日志类型。有关 Palo Alto Networks Cloud NGFW 日志类型的信息，请参阅《帕洛阿尔托网络云 NGFW 部署指南》 AWS中的 “为帕洛阿尔托网络云 NGFW 配置日志记录”。 AWS

    对于日志记录目标，指定 Firewall Manager 何时应写入日志。
11. 选择下一步。
12. 在配置第三方防火墙端点下，根据创建防火墙端点的部署模型（分布式部署模型或集中式部署模型）执行以下操作之一：

    - 如果您为此策略使用分布式部署模型，请在可用区下选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
    - 如果您使用此策略的集中式部署模型，请在检查 VPC 配置下的 AWS Firewall Manager 端点配置中输入检查 VPC 所有者的 AWS 账户 ID 和检查 VPC 的 VPC ID。
        - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
13. 如果要为 Firewall Manager 提供 CIDR 块以用于 VPC 中的防火墙子网，则它们必须全部为 /28 CIDR 块。每行输入一个块。如果省略这些地址，Firewall Manager 将从 VPC 中可用的 IP 地址中为您选择 IP 地址。

    > **Note**
    >
    > Network Fire AWS Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不自动修复的选项。

14. 选择下一步。
15. 对于策略作用域，在 AWS 账户 本策略适用于下，选择以下选项：

- 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
- 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
- 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

16. Network Firewall 策略的资源类型是 VPC。
17. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
18. 对于授予跨账户存取权限，请选择下载 AWS CloudFormation 模板。这将下载一个可用于创建 AWS CloudFormation 堆栈的 AWS CloudFormation 模板。此堆栈创建了一个 AWS Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户管理帕洛阿尔托网络云 NGFW 资源的权限。有关堆栈的信息，请参阅 AWS CloudFormation 用户指南中的使用堆栈。
19. 选择下一步。
20. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
21. 选择下一步。
22. 查看新的政策设置，然后返回需要进行任何调整的页面。

    若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分

钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

为 Fortigate 云原生防火墙 (CNF) 即服务创建 AWS Firewall Manager 策略

借助 Fortigate CNF 的 Firewall Manager 策略，你可以使用 Firewall Manager 在所有账户中部署和管理 Fortigate CNF 资源。 AWS

有关 Firewall Manager Fortigate CNF 策略的信息，请参阅 Fortigate 云原生防火墙 (CNF) 即服务策略。有关如何配置 Fortigate CNF 以支持与 Firewall Manager 配合使用的信息，请参阅 Fortinet 文档。

先决条件

为 AWS Firewall Manager准备您的账户有几个必要步骤。AWS Firewall Manager 先决条件中介绍了这些步骤。在继续执行下一步之前，请完成所有先决条件。

创建适用于 Fortigate CNF 的 Firewall Manager 策略（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择 创建策略。
4. 对于策略类型，选择 Fortigate 云原生防火墙 (CNF) 即服务。如果你还没有在 M arketpl AWS ace 上订阅 Fortigate CNF 服务，则需要先订阅。要在 AWS Marketplace 上订阅，请选择 “查看 AWS 商城详情”。
5. 对于部署模型，选择分布式模型或集中式模型。部署模型决定了 Firewall Manager 如何管理策略的端点。采用分布式模式，Firewall Manager 在策略作用域内的每个 VPC 中维护防火墙端点。在集中式模式下，Firewall Manager 在检查 VPC 中维护单个端点。
6. 对于区域，选择一个 AWS 区域。为了保护多个区域中的资源，您必须为每个区域创建单独的策略。

7. 选择下一步。
8. 对于策略名称，请键入策略的描述性名称。
9. 在策略配置中，选择要与此策略关联的 Fortigate CNF 防火墙策略。Fortigate CNF 防火墙策略列表包含与您的 Fortigate CNF 租户关联的所有 Fortigate CNF 防火墙策略。有关创建和管理 Fortigate CNF 租户的信息，请参阅 Fortinet 文档。
10. 选择下一步。
11. 在配置第三方防火墙端点下，根据创建防火墙端点的部署模型（分布式部署模型或集中式部署模型）执行以下操作之一：

    - 如果您为此策略使用分布式部署模型，请在可用区下选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
    - 如果您使用此策略的集中式部署模型，请在检查 VPC 配置下的 AWS Firewall Manager 端点配置中输入检查 VPC 所有者的 AWS 账户 ID 和检查 VPC 的 VPC ID。
      - 在可用区下，选择要在其中创建防火墙端点的可用区。您可以按可用区名称或可用区 ID 选择可用区。
12. 如果要为 Firewall Manager 提供 CIDR 块以用于 VPC 中的防火墙子网，则它们必须全部为 /28 CIDR 块。每行输入一个块。如果省略这些地址，Firewall Manager 将从 VPC 中可用的 IP 地址中为您选择 IP 地址。

    > **Note**
    >
    > Network Fire AWS Firewall Manager wall 策略会自动进行自动修复，因此您不会在此处看到选择不自动修复的选项。

13. 选择下一步。
14. 对于策略作用域，在 AWS 账户 本策略适用于下，选择以下选项：

    - 如果要将该政策应用于组织中的所有账户，请保留默认选项 “包括我的 AWS 组织下的所有账户”。
    - 如果您只想将策略应用于特定帐户或特定 AWS Organizations 组织单位 (OU) 中的帐户，请选择 “仅包括指定的帐户和组织单位”，然后添加要包括的帐户和 OU。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。
    - 如果要将该策略应用于除一组特定的账户或 AWS Organizations 组织单位 (OU) 之外的所有账户或组织单位，请选择排除指定的账户和组织单位，并包括所有其他账户和组织单位，然后添加要排除的账户和组织单位。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。

您只能选择其中一个选项。

应用策略后，Firewall Manager 会根据您的设置自动评估任何新账户。例如，如果您仅包括了特定账户，Firewall Manager 便不会将策略应用于任何新账户。另一个例子是，如果包括了 OU，则在向 OU 或其任何子 OU 添加账户时，Firewall Manager 会自动将策略应用到新账户。

15. Network Firewall 策略的资源类型是 VPC。
16. 对于资源，您可以使用标记来缩小策略的范围，方法是包括或排除带有您指定标签的资源。您可以使用 “包含” 或 “排除”，但不能两者兼而有之。有关标签的更多信息，请参阅使用标签编辑器。

    如果输入多个标签，则资源必须具有要包括或排除的所有标签。

    资源标签只能有非空值。如果省略标签的值，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。
17. 对于授予跨账户存取权限，请选择下载 AWS CloudFormation 模板。这将下载一个可用于创建 AWS CloudFormation 堆栈的 AWS CloudFormation 模板。此堆栈创建了一个 AWS Identity and Access Management 角色，该角色授予 Firewall Manager 跨账户管理 Fortigate CNF 资源的权限。有关堆栈的信息，请参阅 AWS CloudFormation 用户指南中的使用堆栈。要创建堆栈，您需要来自 Fortigate CNF 门户网站的账户 ID。
18. 选择下一步。
19. 对于策略标记，添加要添加到 Firewall Manager 策略资源的所有标识标记。有关标签的更多信息，请参阅使用标签编辑器。
20. 选择下一步。
21. 查看新的政策设置，然后返回需要进行任何调整的页面。

    若您满意所创建的策略，请选择 创建策略。AWS Firewall Manager 策略窗格下应列出您的策略。它可能会在账户标题下显示 “待处理”，并指示 “自动修复” 设置的状态。策略的创建可能需要几分钟的时间。当 待处理 状态替换为账户计数时，您可以选择策略名称来探索账户和资源的合规状态。有关信息，请参阅。查看 AWS Firewall Manager 策略的合规性信息

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 安全策略。

2. 选择要删除的策略旁的选项。
3. 选择 Delete （ 删除)。

> **Note**
>
> 删除 Firewall Manager 通用安全组策略时，要删除该策略的副本安全组，请选择清理该策略创建的资源的选项。否则，在删除主实例后，副本将保留，需要在每个 Amazon VPC 实例中进行手动管理。

> **Important**
>
> 删除 Firewall Manager Shield Advanced 策略时，该策略将被删除，但您的账户仍有 Shield Advanced 的订阅。

AWS Firewall Manager 政策范围

策略范围定义了策略的适用范围。您可以将集中控制的策略应用于组织中的所有账户和资源 AWS Organizations，也可以对部分账户和资源应用集中控制的策略。有关如何设置策略作用域的说明，请参阅 创建 AWS Firewall Manager 策略。

中的策略范围选项 AWS Firewall Manager

当您向组织添加新账户或资源时，Firewall Manager 会根据您的每项策略设置自动对其进行评测，并根据这些设置应用策略。例如，您可以选择将策略应用于除指定列表中的账号之外的所有账户；也可以选择仅将策略应用于列表中包含所有标签的资源。

AWS 账户 在范围内

您为定义受策略 AWS 账户 影响的账户而提供的设置决定了要将策略应用到 AWS 组织中的哪些账户。您可以选择通过以下一种方式来应用策略：

- 至组织中的所有账户
- 仅应用到包括的账号和 AWS Organizations 组织单位 (OU) 的特定列表
- 应用到除排除的账号和 AWS Organizations 组织单位 (OU) 的特定列表之外的所有账户和组织单位

有关的信息 AWS Organizations，请参阅《AWS Organizations 用户指南》。

范围内资源

与范围内账户的设置类似，您为资源提供的设置决定了要将策略应用于哪些范围内资源类型。您可以选择以下任一种密钥：

- 所有资源
- 具有您指定的所有标签的资源
- 所有资源，除了具有您指定的所有标签的资源

只能指定非空值的资源标签。如果您没有为该值提供任何内容，Firewall Manager 会使用空字符串值保存标记：“”。资源标签仅与具有相同密钥和相同值的标签匹配。

有关标记资源的更多信息，请参阅使用标签编辑器。

中的策略范围管理 AWS Firewall Manager

制定策略后，Firewall Manager 会持续对其进行管理， AWS 账户 并在添加新资源和资源时根据策略范围将其应用于新增资源和资源。

Firewall Manager 如何 AWS 账户 管理和资源

如果账户或资源出于任何原因超出范围，则 AWS Firewall Manager 不会自动移除保护或删除 Firewall Manager 管理的资源，除非您选中 “自动移除对离开策略范围的资源的保护” 复选框。

> **Note**
>
> “自动移除对离开策略范围的资源的保护” 选项不适用于 AWS Shield Advanced 或 AWS WAF Classic 策略。

选中此复选框 AWS Firewall Manager 将指示在帐户离开策略范围时自动清理 Firewall Manager 为这些帐户管理的资源。例如，当客户资源超出策略范围时，Firewall Manager 将取消 Firewall Manager 托管的 Web ACL 与受保护的客户资源的关联。

为了确定当客户资源超出策略范围时应将哪些资源从保护中移除，Firewall Manager 需要遵循以下准则：

- 默认行为：
  - 关联的 AWS Config 托管规则已删除。此行为与复选框无关。

  - 任何不包含任何资源的关联 AWS WAF Web 访问控制列表 (Web ACL) 都将被删除。此行为与复选框无关。
  - 任何超出范围的受保护资源都将保持关联状态并受到保护。例如，与 Web ACL 关联的应用程序负载均衡器或 API Gateway 中的 API 仍与网页 ACL 关联，并且保护仍然有效。
- 选中自动移除对不在策略范围之外的资源的保护复选框后：
  - 关联的 AWS Config 托管规则已删除。此行为与复选框无关。
  - 任何不包含任何资源的关联 AWS WAF Web 访问控制列表 (Web ACL) 都将被删除。此行为与复选框无关。
  - 任何超出范围的受保护资源在离开策略范围时都会自动取消关联并从 Firewall Manager 保护中移除。例如，对于安全组策略，Elastic Inference 加速器或 Amazon EC2 实例在离开策略范围时会自动取消与复制的安全组的关联。复制的安全组及其资源将自动从保护中移除。

托管列表

托管应用程序和协议列表简化了 AWS Firewall Manager 内容审核安全组策略的配置和管理。您可以使用托管列表来定义您的策略允许和不允许的协议与应用程序。有关内容审核安全组策略的信息，请参阅内容审核安全组策略。

您可以在内容审核安全组策略中使用以下类型的托管列表：

- Firewall Manager 应用程序列表和协议列表：这些列表由 Firewall Manager 管理。
  - 应用程序列表包括 `FMS-Default-Public-Access-Apps-Allowed` 和 `FMS-Default-Public-Access-Apps-Denied`，它们描述了应允许或拒绝向公众开放的常用应用程序。
  - 协议列表 `FMS-Default-Protocols-Allowed` 包括应允许公众使用的常用协议列表。您可以使用 Firewall Manager 管理的任何列表，但不能对其进行编辑或删除。
- 自定义应用程序列表和协议列表 – 这些列表由您管理。您可以使用所需的设置创建任一类型的列表。您可以完全控制自己的自定义托管列表，也可以根据需要创建、编辑和删除它们。

> **Note**
>
> 目前，当您删除自定义托管列表时，Firewall Manager 不会检查对它的引用。这意味着，即使处于活动状态的策略正在使用自定义托管应用程序列表或协议列表，您也可以将其删除。但该操作可能导致策略停止运行。因此，在确认任何有效策略均未引用应用程序列表或协议列表之后，才可将其删除。

托管列表是 AWS 资源。您可以为自定义托管列表添加标签。您无法为 Firewall Manager 托管列表添加标签。

托管列表版本控制

自定义托管列表没有版本。编辑自定义列表时，引用该列表的策略会自动使用更新的列表。

Firewall Manager 托管列表已进行版本控制。Firewall Manager 服务团队根据需要发布新版本，以便将最佳安全实践应用于列表。

在策略中使用 Firewall Manager 托管列表时，您可以按如下方式选择版本控制策略：

- 最新可用版本 – 如果您没有为列表指定明确的版本设置，则您的策略将自动使用最新版本。这是控制台中唯一可用的选项。
- 显式版本 – 如果您为列表指定版本，则您的策略将使用该版本。在您修改版本设置之前，您的策略将一直锁定在您指定的版本。要指定版本，您必须在控制台之外定义策略，例如通过 CLI 或其中一个 SDK 来定义策略。

有关为列表选择版本设置的更多信息，请参阅 在内容审核安全组策略中使用托管列表。

在内容审核安全组策略中使用托管列表

创建内容审核安全组策略时，可以选择使用托管审核策略规则。此选项的某些设置需要托管应用程序列表或协议列表。这些设置的示例包括安全组规则中允许的协议以及可以访问互联网的应用程序。

以下限制适用于使用托管列表的每个策略设置：

- 对于任何设置，最多可以指定一个 Firewall Manager 托管列表。默认情况下，您最多可以指定一个自定义列表。自定义列表限制是软限额，因此您可以申请增加该限额。有关更多信息，请参阅 AWS Firewall Manager 配额。
- 在控制台中，如果您选择 Firewall Manager 托管列表，则无法指定版本。该策略将始终使用最新版本的列表。要指定版本，您必须在控制台之外定义策略，例如通过 CLI 或其中一个 SDK 来定义策略。有关 Firewall Manager 托管列表版本控制的信息，请参阅 托管列表版本控制。

有关通过控制台创建内容审核安全组策略的信息，请参阅 创建内容审核安全组策略。

创建自定义托管应用程序列表

要创建自定义托管应用程序列表

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择应用程序列表。
3. 在应用程序列表页面中，选择创建应用程序列表。
4. 在创建应用程序列表页面中，为您的列表命名。请勿使用前缀 `fms-`，因为这是为 Firewall Manager 保留的前缀。
5. 通过提供协议和端口号或从类型下拉列表中选择应用程序来指定应用程序。为您的应用程序规格命名。
6. 根据需要选择添加另一个，然后填写应用程序信息，直到完成列表为止。
7. （可选）为列表应用标签。
8. 选择保存以保存您的列表并返回到应用程序列表页面。

创建自定义托管协议列表

要创建新的自定义托管协议列表

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择协议列表。

3. 在协议列表页面中，选择创建协议列表。
4. 在协议列表创建页面，为列表命名。请勿使用前缀 `fms-`，因为这是为 Firewall Manager 保留的前缀。
5. 指定协议。
6. 根据需要选择添加另一个，然后填写协议信息，直到完成列表为止。
7. （可选）为列表应用标签。
8. 选择保存以保存您的列表并返回到协议列表页面。

查看托管列表

查看应用程序列表或协议列表

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择应用程序列表或协议列表。

   该页面显示了可供您使用的所有选定类型的列表。Firewall Manager 管理的列表的ManagedList列中有一个 Y。

3. 要查看列表的详细信息，请选择列表名称。详情页面显示列表的内容和所有标签。

   对于 Firewall Manager 管理列表，您还可以通过选择版本下拉列表来查看可用版本。

删除自定义托管列表

您可以删除自定义托管名单。您不可对 Firewall Manager 管理的列表进行编辑或删除。

> **Note**
>
> 目前，当您删除自定义托管列表时，Firewall Manager 不会检查对它的引用。这意味着，即使处于活动状态的策略正在使用自定义托管应用程序列表或协议列表，您也可以将其删除。但该

操作可能导致策略停止运行。因此，在确认任何有效策略均未引用应用程序列表或协议列表之后，才可将其删除。

要删除自定义托管应用程序或协议列表

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 通过执行以下操作，确保您的任何审核安全组策略中均未使用您要删除的列表：

   a. 在导航窗格中，选择 安全策略。

   b. 在 AWS Firewall Manager 策略页面中，选择并编辑您的审核安全组，并删除对要删除的自定义列表的所有引用。

      如果您删除审核安全组策略中正在使用的自定义托管列表，则使用该列表的策略可能会停止运行。

3. 在导航窗格中，根据要删除的列表类型，选择应用程序列表或协议列表。
4. 在列表页面中，选择要删除的自定义列表，然后选择删除。

AWS WAF 政策

在 Firew AWS WAF all Manager 策略中，您可以指定要在资源中使用的 AWS WAF 规则组。应用策略时，Firewall Manager 会根据您在策略中配置 Web ACL 管理的方式，在策略范围内的账户中创建 Web ACL。在策略创建的 Web ACL 中，除了您通过 Firewall Manager 定义的规则组外，个人账户管理员还可以添加规则和规则组。

Firewall Manager 如何管理 Web ACL

Firewall Manager 根据您在策略中配置 “管理未关联的网页 ACL” 设置或 API 中SecurityServicePolicyData数据类型的**`optimizeUnassociatedWebACL`**设置来创建 Web ACL。

如果您启用了对未关联 Web ACL 的管理，则只有当至少一个资源使用 Web ACL 时，Firewall Manager 才会在策略范围内的账户中创建 Web ACL。当某个账户在任何时候进入策略范围时，如果至少有一个资源将使用 Web ACL，则 Firewall Manager 会自动在该账户中创建一个 Web ACL。启用对未关联 Web ACL 的管理后，Firewall Manager 会对您账户中的未关联 Web ACL 执行一次性清理。在清理过程中，Firewall Manager 会跳过您在创建后修改的所有 Web ACL，例如，如果您向 Web ACL 添加了规则组或修改了其设置。清理过程可能需要数小时时间。如果资源在 Firewall Manager 创建 Web ACL 后离开策略范围，Firewall Manager 将取消该资源与 Web ACL 的关联，但不会清理未关联的 Web ACL。只有当您在策略中首次启用对未关联的 Web ACL 的管理时，Firewall Manager 才会清理未关联的 Web ACL。

如果您不启用此选项，Firewall Manager 将不管理未关联 Web ACL，并且 Firewall Manager 会自动在策略范围内的每个账户中创建一个 Web ACL。

采样和 CloudWatch 指标

AWS Firewall Manager 为其为 AWS WAF 策略创建的 Web ACL 和规则组启用采样和 Amazon CloudWatch 指标。

Web ACL 命名结构

当 Firewall Manager 为策略创建 Web ACL 时，它会将该 Web ACL 命名为 `FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`*。时间戳以毫秒为单位。例如，`FMManagedWebACLV2-MyWAFPolicyName-1621880374078`。

> **Note**
>
> 如果配置了高级自动应用层 DDoS 防护的资源属于 AWS WAF 策略的范围，则 Firewall Manager 将无法将该 AWS WAF 策略创建的 Web ACL 与该资源相关联。

AWS WAF 策略中的规则组

由 Firewall Manager AWS WAF 策略管理的 Web ACL 包含三组规则。这些规则集为 Web ACL 中的规则和规则组提供了更高级的优先级划分机制：

- 第一个规则组，由您在 Firewall Manager AWS WAF 策略中定义。 AWS WAF 首先评估这些规则组。
- 由账户经理在 Web ACL 中定义的规则和规则组。 AWS WAF 会在中间评估任何客户托管的规则或规则组。

- 最后一个规则组，由您在 Firewall Manager AWS WAF 策略中定义。 AWS WAF 最后评估这些规则组。

在每组规则中，根据规则和规则组在规则集中的优先级设置，照常 AWS WAF 评估规则和规则组。

在策略的“最先运行的规则组”集和“最后运行的规则组”集中，您只能添加规则组。您可以使用托管规则组，由 AWS 托管规则和 AWS Marketplace 卖家为您创建和维护。您也可以管理和使用自己的规则组。有关所有这些操作的更多信息，请参阅AWS WAF 规则组。

如果要使用自己的规则组，请在创建 Firewall Manager AWS WAF 策略之前创建这些规则组。有关操作指南，请参阅 管理您自己的规则组。要使用单个自定义规则，您必须定义自己的规则组，再在其中定义您的规则，然后在策略中使用该规则组。

您通过 Firewall Manager 管理的第一个和最后一个 AWS WAF 规则组的名称分别以PREFMManaged-或POSTFMManaged-开头，后跟防火墙管理器策略名称和规则组创建时间戳（以 UTC 毫秒为单位）。例如，PREFMManaged-MyWAFPolicyName-1621880555123。

有关如何 AWS WAF 评估 Web 请求的信息，请参阅Web ACL 规则和规则组评估。

有关创建 Firewall Manager AWS WAF 策略的过程，请参阅为创建 AWS Firewall Manager 策略 AWS WAF。

Firewall Manager 为您为 AWS WAF 策略定义的规则组启用采样和 Amazon CloudWatch 指标。

个人账户所有者可以完全控制他们添加到策略托管 Web ACL 中的任何规则或规则组的指标和采样配置。

为 AWS WAF 策略配置日志记录

您可以为 AWS WAF 策略启用集中日志记录，以获取有关组织内的 Web ACL 分析的流量的详细信息。日志中的信息包括从您的 AWS 资源 AWS WAF 收到请求的时间、有关该请求的详细信息以及每个请求与所有范围内账户匹配的规则的操作。您可以将日志发送到 Amazon Data Firehose 数据流或亚马逊简单存储服务 (S3) 存储桶。有关 AWS WAF 日志记录的信息，请参阅《AWS WAF 开发人员指南》记录 AWS WAF Web ACL 流量中的。

> **Note**
>
> AWS Firewall Manager 支持此选项 AWS WAFV2，但不适用于 AWS WAF 经典版。

主题

日志记录目标

本节介绍您可以选择发送 AWS WAF 策略日志的日志目的地。每个部分都提供了有关配置目标类型日志记录的指导，以及有关特定于目标类型的任何行为的信息。配置日志目标后，您可以向 Firewall Manager AWS WAF 策略提供其规格以开始登录该目标。

创建日志记录配置后，Firewall Manager 无法查看日志故障。您应负责验证日志传输是否按预期运行。

> **Note**
>
> Firewall Manager 不会修改您组织的成员账户中的任何现有日志记录配置。

主题

Amazon Data Firehose 数据流

本主题提供有关将您的网页 ACL 流量日志发送到 Amazon Data Firehose 数据流的信息。

当您启用 Amazon Data Firehose 日志记录时，Firewall Manager 会将您策略的网页 ACL 中的日志发送到您已配置存储目标的亚马逊数据 Firehose。启用日志记录后，通过 Kinesis Data Firehose 的 HTTPS 端点将每个已配置的 Web ACL 的日志 AWS WAF 传送到配置的存储目标。在使用之前，请测试您的传输流，确保其吞吐量足以容纳组织的日志。有关如何创建 Amazon Kinesis Data Firehose 并查看存储的日志的更多信息，请参阅什么是亚马逊数据 Firehose？

您必须拥有以下权限才能使用 Kinesis 成功启用日志记录：

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

当您在 AWS WAF 策略上配置 Amazon Data Firehose 日志记录目标时，防火墙管理器会在防火墙管理器管理员账户中为该策略创建一个 Web ACL，如下所示：

- Firewall Manager 会在 Firewall Manager 管理员账户中创建 Web ACL，无论该账户是否在策略的范围内。
- Web ACL 启用了日志记录，日志名称为 `FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*，时间戳为 Web ACL 启用日志的 UTC 时间（以毫秒为单位）。例如，`FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`。Web ACL 没有规则组，也没有关联的资源。
- 根据 AWS WAF 定价指南，您需要为 Web ACL 付费。有关更多信息，请参阅AWS WAF 定价。
- 当您删除策略时，Firewall Manager 会删除 Web ACL。

有关服务相关角色以及 `iam:CreateServiceLinkedRole` 权限的信息，请参阅将服务相关角色用于 AWS WAF。

有关创建传输流的更多信息，请参阅创建 Amazon Data Firehose 传送流。

Amazon Simple Storage Service 存储桶

本主题提供有关将 Web ACL 流量日志发送到 Amazon S3 存储桶的信息。

选择作为日志记录目标的存储桶必须由 Firewall Manager 管理员账户所有。有关创建用于日志记录的 Amazon S3 存储桶的要求和存储桶命名要求的信息，请参阅AWS WAF 开发人员指南中的 Amazon 简单存储服务。

最终一致性

当您对配置有 Amazon S3 日志目标的 AWS WAF 策略进行更改时，Firewall Manager 会更新存储桶策略以添加记录所需的权限。在这样做时，Firewall Manager 会遵循亚马逊简单存储服务所遵循的 last-writer-wins 语义和数据一致性模型。如果您在 Firewall Manager 控制台中或通过 PutPolicyAPI 同时对 Amazon S3 目标进行多个策略更新，则可能无法保存某些权限。有关 Amazon S3 数据一致性模型的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的 Amazon S3 数据一致性模型。

向 Amazon S3 存储桶发布日志的权限

在 AWS WAF 策略中为 Amazon S3 存储桶配置 Web ACL 流量日志需要以下权限设置。当您将 Amazon S3 配置为日志记录目标以授予服务向存储桶发布日志的权限时，Firewall Manager 会自动将这些权限附加到您的 Amazon S3 存储桶。如果您希望更精细地管理对日志和 Firewall Manager 资源的访问权限，您可以自己设置这些权限。有关管理权限的信息，请参阅IAM 用户指南中的 AWS 资源的访问权限管理。有关 AWS WAF 托管策略的信息，请参阅AWS 的托管策略 AWS WAF。

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

为防止跨服务混淆代理问题，您可以将 aws:SourceArn 和 aws:SourceAccount 全局条件上下文密钥添加到存储桶的策略中。要添加这些密钥，您可以修改 Firewall Manager 在配置日志记录目标时为您创建的策略，或者如果您想要精细控制，则可以创建自己的策略。如果您将这些条件添加到日志记录目标策略中，Firewall Manager 将无法验证或监控混淆代理保护。有关混淆代理问题的更多信息，请参阅 IAM 用户指南中的混淆代理问题。

当您添加 sourceAccount 添加 sourceArn 属性时，将增加存储桶策略的大小。如果要添加一长串 sourceAccount 添加 sourceArn 属性，请注意不要超过 Amazon S3 存储桶策略大小限额。

以下示例说明了如何通过在存储桶策略中使用 aws:SourceArn 和 aws:SourceAccount 全局条件上下文键来防止混淆代理问题。*member-account-id*替换为组织中成员的账户 ID。

```
{
   "Version":"2012-10-17",
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                    "member-account-id",
                  "member-account-id"
               ]
            },
```

```
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id-1:*",
                  "arn:aws:logs:*:member-account-id-2:*"
               ]
            }
         }
      }
   ]
}
```

Amazon S3 存储桶服务器端加密

您可以启用 Amazon S3 服务器端加密，也可以在 S3 存储桶上使用 AWS Key Management Service 客户托管密钥。如果您选择在 Amazon S3 存储桶上对 AWS WAF 日志使用默认 Amazon S3 加密，则无需采取任何特殊操作。但是，如果您选择使用客户提供的加密密钥对静态的 Amazon S3 数据进行加密，则必须在 AWS Key Management Service 密钥策略中添加以下权限声明：

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
}
```

有关在 Amazon S3 中使用客户提供的加密密钥的信息，请参阅 Amazon Simple Storage Service 用户指南中的使用客户提供的密钥进行服务器端加密 (SSE-C)。

启用日志记录

以下过程介绍如何在 Firewall Manager 控制台中为 AWS WAF 策略启用日志记录。

为 AWS WAF 策略启用日志记录

1. 在启用日志记录之前，必须按以下方式配置日志记录目标资源：

   - Amazon Kinesis Data Streams — 使用你的防火墙管理器管理员账户创建亚马逊数据 Firehose。使用以前缀 `aws-waf-logs-` 开头的名称。例如，`aws-waf-logs-firewall-manager-central`。使用 PUT 源，在您执行操作的区域中创建 Data Firehose。如果您要为 Amazon 捕获日志 CloudFront，请在美国东部（弗吉尼亚北部）创建消防水带。在使用之前，请测试您的传输流，确保其吞吐量足以容纳组织的日志。有关更多信息，请参阅创建 Amazon Data Firehose 传输流。
   - Amazon 简单存储服务存储桶 – 根据AWS WAF 开发人员指南中Amazon 简单存储服务主题中的指南创建 Amazon S3 存储桶。您还必须使用 向 Amazon S3 存储桶发布日志的权限 中列出的权限配置 Amazon S3 存储桶。

2. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

3. 在导航窗格中，选择安全策略。
4. 选择要为其启用日志记录的 AWS WAF 策略。有关 AWS WAF 日志记录的更多信息，请参阅 记录 AWS WAF Web ACL 流量。
5. 在策略详细信息选项卡的策略规则部分，选择编辑。
6. 对于日志记录配置，选择启用日志记录以打开日志记录。日志记录提供了有关 Web ACL 对流量进行分析的详细信息。选择日志记录目标，然后选择您配置的日志记录目标。必须选择名称以 `aws-waf-logs-` 开头的日志记录目标。有关配置 AWS WAF 日志目标的信息，请参阅为 AWS WAF 策略配置日志记录。
7. （可选）如果您不希望在日志中包含特定字段及其值，请编辑这些字段。选择要编辑的字段，然后选择 添加。根据需要重复操作来编辑其他字段。编辑后的字段在日志中显示为 REDACTED。例如，如果您编辑 URI 字段，则日志中的 URI 字段将为 REDACTED。
8. （可选）如果您不想向日志发送所有请求，请添加您的筛选条件和行为。在筛选日志下，对于要应用的每个筛选器，选择添加筛选条件，然后选择您的筛选条件并指定是要保留还是删除符合条件的

请求。添加完筛选条件后，如果需要，可以修改默认日志记录行为。有关更多信息，请参阅 AWS WAF 开发人员指南中的 Web ACL 日志记录配置。

9. 选择下一步。
10. 查看您的设置，然后选择保存以保存对策略的更改。

禁用日志记录

以下过程介绍如何在 Firewall Manager 控制台中禁用 AWS WAF 策略的日志记录。

禁用 AWS WAF 策略的日志记录

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择安全策略。
3. 选择要禁用日志记录的 AWS WAF 策略。
4. 在策略详细信息选项卡的策略规则部分，选择编辑。
5. 对于日志配置状态，请选择禁用。
6. 选择下一步。
7. 查看您的设置，然后选择保存以保存对策略的更改。

AWS Shield Advanced 政策

在 Firew AWS Shield all Manager 策略中，您可以选择要保护的资源。当您在启用自动修复的情况下应用策略时，对于每个尚未与 AWS WAF Web ACL 关联的范围内资源，Firewall Manager 都会关联一个空的 AWS WAF Web ACL。这个空的 Web ACL 将用于 Shield 监控目的。如果您随后将任何其他 Web ACL 关联到该资源，Firewall Manager 将删除这个空 Web ACL 关联。

> **Note**
>
> 当 AWS WAF 策略范围内的资源进入配置了自动应用层 DDoS 缓解的 Shield Advanced 策略的范围时，Firewall Manager 只有在关联该策略创建的 Web ACL 后才会应用 Shield Advanced 保护。 AWS WAF

如何在 Shield 策略中 AWS Firewall Manager 管理未关联的 Web ACL

您可以通过策略中的 “管理未关联的 Web ACL” 设置或 API 中SecurityServicePolicyData数据类型的设置来配置 Firewall Manager 是否为您管理未关联的 Web ACL。`optimizeUnassociatedWebACLs`如果在策略中启用了无关联 Web ACL 管理，则只有在 Web ACL 将被至少一个资源使用的情况下，Firewall Manager 才会在策略作用域内的账户中创建 Web ACL。当某个账户在任何时候进入策略范围时，如果至少有一个资源将使用 Web ACL，则 Firewall Manager 会自动在该账户中创建一个 Web ACL。

启用对未关联 Web ACL 的管理后，Firewall Manager 会对您账户中的未关联 Web ACL 执行一次性清理。清理过程可能需要数小时时间。如果资源在 Firewall Manager 创建 Web ACL 后离开策略范围，Firewall Manager 不会取消该资源与 Web ACL 的关联。如果希望 Firewall Manager 清理 Web ACL，则必须先手动取消资源与 Web ACL 的关联，然后在策略中启用管理未关联 Web ACL选项。

如果您不启用此选项，Firewall Manager 将不管理未关联 Web ACL，并且 Firewall Manager 会自动在策略范围内的每个账户中创建一个 Web ACL。

如何 AWS Firewall Manager 管理 Shield 策略中的范围变化

由于许多更改，例如策略范围设置的更改、资源标签的更改以及将帐户从组织中删除，账户和资源可能会超出 AWS Firewall Manager Shield Advanced 策略的范围。有关策略范围设置的一般信息，请参阅AWS Firewall Manager 政策范围。

使用 AWS Firewall Manager Shield Advanced 策略时，如果账户或资源超出范围，Firewall Manager 将停止监控该账户或资源。

如果账户因从组织中移除而超出范围，则该账户将继续订阅 Shield Advanced。由于账户不再是整合账单账户系列的一部分，因此该账户将产生按比例分配的 Shield Advanced 订阅费用。另一方面，超出范围但仍留在组织中的账户不会产生额外费用。

如果资源超出范围，它将继续受到 Shield Advanced 的保护，并继续chan's产生 Shield Advanced 数据传输费用。

自动应用程序层 DDoS 缓解

当您将 Shield Advanced 策略应用于 Amazon CloudFront 分配或应用程序负载均衡器时，您可以选择在策略中配置 Shield Advanced 自动应用程序层 DDoS 缓解措施。

有关 Shield Advanced 自动缓解的信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

Shield Advanced 应用程序层 DDoS 自动缓解具有以下要求：

- 自动应用层 DDoS 缓解仅适用于 Amazon CloudFront 分配和应用程序负载均衡器。

  如果将您的 Shield Advanced 政策应用于亚马逊 CloudFront 分配，则可以为为全球区域创建的 Shield Advanced 策略选择此选项。如果对应用程序负载均衡器应用保护，则可以将该策略应用于 Firewall Manager 支持的任何区域。
- 自动应用层 DDoS 缓解仅适用于使用最新版本 AWS WAF (v2) 创建的 Web ACL。

  因此，如果您的策略使用 AWS WAF 经典 Web ACL，则需要将该策略替换为自动使用最新版本的新策略，或者让 Firewall Manager 为您的现有策略创建新版本的 Web ACL，然后切换到使用它们。 AWS WAF有关选项的更多信息，请参阅将 AWS WAF 经典 Web ACL 替换为最新版本的 Web ACL。

自动缓解配置

Firewall Manager Shield Advanced 策略的应用程序层 DDoS 自动缓解选项将 Shield Advanced 自动缓解功能应用于您的策略范围内的账户和资源。有关 Shield Advanced 功能的详细信息，请参阅 Shield Advanced 应用程序层 DDoS 自动缓解。

您可以选择让 Firewall Manager 为策略范围内的 CloudFront分配或应用程序负载均衡器启用或禁用自动缓解，也可以选择让策略忽略 Shield 高级自动缓解设置：

- 启用 – 如果您选择启用自动缓解，则还需要设定缓解 Shield Advanced 规则应计算还是应阻止匹配的 Web 请求。如果范围内的资源未启用自动缓解功能，或者使用的规则操作与您为策略指定的规则操作不匹配，则 Firewall Manager 会将其标记为不合规。如果将策略配置为自动修正，则 Firewall Manager 会根据需要更新不合规资源。
- 禁用 – 如果您选择禁用自动缓解，则 Firewall Manager 会将范围内的资源标记为不合规，但前提是这些资源启用了自动缓解。如果将策略配置为自动修正，则 Firewall Manager 会根据需要更新不合规资源。
- 忽略 – 如果您选择忽略自动缓解，则 Firewall Manager 在为该策略执行修正活动时不会考虑该策略中的任何自动缓解设置。此设置允许您通过 Shield Advanced 控制自动缓解，无需让 Firewall

Manager 覆盖这些设置。此设置不适用于通过 Shield Advanced 管理的任何经典负载均衡器或弹性 IP 资源，因为 Shield Advanced 目前不支持这些资源的 L7 自动缓解。

将 AWS WAF 经典 Web ACL 替换为最新版本的 Web ACL

自动应用层 DDoS 缓解仅适用于使用最新版本 AWS WAF (v2) 创建的 Web ACL。

要确定您的 Shield Advanced 策略的 Web ACL 版本，请参阅 确定 Shield Advanced 策略使用的版本 AWS WAF。

如果您想在 Shield Advanced 策略中使用自动缓解，并且您的策略目前使用 AWS WAF 经典 Web ACL，则可以创建一个新的 Shield Advanced 策略来替换当前的 Shield Advanced 策略，也可以使用本节中描述的选项将早期版本的 Web ACL 替换为当前 Shield Advanced 策略中的新 (v2) Web ACL。新策略始终使用最新版本的创建 Web ACL。 AWS WAF如果您替换了整个策略，则在删除策略时，也可以让 Firewall Manager 删除所有早期版本的 Web ACL。本节的其余部分将介绍替换现有策略中的 Web ACL 的选项。

当您修改亚马逊 CloudFront 资源的现有 Shield Advanced 策略时，Firewall Manager 可以在任何还没有 v2 Web ACL 的范围内账户中自动为该策略创建一个新的空 AWS WAF (v2) Web ACL。当 Firewall Manager 创建新的 Web ACL 时，如果该策略在同一个账户中已经有经 AWS WAF 典 Web ACL，Firewall Manager 会使用与现有 Web ACL 相同的默认操作设置来配置新版本的 Web ACL。如果现有 AWS WAF 经典 Web ACL 不存在，Firewall Manager 会在新 Web ACL Allow 中将默认操作设置为。Firewall Manager 创建新的 Web ACL 后，您可以根据需要通过 AWS WAF 控制台对其进行自定义。

当您选择以下任何策略配置选项时，Firewall Manager 会为尚未拥有新 (v2) Web ACL 的范围内账户创建新的 (v2) Web ACL：

- 当您启用或禁用应用程序层 DDoS 自动缓解时。如果仅选择此选项，则 Firewall Manager 只会创建新的 Web ACL，而不会替换策略范围内资源上的任何现有 AWS WAF Classic Web ACL 关联。
- 当您选择自动修复的策略操作并选择将 AWS WAF 经典 Web ACL 替换为 AWS WAF (v2) Web ACL 的选项时。无论您选择哪种配置，您都可以选择替换早期版本的 Web ACL，以实现应用程序层 DDoS 自动缓解。

  选择替换选项时，Firewall Manager 会根据需要创建新版本的 Web ACL，然后为策略的范围内资源执行以下操作：

  - 如果某个资源与任何其他活动的 Firewall Manager 策略中的 Web ACL 关联，则 Firewall Manager 不会对其进行关联。

- 对于任何其他情况，Firewall Manager 都会删除与经 AWS WAF 典 Web ACL 的任何关联，并将该资源与策略的 AWS WAF (v2) Web ACL 相关联。

您可以根据需要选择让 Firewall Manager 以新版本的 Web ACL 替换早期版本的 Web ACL。如果您之前已自定义策略的 AWS WAF Classic Web ACL，则在选择让 Firewall Manager 执行替换步骤之前，可以将新版本的 Web ACL 更新为类似设置。

您可以通过相同版本的控制台或 CI AWS WAF assic 访问策略的任一版本的 Web ACL。 AWS WAF

在您删除策略本身之前，Firewall Manager 不会删除任何替换的 AWS WAF 经典 Web ACL。在该策略不再使用 AWS WAF 经典 Web ACL 之后，您可以根据需要将其删除。

确定 Shield Advanced 策略使用的版本 AWS WAF

您可以通过查看策略的 AWS WAF AWS Config 服务相关规则中的参数密钥来确定使用哪个版本的 Firewall Manager Shield 高级策略。如果使用的 AWS WAF 版本是最新版本，则参数键包括`policyId`和`webAclArn`。如果是早期版本 C AWS WAF lassic，则参数键包括`webAclId`和`resourceTypes`。

该 AWS Config 规则仅列出策略当前在范围内资源中使用的 Web ACL 的密钥。

确定 AWS WAF 您的 Firewall Manager Shield 高级策略使用哪个版本

1. 检索 Shield Advanced 策略的策略 ID：

   a. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   b. 在导航窗格中，选择安全策略。

   c. 为策略选择区域。对于 CloudFront 发行版，这是`Global`。

   d. 找到您想要的策略并复制其策略 ID 的值。

      示例策略 ID：`1111111-2222-3333-4444-a55aa5aaa555`。

2. 通过将策略 ID 附加到字符串`FMManagedShieldConfigRule`来创建策略的 AWS Config 规则名称。

   AWS Config 规则名称示例:`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. 在相关 AWS Config 规则的参数中搜索名为`policyId`和的密钥`webAclArn`：

   a. 打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

   b. 在导航窗格中，选择规则。

   c. 在列表中找到 Firew AWS Config all Manager 策略的规则名称并将其选中。规则页面随即打开。

   d. 在规则详细信息下的参数部分中，查看这些键。如果您找到名为 `policyId` 和 `webAclArn` 的键，则策略将采用使用最新版本的 AWS WAF创建的 Web ACL。如果您找到名为`webAclId`和的密钥`resourceTypes`，则策略将使用使用早期版本 Cl AWS WAF assic 创建的 Web ACL。

安全组策略

您可以使用 AWS Firewall Manager 安全组策略来管理您的组织的 Amazon Virtual Private Cloud 安全组 AWS Organizations。您可以将集中控制的安全组策略应用于整个组织或部分账户和资源。您还可以通过审核和使用安全组策略来监控和管理组织中正在使用的安全组策略。

Firewall Manager 会持续维护您的策略，并且当这些策略在整个组织中添加或更新时将它们应用于账户和资源。有关的信息 AWS Organizations，请参阅《AWS Organizations 用户指南》。

有关 Amazon 虚拟私有云安全组的信息，请参阅 Amazon VPC 用户指南中的 VPC 安全组。

您可以使用 Firewall Manager 安全组策略在整个 AWS 组织中执行以下操作：

- 将通用安全组应用到指定的账户和资源。
- 审核安全组规则，以查找和修复不合规的规则。
- 审核安全组的使用情况，以清理未使用和冗余的安全组。

本节介绍了 Firewall Manager 安全组策略的工作原理，并提供了使用这些策略的指南。有关创建安全组策略的过程，请参阅 创建 AWS Firewall Manager 策略。

通用安全组策略

Firewall Manager 通过通用安全组策略，提供集中控制的安全组与组织中的账户和资源的关联。您可以指定在企业中应用策略的位置和方式。

您可以将通用安全组策略应用于以下资源类型：

- Amazon Elastic Compute Cloud（Amazon EC2）实例
- 弹性网络接口
- 应用程序负载均衡器
- Classic 负载均衡器

有关使用控制台创建通用安全组策略的指导，请参阅 创建通用安全组策略。

共享 VPC

在通用安全组策略的策略范围设置中，可以选择包括共享 VPC。此选项包括由另一个账户拥有并与范围内账户共享的 VPC。始终包括范围内账户拥有的 VPC。有关共享 VPC 的信息，请参阅 Amazon VPC 用户指南中的使用共享 VPC。

在包括共享 VPC 时，注意以下警告。除此之外，安全组策略注意事项和限制 上还提供了有关安全组策略的一般注意事项。

- Firewall Manager 将主要安全组复制到每个范围内账户的 VPC 中。对于共享 VPC，Firewall Manager 会为与之共享 VPC 的每个范围内账户复制一次主要安全组。这可能会导致单个共享 VPC 中存在多个副本。
- 创建新的共享 VPC 后，只有当您在 VPC 中至少创建了一个属于策略范围内的资源之后，您才会在 Firewall Manager 安全组策略详细信息中看到该共享 VPC。
- 在启用共享 VPC 的策略中禁用了共享 VPC 后，在共享 VPC 中，Firewall Manager 将删除与任何资源不关联的副本安全组。Firewall Manager 会保留剩余的副本安全组，但会停止对其进行管理。删除这些其余的安全组时，需要在每个共享 VPC 实例中执行手动管理。

主要安全组

对于每项常用安全组策略，您都需要 AWS Firewall Manager 提供一个或多个主安全组：

- 主要安全组必须由 Firewall Manager 管理员账户创建，并且可以驻留在账户中的任何 Amazon VPC 实例中。
- 您可以通过 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理主要安全组。有关信息，请参阅 Amazon VPC 用户指南中的使用安全组。
- 您可以将一个或多个安全组指定作为 Firewall Manager 安全组策略的主安全组。默认情况下，一个策略中的安全组数量限制为一，但您可以提交请求来增加安全组的数量。有关信息，请参阅 AWS Firewall Manager 配额。

策略规则设置

您可以为通用安全组策略的安全组和资源选择以下一种或多种更改控制行为：

- 识别并报告本地用户对副本安全组所做的任何更改。
- 取消任何其他安全组与策略范围内的 AWS 资源的关联。
- 将标签从主要安全组分配到副本安全组。

> **Important**
>
> Firewall Manager 不会将 AWS 服务添加的系统标签分发到副本安全组中。系统标签以 `aws:` 为前缀。此外，如果现有安全组的标签与组织的标签策略存在冲突，Firewall Manager 将不会更新现有安全组的标签或创建新的安全组。有关标签策略的信息，请参阅《 AWS Organizations 用户指南》中的标签策略。

- 将安全组引用从主要安全组分发到副本安全组。

  这样您能够轻松地在所有范围内资源中为与指定安全组的 VPC 关联的实例建立通用的安全组引用规则。启用此选项后，只有当安全组引用 Amazon Virtual Private Cloud 中的对等安全组时，Firewall Manager 才会传播安全组引用。如果副本安全组未正确引用对等安全组，Firewall Manager 会将这些复制的安全组标记为不合规。有关如何在 Amazon VPC 中引用对等安全组的信息，请参阅 Amazon VPC 对等互连指南中的更新您的安全组以引用对等安全组。

  如果您不启用此选项，Firewall Manager 不会将安全组引用传播到副本安全组。有关亚马逊 VPC 中的 VPC 对等互连的信息，请参阅亚马逊 VPC 对等互连指南。

策略的制定和管理

当您创建通用安全组策略时，Firewall Manager 会将主要安全组复制到策略范围内的每个 Amazon VPC 实例，并将复制的安全组关联到策略范围内的账户和资源。修改主要安全组时，Firewall Manager 会将更改传播到副本。

当您删除通用安全组策略时，您可以选择是否清理该策略创建的资源。对于 Firewall Manager 常见安全组，这些资源是副本安全组。除非您想在删除策略后手动管理每个副本，否则请选择清理选项。在大多数情况下，选择清理选项是最简单的方法。

如何管理副本

Amazon VPC 实例中的副本安全组的管理方式与其他 Amazon VPC 安全组相同。有关信息，请参阅 Amazon VPC 用户指南 中的您的 VPC 的安全组。

内容审核安全组策略

使用 AWS Firewall Manager 内容审计安全组策略来审计您的组织安全组中正在使用的规则，并将其应用于这些规则。根据您在策略中定义的范围，内容审计安全组策略适用于您的 AWS 组织中使用的所有客户创建的安全组。

有关使用控制台创建内容审核安全组策略的指导，请参阅 创建内容审核安全组策略。

策略范围资源类型

您可以将内容审核安全组策略应用于以下资源类型：

- Amazon Elastic Compute Cloud（Amazon EC2）实例
- 弹性网络接口
- Amazon VPC 安全组

如果安全组明确位于范围内，或者与范围内的资源相关联，则将其视为策略范围。

策略规则选项

您可以为每个内容审核策略使用托管策略规则或自定义策略规则，但不能同时使用这两者。

- 托管策略规则 – 在包含托管规则的策略中，您可以使用应用程序和协议列表来控制 Firewall Manager 审核哪些规则，并将哪些规则标记为合规或不合规。您可以使用 Firewall Manager 管理的列表。您也可以创建和使用自己的应用程序和协议列表。有关这些类型的列表以及自定义列表管理选项的信息，请参阅 托管列表。
- 自定义策略规则 – 在包含自定义策略规则的策略中，您可以将现有安全组指定为策略的审核安全组。您可以将审核安全组规则用作模板，用于定义 Firewall Manager 审核的规则，并将其标记为合规或不合规。

审核安全组

必须先使用 Firewall Manager 管理员账户创建审核安全组，然后才能在策略中使用它们。您可以通过 Amazon Virtual Private Cloud (Amazon VPC) 或 Amazon Elastic Compute Cloud (Amazon EC2) 管理安全组。有关信息，请参阅 Amazon VPC 用户指南中的使用安全组。

您用于内容审核安全组策略的安全组仅被 Firewall Manager 用作策略范围内安全组的比较参考。Firewall Manager 不会将其与组织中的任何资源相关联。

您在审核安全组中定义规则的方式取决于您在策略规则设置中的选择：

- 托管策略规则 – 对于托管策略规则设置，您可以使用情况审核安全组覆盖策略中的其他设置，以明确允许或拒绝否则可能产生其他合规性结果的规则。
  - 如果您选择始终允许在审核安全组中定义的规则，则无论其他策略设置如何，任何与审核安全组中定义的规则相匹配的规则都被视为符合该策略。
  - 如果您选择始终拒绝在审核安全组中定义的规则，则无论其他策略设置如何，任何与审核安全组中定义的规则相匹配的规则都将被视为不符合该策略。
- 自定义策略规则 – 对于自定义策略规则设置，审核安全组提供了范围内的安全组规则中可接受或不可接受的示例：
  - 如果您选择允许使用这些规则，则所有范围内安全组必须只拥有在策略的审核安全组规则允许范围内的规则。在这种情况下，策略的安全组规则提供了可以接受的操作示例。
  - 如果您选择拒绝使用这些规则，则所有范围内安全组必须只拥有在策略的审核安全组规则允许范围外的规则。在这种情况下，策略的安全组规则提供了不可接受的操作示例。

策略的制定和管理

创建审核安全组策略时，必须禁用自动修正。建议的做法是在启用自动修正之前先检查策略创建的影响。查看预期效果后，您可以编辑策略并启用自动修正。启用自动修正后，Firewall Manager 会更新或删除范围内安全组中不合规的规则。

受审核安全组策略影响的安全组

您的组织中由客户创建的所有安全组都有资格加入审核安全组策略的范围。

副本安全组不是客户创建的，因此没有资格直接纳入审核安全组策略的范围。但是，由于策略的自动修正活动，它们可能会进行更新。通用安全组策略的主要安全组由客户创建，可以属于审核安全组策略的范围。如果审核安全组策略对主要安全组进行了更改，则 Firewall Manager 会自动将这些更改传播到副本。

使用情况审核安全组策略

使用 AWS Firewall Manager 使用情况审计安全组策略来监控您的组织中是否存在未使用和冗余的安全组，并可以选择执行清理。如果为此策略启用了自动修正，Firewall Manager 会执行以下操作：

1. 合并冗余安全组（如果选择了该选项）。
2. 删除未使用的安全组（如果选择了该选项）。

您可以将使用情况审核安全组策略应用于以下资源类型：

- Amazon VPC 安全组

有关使用控制台创建使用情况审核安全组策略的指导，请参阅 创建使用情况审核安全组策略。

Firewall Manager 如何检测和修复冗余安全组

要将安全组视为冗余，它们必须设置完全相同的规则，并且位于同一 Amazon VPC 实例中。

要修复冗余安全组集，Firewall Manager 会选择保留该安全组集中的一个安全组，然后将其关联到与该安全组集中的其他安全组关联的所有资源。然后，Firewall Manager 将其他安全组与它们所关联的资源断开关联，使它们处于未使用状态。

> **Note**
>
> 如果您还选择删除未使用的安全组，Firewall Manager 将执行接下来的操作。这可能导致删除冗余组中的安全组。

Firewall Manager 如何检测和修复未使用的安全组

如果满足以下两个条件，Firewall Manager 会将安全组视为未使用：

- 任何亚马逊 EC2 实例或 Amazon EC2 弹性网络接口均未使用该安全组。
- 在策略规则时间段中指定的分钟数内，Firewall Manager 尚未收到其配置项目。

策略规则时间段的默认设置为零分钟，但您可以将时间延长到 365 天（525,600 分钟），以便有时间将新的安全组与资源关联起来。

> **Important**
>
> 如果您指定的分钟数不是默认值 0，则必须在中启用间接关系 AWS Config。否则，您的使用情况审核安全组策略将无法按预期运行。有关间接关系的信息 AWS Config，请参阅《AWS Config 开发者指南》 AWS Config中的间接关系。

如果可能，Firewall Manager 会根据您的规则设置将其从您的帐户中删除，从而修复未使用的安全组。如果 Firewall Manager 无法删除安全组，则会将其标记为不符合策略。Firewall Manager 无法删除其他安全组引用的安全组。

根据您使用的是默认时间段设置还是自定义设置，修复的时间会有所不同：

- 时间段设置为零，默认 — 使用此设置，一旦 Amazon EC2 实例或 elastic network interface 未使用安全组，该安全组即被视为未使用。

  对于此零时间段设置，Firewall Manager 会立即修复安全组。
- 时间段大于零 — 使用此设置，当 Amazon EC2 实例或弹性网络接口未使用安全组且 Firewall Manager 在指定的分钟数内未收到该安全组的配置项目时，该安全组被视为未使用。

  对于非零时间段设置，Firewall Manager 会在安全组保持未使用状态 24 小时后对其进行修复。

默认账户规范

通过控制台创建使用情况审核安全组策略时，Firewall Manager 会自动选择排除指定账户并包括所有其他账户。然后，该服务会将 Firewall Manager 管理员账户放入要排除的列表中。这是推荐的方法，它允许您手动管理属于 Firewall Manager 管理员账户的安全组。

安全组策略的最佳实践

此部分列出了针对使用 AWS Firewall Manager管理安全组的建议。

排除 Firewall Manager 管理员账户

在您设置策略范围时，请排除 Firewall Manager 管理员账户。当您通过控制台创建使用情况审核安全组策略时，这是默认选项。

首先禁用自动修正

对于内容或使用情况审核安全组策略，请先禁用自动修正。查看策略详细信息以确定自动修正可能产生哪些影响。在您确定进行了所需的更改时，请编辑策略以启用自动修正。

如果您还使用外部来源来管理安全组，请避免冲突

如果您使用 Firewall Manager 以外的工具或服务来管理安全组，请注意避免 Firewall Manager 中的设置与外部来源中的设置发生冲突。如果您使用自动修正，并且您的设置存在冲突，则可能会造成一个冲突修正循环，从而消耗双方的资源。

例如，假设您配置了另一个服务来维护一组 AWS 资源的安全组，然后配置了一个 Firewall Manager 策略来为部分或全部相同的资源维护不同的安全组。如果您将任何一方配置为不允许任何其他安全组与范围内的资源相关联，则该方将删除由另一方维护的安全组关联。如果双方都以这种方式配置，则最终可能会出现一个相互冲突的取消关联和关联的循环。

此外，假设您创建了 Firewall Manager 审核策略来强制执行与来自其他服务的安全组配置相冲突的安全组配置。Firewall Manager 审核策略应用的修正措施可以更新或删除该安全组，从而使其不符合其他服务的要求。如果将其他服务配置为监控并自动修复发现的任何问题，它将重新创建或更新安全组，使其再次不符合 Firewall Manager 审核策略。如果 Firewall Manager 审核策略配置了自动修正，它将再次更新或删除外部安全组，依此类推。

为避免此类冲突，请在 Firewall Manager 和任何外部来源之间创建互斥的配置。

您可以使用标记将外部安全组排除在 Firewall Manager 策略的自动修正范围之外。为此，请向由外部来源管理的安全组或其他资源添加一个或多个标签。然后，当您在资源规范中定义 Firewall Manager 策略范围时，将带有您添加的一个或多个标签的资源排除在外。

同样，在您的外部工具或服务中，将 Firewall Manager 管理的安全组排除在任何管理或审核活动之外。要么不要导入 Firewall Manager 资源，要么使用 Firewall Manager 特定的标记将其排除在外部管理之外。

使用情况审计安全组策略的最佳实践

使用使用情况审计安全组策略时，请遵循以下准则。

- 避免在短时间内（例如在 15 分钟内）对安全组的关联状态进行多次更改。这样做可能会导致 Firewall Manager 错过部分或全部相应的事件。例如，不要快速将安全组与 elastic network interface 关联和取消关联。

安全组策略注意事项和限制

本节列出了使用 Firewall Manager 安全组策略的注意事项和限制：

- 对于适用于使用 Fargate 服务类型创建的 Amazon EC2 弹性网络接口的安全组，不支持更新。但是，您可以使用 Amazon EC2 服务类型更新 Amazon ECS 弹性网络接口的安全组。
- Firewall Manager 不支持由 Amazon Relational Database Service 创建的 Amazon EC2 弹性网络接口的安全组。
- Amazon ECS 弹性网络接口仅适用于使用滚动更新 (Amazon ECS) 部署控制器的 Amazon ECS 服务。对于其他 Amazon ECS 部署控制器，例如 CODE_DEPLOY 或外部控制器，Firewall Manager 目前无法更新弹性网络接口。
- 使用适用于 Amazon EC2 弹性网络接口的安全组，Firewall Manager 不会立即看到对安全组所做的更改。Firewall Manager 通常会在几个小时内检测到更改，但检测可能会延迟长达六个小时。
- Firewall Manager 不支持针对网络负载均衡器更新弹性网络接口中的安全组。

- 在常见的安全组策略中，如果共享的 VPC 后来被取消与账户共享，Firewall Manager 将不会删除该账户中的副本安全组。
- 对于使用情况审计安全组策略，如果您创建了多个具有自定义延迟时间设置的策略，并且所有策略的范围都相同，则第一个包含合规性发现的策略将是报告发现结果的策略。

安全组策略使用案例

您可以使用 AWS Firewall Manager 常用安全组策略自动配置主机防火墙，以便在 Amazon VPC 实例之间进行通信。本节列出了标准的 Amazon VPC 架构，并介绍了如何使用 Firewall Manager 的常见安全组策略来保护每种架构。这些安全组策略可以帮助您应用一组统一的规则来选择不同账户中的资源，避免在 Amazon Elastic Compute Cloud 和 Amazon VPC 中按账户进行配置。

使用 Firewall Manager 通用安全组策略，您可以仅标记与其他 Amazon VPC 中的实例通信所需的 EC2 弹性网络接口。这样，同一 Amazon VPC 中的其他实例就会更加安全，且隔离性更强。

用例：监视和控制对应用程序负载均衡器和经典负载均衡器的请求

您可以使用 Firewall Manager 通用安全组策略来定义范围内的负载均衡器应处理哪些请求。您可以通过 Firewall Manager 控制台进行配置。只有符合安全组入站规则的请求才能到达您的负载均衡器，而负载均衡器只会分发符合出站规则的请求。

用例：可访问互联网的公用 Amazon VPC

您可以使用 Firewall Manager 通用安全组策略来保护公有 Amazon VPC，例如，仅允许入站端口 443。这就如同针对公有 VPC 仅允许入站 HTTPS 流量。您可以标记 VPC 内的公共资源（例如，作为“PublicVPC”），然后将 Firewall Manager 策略范围设置为仅限具有该标签的资源。Firewall Manager 会自动将策略应用于这些资源。

用例：公有和私有 Amazon VPC 实例

对于可访问互联网的公有 Amazon VPC 实例，您可以对公共资源使用相同的通用安全组策略，正如之前用例中的建议。您可以使用第二项通用安全组策略来限制公共资源和私有资源之间的通信。使用类似 “PublicPrivate” 的内容标记公有和私有 Amazon VPC 实例中的资源，以对其应用第二项策略。您可以使用第三项策略来定义允许私有资源与其他公司或私有 Amazon VPC 实例之间进行的通信。对于此策略，您可以在私有资源上使用另一个标识标签。

用例：中心和分支 Amazon VPC 实例

您可以使用通用安全组策略来定义中心 Amazon VPC 实例和分支 Amazon VPC 实例之间的通信。您可以使用第二项策略来定义从每个分支 Amazon VPC 实例到中心 Amazon VPC 实例的通信。

用例：Amazon EC2 实例的默认网络接口

您可以将通用安全组策略用于仅允许标准通信，例如内部 SSH 和补丁/操作系统更新服务，并禁止其他不安全的通信。

用例：识别具有开放权限的资源

您可以使用情况审核安全组策略来识别组织内有权与公有 IP 地址通信或拥有属于第三方供应商的 IP 地址的所有资源。

亚马逊 VPC 网络访问控制列表 (ACL) 策略

本节介绍 AWS Firewall Manager 网络 ACL 策略的工作原理，并提供使用这些策略的指导。有关使用控制台创建网络 ACL 策略的指南，请参阅创建网络 ACL 策略。

有关 Amazon VPC 网络访问控制列表 (ACL) 的信息，请参阅 Amazon VPC 用户指南中的使用网络 ACL 控制子网的流量。

您可以使用 Firewall Manager 网络 ACL 策略来管理您的组织的亚马逊虚拟私有云 (Amazon VPC) 网络访问控制列表 (ACL)。 AWS Organizations您可以定义策略的网络 ACL 规则设置以及要在其中强制执行这些设置的帐户和子网。在整个组织中添加或更新账户和子网时，Firewall Manager 会持续将您的策略设置应用于账户和子网。有关策略范围和的信息 AWS Organizations，请参阅AWS Firewall Manager 政策范围和《AWS Organizations 用户指南》。

在定义 Firewall Manager 网络 ACL 策略时，除了标准的防火墙管理器策略设置（例如名称和范围）外，还需要提供以下内容：

- 入站和出站流量处理的第一条和最后一条规则。Firewall Manager 在策略范围内的网络 ACL 中强制其存在和排序，或者报告不合规。您的个人账户可以创建自定义规则，在政策的第一条和最后一条规则之间运行。
- 当修复会导致网络 ACL 中的规则之间的流量管理冲突时，是否强制修复。这仅在为策略启用修复时适用。

Firewall Manager 网络 ACL 规则和标记

本节介绍网络 ACL 策略规则规范和由 Firewall Manager 管理的网络 ACL。

在托管网络 ACL 上进行标记

Firewall Manager 使用值为的`FMManaged`标记来标记托管网络 ACL `true`。Firewall Manager 仅对设置了此标记的网络 ACL 执行修复。

您在策略中定义的规则

在您的网络 ACL 策略规范中，您可以为入站流量定义要首先和最后运行的规则，以及要为出站流量首先和最后运行的规则。

默认情况下，您最多可以定义 5 个入站规则，用于策略中第一个和最后一个规则的任意组合。同样，您最多可以定义 5 个出站规则。有关这些限制的更多信息，请参阅软限额。有关网络 ACL 的一般限制的信息，请参阅《亚马逊 VPC 用户指南》中的 Amazon VPC 网络 ACL 配额。

您不为策略规则分配规则编号。相反，您可以按照评估规则的顺序指定规则，然后 Firewall Manager 使用该顺序在其管理的网络 ACL 中分配规则编号。

除此之外，您还可以管理策略的网络 ACL 规则规范，就像通过 Amazon VPC 管理网络 ACL 中的规则一样。有关 Amazon VPC 中网络 ACL 管理的信息，请参阅 Amazon VP C 用户指南中的使用网络 ACL 控制子网流量和使用网络 ACL。

托管网络 ACL 中的规则

Firewall Manager 在其管理的网络 ACL 中配置规则，方法是将策略的第一条和最后一条规则放在个人账户管理员定义的任何自定义规则之前和之后。Firewall Manager 会保留自定义规则的顺序。从编号最低的规则开始评估网络 ACL。

Firewall Manager 首次创建网络 ACL 时，它会使用以下编号定义规则：

- 第一条规则：1、2、... — 由您在 Firewall Manager 网络 ACL 策略中定义。

  Firewall Manager 分配从 1 开始的规则编号，增量为 1，规则的顺序与您在策略规范中的顺序相同。
- 自定义规则：5,000、5,100、... — 由个人账户管理员通过 Amazon VPC 进行管理。

  Firewall Manager 为这些规则分配的数字从 5,000 开始，后续每条规则以 100 为递增。
- 最后的规则：... 32,765、32,766 — 由您在 Firewall Manager 网络 ACL 策略中定义。

  Firewall Manager 会分配以尽可能高的数字（32766）结尾的规则编号，增量为 1，规则的顺序与您在策略规范中的顺序相同。

网络 ACL 初始化后，Firewall Manager 无法控制各个帐户在其托管网络 ACL 中所做的更改。个人账户可以在不影响其合规性的情况下更改网络 ACL，前提是任何自定义规则在策略的第一条和最后一条规则之间保持编号，并且第一条和最后一条规则保持其指定的顺序。作为最佳实践，在管理自定义规则时，请遵守本节中描述的编号。

Firewall Manager 如何启动子网的网络 ACL 管理

当 Firewall Manager 将子网与 Firewall Manager 创建并标记为的网络 ACL 关联时，它将开始管理该子网的FMManaged网络 ACL `true`。

遵守网络 ACL 策略要求子网的网络 ACL 将策略的第一条规则放在第一位，按策略中指定的顺序排在最后，将最后一条规则按顺序排在最后，所有其他自定义规则位于中间。这些要求可以通过子网已关联的非托管网络 ACL 或托管网络 ACL 来满足。

当 Firewall Manager 将网络 ACL 策略应用于与非托管网络 ACL 关联的子网时，Firewall Manager 会按顺序检查以下内容，并在确定可行的选项时停止：

1. 关联的网络 ACL 已经合规 — 如果当前与子网关联的网络 ACL 合规，则 Firewall Manager 会保留该关联，并且不会启动该子网的网络 ACL 管理。

   Firewall Manager 不会更改或以其他方式管理它不拥有的网络 ACL，但只要它合规，Firewall Manager 就会将其保留在原处，只监控其策略合规性。
2. 兼容的托管网络 ACL 可用 — 如果 Firewall Manager 已经在管理符合所需配置的网络 ACL，则可以选择此选项。如果启用了修复，Firewall Manager 会将子网与其关联起来。如果禁用修复，Firewall Manager 会将子网标记为不合规，并提供替换网络 ACL 关联作为补救选项。
3. 创建新的合规托管网络 ACL-如果启用了修复，Firewall Manager 将创建一个新的网络 ACL 并将其与子网关联。否则，Firewall Manager 会将子网标记为不合规，并提供修复选项，包括创建新的网络 ACL 和替换网络 ACL 关联。

如果这些步骤失败，Firewall Manager 会报告子网的不合规。

当子网首次进入作用域以及子网的非托管网络 ACL 不合规时，Firewall Manager 会遵循以下步骤。

Firewall Manager 如何修复不合规的托管网络 ACL

本节介绍当其托管网络 ACL 不符合策略时，Firewall Manager 如何对其进行修复。Firewall Manager 仅修复托管网络 ACL（标签设置为）。FMManaged `true`有关不由 Firewall Manager 管理的网络 ACL，请参阅初始网络 ACL 管理。

修复可恢复第一条、自定义规则和最后一条规则的相对位置，并恢复第一条和最后一条规则的顺序。在修复期间，Firewall Manager 不一定会将规则移动到它在网络 ACL 初始化中使用的规则编号。有关这些规则类别的初始数字设置和说明，请参见初始网络 ACL 管理。

为了建立合规的规则和规则顺序，Firewall Manager 可能需要在网络 ACL 内移动规则。Firewall Manager 尽可能通过维护现有合规规则顺序来保留网络 ACL 的保护。例如，它可能会暂时将规则复制到新位置，然后对原始规则执行有序移除，在此过程中保留相对位置。

这种方法可以保护您的设置，但也需要在网络 ACL 中留出空间来存放临时规则。如果 Firewall Manager 达到网络 ACL 中规则的限制，它将停止修复。发生这种情况时，网络 ACL 仍然不合规，Firewall Manager 会报告原因。

如果某个帐户向由 Firewall Manager 管理的网络 ACL 添加了自定义规则，并且这些规则干扰了防火墙管理器的修复，Firewall Manager 会停止网络 ACL 上的任何修复活动并报告冲突。

强制补救

如果为策略选择 auto 修复，则还需要指定是对第一条规则还是最后一条规则强制修正。

当 Firewall Manager 在自定义规则和策略规则之间的流量处理中遇到冲突时，它会引用相应的强制修复设置。如果启用了强制修复，则无论存在冲突，Firewall Manager 都会应用补救措施。如果未启用此选项，Firewall Manager 将停止修复。无论哪种情况，Firewall Manager 都会报告规则冲突并提供补救选项。

规则计数要求和限制

在修复期间，Firewall Manager 可能会临时复制规则，以便在不更改规则提供的保护的情况下移动规则。

对于入站或出站规则，Firewall Manager 执行补救可能需要的最大规则数量如下：

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

网络 ACL 和网络 ACL 策略受可变规则限制的约束。如果 Firewall Manager 的修复工作达到极限，它将停止尝试修复并报告违规行为。

要为 Firewall Manager 腾出空间来执行其修复活动，您可以请求提高限制。或者，您可以更改策略或网络 ACL 中的配置以减少使用的规则数量。

有关网络 ACL 限制的信息，请参阅 Amazon VPC 用户指南中的网络 ACL 上的 Amazon VPC 配额。

补救失败时

更新网络 ACL 时，如果 Firewall Manager 出于任何原因需要停止，它不会回滚更改，而是使网络 ACL 处于临时状态。如果您在FMManaged标记设置为的网络 ACL 中看到重复的规则，则 Firewall Manager

可能正在对其进行修复。`true`更改可能会在一段时间内部分完成，但由于 Firewall Manager 采用的补救方法，这不会中断流量或降低对关联子网的保护。

当 Firewall Manager 不能完全修复不合规的网络 ACL 时，它会报告关联子网的不合规情况，并建议可能的补救选项。

修复失败后重试

在大多数情况下，如果 Firewall Manager 未能完成对网络 ACL 的补救更改，它最终会重试更改。

当补救达到网络 ACL 规则计数限制或 VPC 网络 ACL 计数限制时，情况除外。Firewall Manager 无法执行占用超过其限制设置的 AWS 资源的补救活动。在这些情况下，您需要减少计数或增加限制才能继续。有关限制的信息，请参阅《亚马逊 VPC 用户指南》中的 Amazon VPC 网络 ACL 配额。

Firewall Manager 网络 ACL 合规性报告

Firewall Manager 监控并报告连接到范围内子网的所有网络 ACL 的合规性。

一般而言，不合规发生在诸如规则顺序不正确或策略规则与自定义规则之间的流量处理行为冲突之类的情况。不合规报告包括违规行为和补救选项。

Firewall Manager 报告网络 ACL 策略的合规性违规情况的方式与其他策略类型相同。有关合规性报告的信息，请参阅查看 AWS Firewall Manager 策略的合规性信息。

政策更新期间不合规

修改网络 ACL 策略后，在 Firewall Manager 更新该策略范围内的网络 ACL 之前，Firewall Manager 会将这些网络 ACL 标记为不合规。严格来说，即使网络 ACL 可能合规，Firewall Manager 也会这样做。

例如，如果您从策略规范中删除规则，而范围内的网络 ACL 仍有额外的规则，则其规则定义可能仍符合该策略。但是，由于额外规则是防火墙管理器管理的规则的一部分，因此防火墙管理器将其视为违反当前策略设置的行为。这与 Firewall Manager 查看添加到防火墙管理器托管网络 ACL 的自定义规则的方式不同。

使用 Firewall Manager 网络 ACL 策略的最佳实践

本节列出了有关使用 Firewall Manager 网络 ACL 策略和托管网络 ACL 的建议。

参考**FMManaged**标签以识别由 Firewall Manager 管理的网络 ACL

Firewall Manager 管理的网络 ACL 的`FMManaged`标签设置为。`true`使用此标签可以帮助区分您自己的自定义网络 ACL 和通过 Firewall Manager 管理的网络 ACL。

不要修改网络 ACL 上**FMManaged**标签的值

Firewall Manager 使用此标签通过网络 ACL 设置和确定其管理状态。

不要修改具有 Firewall Manager 托管的网络 ACL 的子网的关联

请勿手动更改子网与 Firewall Manager 管理的任何网络 ACL 之间的关联。这样做可能会禁用 Firewall Manager 管理这些子网的保护功能。您可以通过查找的FMManaged标签设置来识别由 Firewall Manager 管理的网络 ACL。`true`

要从 Firewall Manager 策略管理中移除子网，请使用 Firewall Manager 策略范围设置来排除该子网。例如，您可以标记子网，然后将该标签排除在策略范围之外。有关更多信息，请参阅 AWS Firewall Manager 政策范围。

更新托管网络 ACL 时，请勿修改由 Firewall Manager 管理的规则

在由 Firewall Manager 管理的网络 ACL 中，遵循中描述的编号方案，将您的自定义规则与策略规则分开。Firewall Manager 网络 ACL 规则和标记仅添加或修改数字介于 5,000 到 32,000 之间的规则。

避免为账户限额添加太多规则

在修复网络 ACL 期间，Firewall Manager 通常会临时增加网络 ACL 规则数量。为避免出现不合规问题，请确保有足够的空间容纳正在使用的规则。有关更多信息，请参阅 Firewall Manager 如何修复不合规的托管网络 ACL。

首先禁用自动修正

从禁用自动修复开始，然后查看策略详细信息以确定自动修复会产生的影响。在您确定进行了所需的更改时，请编辑策略以启用自动修正。

Firewall Manager 网络 ACL 策略注意事项

本节列出了使用 Firewall Manager 网络 ACL 策略的注意事项和限制。

- 更新时间比其他策略慢 — 由于 Amazon EC2 网络 ACL API 处理请求的速度有限，Firewall Manager 应用网络 ACL 策略和策略更改的速度通常比其他防火墙管理器策略要慢。您可能会注意到，与其他 Firewall Manager 策略的类似更改相比，策略更改所需的时间更长，尤其是在您首次添加策略时。
- 对于初始子网保护，Firewall Manager 首选较旧的策略 — 这仅适用于尚未受到 Firewall Manager 网络 ACL 策略保护的子网。如果一个子网同时属于多个网络 ACL 策略的范围，则 Firewall Manager 会使用最旧的策略来保护该子网。

- 策略停止保护子网的原因 — 管理子网网络 ACL 的策略会保留管理，直到出现以下情况之一：
  - 子网超出了策略的范围。
  - 该策略已删除。
  - 您可以手动更改子网与由其他 Firewall Manager 策略管理且子网在其范围内的网络 ACL 的关联。

删除 Firewall Manager 网络 ACL 策略

当您删除 Firewall Manager 网络 ACL 策略时，Firewall Manager 会将其为该策略管理的所有网络 ACL `false` 上的`FMManaged`标签值更改为。

此外，您可以选择是否清理策略创建的资源。如果您选择清理，Firewall Manager 将按顺序尝试以下步骤：

1. 将关联恢复到原始状态 — F irewall Manager 会尝试将子网关联回在 Firewall Manager 开始管理之前与之关联的网络 ACL。
2. 从网络 ACL 中移除第一条和最后一条规则-如果它无法更改关联，Firewall Manager 会尝试删除策略的第一条和最后一条规则，只保留与子网关联的网络 ACL 中的自定义规则。
3. 不@@ 对规则或关联执行任何操作 — 如果它无法执行上述任一操作，Firewall Manager 将保持网络 ACL 及其关联不变。

如果您不选择清理选项，则需要在删除策略后手动管理每个网络 ACL。在大多数情况下，选择清理选项是最简单的方法。

AWS Network Firewall 政策

您可以使用 AWS Firewall Manager Network AWS Network Firewall Firewall 策略来管理组织中的亚马逊虚拟私有云 VPC 的防火墙。 AWS Organizations您可以将集中控制的防火墙应用于整个组织或部分账户和 VPC。

Network Firewall 为您的 VPC 中的公共子网提供网络流量过滤保护。Firewall Manager 根据您的策略所定义的防火墙管理类型创建和管理您的防火墙。Firewall Manager 提供以下防火墙管理模型：

- 分布式 – 对于策略范围内的每个账户和 VPC，Firewall Manager 都会创建网络防火墙防火墙，并将防火墙端点部署到 VPC 子网以过滤网络流量。
- 集中式 – Firewall Manager 在单个 Amazon VPC 中创建单个 Network Firewall 防火墙。
- 导入现有防火墙 – Firewall Manager 在单个 Firewall Manager 策略中导入现有防火墙进行管理。您可以对策略管理的导入防火墙应用其他规则，以确保您的防火墙符合您的安全标准。

> **Note**
>
> Firewall Manager 网络防火墙策略是 Firewall Manager 策略，用于管理组织中 VPC 的网络防火墙保护。
> Network Firewall 保护在 Network Firewall 服务的资源中指定，这些资源被称为防火墙策略。

有关使用 Network Firewall 的信息，请参阅 AWS Network Firewall 开发人员指南。

以下各节介绍使用 Firewall Manager Network Firewall 策略的要求，并描述了这些策略的工作原理。有关创建策略的过程，请参阅 为创建 AWS Firewall Manager 策略 AWS Network Firewall。

您必须启用资源共享

Network Firewall 策略在组织中的账户之间共享 Network Firewall 规则组。要启用此功能，必须为 AWS Organizations启用资源共享。有关如何启用资源共享的信息，请参阅 Network Firewall 和 DNS 防火墙策略的资源共享。

您必须定义您的 Network Firewall 规则组

当您指定新的 Network Firewall 策略时，您可以像 AWS Network Firewall 直接使用时一样定义防火墙策略。您可以指定要添加的无状态规则组、默认的无状态操作和有状态规则组。您的规则组必须已存在于 Firewall Manager 管理员账户中，才能将其包含在策略中。有关创建 Network Firewall 规则组的信息，请参阅 AWS Network Firewall 规则组。

Firewall Manager 如何创建防火墙端点

策略中的防火墙管理类型决定了 Firewall Manager 如何创建防火墙。您的策略可以创建分布式防火墙、集中式防火墙，也可以导入现有防火墙：

- 分布式 – 在分布式部署模型下，Firewall Manager 会为策略范围内的每个 VPC 创建端点。您可以通过指定要在哪些可用区域中创建防火墙端点来自定义端点位置，也可以通过 Firewall Manager 在具有公用子网的可用区中自动创建端点。如果您手动选择可用区，则可以选择限制每个可用区允许的 CIDR 集。如果您决定让 Firewall Manager 自动创建端点，则还必须指定该服务是在您的 VPC 中创建单个端点还是多个防火墙端点。
  - 对于多个防火墙端点，Firewall Manager 会在每个可用区部署一个防火墙端点，在该可用区中，您的子网中或带有一个互联网网关，或在路由表中有一个由 Firewall Manager 创建的防火墙端点路由。这是 Network Firewall 策略的默认选项。
  - 对于单个防火墙端点，Firewall Manager 在任何具有互联网网关路由的子网中的单个可用区中部署防火墙端点。使用此选项，其他区域的流量需要跨越区域边界才能被防火墙过滤。

> **Note**
>
> 对于这两个选项，都必须有一个子网与其中包含 IPv4/PrefixList 路由的路由表相关联。Firewall Manager 不检查任何其他资源。

- 集中式 – 使用集中部署模型，Firewall Manager 可在检查 VPC 内创建一个或多个防火墙端点。检查 VPC 是一个中央 VPC，Firewall Manager 可以在其中启动您的端点。当您使用集中式部署模型时，您还需要指定要在哪些可用区中创建防火墙端点。创建策略后不能更改检查 VPC。要使用其他检查 VPC，您必须创建新的策略。
- 导入现有防火墙 – 导入现有防火墙时，您可以通过向策略中添加一个或多个资源集来选择要在策略中管理的防火墙。资源集是指由组织中的账户管理的资源集合，在本例中这些资源就是 Network Firewall 中的现有防火墙。在策略中使用资源集之前，必须首先创建一个资源集。有关 Firewall Manager 资源集的信息，请参阅 在 Firewall Manager 中使用资源集。

  使用导入的防火墙时请注意以下事项：

  - 如果导入的防火墙不合规，Firewall Manager 将尝试自动解决违规问题，但以下情况除外：
    - Firewall Manager 和 Network Firewall 策略的有状态或无状态默认操作不匹配。
    - 导入的防火墙的防火墙策略中的规则组与 Firewall Manager 策略中的规则组具有相同的优先级。
    - 导入的防火墙使用的防火墙策略与该策略资源集以外的防火墙关联。之所以会发生这种情况，是因为一个防火墙只能具有一个防火墙策略，但是一个防火墙策略可以与多个防火墙相关联。
    - 属于已导入的防火墙的防火墙策略（也在防火墙管理器策略中指定）的已有规则组被赋予不同的优先级。
  - 如果在策略中启用资源清理，Firewall Manager 将从资源集范围内的防火墙中删除 FMS 导入策略中的规则组。
  - 由防火墙管理器导入现有防火墙管理类型所管理的防火墙，一次只能由一个策略管理。如果将相同的资源集添加到多个导入网络防火墙策略中，则该资源集中的防火墙将由资源集所加入的第一个策略管理，而第二个策略将忽略该资源集中的防火墙。
  - Firewall Manager 当前不支持异常策略配置的流式传输。有关直播异常策略的信息，请参阅 AWS Network Firewall 开发人员指南中的直播异常策略。

如果您使用分布式或集中式防火墙管理更改策略的可用区域列表，Firewall Manager 将尝试清理过去创建但当前不在策略范围内的任何端点。只有在没有引用超出范围端点的路由表路由时，Firewall

Manager 才会删除该端点。如果 Firewall Manager 发现无法删除这些端点，它会将防火墙子网标记为不合规，并将继续尝试删除该端点，直到可以安全删除为止。

Firewall Manager 如何管理您的防火墙子网

防火墙子网是 Firewall Manager 为过滤网络流量的防火墙端点创建的 VPC 子网。每个防火墙端点都必须部署在专用 VPC 子网中。Firewall Manager 在策略范围内的每个 VPC 中至少创建一个防火墙子网。

对于使用分布式部署模型和自动端点配置的策略，Firewall Manager 仅在可用区域中创建防火墙子网，这些子网的子网带有互联网网关路由，或者子网具有通往 Firewall Manager 为其策略创建的防火墙端点的路由。有关更多信息，请参阅 Amazon VPC 用户指南中的 VPC 和子网。

对于使用分布式或集中式模式（您指定 Firewall Manager 在哪个可用区中创建防火墙端点）的策略，无论可用区中是否有其他资源，Firewall Manager 都会在这些特定的可用区中创建一个端点。

首次定义 Network Firewall 策略时，需要指定 Firewall Manager 如何管理范围内每个 VPC 中的防火墙子网。此后您不能对此选项进行更改。

对于使用分布式部署模型和自动端点配置的策略，您可以在以下选项中进行选择：

- 为每个具有公有子网的可用区部署防火墙子网。这是默认行为。这为您的流量过滤保护提供了高可用性。
- 在一个可用区中部署单个防火墙子网。通过此选项，Firewall Manager 可以识别 VPC 中哪个区域的公有子网最多，并在该区域创建防火墙子网。单个防火墙端点可过滤 VPC 的所有网络流量。这种方式可以降低防火墙成本，但其可用性不高，需要来自其他区域的流量才能跨越区域边界，以实现过滤。

对于使用带有自定义端点配置的分布式部署模型或集中式部署模型的策略，Firewall Manager 会在策略范围内的指定可用区中创建子网。

您可以提供 VPC CIDR 块供 Firewall Manager 用于防火墙子网，也可以将防火墙端点地址的选择留给 Firewall Manager 来决定。

- 如果您不提供 CIDR 块，Firewall Manager 会查询您的 VPC 以获取可供使用的 IP 地址。
- 如果您提供 CIDR 块列表，Firewall Manager 将仅在您提供的 CIDR 块中搜索新子网。您必须使用 /28 CIDR 块。对于 Firewall Manager 创建的每个防火墙子网，它会遍历您的 CIDR 阻止列表，并使用它找到的第一个适用于可用区和 VPC 且具有可用地址的子网。如果 Firewall Manager 无法在 VPC 中找到开放空间（有或没有限制），则该服务不会在 VPC 中创建防火墙。

如果 Firewall Manager 无法在可用区中创建所需的防火墙子网，则会将该子网标记为不符合策略。当该区域处于这种状态时，该区域的流量必须跨越区域边界，才能被其他区域中的端点过滤。这与单防火墙子网场景类似。

Firewall Manager 如何管理您的 Network Firewall 资源

在 Firewall Manager 中定义策略时，需要提供标准 AWS Network Firewall 防火墙策略的网络流量过滤行为。您可以添加无状态和有状态的 Network Firewall 规则组，并为与任何无状态规则不匹配的数据包指定默认操作。有关在中使用防火墙策略的信息 AWS Network Firewall，请参阅AWS Network Firewall 防火墙策略。

对于分布式和集中式策略，当您保存网络防火墙策略时，Firewall Manager 会在策略范围内的每个 VPC 中创建防火墙和防火墙策略。Firewall Manager 通过连接以下值来命名这些网络防火墙资源：

- 固定字符串，可以是 `FMManagedNetworkFirewall` 或 `FMManagedNetworkFirewallPolicy`，具体取决于资源类型。
- Firewall Manager 策略名称。这是您在创建策略时为其分配的名称。
- Firewall Manager 策略 ID。这是 Firewall Manager 策略的 AWS 资源 ID。
- Amazon VPC ID。这是 Firewall Manager 在其中创建防火墙和防火墙策略的 VPC 的 AWS 资源 ID。

以下是由 Firewall Manager 管理的防火墙的名称示例：

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

下面显示了一个防火墙策略名称示例：

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

创建策略后，VPC 中的成员账户无法覆盖您的防火墙策略设置或规则组，但他们可以将规则组添加到 Firewall Manager 创建的防火墙策略中。

Firewall Manager 如何为您的策略管理和监控 VPC 路由表

> **Note**
>
> 使用集中部署模型的策略目前不支持路由表管理。

当 Firewall Manager 创建您的防火墙端点时，它还会为它们创建 VPC 路由表。但是，Firewall Manager 并不管理您的 VPC 路由表。您必须将 VPC 路由表配置为将网络流量导向由 Firewall Manager 创建的防火墙端点。使用 Amazon VPC 入口路由增强功能，更改您的路由表以通过新的防火墙端点来路由流量。您的更改必须在要保护的子网和外部位置之间插入防火墙端点。您需要执行的确切路由取决于您的架构及其组件。

当前，Firewall Manager 允许监控您的 VPC 路由表路由，以查看任何绕过防火墙而流向互联网网关的流量。Firewall Manager 不支持其他目标网关，例如 NAT 网关。

有关管理您的 VPC 路由表的信息，请参阅 Amazon Virtual Private Cloud 用户指南中的管理 VPC 的路由表。有关管理 Network Firewall 路由表的信息，请参阅 AWS Network Firewall 开发人员指南中的 AWS Network Firewall的路由表配置。

当您为策略启用监控时，Firewall Manager 会持续监控 VPC 路由配置，并提醒您注意绕过该 VPC 的防火墙检查的流量。如果子网有防火墙端点路由，Firewall Manager 会查找以下路由：

- 将流量发送至 Network Firewall 端点的路由。
- 用于将流量从 Network Firewall 端点转发到互联网网关的路由。
- 从互联网网关到 Network Firewall 端点的入站路由。
- 来自防火墙子网的路由。

如果子网有网络防火墙路由，但网络防火墙和您的互联网网关路由表中存在非对称路由，Firewall Manager 会将该子网报告为不合规。Firewall Manager 还会在 Firewall Manager 创建的防火墙路由表以及子网的路由表中检测到互联网网关的路由，并将其报告为不合规。Network Firewall 子网路由表和您的互联网网关路由表中的其他路由也被报告为不合规。根据违规类型，Firewall Manager 会建议采取修正措施，使路由配置合规。Firewall Manager 并非在所有情况下都提供建议。例如，如果您的客户子网中有一个在 Firewall Manager 之外创建的防火墙端点，则 Firewall Manager 不会建议采取修正措施。

默认情况下，Firewall Manager 会将所有跨可用区边界以供检查的流量标记为不合规。但是，如果您选择在您的 VPC 中自动创建单个端点，Firewall Manager 不会将跨可用区边界的流量标记为不合规。

对于使用带有自定义端点配置的分布式部署模型的策略，您可以选择将从没有防火墙端点的可用区跨可用区边界的流量标记为合规或不合规。

> **Note**
>
> - Firewall Manager 不建议对非 IPv4 路由（例如 IPv6 和前缀列表路由）采取修正措施。

- 使用 `DisassociateRouteTable` API 调用发出的调用最长可能需要 12 小时才会被检测到。
- Firewall Manager 为包含防火墙端点的子网创建网络防火墙路由表。Firewall Manager 假设此路由表仅包含有效的互联网网关和 VPC 默认路由。此路由表中的任何额外或无效路由都被视为不合规。

在配置 Firewall Manager 策略时，如果选择监控模式，Firewall Manager 将提供有关您的资源的资源违规和修正详细信息。您可以使用这些建议的修正措施来修正路由表中的路由问题。如果您选择关闭模式，Firewall Manager 不会为您监控您的路由表内容。使用此选项，您可以自己管理 VPC 路由表。有关这些资源违规行为的更多信息，请参阅 查看 AWS Firewall Manager 策略的合规性信息。

Warning

如果您在创建策略时在 “ AWS Network Firewall 路由配置” 下选择 “监控”，则无法为该策略将其关闭。但是，如果您选择关闭，则可以稍后再启用该配置。

为 AWS Network Firewall 策略配置日志记录

您可以为 Network Firewall 策略启用集中日志记录，以获取有关组织内流量的详细信息。您可以选择流量日志来捕获网络流量，也可以选择警报日志来报告与规则操作设置为 `DROP` 或 `ALERT` 的规则相匹配的流量。有关 AWS Network Firewall 日志记录的更多信息，请参阅 AWS Network Firewall 开发人员指南中的录入来自 AWS Network Firewall的网络流量。

您将日志从策略的 Network Firewall 防火墙发送到 Amazon S3 存储桶。启用日志记录后，通过更新防火墙设置来 AWS Network Firewall 传送每个已配置的 Network Firewall 的日志，将日志传送到您选定的带有保留 AWS Firewall Manager 前缀的 Amazon S3 存储桶。`<policy-name>-<policy-id>`

Note

Firewall Manager 使用此前缀来确定日志配置是由 Firewall Manager 添加的，还是由账户所有者添加的。如果账户所有者尝试将保留的前缀用于自己的自定义日志记录，则该前缀会被 Firewall Manager 策略中的日志配置覆盖。

有关如何创建 Amazon S3 存储桶和查看存储日志的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的什么是 Amazon S3？。

要启用日志记录功能，您必须满足以下要求：

- 您在Firewall Manager 策略中指定的 Amazon S3 必须存在。
- 您必须拥有以下权限：
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- 如果作为您的日志目标的 Amazon S3 存储桶使用服务器端加密，且密钥存储在中 AWS Key Management Service，则必须将以下策略添加到 AWS KMS 客户管理的密钥中，以允许 Firewall Manager 登录到您的 CloudWatch 日志组：

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

请注意，只有 Firewall Manager 管理员账户中的存储分区可以用于 AWS Network Firewall 集中日志记录。

在 Network Firewall 策略上启用集中日志记录时，Firewall Manager 会对您的账户执行以下操作：

- Firewall Manager 会更新所选 S3 存储桶的权限以允许传送日志。
- Firewall Manager 在 S3 存储桶中为策略范围内的每个成员账户创建目录。每个账户的日志可在 `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>` 找到。

启用 Network Firewall 策略的日志记录

1. 使用 Firewall Manager 管理员账户创建 Amazon S3 存储桶。有关更多信息，请参阅 Amazon Simple Storage Service 用户指南中的创建存储桶。
2. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

3. 在导航窗格中，选择安全策略。
4. 选择要为其启用日志记录的 Network Firewall 策略。有关 AWS Network Firewall 日志记录的更多信息，请参阅AWS Network Firewall 开发者指南 AWS Network Firewall中的记录网络流量。
5. 在策略详细信息选项卡的策略规则部分，选择编辑。
6. 要启用和聚合日志，请在日志配置下选择一个或多个选项：
   - 启用和聚合流日志
   - 启用和聚合警报日志
7. 选择需要将日志传输到哪个 Amazon S3 存储桶。您必须为启用的每种日志类型选择一个存储桶。同一存储桶可以同时用于两种日志类型。
8. （可选）如果您希望将自定义成员账户创建的日志记录替换为策略的日志配置，请选择覆盖现有日志配置。
9. 选择下一步。
10. 查看您的设置，然后选择保存以保存对策略的更改。

禁用 Network Firewall 策略的日志记录

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

> **Note**
>
> 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择安全策略。
3. 选择要为其禁用日志记录的 Network Firewall 策略。
4. 在策略详细信息选项卡的策略规则部分，选择编辑。
5. 在日志配置状态下，取消选择启用并聚合流日志和启用并聚合警报日志（如果已选中）。
6. 选择下一步。
7. 查看您的设置，然后选择保存以保存对策略的更改。

Amazon Route 53 Resolver DNS 防火墙策略

您可以使用 AWS Firewall Manager DNS 防火墙策略来管理 Amazon Route 53 Resolver DNS 防火墙规则组与您的组织中的亚马逊虚拟私有云 VPC 之间的关联。 AWS Organizations您可以将集中控制的防火墙应用于整个组织，也可以应用于选定的账户和 VPC 子集。

DNS Firewall 为您的 VPC 提供出站 DNS 流量筛选和监管。您可以在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，并将规则组关联到您的 VPC。当您应用 Firewall Manager 策略时，对于策略范围内的每个账户和 VPC，Firewall Manager 会使用您在 Firewall Manager 策略中指定的关联优先级设置，在策略中的每个 DNS 防火墙规则组与策略范围内的每个 VPC 之间创建关联。

有关使用 DNS 防火墙的信息，请参阅 Amazon Route 53 开发人员指南中的 Amazon Route 53 Resolver DNS 防火墙。

以下各节介绍使用 Firewall Manager DNS 防火墙策略的要求，并描述了这些策略的工作原理。有关创建策略的过程，请参阅 为 Amazon Route 53 解析器 DNS 防火墙创建 AWS Firewall Manager 策略。

您必须启用资源共享

DNS 防火墙策略在您组织中的账户之间共享 DNS 防火墙规则组。要使此功能起作用，您必须使用启用资源共享 AWS Organizations。有关如何启用资源共享的信息，请参阅 Network Firewall 和 DNS 防火墙策略的资源共享。

您必须定义 DNS Firewall 规则组

当您指定新的 DNS 防火墙策略时，您可以如同直接使用 Amazon Route 53 Resolver DNS 防火墙一样定义规则组。您的规则组必须已存在于 Firewall Manager 管理员账户中，才能将其包含在策略中。有关创建 DNS 防火墙规则组的信息，请参阅 DNS 防火墙规则组和规则。

您可以定义优先级最低和最高的规则组关联

通过 Firewall Manager DNS 防火墙策略管理的 DNS 防火墙规则组关联包含 VPC 的最低优先级关联和最高优先级关联。在您的策略配置中，这些规则组显示为第一个和最后一个规则组。

DNS 防火墙按以下顺序筛选 VPC 的 DNS 流量：

1. 第一个规则组，由您在 Firewall Manager DNS Firewall 策略中定义。有效值在 1 到 99 之间。
2. 由个人账户管理员通过 DNS 防火墙关联的 DNS 防火墙规则组。
3. 最后一个规则组，由您在 Firewall Manager DNS Firewall 策略中定义。有效值介于 9,901 到 10,000 之间。

删除规则组

如需从 Firewall Manager DNS 防火墙策略中删除规则组，必须执行以下步骤：

1. 从 Firewall Manager DNS Firewall 策略中删除规则组。
2. 取消共享中的规则组。 AWS Resource Access Manager要取消共享自己拥有的规则组，必须从资源共享中将其删除。您可以使用 AWS RAM 控制台或 AWS CLI 执行此操作。有关取消资源共享的信息，请参阅AWS RAM 用户指南中的更新资源共享 AWS RAM。
3. 使用 DNS 防火墙控制台或 AWS CLI 删除规则组。

Firewall Manager 如何命名其创建的规则组关联

保存 DNS 防火墙策略时，如果您启用了自动修正，Firewall Manager 将在您在策略中提供的规则组与策略范围内的 VPC 之间创建 DNS 防火墙关联。Firewall Manager 通过连接以下值来命名这些关联：

- 固定字符串，`FMManaged_`。
- Firewall Manager 策略 ID。这是 Firewall Manager 策略的 AWS 资源 ID。

以下是由 Firewall Manager 管理的防火墙的名称示例：

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

创建策略后，如果 VPC 中的账户所有者覆盖了您的防火墙策略设置或规则组关联，则 Firewall Manager 会将该策略标记为不合规并尝试提出补救措施。账户所有者可以将其他 DNS 防火墙规则组关联到 DNS 防火墙策略范围内的 VPC。个人账户所有者创建的任何关联都必须在第一个和最后一个规则组关联之间设置优先级。

Palo Alto Networks Cloud NGFW 策略

Palo Alto Networks Cloud 下一代防火墙 (NGFW) 是一项第三方防火墙服务，您可以将其用于您的策略。 AWS Firewall Manager 使用适用于 Firewall Manager 的 Palo Alto Networks Cloud NGFW，你可以在所有账户中创建和集中部署 Palo Alto Networks Cloud NGFW 资源和规则堆栈。 AWS

要将 Palo Alto Networks Cloud NGFW 与 Firewall Manager 配合使用，你首先要在 Marketplace 上订阅 Palo Alto Networks Cloud NGFW 即付即用服务。 AWS 订阅后，您可以在 Palo Alto Networks Cloud NGFW 服务中执行一系列步骤来配置您的账户和 Cloud NGFW 设置。然后，你创建一个 Firewall Manager Cloud FMS 策略，用于集中部署和管理组织中所有账户的 Palo Alto Networks Cloud NGFW 资源和规则。 AWS

有关创建 Firewall Manager 策略的过程，请参阅 为 Palo Alto Networks Cloud AWS Firewall Manager 制定政策 NGFW。有关如何配置和管理适用于 Firewall Manager 的 Palo Alto Networks Cloud NGFW 的信息，请参阅 AWS文档中的 Palo Alto Networks Cloud NGFW。

Fortigate 云原生防火墙 (CNF) 即服务策略

Fortigate 云原生防火墙 (CNF) 即服务是一项第三方防火墙服务，您可以将其用于您的策略。 AWS Firewall Manager Fortigate CNF 是下一代防火墙服务，可以帮助您轻松保护云网络和管理安全策略。使用 Fortigate CNF for Firewall Manager，您可以在所有账户中创建和集中部署 Fortigate CNF 资源和策略集。 AWS

要将 Fortigate CNF 与 Firewall Manager 配合使用，您需要先在 Marketplace 上订阅 F ortigate 云原生防火墙 (CNF) 即服务。 AWS 订阅后，您可以在 Fortigate CNF 服务中执行一系列步骤来配置您的全局策略集和其他设置。然后，您可以创建 Firewall Manager 策略，以便在组织中的所有账户中集中部署和管理 Fortigate CNF 资源。 AWS

有关创建 Fortigate CNF Firewall Manager 策略的过程，请参阅 为 Fortigate 云原生防火墙 (CNF) 即服务创建 AWS Firewall Manager 策略。有关如何配置和管理 Fortigate CNF 从而与 Firewall Manager 配合使用的信息，请参阅 Fortigate CNF 文档。

Network Firewall 和 DNS 防火墙策略的资源共享

要管理 Firewall Manager 网络防火墙和 DNS 防火墙策略，必须启用与 AWS Organizations 中的资源共享 AWS Resource Access Manager。启用该功能后，Firewall Manager 可以在您创建这些策略类型时跨账户地部署保护。

要启用资源共享，请按照 AWS Resource Access Manager 用户指南中的启用与 AWS Organizations 的共享中的说明进行操作。

资源共享问题

在使用 AWS RAM 资源共享时，或者在处理需要资源共享的 Firewall Manager 策略时，您可能会遇到资源共享问题。

例如：

- 当您按照说明启用共享时，在 AWS RAM 控制台中，“启用与之共享” 选项显示 AWS Organizations 为灰色，不可选择。
- 当您在 Firewall Manager 中处理需要资源共享的策略时，该策略标记为不合规，并且消息显示资源共享或 AWS RAM 未启用。

如果您遇到资源共享问题，请尝试通过以下过程启用资源共享。

再次尝试启用资源共享

- 使用以下任一选项再次尝试启用共享：
  - （可选）通过 AWS RAM 控制台，按照《AWS Resource Access Manager 用户指南》中的 “启用与共享” AWS Organizations中的说明进行操作。
  - （选项）使用 AWS RAM API 调用`EnableSharingWithAwsOrganization`。请参阅中的文档EnableSharingWithAwsOrganization。

在 Firewall Manager 中使用资源集

AWS Firewall Manager 资源集是诸如防火墙之类的资源集合，您可以将其组合在一起并在 Firewall Manager 策略中进行管理。资源集使组织中的成员能够精细控制要在策略中管理哪些资源。要使用资源集，请在控制台中或使用 PutResourceSetAPI 创建资源集，然后将该资源集添加到 Firewall Manager 策略中。

您可以为以下资源和安全策略类型创建和管理资源集：

资源类型	Firewall Manager 安全策略类型
AWS Network Firewall -防火墙	Network Firewall 策略 - 使用资源集从 Network Firewall 导入现有防火墙。有关在 Network Firewall 策略中使用资源集的信息，请参阅 为创建 AWS Firewall Manager 策略 AWS Network Firewall 过程中的导入现有防火墙步骤。

以下各节介绍创建和删除资源集的要求。

主题

在 Firewall Manager 中使用资源集的注意事项

在使用资源集时，请注意以下事项

对不存在的资源的引用

当您将资源添加到资源集时，您可以使用 Amazon 资源名称（ARN）来创建对该资源的引用。Firewall Manager 会验证 Amazon 资源名称（ARN）的格式是否正确，但 Firewall Manager 不会检查引用的资源是否存在。如果资源尚不存在但通过了 ARN 验证，则 Firewall Manager 会将资源引用包含在资源集中。如果以后创建了具有相同 ARN 的新资源，Firewall Manager 会将该资源集的关联策略中的规则组应用于新资源。

删除的资源

删除资源集中的资源后，对该资源的引用将保留在资源集中，直到 Firewall Manager 管理员将其删除。

已离开 AWS Organizations 组织的成员账户拥有的资源

如果成员账户离开组织，则对该成员账户拥有的资源的任何引用都将保留在资源集中，但不再受与该资源集关联的任何策略的管理。

与多个策略的关联

一个资源集可以与多个策略相关联，但并非所有策略类型都支持管理同一资源的多个策略。有关不支持的场景的信息，请参阅您的特定策略类型的文档。

创建资源集

创建资源集（控制台）

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择资源。
3. 选择创建资源集。
4. 对于资源集名称，输入描述性名称。
5. （可选）输入资源集的描述。
6. 选择 下一步。
7. 在选择资源中，选择一个 AWS 账户 ID，然后选择选择资源，将该账户拥有和管理的资源添加到资源集中。选择资源后，选择添加，将资源添加到资源集中。
8. 选择下一步。
9. 对于资源集标签，请为资源集添加所需的任何标识标签。有关标签的更多信息，请参阅使用标签编辑器。
10. 选择下一步。

11. 查看新的资源集。要进行任何更改，请在要更改的区域中选择 编辑。此操作会将您返回到创建向导中的相应步骤。如果您对资源集感到满意，请选择创建资源集。

删除资源集

在删除资源集之前，必须使用该资源集取消该资源集与所有策略的关联。您可以使用控制台或PutPolicyAPI 在策略详细信息页面中取消资源组的关联。

删除资源集（控制台）

1. 在导航窗格中，选择资源。
2. 选中想要删除的资源集旁边的选项。
3. 选择 删除。

查看 AWS Firewall Manager 策略的合规性信息

本节为查看 AWS Firewall Manager 策略范围内的账户和资源的合规状态提供了指导。有关为维护云的安全性和合规性而采取的控制措施的信息，请参阅Firewall Manager 的合规性验证。 AWS

> **Note**
>
> 为了让 Firewall Manager 监控策略合规性， AWS Config 必须持续记录受保护资源的配置更改。在您的 AWS Config 配置中，必须将录制频率设置为 “连续”，这是默认设置。

> **Note**
>
> 要在受保护的资源中保持适当的合规状态，请避免重复自动或手动更改 Firewall Manager 保护的状态。Firewall Manager 使用来自 AWS Config 的信息来检测对资源配置的更改。如果应用更改的速度足够快，则 AWS Config 可能会丢失对其中一些更改的跟踪，从而导致 Firewall Manager 中有关合规性或补救状态的信息丢失。
>
> 如果您发现使用 Firewall Manager 保护的资源的合规性或修复状态不正确，请首先确保您没有运行任何更改或重置防火墙管理器保护的进程，然后通过重新评估中的关联配置规则来刷新对资源的 AWS Config 跟踪。 AWS Config

对于所有 AWS Firewall Manager 策略，您可以查看策略范围内账户和资源的合规性状态。如果策略的设置反映在账户或资源的设置中，则该账户或资源符合 Firewall Manager 策略。每种策略类型都有自己的合规性要求，您可以在定义策略时对其进行调整。对于某些策略，您还可以查看其适用资源的详细违规信息，以帮助您更好地了解和管理安全风险。

查看策略的信息

1. AWS Management Console 使用您的 Firewall Manager 管理员帐户登录，然后打开防火墙管理器控制台，网址为https://console.aws.amazon.com/wafv2/fmsv2。有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

   > **Note**
   >
   > 有关设置 Firewall Manager 管理员账户的信息，请参阅AWS Firewall Manager 先决条件。

2. 在导航窗格中，选择 安全策略。
3. 选择一个策略。在策略页面的账户和资源选项卡中，Firewall Manager 列出了您组织中的账户，这些账户分组为该策略范围内的账户和策略范围外的账户。

   策略范围内的账户窗格列出了每个账户的合规性状态。合规状态表示该策略已成功应用于账户的所有范围内资源。不合规状态表示该策略尚未应用于该账户下适用于该策略的一个或多个资源。
4. 选择一个不合规的账户。在账户页面中，Firewall Manager 列出了每个不合规资源的 ID 和类型，以及该资源违反策略的原因。

   > **Note**
   >
   > 对于资源类型 `AWS::EC2::NetworkInterface` (ENI) 和 `AWS::EC2::Instance`，Firewall Manager 可能会显示有限数量的不合规资源。要列出其他不合规的资源，请修复最初为该账户显示的资源。

5. 如果 Firewall Manager 策略类型为内容审核安全组策略，则可以访问资源的详细违规信息。

   要查看违规详细信息，请选择资源。

   > **Note**
   >
   > 在添加详细资源违例页面之前，Firewall Manager 发现不合规的资源可能没有违规详情。

在资源页面中，Firewall Manager 根据资源类型列出了有关违规的具体细节。

- **AWS::EC2::NetworkInterface** (ENI)：Firewall Manager 显示有关资源不符合的安全组的信息。选择安全组以查看有关它的更多详细信息。
- **AWS::EC2::Instance**：Firewall Manager 显示连接到 EC2 实例的不合规 ENI。它还会显示资源不符合的安全组的信息。选择安全组以查看有关它的更多详细信息。
- **AWS::EC2::SecurityGroup**：Firewall Manager 显示以下违规详情：
  - 不合规的安全组规则：违规的规则，包括其协议、端口范围、IP CIDR 范围和描述。
  - 引用的规则：不合规安全组规则违反的审核安全组规则及其详细信息。
  - 违规原因：对违规调查发现的解释。
  - 补救措施：建议采取的措施。如果 Firewall Manager 无法确定安全补救措施，则此字段为空。
- **AWS::EC2::Subnet**— 这用于网络 ACL 和 Network Firewall 策略。

  Firewall Manager 显示子网 ID、VPC ID 和可用区域。如果适用，Firewall Manager 会包含有关违规的其他信息。违规描述部分包含对资源的预期状态、当前不合规状态的描述，以及对导致差异的原因的描述（如有）。

  网络防火墙违规

  - 路由管理违规：对于使用监控模式的 Network Firewall 策略，Firewall Manager 会显示基本子网信息，以及子网、互联网网关和 Network Firewall 子网路由表中的预期和实际路由。如果实际路由与路由表中的预期路由不匹配，Firewall Manager 会提醒您存在违规。
  - 路由管理违规的补救措施：对于使用监控模式的 Network Firewall 策略，Firewall Manager 会建议对存在违规的路由配置采取可能的补救措施。

  例如，假设子网应通过防火墙端点发送流量，但当前子网将流量直接发送到互联网网关。这属于路由管理违规行为。在这种情况下，建议有序采取一系列补救措施。第一个建议是将所需路由添加到 Network Firewall 子网的路由表中，以将传出流量定向到互联网网关，并将发往 VPC 内目的地的传入流量定向到 `local`。第二个建议是替换子网路由表中的互联网网关路由或无效的 Network Firewall 路由，将传出流量定向到防火墙端点。第三个建议是将所需的路由添加到互联网网关的路由表中，以将传入流量定向到防火墙端点。
- **AWS::EC2:InternetGateway**：这用于启用监控模式的 Network Firewall 策略。
  - 路由管理违规：如果互联网网关未与路由表关联，或者互联网网关路由表中有无效路由，则互联网网关不合规。

- 针对路由管理违规的补救措施：Firewall Manager 会建议可能的补救措施，以补救路由管理违规。

  Example 1：路由管理违规和补救建议

  互联网网关与路由表无关。建议有序采取一系列补救措施。第一项操作是创建路由表。第二项操作是将路由表与互联网网关联。第三项操作是将所需的路由添加到互联网网关路由表中。

  Example 2：路由管理违规和补救建议

  互联网网关与有效的路由表关联，但路由配置不正确。建议有序采取一系列补救措施。第一项建议是移除无效路由。第二项建议是将所需的路由添加到互联网网关路由表中。

- **`AWS::NetworkFirewall::FirewallPolicy`**：用于 Network Firewall 策略。Firewall Manager 显示有关 Network Firewall 防火墙策略的信息，该策略已被修改为不合规。这些信息提供了预期的防火墙策略及其在客户账户中找到的策略，因此您可以比较无状态和有状态的规则组名称与优先级设置、自定义操作名称以及默认的无状态操作设置。违规描述部分包含对资源的预期状态、当前不合规状态的描述，以及对导致差异的原因的描述（如有）。
- **`AWS::EC2::VPC`**：这用于 DNS 防火墙策略。Firewall Manager 显示有关在 Firewall Manager DNS 防火墙策略作用域内且不符合该策略的 VPC 的信息。提供的信息包括预期与 VPC 关联的预期规则组和实际规则组。违规描述部分包含对资源的预期状态、当前不合规状态的描述，以及对导致差异的原因的描述（如有）。

AWS Firewall Manager 调查结果

AWS Firewall Manager 为不合规的资源和它检测到的攻击创建调查结果，然后将其发送到 AWS Security Hub。有关 Security Hub 检测结果的更多信息，请参阅 AWS Security Hub中的检测结果。

当您使用 Security Hub 和 Firewall Manager 时，Firewall Manager 会自动将您的检测结果发送到 Security Hub。有关开始使用 Security Hub 的信息，请参阅 AWS Security Hub 用户指南中的设置 Security Hub AWS Security Hub。

> **Note**
>
> Firewall Manager 仅更新其管理下的策略及其所监控资源的调查结果。
> Firewall Manager 无法解析以下问题的搜索结果：
>
> - 已删除的策略。
> - 已删除的资源。

- 已超出 Firewall Manager 策略范围的资源，例如由于标签更改或策略定义更改所致。

如何查看 Firewall Manager 的检测结果？

要在 Security Hub 中查看 Firewall Manager 的检测结果，请按照在 Security Hub 中使用检测结果中的指导进行操作，并使用以下设置创建筛选条件：

- 属性设置为产品名称。
- 运算符设置为等于。
- 值设置为 `Firewall Manager`。该设置区分大小写。

我能不能禁用这个功能？

您可以通过 Security Hub 控制台禁用搜索 AWS Firewall Manager 结果与 Security Hub 的集成。在导航栏中选择集成，然后在 Firewall Manager 窗格中选择禁用集成。有关更多信息，请参阅《AWS Security Hub 用户指南》。

AWS Firewall Manager 查找类型

- AWS WAF 政策调查结果
- AWS Shield Advanced 政策调查结果
- 安全组通用策略检测结果
- 安全组内容审核策略检测结果
- 安全组使用情况审核策略检测结果
- Amazon Route 53 Resolver DNS 防火墙策略检测结果

AWS WAF 政策调查结果

您可以使用 Firewall Manager AWS WAF 策略将 AWS WAF 规则组应用于中的资源 AWS Organizations。有关更多信息，请参阅 使用 AWS Firewall Manager 策略。

资源缺少 Firewall Manager 托管的 Web ACL。

根据 Firewall Manager 策略， AWS 资源没有 AWS Firewall Manager 托管 Web ACL 关联。您可以对此策略启用 Firewall Manager 补救以更正此问题。

- 严重性 – 80
- 状态设置 – 通过/失败
- 更新 – 如果 Firewall Manager 执行补救操作，它将更新检测结果，严重性将从 HIGH 降低到 INFORMATIONAL。如果您执行修复，Firewall Manager 将不会更新检测结果。

Firewall Manager 托管的 Web ACL 的规则组配置不正确。

根据 Firewall Manager 策略，由 Firewall Manager 托管的 Web ACL 中的规则组配置不正确。也就是说，此 Web ACL 缺少该策略所需的规则组。您可以对此策略启用 Firewall Manager 补救以更正此问题。

- 严重性 – 80
- 状态设置 – 通过/失败
- 更新 – 如果 Firewall Manager 执行补救操作，它将更新检测结果，严重性将从 HIGH 降低到 INFORMATIONAL。如果您执行修复，Firewall Manager 将不会更新检测结果。

AWS Shield Advanced 政策调查结果

有关 AWS Shield Advanced 策略的信息，请参阅安全组策略。

资源缺乏 Shield Advanced 保护。

根据防火墙管理器策略，本应具有 Shield Advanced 保护的 AWS 资源却没有 Shield 高级保护。您可以对策略启用 Firewall Manager 修复，以启用对资源的保护。

- 严重性 – 60
- 状态设置 – 通过/失败
- 更新 – 如果 Firewall Manager 执行补救操作，它将更新检测结果，严重性将从 HIGH 降低到 INFORMATIONAL。如果您执行修复，Firewall Manager 将不会更新检测结果。

Shield Advanced 检测到针对受监控资源的攻击。

Shield Advanced 检测到对受保护 AWS 资源的攻击。您可以在策略上启用 Firewall Manager 补救。

- 严重性 – 70
- 状态设置 – 无

- 更新 – Firewall Manager 不会更新此检测结果。

安全组通用策略检测结果

有关安全组通用策略的更多信息，请参阅 安全组策略。

资源的安全组配置不正确。

根据 Firewall Manager 策略，Firewall Manager 已发现一种资源缺少应有的 Firewall Manager 托管安全组关联。您可以对策略启用 Firewall Manager 修复，以根据策略设置创建关联。

- 严重性 – 70
- 状态设置 – 通过/失败
- 更新 – Firewall Manager 更新了这一检测结果。

Firewall Manager 副本安全组与主要安全组不同步。

根据其通用安全组策略，Firewall Manager 副本安全组与其主要安全组不同步。您可以对策略启用 Firewall Manager 修复，这样可以将副本安全组与主安全组同步。

- 严重性 – 80
- 状态设置 – 通过/失败
- 更新 – Firewall Manager 更新了这一检测结果。

安全组内容审核策略检测结果

有关安全组内容审核策略的更多信息，请参阅 安全组策略。

安全组不符合内容审核安全组的要求。

Firewall Manager 安全组内容审核策略发现了一个不合规的安全组。这是一个客户创建的安全组，属于内容审核策略的作用域，并且不符合该策略及其审核安全组所定义的设置。您可以对策略启用 Firewall Manager 补救，该策略会修改不合规的安全组以使其合规。

- 严重性 – 70
- 状态设置 – 通过/失败
- 更新 – Firewall Manager 更新了这一检测结果。

安全组使用情况审核策略检测结果

有关安全组使用情况审核策略的更多信息，请参阅 安全组策略。

Firewall Manager 发现了冗余安全组。

Firewall Manager 安全组使用情况审核发现了一个冗余的安全组。这是一个安全组，其规则集与同一 Amazon Virtual Private Cloud 实例中的另一个安全组相同。您可以对使用情况审核策略启用 Firewall Manager 自动修复，该策略将冗余的安全组替换为单个安全组。

- 严重性 – 30
- 状态设置 – 无
- 更新 – Firewall Manager 不会更新此检测结果。

Firewall Manager 发现了未使用的安全组。

Firewall Manager 安全组使用情况审核发现了一个未使用的安全组。这是任何 Firewall Manager 通用安全组策略都未引用的安全组。您可以对使用情况审核策略启用 Firewall Manager 自动修复，从而删除未使用的安全组。

- 严重性 – 30
- 状态设置 – 无
- 更新 – Firewall Manager 不会更新此检测结果。

Amazon Route 53 Resolver DNS 防火墙策略检测结果

有关 DNS 防火墙策略的更多信息，请参阅 Amazon Route 53 Resolver DNS 防火墙策略。

资源缺少 DNS 防火墙保护

VPC 缺少在 Firewall Manager DNS 防火墙策略中定义的 DNS 防火墙规则组关联。检测结果列出了策略指定的规则组。

- 严重性 – 80

您使用 AWS Firewall Manager 服务的安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

> **Note**
>
> 本节提供了有关您使用 AWS Firewall Manager 服务及其 AWS 资源的标准 AWS 安全指南，例如 Firewall Manager Network Firewall 策略和安全组策略。
> 有关使用 Firewall Manager 保护 AWS 资源的信息，请参阅《防火墙管理器》指南的其余部分。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Firewall Manager 的合规性计划，请参阅合规性计划范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Firewall Manager 时应用责任共担模型。以下主题说明如何配置 Firewall Manager 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Firewall Manager 资源。

主题

Firewall Manager 中的数据保护

分 AWS 担责任模型适用于中的数据保护 AWS Firewall Manager。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API 或 SDK AWS 服务 使用 Firewall Manager 或其他 AWS 软件开发工具包的情况。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

Firewall Manager 实体（如策略）是静态加密的，但某些不提供加密的区域除外，包括中国（北京）和中国（宁夏）。每个区域使用唯一的加密密钥。

Identity and Access Management AWS Firewall Manager

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Firewall Manager 资源的人员。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Firewall Manager 中所做的工作。

服务用户：如果使用 Firewall Manager 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Firewall Manager 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Firewall Manager 中的功能，请参阅 对 AWS Shield 身份和访问进行故障排除。

服务管理员：如果您在公司负责管理 Firewall Manager 资源，则您可能具有 Firewall Manager 的完全访问权限。您有责任确定您的服务用户应访问哪些 Firewall Manager 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Firewall Manager 搭配使用的更多信息，请参阅 如何 AWS Shield 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解有关如何编写策略以管理对 Firewall Manager 的访问权限的详细信息。要查看您可在 IAM 中使用的 Firewall Manager 基于身份的策略示例，请参阅 适用于 AWS Shield的基于身份的策略示例。

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS中使用多重身份验证（ MFA ）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，我们建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定

的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon QLDB 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他

AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组

和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。

- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Firewall Manager 与 IAM 配合使用

在使用 IAM 管理对 Firewall Manager 的访问权限之前，您应该了解哪些 IAM 功能可与 Firewall Manager 搭配使用。

您可以搭配使用的 IAM 功能 AWS Firewall Manager

IAM 功能	Firewall Manager 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	支持
策略条件键（特定于服务）	不支持
ACL	否
ABAC（策略中的标签）	支持
临时凭证	支持
转发访问会话（FAS）	支持

IAM 功能	Firewall Manager 支持
服务角色	部分
服务相关角色	支持

要全面了解 Firewall Manager 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

适用于 Firewall Manager 的基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM policy。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

要查看 Firewall Manager 基于身份的策略示例，请参阅 基于身份的策略示例 AWS Firewall Manager。

适用于 Firewall Manager 的基于身份的策略示例

要查看 Firewall Manager 基于身份的策略示例，请参阅 基于身份的策略示例 AWS Firewall Manager。

Firewall Manager 内基于资源的策略

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

Firewall Manager 的策略操作

支持策略操作	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Firewall Manager 操作的列表，请参阅服务授权参考中的 AWS Firewall Manager定义的操作。

Firewall Manager 中的策略操作在此操作之前使用以下前缀：

```
fms
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "fms:Describe*"
```

要查看 Firewall Manager 基于身份的策略示例，请参阅 基于身份的策略示例 AWS Firewall Manager。

Firewall Manager 的策略资源

支持策略资源	支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Firewall Manager 的资源类型及其 ARN 的列表，请参阅服务授权参考中的 AWS Firewall Manager定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Firewall Manager 定义的操作。

要查看 Firewall Manager 基于身份的策略示例，请参阅 基于身份的策略示例 AWS Firewall Manager。

Firewall Manager 的策略条件键

支持特定于服务的策略条件密钥	不支持

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑0R运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

有关 Firewall Manager 条件键的列表，请参阅服务授权参考中的 AWS Firewall Manager的条件键。要了解可以使用条件键的操作和资源，请参阅由定义的操作 AWS Firewall Manager。

要查看 Firewall Manager 基于身份的策略示例，请参阅 基于身份的策略示例 AWS Firewall Manager。

Firewall Manager 中的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

使用 Firewall Manager 的 ABAC

支持 ABAC（策略中的标签）	支持

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

借助 Firewall Manager 使用临时凭证

支持临时凭证	支持

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Firewall Manager 的转发访问会话

支持转发访问会话 (FAS)	支持

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Firewall Manager 的服务角色

支持服务角色	部分

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Firewall Manager 的功能。仅当 Firewall Manager 提供相关指导时才编辑服务角色。

在 Firewall Manager 中选择 IAM 角色

要在防火墙管理器中使用 *PutNotificationChannel*API 操作，您必须选择一个角色以允许防火墙管理员访问亚马逊 SNS，以便该服务可以代表您发布 Amazon SNS 消息。有关更多信息，请参阅 AWS Firewall Manager API 参考PutNotificationChannel中的。

下面显示了一个 SNS 主题权限设置的示例。要将此策略用于您的自定义角色，将 AWSServiceRoleForFMS Amazon 资源名称（ARN） 替换为您的 SnsRoleName ARN。

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

有关 Firewall Manager 操作和资源的更多信息，请参阅 AWS Identity and Access Management 指南主题操作定义者 AWS Firewall Manager

Firewall Manager 的服务相关角色

支持服务相关角色	支持

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

基于身份的策略示例 AWS Firewall Manager

默认情况下，用户和角色没有创建或修改 Firewall Manager 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅IAM 用户指南中的 创建 IAM policy。

有关 Firewall Manager 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考中的 AWS Firewall Manager的操作、资源和条件键。

主题

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Firewall Manager 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM

Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。

- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实践的更多信息，请参阅IAM 用户指南中的 IAM 中的安全最佳实践。

使用 Firewall Manager 控制台

要访问 AWS Firewall Manager 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 AWS 账户中的 Firewall Manager 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Firewall Manager 控制台，还要将防火墙管理器*ConsoleAccess*或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

授予对 Firewall Manager 安全组的读取权限

Firewall Manager 允许跨账户资源访问，但它不允许您创建跨账户资源保护。您只能为拥有这些资源的账户中的资源创建保护。

以下示例策略授予对所有资源执行fms:Get、fms:List 和 ec2:DescribeSecurityGroups 操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 的托管策略 AWS Firewall Manager

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：**`AWSFMAdminFullAccess`**

使用`AWSFMAdminFullAccess` AWS 托管策略允许您的管理员访问 AWS Firewall Manager 资源，包括所有 Firewall Manager 策略类型。此策略不包括在 AWS Firewall Manager中设置 Amazon Simple Notification Service 通知的权限。有关如何设置 Amazon Simple Notification Service 的访问权限的信息，请参阅设置 Amazon Simple Notification Service 的访问权限。

有关策略列表和详细信息，请参阅 IAM 控制台，网址为AWSFMAdminFullAccess。本节的其余部分概述了策略设置。

权限声明

此策略根据权限集分为多个语句。

- AWS Firewall Manager 策略资源-允许对中的 AWS Firewall Manager资源（包括所有 Firewall Manager 策略类型）拥有完全管理权限。
- 将 AWS WAF 日志写入亚马逊简单存储服务-允许 Firewall Manager 在 Amazon S3 中写入和读取 AWS WAF 日志。
- 创建服务链接角色：允许管理员创建服务关联角色，它允许 Firewall Manager 代表您分析其他服务中的资源。此权限允许创建仅供 Firewall Manager 使用的服务关联角色。有关 Firewall Manager 如何使用服务相关角色的更多信息，请参阅 使用 Firewall Manager 的服务相关角色。
- AWS Organizations：允许管理员将 Firewall Manager 用于 AWS Organizations中的企业。在中启用 Firewall Manager 的可信访问后 AWS Organizations，管理员帐户的成员可以查看其组织中的发现结果。有关 AWS Organizations 与一起使用的信息 AWS Firewall Manager，请参阅《AWS Organizations 用户指南》中的AWS Organizations 与其他 AWS 服务一起使用。

权限类别

以下列出了策略中的权限类型及其提供的权限。

- `fms`— 使用 AWS Firewall Manager 资源。
- `waf`和 `waf-regional`-使用 AWS WAF 经典策略。
- `elasticloadbalancing`— 将 AWS WAF Web ACL 关联到弹性负载均衡器。
- `firehose`— 查看有关 AWS WAF 日志的信息。
- `organizations`— 使用 Organiz AWS ations 资源。
- `shield`— 查看 AWS Shield 策略的订阅状态。
- `route53resolver`— 在 Route 53 VPC 私有 DNS 策略中使用 Route 53 VPC 私有 DNS 规则组。
- `wafv2`— 使用 AWS WAFV2 策略。
- `network-firewall`— 使用 AWS Network Firewall 策略。
- `ec2`— 查看策略可用区和区域。
- `s3`— 查看有关 AWS WAF 日志的信息。

AWS 托管策略：**`FMSServiceRolePolicy`**

此策略 AWS Firewall Manager 允许您在 Firewall Manager 和集成服务中代表您管理 AWS 资源。此策略附加到 `AWSServiceRoleForFMS` 服务相关角色。有关服务相关角色的更多信息，请参阅 使用 Firewall Manager 的服务相关角色。

有关政策的详细信息，请参阅 FMS ServiceRolePolicy 上的 IAM 控制台。

AWS 托管策略： AWSFMAdminReadOnlyAccess

授予对所有 Fi AWS rewall Manager 资源的只读访问权限。

有关策略列表和详细信息，请参阅 IAM 控制台，网址为AWSFMAdminReadOnlyAccess。本节的其余部分概述了策略设置。

权限类别

下面列出了策略中的权限类型以及这些权限允许只读访问的信息。

- `fms`— AWS Firewall Manager 资源。
- `waf`和 `waf-regional`- AWS WAF 经典策略。

- `firehose`— AWS WAF 日志。
- `organizations`— AWS Organitions 资源。
- `shield`— AWS Shield 政策。
- `route53resolver`— Route 53 VPC 私有 DNS 规则组中的 Route 53 VPC 私有 DNS 策略中。
- `wafv2`— 中可用的 AWS WAFV2 规则组和 AWS 托管规则规则组 AWS WAFV2。
- `network-firewall`— AWS Network Firewall 规则组和规则组元数据。
- `ec2`— AWS Network Firewall 政策可用区和区域。
- `s3`— AWS WAF 日志。

AWS 托管策略： AWSFMMemberReadOnlyAccess

授予对 AWS Firewall Manager 成员资源的只读访问权限。有关策略列表和详细信息，请参阅 IAM 控制台，网址为AWSFMMemberReadOnlyAccess。

Firewall Manager 对 AWS 托管策略的更新

查看自该服务开始跟踪这些更改以来 Firewall Manager AWS 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅 Firewall Manager 文档历史记录页面上的 RSS 源，网址为 文档历史记录。

更改	描述	日期
FMS ServiceRolePolicy — 更新政策	增加了管理网络 ACL 的权限。 在 IAM 控制台中查看更新的政策：FMS ServiceRolePolicy。	2024-04-22
FMS ServiceRolePolicy — 更新政策	添加了允许 Firewall Manager 描述指定 AWS Config 规则是否合规的权限。 在 IAM 控制台中查看更新的政策：FMS ServiceRolePolicy。	2023-04-21

更改	描述	日期
FMS ServiceRolePolicy — 更新政策	添加了允许 Firewall Manager 描述 Amazon EC2 实例和网络接口属性的权限。 在 IAM 控制台中查看更新的政策：FMS ServiceRolePolicy。	2022-11-15
AWSFMAdminReadOnlyAccess - 更新的策略	增加了支持 AWS WAFV2、Shield、Network Firewall、DNS 防火墙、Amazon VPC 安全组、策略的权限。 在 IAM 控制台中查看更新的政策：AWSFMAdminReadOnlyAccess。	2022-11-02
AWSFMAdminFullAccess - 更新的策略	增加了支持 AWS WAFV2、Shield、Network Firewall、DNS 防火墙、Amazon VPC 安全组、策略的权限。移除了 Amazon SNS 权限。 在 IAM 控制台中查看更新的政策：AWSFMAdminFullAccess。	2022-10-21
`FMSServiceRolePolicy` — AWS Firewall Manager 第三方防火墙策略的新权限	此更改允许 Firewall Manager 创建和删除与第三方防火墙策略关联的 Amazon EC2 VPC 终端节点。	2022-03-30

更改	描述	日期
FMSServiceRolePolicy — AWS Network Firewall 策略的新权限	添加了新权限，以支持为 Network Firewall 策略部署防火墙。新权限允许为策略范围内的账户检索有关可用区的信息。	2022-02-16
FMSServiceRolePolicy — AWS Shield 策略的新权限	增加了检索 AWS WAF 区域和 AWS WAF 全球资源标签的新权限。添加了使用资源 ARN 检索网页 ACL 的 AWS WAF 区域权限。添加了权限以支持 Shield 自动应用程序层 DDoS 缓解功能。	2022-01-07
FMSServiceRolePolicy — AWS Shield 策略的新权限	添加了新权限，以检索 Elastic Load Balancing 资源的标签。	2021-11-18
FMSServiceRolePolicy — 安全组和 AWS Network Firewall 策略的新权限	添加了新的权限以启用 AWS Network Firewall 策略的集中日志记录。此外，还添加了只读 Amazon EC2 权限，以支持对 Config 服务的更改，这些更改会影响 AWS Firewall Manager 查询资源以获取安全组策略的方式。	2021-09-29
FMSServiceRolePolicy — 资源的 ARN 格式 AWS WAF	更新了 FMSServiceRolePolicy ，以实现 AWS WAF 资源 ARN 格式的标准化。更新后的 ARN 格式为 arn:aws:waf:*:*:* 和 arn:aws:waf-regional:*:*:* 。	2021-08-12

更改	描述	日期
FMSServiceRolePolicy – 中国的其他地区	AWS Firewall Manager 已FMSServiceRolePolicy 为中国的 BJS 和 ZHY 区域启用。	2021-08-12
FMSServiceRolePolicy – 对现有策略的更新	添加了允许 AWS Firewall Manager 管理 Amazon Route 53 Resolver DNS 防火墙的新权限。 此更改允许 Firewall Manager 配置 Amazon Route 53 Resolver DNS 防火墙关联。这允许您在 AWS Organizations 中使用 Firewall Manager 为整个组织中的 VPC 提供 DNS 防火墙保护。	2021-03-17
Firewall Manager 已开启跟踪更改	Firewall Manager 开始跟踪其 AWS 托管策略的更改。	2021-03-02

对 AWS Firewall Manager 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Firewall Manager 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Firewall Manager 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我的 Fire AWS 账户 wall Manager 资源

我无权在 Firewall Manager 中执行操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 fms:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 fms:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Firewall Manager。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Firewall Manager 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 Fire AWS 账户 wall Manager 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 如需了解 Firewall Manager 是否支持这些功能，请参阅 如何 AWS Shield 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。

- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

使用 Firewall Manager 的服务相关角色

AWS Firewall Manager 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Firewall Manager 直接关联的独特类型的 IAM 角色。服务相关角色由 Firewall Manager 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 Firewall Manager，因为您不必手动添加必要的权限。Firewall Manager 定义其服务相关角色的权限，除非另外定义，否则只有 Firewall Manager 可以代入该角色。定义的权限包括信任策略和权限策略。这些权限策略不能附加到任何其他 IAM 实体。

只有在先删除角色的相关资源后，才能删除服务相关角色。这将保护您的 Firewall Manager 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

Firewall Manager 的服务相关角色权限

AWS Firewall Manager 使用服务相关角色名 AWSServiceRoleForFMS 允许 Firewall Manager 代表您调用 AWS 服务以管理防火墙策略和 AWS Organizations 帐户资源。此策略已附加到 AWS 托管角色`AWSServiceRoleForFMS`。有关托管策略的更多信息，请参阅 AWS 托管策略：`FMSServiceRolePolicy`。

与 AWSServiceRoleForFMS 服务相关的角色信任服务来代替 角色`fms.amazonaws.com`。

角色权限策略允许 Firewall Manager 对指定资源完成以下操作：

- `waf`-管理账户中的 AWS WAF 经典 Web ACL、规则组权限和网页 ACL 关联。
- `ec2` - 管理弹性网络接口和 Amazon EC2 实例上的安全组。管理 Amazon VPC 子网上的网络 ACL。
- `vpc` - 管理 Amazon VPC 中的子网、路由表、标签和终端节点。
- `wafv2`-管理您账户中的 AWS WAF 网页 ACL、规则组权限和网页 ACL 关联。

- `cloudfront`-创建 Web ACL 以保护 CloudFront 发行版。
- `config`-在您的账户中管理防火墙管理器拥有的 AWS Config 规则。
- `iam`-管理此服务相关角色，如果配置日志记录 AWS WAF 和 Shield 策略，则创建必需角色和 AWS WAF Shield 服务相关角色。
- `organization`-创建由 Firewall Manager 拥有的服务相关角色来管理防火墙管理器使用的 AWS Organizations 资源。
- `shield`-管理您账户中资源的 AWS Shield 保护和 L7 缓解配置。
- `ram`-管理 DNS 防火墙规则组和 Network Firewall 规则组的 AWS RAM 资源共享。
- `network-firewall`-管理您的账户中防火墙管理器拥有的 AWS Network Firewall 资源和相关的 Amazon VPC 资源。
- `route53resolver` - 管理账户中 Firewall Manager 拥有的 DNS 防火墙关联。

在 IAM 控制台中查看完整策略：FMS ServiceRolePolicy。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Firewall Manager 创建服务相关角色

您无需手动创建服务相关角色。当你在上启用 Firewall Manager 登录时 AWS Management Console，或者在防火墙管理器 CLI 或 Firewall Manager API 中`PutLoggingConfiguration`提出请求时，Firewall Manager 会为你创建服务相关角色。

您必须具有 `iam:CreateServiceLinkedRole` 权限以启用日志记录。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您启用 Firewall Manager 日志记录时，Firewall Manager 再次为您创建服务相关角色。

编辑 Firewall Manager 的服务相关角色

Firewall Manager 不允许您编辑 AWSServiceRoleForFMS 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 Firewall Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时 Firewall Manager 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForFMS服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

Firewall Manager 服务相关角色支持的区域

Firewall Manager 支持在服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 Firewall Manager 端点和限额。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况， AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用`aws:SourceArn`和`aws:SourceAccount`全局条件上下文密钥来限制为资源 AWS Firewall Manager 提供其他服务的权限。如果您只希望将一个资源与跨服务访问相关联，请使用 `aws:SourceArn`。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 `aws:SourceAccount`。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符字符 (*) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:fms:*:`*`account-id`*`:*`。

如果 `aws:SourceArn` 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文键来限制权限。

的值`aws:SourceArn`必须是 AWS Firewall Manager 管理员的 AWS 帐户。

以下示例演示如何在 Firewall Manager 中使用 `aws:SourceArn` 全局条件上下文键来防范混淆代理问题。

以下示例说明了如何通过使用 Firewall Manager 角色信任策略中的 aws:SourceArn 全局条件上下文键防止混淆代理问题。请将##和 *account-id* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
}
```

在 Firewall Manager 中进行日志记录和监控

监控是维护 Firewall Manager 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。您应该从 AWS 解决方案的各个部分收集监控数据，以便在出现多点故障时可以更轻松地进行调试。 AWS 提供了多种用于监控 Firewall Manager 资源和响应潜在事件的工具：

亚马逊 CloudWatch 警报

使用 CloudWatch 警报，您可以监视您指定的时间段内的单个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 AWS Auto Scaling 政策 CloudWatch 发送通知。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

AWS CloudTrail 日志

CloudTrail 提供了用户、角色或 AWS 服务在 Firewall Manager 中采取的操作的记录。使用收集的信息 CloudTrail，您可以确定向 Firewall Manager 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。有关更多信息，请参阅 使用 记录 AWS CloudTrail API 调用。

Firewall Manager 的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

Firewall Manager 中的恢复能力

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS Firewall Manager中的基础设施安全性

作为一项托管服务 AWS Firewall Manager ，受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Firewall Manager。客户端必须支持以下内容：

- 传输层安全性协议 (TLS) 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

AWS Firewall Manager 配额

AWS Firewall Manager 受以下配额（以前称为限制）的约束。

AWS Firewall Manager 有您可以增加的默认配额和固定配额。

由 Firewall Manager 管理的安全组策略和网络 ACL 策略受标准的 Amazon VPC 配额限制。有关更多信息，请参阅 Amazon VPC 用户指南中的 Amazon VPC 限额。

每个 Firewall Manager Network Firewall 策略都会创建一个Network Firewall 防火墙，其中包含相关的防火墙策略及其规则组。这些 Network Firewall 资源遵循 Network Firewall 开发人员指南中列出的 AWS Network Firewall 限额。

软限额

AWS Firewall Manager 对每个区域的实体数量有默认配额。您可以请求提高这些限额。

所有策略类型

资源	每个区域的默认限额
中每个组织的账户数 AWS Organizations	可变。发送到账户的邀请将计入此限额。如果受邀账户拒绝邀请、管理账户取消邀请或邀请过期，则撤销此计数。
AWS Organizations中每个组织的 Firewall Manager 策略数	50。区域规格 `Global` 和 `US East (N. Virginia) Region` 所指的区域相同，因此此限制适用于这两个区域的总组合策略。
每个 Firewall Manager 策略在范围内的组织单位数	20
如果您明确包含和排除个人账户，Firewall Manager 策略作用域内的账户。	200
如果您未明确包含或排除个人账户，Firewall Manager 策略作用域内的账户。	2,500
每个 Firewall Manager 策略的包含或排除资源的标签数	8
每个账户的资源集数。	20
每个资源集的资源数量。	100
每个 Firewall Manager 策略的资源集数。	5

AWS WAF 政策

资源	每个区域的默认限额
AWS WAF 每个 Firewall Manager 管理员帐户的规则组。	100
AWS WAF 每个 Firewall Manager 管理员帐户的经典规则组。	10
每个 AWS WAF 策略的规则组。	50

通用安全组策略

资源	每个区域的默认限额
每个策略的主要安全组数	3
每个账户每个策略作用域内的 Amazon VPC 实例，包括共享 VPC。	100

内容审核安全组策略

资源	每个区域的默认限额
每个策略的审核安全组。	1
每个应用程序列表的应用程序数	50
允许所有流量的规则的自定义托管应用程序列表。	1
每个策略规则的自定义托管应用程序列表数。	1
每个账户的自定义托管式应用程序列表数	10
每个协议列表的协议数	5
策略中任何设置的自定义托管协议列表。	1
每个账户的自定义托管式协议列表数	10

网络 ACL 策略

资源	每个区域的默认限额
每个网络 ACL 策略的入站规则数，用于第一个或最后一个规则。例如，您可以有 5 条第一条和 0 条最后一条入站规则，或者有 2 条第一条和 3 条最后一条规则，但不能有 4 条第一条和 2 条最后一条规则。	5
每个网络 ACL 策略的出站规则数，用于第一个或最后一个规则。例如，您可以有 5 个第一个出站规则和 0 个最后一个出站规则，或者有 2 个第一个出站规则和 3 个最后一个出站规则，但不能有 4 个第一个出站规则和 2 个最后一个出站规则。	5

DNS 防火墙策略

资源	每个区域的默认限额
根据 DNS 防火墙策略，DNS 防火墙规则组。	2

硬限额

以下与之相关的每个区域的配额 AWS Firewall Manager 无法更改。

所有策略类型

资源	每个区域的限额
一个 AWS Organizations 组织中可以拥有的最大 Firewall Manager 管理员人数。必须有一个默认管理员和多达九个 Firewall Manager 管理员。	10

AWS WAF 政策

资源	每个区域的限额
一个 AWS WAF 策略中的规则组的总 Web ACL 容量单位 (WCU) 数。	5000

AWS WAF 经典策略

资源	每个区域的限额
AWS WAF 每个策略的经典规则组。	2：1 个客户创建的规则组和 1 个 AWS Marketplace 规则组。
AWS WAF 每个 Firewall Manager AWS WAF 经典规则组的经典规则。	10

安全组内容审核策略

资源	每个区域的限额
策略中任何设置的 Firewall Manager 托管应用程序列表。	1
策略中任何设置的 Firewall Manager 托管协议列表。	1

Network Firewall 策略

资源	每个区域的限额
单个策略可以自动修复的 VPC 数量。	1000
您可以为单个策略提供的 IPV4 CIDR 数量。	50

监控 AWS WAFAWS Firewall Manager、和 AWS Shield Advanced

监控是维护您的服务的可靠性、可用性和性能的重要环节。

> **Note**
>
> 有关使用 Shield Advanced 监控您的 Shield Advanced 资源和识别可能的 DDoS 事件的信息，请参阅 AWS Shield。

在开始监控这些服务时，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

下一步，通过在不同时间和不同负载条件下测量性能，在您的环境中建立正常 性能的基准。在您监控时 AWS WAF，Firewall Manager、Shield Advanced 和相关服务会存储历史监控数据，以便您可以将其与当前性能数据进行比较，识别正常性能模式和性能异常，并设计解决问题的方法。

对于 AWS WAF，您至少应监控以下项目以建立基准：

- 允许的 Web 请求数
- 阻止的 Web 请求数

主题

- 监控工具
- 使用 Amazon 进行监控 CloudWatch
- 使用 记录 AWS CloudTrail API 调用

监控工具

AWS 提供了各种可用于监视 AWS WAF 和的工具 AWS Shield Advanced。您可以配置其中的一些工具来为您执行监控任务，但其他工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动监控工具来监视 AWS WAF AWS Shield Advanced 和报告何时出现问题：

- Web ACL 流量概述仪表板 — 访问 AWS WAF 控制台中的 Web ACL 页面并打开 “流量概述” 选项卡，即可访问 Web ACL 评估的 Web 流量摘要。

  流量概述控制面板提供了在评估您的应用程序网络流量时 AWS WAF 收集的 Amazon CloudWatch 指标的近乎实时的摘要。您可以查看所有网络流量以及智能威胁缓解规则组评估的流量的摘要。

  有关更多信息，请参阅 Web ACL 流量概述控制面板 或转到控制台中的控制面板。
- A CloudWatch mazon Alarms — 在您指定的时间段内观察单个指标，并根据该指标在多个时间段内相对于给定阈值的值执行一项或多项操作。具体操作是：通知已发送到 Amazon Simple Notification Service（Amazon SNS）主题或 Amazon EC2 Auto Scaling 策略。警报仅针对持续的状态变化调用操作。 CloudWatch 警报不会仅仅因为处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关更多信息，请参阅使用监控 CloudFront活动 CloudWatch。

  > **Note**
  >
  > CloudWatch 未为启用指标和警报 AWS Firewall Manager。

  您不仅可以像中所述的那样使用 CloudWatch 监控 AWS WAF 和屏蔽高级指标使用 Amazon 进行监控 CloudWatch，还应该使用 CloudWatch 来监控受保护资源的活动。有关更多信息，请参阅下列内容：
  - 在 Amazon CloudFront 开发者指南 CloudWatch中@@ 使用监控 CloudFront 活动
  - API Gateway 开发人员指南中的Amazon API Gateway 中的日志记录和监控
  - CloudWatch 《E lastic Load Balancing 用户指南》中应用程序负载均衡器的指标
  - AWS AppSync 开发人员指南中的监控和日志记录
  - Amazon Cognito 开发人员指南中的在 Amazon Cognito 中进行日志记录和监控
  - 查看流到日志的 App Runner CloudWatch 日志和查看AWS App Runner 开发者指南 CloudWatch中报告的 App Runner 服务指标

- Amazon CloudWatch Logs — 监控、存储和访问来自 AWS CloudTrail 或其他来源的日志文件。有关更多信息，请参阅什么是 Amazon CloudWatch 日志？ 。
- Amazon CloudWatch Events — 自动化您的 AWS 服务并自动响应系统事件。来自 AWS 服务的事 CloudWatch 件以近乎实时的方式传递到事件，您可以指定当事件与您编写的规则匹配时要采取的自动操作。有关更多信息，请参阅什么是 Amazon CloudWatch 活动？
- AWS CloudTrail 日志监控-在账户之间共享日志文件，通过将 CloudTrail 日志文件发送到 “日志” 来实时监控 CloudWatch 日志文件，用 Java 编写日志处理应用程序，并验证您的日志文件在传送后是否未更改。 CloudTrail有关更多信息，请参阅使用 记录 AWS CloudTrail API 调用《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 日志文件”。
- AWS Config— 查看您 AWS 账户中 AWS 资源的配置，包括资源之间的关联方式以及它们过去的配置方式，以便您可以看到配置和关系如何随着时间的推移而发生变化。

手动监控工具

监控 AWS WAF 的另一个重要部分 AWS Shield Advanced 涉及手动监视 CloudWatch 警报未涵盖的项目。您可以查看 AWS WAF、Shield Advanced 和其他 AWS Management Console 仪表板以查看您的 AWS 环境状态。 CloudWatch建议您还要查看 Web ACL 和规则的日志文件。

- 例如，要查看 AWS WAF 控制面板，请执行以下操作：
  - 在 AWS WAF Web ACL 页面的请求选项卡上，查看与您创建的每条规则相匹配的请求总数和请求总数的图表。有关更多信息，请参阅 查看 Web 请求示例。
- 查看以下内容的 CloudWatch 主页：
  - 当前告警和状态
  - 告警和资源图表
  - 服务运行状况

  此外，您还可以使用 CloudWatch 执行以下操作：
  - 创建自定义控制面板以监控您关注的服务。
  - 绘制指标数据图，以排除问题并弄清楚趋势。
  - 搜索并浏览您的所有 AWS 资源指标。
  - 创建和编辑告警接收有关问题的通知。

使用 Amazon 进行监控 CloudWatch

您可以使用 Amazon 监控网络请求、Web ACL 和规则 CloudWatch，Amazon 会收集原始数据，AWS WAF 并将其处理 AWS Shield Advanced 为可读的、近乎实时的指标。您可以使用 Amazon 中的统计数据 CloudWatch 来了解您的 Web 应用程序或服务的性能。有关更多信息，请参阅《Amazon CloudWatch 用户指南》 CloudWatch中的内容。

> **Note**
>
> CloudWatch 未为 Firewall Manager 启用指标和警报。

您可以创建一个 Amazon CloudWatch 警报，当警报状态发生变化时，该警报会发送 Amazon SNS 消息。警报会监控某个指标在一定时间段 (由您指定) 的变化情况，并根据相对于指定阈值的指标值每隔若干个时间段执行一项或多项操作。操作是一个发送到 Amazon SNS 主题或自动扩缩策略的通知。警报仅针对持续的状态变化调用操作。 CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。

主题

- 查看 指标和维度
- AWS WAF 指标和维度
- AWS Shield Advanced 指标
- AWS Firewall Manager 通知

查看 指标和维度

指标首先按服务命名空间分组，然后按每个命名空间内的各种维度组合进行分组。 AWS Firewall Manager 不记录指标。

- AWS WAF 命名空间是 `AWS/WAFV2`
- Shield Advanced 命名空间是 `AWS/DDoSProtection`

> **Note**
>
> AWS WAF 每分钟报告一次指标。

Shield Advanced 在活动期间每分钟报告一次指标，其他时间则不那么频繁。

使用以下过程查看 AWS WAF 和的指标 AWS Shield Advanced。

使用 CloudWatch 控制台查看指标

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 如有必要，请将区域更改为 AWS 资源所在的区域。对于 CloudFront，请选择美国东部（弗吉尼亚北部）区域。
3. 在导航窗格的指标下，选择所有指标，然后在浏览选项卡下搜索该服务。

使用 AWS CLI 查看指标

- 对于 AWS/WAFV2，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

对于 Shield Advanced，在命令提示符处使用以下命令：

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF 指标和维度

AWS WAF 每分钟报告一次指标。 AWS WAF 在AWS/WAFV2命名空间中提供指标和维度。

您可以通过 AWS WAF 控制台在 Web ACL 的流量概述选项卡中查看 AWS WAF 指标的摘要信息。有关更多信息，请转到控制台或参见Web ACL 流量概述控制面板。

您可以查看 Web ACL、规则、规则组和标签的以下指标。

- 您的规则-指标按规则操作分组。例如，当您在Count模式下测试规则时，其匹配项将列为 Web ACL 的Count指标。
- 您的规则组-规则组的指标列在规则组指标下。

- 其他账户拥有的规则组-规则组指标通常仅对规则组所有者可见。但是，如果您覆盖规则的规则操作，则该规则的指标将列在您的 Web ACL 指标下。此外，任何规则组添加的标签都会列在您的 Web ACL 指标中

  此类别中的规则组是其他账户与您共享的AWS 的托管规则 AWS WAFAWS Marketplace 托管规则组其他服务提供的规则组、、和规则组。
- 标签-评估期间添加到 Web 请求的标签列在 Web ACL 标签指标中。您可以访问所有标签的指标，无论它们是由您的规则和规则组添加的，还是由其他账户拥有的规则组中的规则添加的。

主题

Web ACL、规则组、规则指标和维度

Web ACL、规则组和规则指标

指标	描述
`AllowedRequests`	允许的 Web 请求数。 报告标准：有非零值。 有效统计数据：Sum
`BlockedRequests`	阻止的 Web 请求数。 报告标准：有非零值。 有效统计数据：Sum
`CountedRequests`	计数的 Web 请求数。 报告标准：有非零值。 已计数的 Web 请求是至少匹配了一个规则的请求。请求计数通常用于测试。

指标	描述
	有效统计数据：Sum
CaptchaRequests	应用了验证码控制的网络请求数量。 报告标准：有非零值。 验证码 Web 请求是指与具有 CAPTCHA 操作设置的规则相匹配的请求。此指标记录所有匹配的请求，无论它们是否具有有效的验证码令牌。 有效统计数据：Sum
RequestsWithValidCaptchaToken	应用了验证码控件且验证码令牌有效的 Web 请求数量。 报告标准：有非零值。 有效统计数据：Sum
CaptchasAttempted	最终用户为响应验证码拼图挑战而提交的解决方案数量。 报告标准：有非零值。 有效统计数据：Sum
CaptchasSolved	已提交的成功完成的验证码拼图解决方案的数量。 报告标准：有非零值。 有效统计数据：Sum

指标	描述
ChallengeRequests	应用了质询控件的 Web 请求数量。 报告标准：有非零值。 质询 Web 请求是指与具有 Challenge 操作设置的规则相匹配的请求。此指标记录所有匹配的请求，无论它们是否具有有效的质询令牌。 有效统计数据：Sum
RequestsWithValidChallengeToken	应用了质询控件且质询令牌有效的 Web 请求数量。 报告标准：有非零值。 有效统计数据：Sum
PassedRequests	已通过的请求数。这仅用于通过规则组评估但不匹配任何规则组规则的请求。 报告标准：有非零值。 传递的请求是指不符合规则组中任何规则的请求。 有效统计数据：Sum

Web ACL、规则组和规则维度

维度	描述
Region	除 Amazon CloudFront 分配以外的所有受保护资源类型均为必填项。
Rule	下列情况之一： • Rule 的指标名称。 • ALL，表示 WebACL 或 RuleGroup 中的所有规则。

维度	描述
	• Default_Action （仅当与 WebACL 维度结合使用时），表示分配给未因 Web ACL 中规则的操作而终止评估的任何请求的操作。
RuleGroup	RuleGroup 的指标名称。
WebACL	WebACL 的指标名称。
Country	请求的源国家/地区。这是国际标准化组织 (ISO) 3166 标准中的双字符名称。例如，US 代表美国，UA 代表乌克兰。 如果请求有 X-Forwarded-For 标头，则 AWS WAF 使用该标头来确定此设置。否则， AWS WAF 使用客户端 IP 所在的国家/地区。此决定与您在规则中用于确定原产国的任何逻辑无关。 AWS WAF 使用 MaxMind GeoIP 数据库确定 IP 的位置。
Attack	根据您在 Web ACL 中使用的规则和规则组，在请求中 AWS WAF 识别的攻击类型。 您的规则和基准 AWS 托管规则组中的规则可以识别攻击类型。例如，跨站脚本攻击（XSS）规则匹配标识 XSS 攻击类型，基于速率的规则识别容量攻击类型。攻击类型通常表示终止 Web 请求评估的规则类型。
Device	发送请求的客户端的设备类型，从 Web 请求的 user-agent 标头中获取。
ManagedRuleGroup	ManagedRuleGroup 的指标名称。
ManagedRuleGroupRule	中的规则ManagedRuleGroup 已匹配。

标签指标和维度

根据您的规则和您在 Web ACL 中使用的托管规则组在评估期间向请求添加的标签的指标。有关信息，请参阅 Web 请求上的标签。

对于任何一个 Web 请求，最多可 AWS WAF 存储 100 个标签的指标。Web ACL 评估可以应用 100 多个标签，并与 100 多个标签进行匹配，但只有前 100 个标签会反映在指标中。

标签指标

指标	描述
AllowedRequests	Allow 应用了操作设置的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
BlockedRequests	Block 应用了操作设置的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
CountedRequests	具有 Count 操作设置的规则组规则向 Web 请求添加的标签数量。 此指标仅适用于规则组的所有者，适用于规则组内的规则。对于其他情况，计数标签指标会汇总到应用于请求的终止操作中，例如 Allow 或 Block。 报告标准：有非零值。 有效统计数据：Sum
CaptchaRequests	已应用终止 CAPTCHA 操作的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。

指标	描述
	有效统计数据：Sum
ChallengeRequests	已应用终止 Challenge 操作的 Web 请求上的标签数量。在 Web 请求评估期间，可以随时添加标签。 报告标准：有非零值。 有效统计数据：Sum
AllowRuleMatch	生成关联标签并通过Allow操作终止请求评估的匹配规则的数量。 报告标准：有非零值。 有效统计数据：Sum
BlockRuleMatch	生成关联标签并通过Block操作终止请求评估的匹配规则的数量。 报告标准：有非零值。 有效统计数据：Sum
CountRuleMatch	生成关联标签并应用Count操作的匹配规则的数量。 如果使用相同的标签和操作配置了多个规则，则一个请求可能会导致该指标的多个实例。 报告标准：有非零值。 有效统计数据：Sum
CaptchaRuleMatch	生成关联标签并通过CAPTCHA操作终止请求评估的匹配规则的数量。 报告标准：有非零值。 有效统计数据：Sum

指标	描述
ChallengeRuleMatch	生成关联标签并通过Challenge操作终止请求评估的匹配规则的数量。 报告标准：有非零值。 有效统计数据：Sum
CaptchaRuleMatchWithValidToken	生成关联标签并应用非终止操作CAPTCHA的匹配规则的数量。 如果使用相同的标签和操作配置了多个规则，则一个请求可能会导致该指标的多个实例。 报告标准：有非零值。 有效统计数据：Sum
ChallengeRuleMatchWithValidToken	生成关联标签并应用非终止操作Challenge的匹配规则的数量。 如果使用相同的标签和操作配置了多个规则，则一个请求可能会导致该指标的多个实例。 报告标准：有非零值。 有效统计数据：Sum

标签维度

维度	描述
Region	除 Amazon CloudFront 分配以外的所有受保护资源类型均为必填项。
WebACL	WebACL 的指标名称。
RuleGroup	RuleGroup 的指标名称。用于指标 CountedRequests

维度	描述
LabelNamespace	添加到请求中的标签的命名空间前缀。
Label	添加到请求中的标签的名称。
Context	作为标签添加上下文的托管规则组。例如，令牌管理标签的上下文，例如awswaf:managed:token:accepted 对请求使用令牌管理的 AWS WAF 托管规则组，例如 Bot Control 或 ATP 托管规则组。该维度不适用于所有标签。

免费机器人可见性指标和维度

如果您不在 Web ACL 中使用 Bot Control，则无需支付额外费用即可将 Bot Control 托管规则组 AWS WAF 应用于您的 Web 请求样本。这可以让您了解流向受保护资源的机器人流量。有关机器人控制功能的详细信息，请参阅 AWS WAF 机器人控制规则组。

免费机器人可见度指标

指标	描述
SampleAllowedRequest	已执行Allow操作的抽样请求数。 报告标准：有非零值。 有效统计数据：Sum
SampleBlockedRequest	已执行Block操作的抽样请求数。 报告标准：有非零值。 有效统计数据：Sum
SampleCaptchaRequest	已执行CAPTCHA操作的抽样请求数。 报告标准：有非零值。 有效统计数据：Sum
SampleChallengeRequest	已执行Challenge操作的抽样请求数。

指标	描述
	报告标准：有非零值。 有效统计数据：Sum
SampleCountRequest	已执行Count操作的抽样请求数。 报告标准：有非零值。 有效统计数据：Sum

免费机器人可见度维度

维度	描述
Region	除 Amazon CloudFront 分配以外的所有受保护资源类型均为必填项。
WebACL	WebACL 的指标名称。
BotCategory	检测到的机器人类别的名称，基于网络请求标签。
VerificationStatus	检测到的机器人验证状态的名称，基于网络请求标签。
Signal	检测到的机器人信号的名称，基于网络请求标签。

AWS Shield Advanced 指标

Shield Advanced 会发布其保护的所有资源的亚马逊 CloudWatch 检测、缓解和主要贡献者指标。这些指标使您可以为资源创建和配置 CloudWatch 仪表板和警报，从而提高您监控资源的能力。

Shield Advanced 控制台提供了其记录的许多指标的摘要。有关信息，请参阅 对 DDoS 事件的可见性。

如果您为应用层保护启用自动应用层 DDoS 缓解，

指标报告位置

Shield Advanced 报告的美国东部（弗吉尼亚州北部）区域 us-east-1 的指标如下：

- 全球服务亚马逊 CloudFront 和亚马逊 Route 53。
- 保护组 有关保护组的信息，请参阅 AWS Shield Advanced 保护小组。

对于其他资源类型，Shield Advanced 会报告资源所在区域的指标。

指标报告的时间

CloudWatch 在 DDoS 事件期间，Shield Advanced 向亚马逊报告 AWS 资源指标的频率要高于没有事件发生时的频率。Shield Advanced 在活动期间每分钟报告一次指标，然后在活动结束后立即报告一次。

在没有事件的情况下，Shield Advanced 会每天报告一次分配给指定资源的指标。此定期报告可保持指标处于活动状态，可在自定义 CloudWatch 警报和仪表板中使用。

警报建议

我们建议您创建警报，以通知您需要注意的情况。首先，您可以为每个受保护的资源创建一个警报，在DDoSDetected检测指标不为零时进行报告。此指标中的非零值并不一定表示正在进行 DDoS 攻击，但我们建议在指标处于此状态时仔细查看资源状态。

对于请求泛洪，我们建议您为综合检查创建警报，同时考虑应用程序运行状况和 Web 请求量等因素。您可以选择对报告不同攻击向量维度的流量的其他三个指标发出警报。通过考虑应用程序的容量并在流量接近应用程序限制时发出警报，您可以创建一组规则，在需要时通知您，而不会产生太多不必要的噪音。

主题

检测指标

Shield Advanced 提供AWS/DDoSProtection命名空间中的指标和维度。

检测指标

指标	描述
DDoSDetected	指示特定 Amazon 资源名称 (ARN) 的 DDoS 事件是否正在进行中。

指标	描述
	在事件发生期间，此指标的值为非零。
DDoSAttackBitsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的位数。该指标仅适用于网络层和传输层（第 3 层和第 4 层）DDoS 事件。 在事件发生期间，此指标的值为非零。 单位：位
DDoSAttackPacketsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的数据包数。该指标仅适用于网络层和传输层（第 3 层和第 4 层）DDoS 事件。 在事件发生期间，此指标的值为非零。 单位：数据包
DDoSAttackRequestsPerSecond	特定 Amazon 资源名称 (ARN) 的 DDoS 事件期间观察到的请求数。该指标仅适用于第 7 层 DDoS 事件。仅针对最重要的第 7 层事件报告指标。 在事件发生期间，此指标的值为非零。 单位：请求

Shield Advanced 发布不具有其他维度的 DDoSDetected 指标。其余的检测指标包括以下列表中与攻击类型相对应的 AttackVector 维度：

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection

- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood
- UDPFragment
- UDPTraffic
- UDPReflection

缓解指标

Shield Advanced 在AWS/DDoSProtection命名空间中提供指标和维度。

缓解指标

指标	描述
VolumePacketsPerSecond	为响应检测到的事件而部署的缓解措施每秒丢弃或通过的数据包数量。 单位：数据包

缓解维度

维度	描述
ResourceArn	Amazon 资源名称 (ARN)
MitigationAction	应用缓解措施的结果。可能的值为 Pass 或 Drop。

排名靠前的贡献者指标

Shield Advanced 在AWS/DDoSProtection命名空间中提供指标。

排名靠前的贡献者指标

指标	描述
VolumePacketsPerSecond	排名靠前的贡献者的每秒数据包数。 单位：数据包
VolumeBitsPerSecond	排名靠前的贡献者的每秒比特数。 单位：位

Shield Advanced 按代表事件贡献者的维度组合发布排名靠前的贡献者的指标。您能够将以下维度组合作为排名靠前的贡献者的指标使用：

- ResourceArn, Protocol
- ResourceArn, Protocol, SourcePort
- ResourceArn, Protocol, DestinationPort
- ResourceArn, Protocol, SourceIp
- ResourceArn, Protocol, SourceAsn
- ResourceArn, TcpFlags

排名靠前的贡献者维度

维度	描述
ResourceArn	Amazon 资源名称（ARN）。
Protocol	IP 协议名称，TCP 或 UDP。
SourcePort	源 TCP 或 UDP 端口。
DestinationPort	目标 TCP 或 UDP 端口。
SourceIp	源 IP 地址
SourceAsn	源自治系统号（ASN）。

维度	描述
TcpFlags	TCP 数据包中存在的标志组合，用短划线 (-) 分隔。受监控的标志是 ACK、FIN、RST、SYN。此维度值始终按字母顺序显示。例如：ACK-FIN-RST-SYN、ACK-SYN 和 FIN-RST。

AWS Firewall Manager 通知

AWS Firewall Manager 不记录指标，因此您无法专门为 Firewall Manager 创建亚马逊 CloudWatch 警报。但是，您可以配置 Amazon SNS 通知以提醒您有潜在攻击。要在 Firewall Manager 中创建 Amazon SNS 通知，请参阅 步骤 4：配置亚马逊 SNS 通知和亚马逊警报 CloudWatch 。

使用 记录 AWS CloudTrail API 调用

AWS WAF AWS Shield Advanced、并 AWS Firewall Manager 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务所采取的操作的记录。 CloudTrail 将这些服务的 API 调用子集捕获为事件，包括来自、Shield Advanced 或 Firewall Manager 控制台的调用，以及对 Shield Advanced 或 Firewall Manager API 的代码调用。 AWS WAF AWS WAF如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 Shield Advanced 或 Firewall Manager 的事件。 AWS WAF如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集到的信息 CloudTrail，您可以确定向这些服务发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，包括如何配置和启用它，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当支持的事件活动发生在 AWS WAF、Shield Advanced 或 Firewall Manager 中时，该活动将与其他 AWS 服务 CloudTrail事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的事件 AWS 账户，包括 Shield Advanced 或 AWS WAF Firewall Manager 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。在控制台创建跟踪时，跟踪默认应用于所有区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪概述

- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

AWS WAF 信息在 AWS CloudTrail

所有 AWS WAF 操作均由《API 参考》记录 AWS CloudTrail 并记录在《AWS WAF API 参考》中。例如，调用ListWebACLUpdateWebACL、并在 CloudTrail 日志文件中DeleteWebACL生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是否使用根用户凭证发出。
- 请求是使用角色还是联合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用户身份元素。

示例： AWS WAF 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 AWS CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

以下是 AWS WAF Web ACL 操作的 CloudTrail 日志条目示例。

示例：的 CloudTrail 日志条目 CreateWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
```

```
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


示例：的 CloudTrail 日志条目 GetWebACL


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
```

```
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


示例：的 CloudTrail 日志条目 UpdateWebACL


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
```

```
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

示例：的 CloudTrail 日志条目 `DeleteWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
```

```
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

示例： AWS WAF 经典日志文件条目

AWS WAF 经典版是的先前版本 AWS WAF。有关信息，请参阅 AWS WAF 经典。

日志条目演示了 `CreateRule`、`GetRule`、`UpdateRule` 和 `DeleteRule` 操作：

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
```

```
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-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-east-1",
      "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-east-1",
    "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-east-1",
      "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"
    }
  ]
}
```


AWS Shield Advanced 信息在 CloudTrail

AWS Shield Advanced 支持将以下操作作为事件记录在 CloudTrail 日志文件中：

- ListAttacks
- DescribeAttack
- CreateProtection

- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是否使用根用户凭证发出。
- 请求是使用角色还是联合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 用户身份元素。

示例：Shield Advanced 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序出现。

以下示例显示了一个演示`DeleteProtection`和`ListProtections`操作的 CloudTrail 日志条目。

```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
   "eventTime": "2018-01-10T21:31:14Z",
   "eventSource": "shield.amazonaws.com",
```

```
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "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-east-1",
    "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": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```


AWS Firewall Manager 信息在 CloudTrail

AWS Firewall Manager 支持将以下操作作为事件记录在 CloudTrail 日志文件中：

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是否使用根用户凭证发出。
- 请求是使用角色还是联合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 用户身份元素。

示例：Firewall Manager 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示 `GetAdminAccount-->` 操作的 CloudTrail 日志条目。

```
{
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
```

```
                                "principalId": "123456789098765432123",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                               },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

使用 AWS WAF 和 AWS Shield Advanced API

本节介绍如何向 AWS WAF 和 Shield Advanced API 发出请求，以便在中创建和管理匹配集、规则和网页 ACL， AWS WAF 以及您在 Shield Advanced 中的订阅和保护。在本部分中，您将了解请求的组成部分、响应的内容以及如何验证请求。

主题

使用 AWS 软件开发工具包

如果您使用的语言为 AWS 提供 SDK，请使用 SDK，而不是尝试使用 API。这些软件开发工具包简化了身份验证，可轻松与您的开发环境集成，并提供对 Shield Advanced 命令的轻松访问。 AWS WAF 有关 AWS 软件开发工具包的更多信息，请参阅主题下载工具设置您的账户以使用服务中的。

向 AWS WAF 或 Shield Advanced 发出HTTPS请求

AWS WAF 而且 Shield Advanced 请求是 HTTPS 请求，如 RFC 26 16 所定义。与任何 HTTP 请求一样，对 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 而且 Shield Advanced 要求在 HTTP 请求的标头中包含以下信息：

Host（必需）

指定资源创建位置的终端节点。有关端点的信息，请参阅AWS 服务端点。例如， CloudFront 分配的标Host题 AWS WAF 的值为waf.amazonaws.com:443。

x-amz-date 或日期（必填）

用于创建 Authorization 标头中包含的签名的日期。采用 ISO 8601 标准格式以 UTC 时间指定日期，如以下示例所示：

```
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。) 如果存在x-amz-date标头，则在对请求进行身份验证时 AWS WAF 会忽略任何Date标头。

时间戳必须在收到请求的 AWS 系统时间的 15 分钟以内。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。

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：POST 请求时为必填项。

Content-Length（条件性）

符合 RFC 2616 的消息的长度（不带标头）。

条件：必需，如果请求主体本身包含信息（大多数工具包自动添加此标题）。

以下示例为在 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 and 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，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

由 AWS WAF 或 Shield Advanced 创建的用于唯一标识您的请求的值，例如，K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG。如果您有问题 AWS WAF， AWS 可以使用此值来解决问题。

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

Date

AWS WAF 或 Shield Advanced 回复的日期和时间，例如，格林威治标准时间 2015 年 10 月 7 日星期三 12:00:00。

类型：字符串

错误响应

如果请求导致错误，HTTP 响应将包含以下值：

- 作为响应正文的 JSON 错误文档
- Content-Type
- 合适的 3xx、4xx 或 5xx HTTP 状态代码

下面是 JSON 错误文档的示例：

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

对请求进行身份验证

如果您使用的语言为 AWS 提供 SDK，我们建议您使用 SDK。与使用 AWS WAF 或 Shield Advanced API 相比，所有 AWS 软件开发工具包都极大地简化了签署请求的过程，并为您节省了大量时间。此外，开发工具包还可轻松与您的开发环境集成，并可让您轻松访问相关命令。

AWS WAF 而且 Shield Advanced 要求您通过签署请求来验证您发送的每个请求。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 会使用您签署请求时使用的相同哈希函数和输入重新计算签名。如果生成的签名与请求中的签名相匹配， AWS WAF 或者 Shield Advanced 会处理该请求。如果不匹配，则拒绝请求。

AWS WAF 而且 Shield Advanced 支持使用AWS 签名版本 4 进行身份验证。计算签名的过程可分为三个任务：

任务 1：创建规范请求

按照https://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html中的 Amazon Web Services 一般参考任务 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凭证范围字符串来创建一系列 HMAC 散列消息认证码 (HMAC)。

相关信息

下列相关资源在您使用此服务的过程中会有所帮助。

以下资源可用于 AWS WAF AWS Shield Advanced、和 AWS Firewall Manager。

- 实施指南 AWS WAF — 技术出版物，其中包含最新的实施建议 AWS WAF ，以保护现有和新的 Web 应用程序。
- AWS 讨论论坛 — 一个基于社区的论坛，用于讨论与该 AWS 服务和其他服务相关的技术问题。
- AWS WAF 讨论论坛 — 一个基于社区的论坛，供开发人员讨论与之相关的技术问题 AWS WAF。
- 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 — 有关信息（包括功能 AWS WAF、定价等）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。

以下资源可用于 Amazon Web Services。

- 课程和研讨会 — 指向基于角色的课程和专业课程的链接，以及自定进度的实验室，可帮助您提高 AWS 技能并获得实践经验。
- AWS 开发者中心 — 浏览教程、下载工具并了解 AWS 开发者活动。
- AWS 开发者工具-指向开发者工具、SDK、IDE 工具包和命令行工具的链接，用于开发和管理 AWS 应用程序。
- 入门资源中心 — 了解如何设置你的 AWS 账户、加入 AWS 社区和启动你的第一个应用程序。
- 动手教 step-by-step 程 — 按照教程启动您的第一个应用程序 AWS。
- AWS 白皮书 — 由 AWS 解决方案架构师或其他技术专家撰写的技术 AWS 白皮书完整列表的链接，这些白皮书涵盖架构、安全和经济学等主题。
- AWS Support 中心 — 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，例如论坛、技术常见问题解答、服务运行状况和 AWS Trusted Advisor。
- AWS Support— 提供有关 AWS Support快速响应支持渠道信息的主要网页 one-on-one，该渠道可帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关 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、您的帐户、许可证和网站访问权限以及其他主题的详细信息。

文档历史记录

本页列出了本文档的重大更改。

服务功能有时会逐步推广到提供服务的 AWS 区域。我们仅在第一次发布时更新了此文档。我们不提供有关区域可用性的信息，也不会宣布后续区域支持情况。有关服务功能的区域可用性以及订阅更新通知的信息，请参阅新增内容 AWS？ 。

变更	说明	日期
更新了的 AWS 托管规则 AWS WAF	Bot Control、ATP 和 ACFP 托管规则组现已版本化，将与其他版本化托管规则一样，提供版本更新的 SNS 通知。 AWS	2024年5月29日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新 POSIX 操作系统规则组的托管规则，`AWSManagedRulesUnixRuleSet` 。	2024年5月28日
CAPTCHA和Challenge行动	添加了关于浏览器客户端需要 HTTPS 才能运行 CAPTCHA 谜题和静默挑战的说明。	2024年5月24日
与 Amazon 安全湖集成	现在，您可以使用 Security Lake 收集 Web ACL 流量数据。有关信息，请参阅 Amazon Security Lake 用户指南中的从 AWS 服务收集数据。	2024年5月22日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2024年5月21日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新的 SQLi 数据库规则组的托管规则。	2024 年 5 月 14 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新已知错误输入和 POSIX 操作系统规则组的托管规则。	2024 年 5 月 8 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新的 Windows 操作系统规则组的托管规则。	2024 年 5 月 3 日
AWS WAF 移动 SDK 安卓 Kotlin 代码示例	为基于 Kotlin 的安卓集成添加了示例代码。	2024年5月2日
AWS WAF 指标添加了维度和新指标	AWS WAF 为规则`ManagedRuleSetRule` 内指标添加了新维度，为标签指标的匹配规则操作添加了新指标。	2024年5月2日
AWS Firewall Manager 支持网络 ACL 策略	Firewall Manager 现在支持通过防火墙管理器网络 ACL 策略管理 Amazon VPC 网络访问控制列表 (ACL)。	2024 年 4 月 25 日
AWS Firewall Manager 安全策略更新	更新`FMSServiceRolePolicy` 以添加管理网络 ACL 的权限。	2024 年 4 月 22 日
更新了运行状况检查指标列表	我们从健康检查中常用的指标列表中删除了一些指标。	2024 年 4 月 16 日
Firewall Manager 安全组策略的更新	我们更新了使用情况审计安全组政策并改进了文档。请参阅使用情况审计政策部分以及有关最佳做法和限制的部分。	2024 年 4 月 2 日
更新了机器人控制示例	添加了描述目标检查级别的示例，并更新了现有示例以反映最佳实践。	2024 年 3 月 27 日

更新了 ATP 示例	添加了描述响应检查配置的示例，并更新了现有示例以反映最佳实践。	2024 年 3 月 27 日
更新了 ACFP 示例	添加了描述响应检查配置的示例。	2024 年 3 月 27 日
更新 Amazon CloudWatch 日志流限制	AWS WAF 不再对将日志发布到 CloudWatch 日志流设置每个 Web 的 ACL 限制。	2024 年 3 月 27 日
AWS Shield Advanced 应用层（第 7 层）保护	更新了应用层检测和缓解、Web ACL 使用、基于速率的规则和自动应用层 DDoS 缓解的一般和最佳实践指南。	2024 年 3 月 14 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新的 IP 信誉规则组的托管规则。	2024 年 3 月 13 日
车身检查尺寸限制的变更	AWS WAF 现在支持对某些区域资源实行更大的机构检查规模限制。	2024 年 3 月 7 日
AWS WAF 基于费率的规则的可配置评估窗口	现在，您可以将基于速率的规则用于计算请求的时间窗口配置为 1、2、5 或 10 分钟。默认值为 5，这是此版本之前的唯一选项。	2024年2月28日
扩展了CAPTCHA和的日志信息 Challenge	现在，顶层`captchaResponse` 和`challengeResponse` 字段中填充了要应用于请求的最后一个操作，无论是终止请求还是非终止请求。在此之前，这些字段仅用于终止操作。	2024年2月22日

JavaScript 验证码 API 密钥管理	现在，你可以通过 API 删除 CAPTCHA JS API 密钥。AWS WAF	2024年2月6日
AWS WAF 验证码拼图音频	验证码拼图的音频版本现在支持多种语言。	2024年2月6日
AWS WAF 挑战和验证码代币标签	令牌管理现在为 CAPTCHA 令牌添加了标签，并增强了质询令牌的令牌标签。	2023 年 12 月 20 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新已知错误输入规则组的托管规则。	2023 年 12 月 16 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新已知错误输入规则组的托管规则。	2023 年 12 月 14 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 12 月 6 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则： AWS WAF 机器人控制。	2023 年 12 月 5 日
更新了 Firewall Manager AWS Config 先	如果您使用自定义 IAM 角色而不是 Firewall Manager 托管角色 AWS Config，则必须确保您的权限策略允许 AWS Config 记录器记录 Firewall Manager 资源。	2023 年 11 月 17 日
AWS WAF 控制台仪表板	我们更正了在 AWS WAF 控制台中查看 Web ACL 的所有规则和样本请求的指南。	2023 年 11 月 17 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新机器人控制规则组的托管规则。	2023 年 11 月 14 日
AWS WAF 控制台有新的 Web ACL 控制面板	AWS WAF 控制台中的 Web ACL 页面上有新的 Web 流量概述仪表板。	2023 年 11 月 14 日
更新了 ATP 托管规则组	更正了规则 `VolumetricIpFailedLoginResponseHigh` 和 `VolumetricSessionFailedLoginResponseHigh` 的标签信息。	2023 年 11 月 13 日
更新了 ACFP 托管规则组	更正了规则 `VolumetricIPSuccessfulResponse` 和 `VolumetricSessionSuccessfulResponse` 的标签信息。	2023 年 11 月 13 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 11 月 2 日
Shield Advanced 应用程序层 DDoS 自动缓解	Shield Advanced 现在在自动缓解规则组中维护基于速率的规则，该规则限制了来自已知是 DDoS 攻击来源的 IP 地址的请求量。	2023 年 10 月 31 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 10 月 30 日
机器人控制功能规则组移除了请求 CSP 的信号标签	机器人控制功能规则组删除了表示云服务提供商（CSP）的信号标签。	2023 年 10 月 28 日

用于请求 CSP 的机器人控制功能规则组信号标签	机器人控制功能托管规则组信号标签包括一个表示云服务提供商（CSP）的标签。	2023 年 10 月 27 日
更新了 AWS WAF IAM 权限信息	对于管理 Web ACL 关联的操作，策略操作部分现在列出了每种 Web 应用程序资源类型的权限要求。 AWS WAF	2023 年 10 月 25 日
Firewall Manager 对修改后 Web ACL 的管理	启用对未关联 Web ACL 的管理后，Firewall Manager 不会在一次性清理未使用资源时包含修改过的 Web ACL。	2023 年 10 月 19 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新 POSIX 操作系统规则组的托管规则，`AWSManagedRulesUnixRuleSet` 。	2023 年 10 月 12 日
AWS WAF 指标已添加维度	AWS WAF 添加了用于查看 Web ACL 指标的新维度。	2023 年 10 月 12 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 10 月 11 日
更新移 AWS WAF 动 SDK 规范	已将 `storeTokenInCookieStorage` 操作添加到 `WAFTokenProvider` 。	2023 年 10 月 11 日
异常部署的 AWS 托管规则 AWS WAF	AWS Managed Rule AWS WAF s 发布了两个静态版本的已知错误输入规则组，并更新了默认版本以指向最新的静态版本。	2023 年 10 月 4 日
AWS WAF HTML 实体解码文本转换	扩展了 HTML 实体解码文本转换的功能。	2023 年 10 月 4 日

在 Firewall Manager 安全组通用策略中添加了新选项	Firewall Manager 现在可以将安全组引用分配给副本安全组。	2023 年 10 月 3 日
AWS WAF 增加了对 JA3 指纹的检查	现在，您可以对 Amazon CloudFront 分配和应用程序负载均衡器的 Web 请求的 JA3 指纹进行精确匹配。	2023 年 9 月 26 日
Firewall Manager 安全组策略规则设置的更新	Firewall Manager 现在支持将安全组从主要安全组引用到副本安全组。	2023 年 9 月 25 日
更新了 Shield Advanced 应用程序层 DDoS 自动缓解措施	Firewall Manager 现在支持配置了应用程序层 DDoS 自动缓解的 Shield Advanced 策略的应用程序负载均衡器资源。	2023 年 9 月 14 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则： AWS WAF 机器人控制。	2023 年 9 月 6 日
AWS WAF 机器人控制	机器人控制功能托管规则组的定向保护级别现在会检查 IP 地址之间是否存在令牌重复使用。现在，它还提供可选的流量统计数据机器学习分析，以检测一些与机器人相关的活动。	2023 年 9 月 6 日
更新移 AWS WAF 动 SDK 规范	将 `tokenRefreshDelaySec` 的最小 300、最大 600 和默认 300 的最小值、最大值和默认值降低到最小 88、最大 300 和默认 88。	2023 年 9 月 5 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新 AWS WAF 机器人控制规则组的托管规则。	2023 年 8 月 30 日
Shield Advanced 应用程序层 DDoS 自动缓解	添加了有关使用管理 AWS CloudFormation 用于自动应用层 DDoS 缓解的 Web ACL 的指南。	2023 年 8 月 30 日
新 Firewall Manager 内容审核安全组策略选项	添加了用于审核过于宽松的规则组的新选项，并改进了控制台过程描述。	2023 年 8 月 29 日
全新 Firewall Manager Shield 和 AWS WAF 策略选项	如果您在 an AWS WAF d Shield 中启用了对未关联的 Web ACL 的管理，则只有当至少一个资源使用 Web ACL 时，Firewall Manager 才会在策略范围内的账户中创建 Web ACL。	2023 年 8 月 9 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 7 月 26 日
URI 路径上基于速率的规则聚合	现在，您可以在基于速率的规则的自定义聚合键中指定 URI 路径。	2023 年 7 月 19 日
中的新 AWS WAF策略规则选项 AWS Firewall Manager	AWS Firewall Manager 增加了对配置 AWS WAF Web 请求正文检查大小限制的支持。	2023 年 7 月 18 日

AWS WAF 托管策略变更	更新了AWSWAFFullAccessPolicy AWSWAFConsoleFullAccess 、AWSWAFReadOnlyAccess 、和，AWSWAFConsoleReadOnlyAccess 为你可以保护的资源类型添加了 AWS 经过验证的访问权限 AWS WAF。	2023 年 6 月 17 日
更新了的 AWS 托管规则 AWS WAF	AWS AWS WAF 已添加规则组的托管规则AWSManagedRulesACFPRuleSet 。	2023 年 6 月 13 日
防欺 AWS WAF 诈控制账户盗用 (ATP) 更新	现在，您可以使用正则表达式为 ATP 管理的规则组指定登录端点。	2023 年 6 月 13 日
CAPTCHA API JavaScript 的新信息	新章节介绍如何在使用验证码 AWS WAF 响应请求时提供自定义验证码拼图。	2023 年 6 月 13 日
新 ACFP 托管规则组	使用新规则组 AWSManagedRulesACFPRuleSet 来检测和阻止欺诈账户创建尝试。	2023 年 6 月 13 日
新的 AWS WAF 欺诈控制账户创建防作弊 (ACFP)	您可以使用新的 F AWS WAF raud Control 账户创建防作弊 (ACFP) 托管规则组AWSManagedRulesACFPRuleSet 来检测和阻止欺诈性账户创建尝试。借助受保护的 CloudFront 分配，您还可以使用 ACFP 阻止最近提交过多失败账户创建尝试的客户尝试创建新账户。	2023 年 6 月 13 日

AWS WAF 托管策略变更	已更新AWSWAFFullAccessPolicy AWSWAFConsoleFullAccess 、AWSWAFReadOnlyAccess 、和AWSWAFConsoleReadOnlyAccess 以更正 AWS App Runner 服务的访问设置。	2023 年 6 月 6 日
添加了对 Firewall Manager 安全组策略的限制	如果共享的 VPC 后来被取消共享，Firewall Manager 将不会删除关联账户中的副本安全组。	2023 年 6 月 2 日
新的 AWS WAF 请求组件：Header order	现在，您可以与请求中标头名称的有序列表进行匹配。	2023 年 5 月 30 日
更新了的 AWS 托管规则 AWS WAF	更新了 Linux 操作系统规则组。	2023 年 5 月 22 日
更新了 AWS WAF 规则部分的组织结构	规则语句列表现在按语句类型分组。	2023 年 5 月 16 日
已移动主题：列出受到速率限制的 IP 地址	列出受到速率限制的 IP 地址的主题现在位于基于速率的规则主题下。	2023 年 5 月 16 日
基于速率的规则的扩展选项	现在，您可以根据 IP 地址以外的聚合键对 Web 请求进行速率限制，也可以使用键组合进行聚合。您还可以对所有与范围缩小语句匹配的请求进行速率限制，而无需进一步聚合。	2023 年 5 月 16 日

Firewall Manager 限额增加	将每个组织的 Firewall Manager 策略数量 AWS Organizations 从 20 个增加到 50 个。将每个策略的主要安全组的最大数量从一个增加到三个。将 WCU 的最大数量从软限额更改为硬限额。	2023 年 5 月 5 日
添加了每个规则组的最大 WCU	现在，每个规则组最多可以使用 5,000 个 Web ACL 容量单位 (WCU)，而无需请求增加支持。此新限制无法提高。	2023 年 5 月 1 日
AWS WAF 带前缀的 Amazon S3 日志存储桶位置	AWS WAF 现在允许在 Amazon S3 日志存储桶名称中添加前缀。	2023 年 5 月 1 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2023 年 4 月 28 日
添加了对 AWS 已验证访问权限实例的支持 AWS WAF	现在，您可以将 AWS WAF Web ACL 与已验证的访问权限实例关联。此更改仅在最新版本的 CI AWS WAF assic 中可用。 AWS WAF	2023 年 4 月 28 日
修订了有关与多个 Firewall Manager 管理员合作的章节	现在，您可以指定多个 Firewall Manager 管理员来创建和管理您组织的防火墙资源。	2023 年 4 月 24 日
AWS Firewall Manager 托管策略更新	已更新 `FMSServiceRolePolicy` 。	2023 年 4 月 21 日
CAPTCHA 的新 JavaScript 客户端应用程序集成	现在，您可以自定义验证码拼图在 JavaScript 客户端应用程序中的位置和特征。	2023 年 4 月 20 日

应用程序集成已重命名为智能威胁集成	我们将客户端应用程序集成的现有功能重命名为智能威胁集成，以帮助区分该功能和新的 CAPTCHA 应用程序集成。JavaScript	2023 年 4 月 20 日
超 1,500 个 Web ACL WCU 的可变定价	在 Web ACL 中使用超过 1,500 个 Web ACL 容量单位 (WCU) 会产生额外成本，这些费用会随着Web ACL WCU 使用量的增加和减少而自动调整。Web ACL 的最大值为 5,000 个 WCU。	2023 年 4 月 11 日
添加了每个 Web ACL 的最大 WCU	现在，每个 Web ACL 最多可以使用 5,000 个 Web ACL 容量单位 (WCU)，而无需请求增加支持。此新限制无法提高。	2023 年 4 月 11 日
CloudFront Web ACL 的身体检查大小限制	对于保护 Amazon CloudFront 分发的 Web ACL，您可以将网页 ACL 配置中的身体检查大小限制提高到 64 KB。	2023 年 4 月 11 日
车身检查尺寸增加 CloudFront	Amazon CloudFront 分发的最大 AWS WAF 身体检查大小限制从 8 KB 增加到 64 KB。的默认检查大小限制 CloudFront 为 16 KB。	2023 年 4 月 11 日

中的新 AWS WAF政策规则选项 AWS Firewall Manager	AWS Firewall Manager 增加了对 AWS WAF 欺诈控制账户接管预防 (ATP) 和 AWS WAF 机器人控制 AWS 托管规则组、Amazon S3 日志目标、规则操作替代CAPTCHA和Challenge 规则操作以及令牌域列表的支持。	2023 年 4 月 7 日
Firewall Manager 支持 Amazon S3 存储桶作为日志记录目的 AWS WAF 地	现在，您可以在 AWS WAF 策略中使用 Amazon S3 存储桶作为日志目标。	2023 年 4 月 7 日
AWS WAF 托管策略变更	更新AWSWAFFullAccessPolicy 、AWSWAFConsoleFullAccess AWSWAFReadOnlyAccess 、和，AWSWAFConsoleReadOnlyAccess 以向可用来保护的资源类型添加 AWS App Runner 服务 AWS WAF。	2023 年 3 月 30 日
添加了有关在安全组策略中使用标签的警告	如果现有安全组的标签与组织的标签策略存在冲突，Firewall Manager 将不会更新现有安全组的标签或创建新的安全组。	2023 年 3 月 28 日
更新服务角色信息	更新了如何在 Firewall Manager 中使用服务角色。	2023 年 3 月 8 日

更正了有关基于速率的规则如何执行速率限制的信息	带有范围缩小语句的基于速率的规则仅限对与规则的范围缩小语句匹配的请求进行速率限制。我们说，该限制适用于对任何速率受限 IP 地址的所有请求。	2023 年 3 月 1 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新了 PHP 应用程序规则组的托管规则。	2023 年 2 月 27 日
添加了对 AWS App Runner 的支持 AWS WAF	现在，您可以将 AWS WAF Web ACL 与 AWS App Runner 服务相关联。此更改仅在最新版本的 CI AWS WAF assic 中可用。 AWS WAF	2023 年 2 月 23 日
更新了 IAM 指南 AWS Firewall Manager	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 2 月 16 日
更新了的 AWS 托管规则 AWS WAF	AWS 托管规则 AWS WAF 更新了规则组，`AWSManagedRulesATPRuleSet` 以在保护 Amazon CloudFront 分销的 Web ACL 中添加登录响应检查。	2023 年 2 月 15 日
AWS WAF 防欺诈控制账户接管 (ATP) 登录响应检查	对于受保护的 CloudFront 分配，您现在可以使用 ATP 来屏蔽最近提交过多失败登录尝试次数的客户的新登录尝试。	2023 年 2 月 15 日
更新了的 AWS 托管规则 AWS WAF	更新了核心规则集。	2023 年 1 月 25 日

智能威胁缓解的最佳实践	添加了一个章节，其中包含实施机器人控制功能、ATP 和其他智能威胁缓解功能的最佳实践。	2023 年 1 月 22 日
如何检查 HTTP/2 伪标头	添加了一个部分，关于将 HTTP/2 伪标头映射到相应的 Web 请求组件。	2023 年 1 月 20 日
更新了 C AWS WAF lassic 的 IAM 指南	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 1 月 3 日
更新了 IAM 指南 AWS WAF	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 1 月 3 日
更新了 IAM 指南 AWS Shield	更新了指南，使其符合 IAM 最佳实践。有关更多信息，请参阅 IAM 安全最佳实践。	2023 年 1 月 3 日
更新 Amazon Route 53 Resolver DNS 防火墙策略	添加了有关删除 Amazon Route 53 Resolver DNS 防火墙规则组的信息。	2022 年 12 月 29 日
更新了的 AWS 托管规则 AWS WAF	更新了 Linux 操作系统规则组。	2022 年 12 月 15 日
更新了的 AWS 托管规则 AWS WAF	更新了核心规则集。	2022 年 12 月 5 日
Firewall Manager 添加了对 Fortigate 云原生防火墙 (CNF) 即服务策略的支持	Firewall Manager 现在支持 Fortigate CNF 策略。	2022 年 12 月 2 日
删除了 DNS 防火墙策略的 AWS Config 要求	对于 DNS 防火墙策略，您现在只需要为 EC2 VPC 的资源类型启用“配置”。	2022 年 11 月 17 日

AWS Firewall Manager 托管策略更新	已更新 `FMSServiceRolePolicy` 。	2022 年 11 月 15 日
扩展 AWS WAF 验证码拼图的语言选项	验证码拼图现在提供多种语言的书面说明。每个音频拼图中的说明仍然仅以英文提供。	2022 年 11 月 11 日
资源集的 Firewall Manager 新限额	为资源集添加了新限额。	2022 年 11 月 8 日
添加对资源集的支持	您可以创建资源集以对要在 Firewall Manager 策略中管理的资源进行分组。	2022 年 11 月 8 日
添加对从 Network Firewall 导入防火墙的支持	现在，您可以使用资源集导入和管理 Network Firewall 策略中的现有防火墙。	2022 年 11 月 8 日
AWS Firewall Manager 托管策略更新	已更新 `AWSFMAdminReadOnlyAccess` 。	2022 年 11 月 2 日
地理匹配语句现在为国家和地区的请求添加标签	现在，您可以将地理匹配与标签匹配相结合以管理区域级别的地理请求来源。	2022 年 10 月 31 日
重命名顶级部分：托管保护	该部分现在被命名为 AWS WAF 智能威胁缓解，与我们的营销页面保持一致。	2022 年 10 月 27 日
机器人控制功能托管规则组中的新目标保护级别	机器人控制功能托管规则组现在额外提供定向规则，用于检测和缓解复杂机器人。此保护级别需额外付费。	2022 年 10 月 27 日
关于 AWS WAF 代币的新章节	了解如何 AWS WAF 使用令牌进行智能威胁缓解。	2022 年 10 月 27 日

添加了有关更新 Firewall Manager Network Firewall 策略的重要说明	更新 Firewall Manager 策略时，该策略创建的所有 Network Firewall 策略都将使用 Firewall Manager 策略的 Network Firewall 策略配置进行更新。	2022 年 10 月 27 日
规则组中的操作覆盖	现在，您可以将规则组中规则的操作覆盖到任何规则操作设置。与之前的 Count 操作覆盖一样，您可以将覆盖应用于规则组中的所有规则和单个规则。	2022 年 10 月 27 日
AWS WAF 新Challenge规则操作选项	您可以将规则配置为使用 Challenge，以验证请求是否由浏览器发送。	2022 年 10 月 27 日
AWS WAF 允许在多个受保护的应用程序之间共享令牌	通过为 Web ACL 配置令牌域列表，您可以允许在多个受保护的应用程序中使用令牌。	2022 年 10 月 27 日
所有标头规格不区分大小写	将所有标头的规格更改为不区分大小写。这与单个标头行为相匹配。	2022 年 10 月 26 日
AWS Firewall Manager 托管策略变更	对 `AWSFMAdminFullAccess` 的更正。	2022 年 10 月 21 日
更新了的 AWS 托管规则 AWS WAF	更新了已知错误输入规则组。	2022 年 10 月 20 日
更新了的 AWS 托管规则 AWS WAF	更新了已知错误输入规则组。	2022 年 10 月 5 日
更新移 AWS WAF 动 SDK 规范	将 `tokenRefreshDelaySec` 的默认值从 600（10 分钟）降低到 300（5 分钟）。	2022 年 9 月 30 日

更新了的 AWS 托管规则 AWS WAF	更正了本文档中为以下规则组提供的标签名称：POSIX 操作系统、PHP 应用程序、WordPress 应用程序。	2022 年 9 月 19 日
中的新 AWS WAF策略规则选项 AWS Firewall Manager	AWS Firewall Manager 现在支持 AWS WAF 策略中默认 Web 操作的自定义 Web 请求和响应。	2022 年 9 月 9 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：IP 信誉。	2022 年 8 月 30 日
AWS WAF 托管策略变更	已更新`AWSWAFFullAccessPolicy`、`AWSWAFConsoleFullAccess` `AWSWAFReadOnlyAccess`、和，`AWSWAFConsoleReadOnlyAccess` 将 Amazon Cognito 用户池添加到您可以用来保护的资源类型中。 AWS WAF	2022 年 8 月 25 日
AWS WAF 防欺诈控制账户接管 (ATP)	现在，您可以在 Amazon CloudFront 分销中使用防 AWS WAF 欺诈控制账户接管 (ATP) 功能。	2022 年 8 月 24 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2022 年 8 月 22 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则:`AWSManagedRulesATPRuleSet` .	2022 年 8 月 11 日
增加了对 Amazon Cognito 用户池的支持 AWS WAF	现在，您可以将 AWS WAF 网页 ACL 与 Amazon Cognito 用户池相关联。此更改仅在最新版本的 CI AWS WAF assic 中可用。 AWS WAF	2022 年 8 月 11 日
添加了有关版本化 AWS 托管规则规则组部署的部分	添加了记录版本化 AWS 托管规则规则组部署的新章节。本节包含有关在候选发布版本部署期间如何命名默认版本的信息。	2022 年 7 月 29 日
更新了为 Network Firewall 策略配置日志记录的要求	添加了对使用加密的 Amazon S3 存储桶作为日志记录目标的 Network Firewall 策略的要求。	2022 年 7 月 26 日
SQLi 规则语句的敏感度级别选项	现在，您可以提高 SQL 注入规则语句的敏感度。这不会改变现有语句的行为，其敏感度级别默认为 LOW。	2022 年 7 月 15 日
添加了 Network Firewall 策略配置选项	Firewall Manager 现在支持 Network Firewall 防火墙策略配置中的状态评测顺序和默认操作。	2022 年 7 月 14 日
Firewall Manager 安全组策略规则设置的更新	Firewall Manager 现在支持从主要安全组向副本安全组分配标签。	2022 年 7 月 7 日
AWS Shield 指南的更新	扩展了 Shield 指南中的信息，描述了 Shield 如何执行事件缓解。	2022 年 6 月 24 日

更新了测试和调整 AWS WAF 保护指南	测试和调整 AWS WAF 的一般指南已更新，现在已成为顶级主题。	2022 年 6 月 20 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：核心规则集 (CRS)。	2022 年 6 月 9 日
关于新 Firewall Manager 混淆代理的指南	添加了有关如何防止 Firewall Manager 出现混淆代理问题的指南。	2022 年 6 月 1 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：核心规则集 (CRS)。	2022 年 5 月 24 日
新的 AWS WAF 请求组件：Headers和 Cookies	现在，您可以检查 Web 请求中的 Cookie，也可以检查 Web 请求中的所有标头，此外还可以只检查单个标头。	2022 年 4 月 29 日
AWS WAF 处理超大正文、标头和 Cookie 请求组件	现在，您可以指定 AWS WAF 应如何处理检查这些组件的规则中的超大请求正文、标头和 Cookie。您已经创建的用于检查这些组件的规则的行为与处理超大尺寸的新 Continue 选项相匹配。	2022 年 4 月 29 日
AWS WAF 亚马逊 S3 日志策略变更	更新了 Amazon S3 日志权限策略和示例。	2022 年 4 月 12 日

Application Load Balancer 现已推出自动应用层 DDoS 缓解选项 AWS Shield Advanced	Shield Advanced 现在支持应用程序负载均衡器的应用程序层 DDoS 自动缓解，使其可用于所有应用程序层保护。您可以将 Shield Advanced 配置为自动计数或阻止应用程序层 DDoS 攻击中针对受保护资源的 Web 请求。	2022 年 4 月 8 日
为托管规则组添加了当前默认版本设置的指示器	托管规则组版本列表现在会显示当前的默认版本。	2022 年 4 月 8 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则： AWS WAF 机器人控制。	2022 年 4 月 6 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2022 年 3 月 31 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2022 年 3 月 30 日
Firewall Manager 增加了对 Palo Alto Networks 云下一代防火墙 (Cloud NGFW) 的支持	Firewall Manager 现在支持 Palo Alto Networks 云下一代防火墙 (Cloud NGFW)。	2022 年 3 月 30 日
将对帕洛阿尔托网络云 NGFW 的支持添加到 AWS Firewall Manager	AWS Firewall Manager 现在支持 Palo Alto Networks 云下一代防火墙 (NGFW) 策略。	2022 年 3 月 30 日
AWS Shield 指南的更新	扩展了 Shield 指南中的信息，描述了 Shield 如何执行事件检测，并提供了 DDoS 弹性架构的示例。	2022 年 3 月 16 日

AWS Shield 指南的更新	扩展了 Shield 指南中的信息，并改进了各个部分的组织结构。主要更改在以下 Shield 指南章节中：盾牌响应小组 (SRT) 支持 AWS Shield Advanced、中的资源保护和 DDoS 事件的可见性。	2022 年 2 月 28 日
Firewall Manager 现在支持 Network Firewall 集中部署模型	添加了一个新程序，说明如何配置使用分布式和集中式部署模型的策略。	2022 年 2 月 24 日
Firewall Manager 增加了对 AWS Network Firewall 集中部署模式的支持	现在，您可以将 AWS Network Firewall 策略配置为使用分布式或集中式部署模式。采用分布式部署模式，Firewall Manager 在策略范围内的每个 VPC 中创建和维护防火墙终端节点。采用集中式部署模式，Firewall Manager 在单个检测 VPC 中创建和维护防火墙终端节点。	2022 年 2 月 24 日
添加对 AWS WAF 托管规则组版本控制的支持 AWS Firewall Manager	AWS Firewall Manager 现在支持 Firewall Manager AWS WAF 策略中的 AWS WAF 托管规则组版本控制。	2022 年 2 月 18 日
AWS Firewall Manager 托管策略变更	更新为 `FMSServiceRolePolicy` 。	2022 年 2 月 16 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：IP 信誉列表。	2022 年 2 月 15 日

更新了的 AWS 托管规则 AWS WAF	AWS 的托管规则 AWS WAF 添加了防 AWS WAF 欺诈控制账户接管 (ATP) 规则组`AWSManagedRulesATPRuleSet` 。	2022 年 2 月 11 日
AWS WAF 指南组织结构的变化	为托管保护添加了一个新的顶级部分。将验证码部分从规则下移至新的托管保护部分。将标签部分从规则下移至其自己的顶级部分。	2022 年 2 月 11 日
AWS WAF 客户端应用程序集成	使用 AWS WAF JavaScript 和移动客户端 API 将您的客户端应用程序与智能威胁缓解 AWS 托管规则组集成，以增强检测能力。	2022 年 2 月 11 日
AWS WAF 防欺诈控制账户接管 (ATP)	您可以使用新的 F AWS WAF raud Control 账户接管预防 (ATP) 托管规则组来检测和阻止账户盗用企图。`AWSManagedRulesATPRuleSet`	2022 年 2 月 11 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2022 年 1 月 28 日
AWS WAF 托管策略变更	更新了 `AWSWAFFullAccessPolicy` 和 `AWSWAFConsoleFullAccess` 以更正日志记录权限。	2022 年 1 月 11 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：核心规则集 (CRS)、SQLi 数据库。	2022 年 1 月 10 日

Firewall Manager 支持 Shield Advanced 应用程序层 DDoS 自动缓解	Firewall Manager Shield Amazon CloudFront 资源的高级策略现在包括对应用程序层 DDoS 自动缓解的支持。	2022 年 1 月 7 日
AWS Firewall Manager 托管策略变更	更新为 `FMSServiceRolePolicy` 。	2022 年 1 月 7 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2021 年 12 月 17 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2021 年 12 月 11 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：已知的错误输入。	2021 年 12 月 10 日
新的 AWS Shield Advanced 服务相关角色	添加了 `AWSServiceRoleForAWSShield` 以支持应用程序层 DDoS 自动缓解功能。	2021 年 12 月 1 日
新的 AWS Shield 托管策略	添加了 `AWSShieldServiceRolePolicy` 以支持应用程序层 DDoS 自动缓解功能。	2021 年 12 月 1 日
应用程序层 DDoS 自动缓解选项现已推出 AWS Shield Advanced CloudFront	Shield Advanced 现在支持亚马逊 CloudFront分发的应用程序层 DDoS 自动缓解。您可以将 Shield Advanced 配置为自动计数或阻止应用层 DDoS 攻击中针对 CloudFront分布的 Web 请求。	2021 年 12 月 1 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：核心规则集 (CRS)、Windows 操作系统、Linux 操作系统和 IP 信誉列表。	2021 年 11 月 23 日
AWS Firewall Manager 托管策略变更	更新为 `FMSServiceRolePolicy` 。	2021 年 11 月 18 日
扩展了的日志记录选项 AWS WAF	现在，您可以将网页 ACL 流量记录到 Amazon Lo CloudWatch gs 日志组或亚马逊简单存储服务 (Amazon S3) Simple Service 存储桶。这些选项是对登录到 Amazon Data Firehose 传输流的现有选项的补充。	2021 年 11 月 15 日
AWS WAF 托管策略变更	更新了 `AWSWAFFullAccessPolicy` 和 `AWSWAFConsoleFullAccess` 以支持其他日志记录目标。	2021 年 11 月 15 日
AWS WAF 新CAPTCHA规则操作选项	您可以配置规则以针对 Web 请求运行验证码，并根据需要将验证码问题发送给客户端。	2021 年 11 月 8 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集 (CRS) 规则组的托管规则。	2021 年 10 月 27 日
更新了的 AWS 托管规则 AWS WAF	所有 AWS 托管规则规则组现在都支持标记。规则描述包括标签规范。	2021 年 10 月 25 日
Firewall Manager 支持 Network Firewall 日志筛选	AWS Firewall Manager 现在支持 Network Firewall 策略的日志过滤。	2021 年 10 月 4 日

AWS Firewall Manager 托管策略变更	更新为 FMSServiceRolePolicy 。	2021 年 9 月 29 日
添加了正则表达式匹配语句	现在，您可以将 Web 请求与单个正则表达式进行匹配。	2021 年 9 月 22 日
规则组内基于费率的 AWS WAF 规则	现在，您可以在规则组中 AWS WAF 定义基于费率的规则。在中 AWS Firewall Manager，AWS WAF 策略完全支持此功能。	2021 年 9 月 13 日
Firewall Manager 支持 AWS WAF 日志过滤	AWS Firewall Manager 现在支持 AWS WAF 策略的日志过滤。	2021 年 8 月 31 日
自动移除中的 out-of-scope 资源保护 AWS Firewall Manager	AWS Firewall Manager 允许您自动移除对离开策略范围的资源的保护。	2021 年 8 月 25 日
AWS Firewall Manager 托管策略变更	更新为 FMSServiceRolePolicy 。	2021 年 8 月 12 日
为托管规则组添加版本控制	托管规则组提供程序现在可以对其规则组进行版本控制。	2021 年 8 月 9 日
修改 AWS Firewall Manager 管理员要求	您可以使用组织的管理账户作为 Firewall Manager 管理员账户。这是不允许的。	2021 年 8 月 2 日
Firewall Manager 限额增加	将在 Firewall Manager 策略作用域内可以拥有的 Amazon VPC 实例数量从 10 个增加到 100 个。	2021 年 7 月 28 日

AWS Firewall Manager 支持 AWS Network Firewall 路由表监控	AWS Firewall Manager 现在支持路由表监控，并针对路由配置错误的 AWS Network Firewall 策略向安全管理员提供补救措施建议。	2021 年 7 月 8 日
AWS WAF 其他文本转换选项	扩展了文本转换选项，您可以在检查 Web 请求组件之前将其应用于 Web 请求组件。	2021 年 6 月 24 日
修改了 Firewall Manager AWS WAF 策略资源的命名	Firewall Manager 为您的 AWS WAF 策略管理的 Web ACL、规则组和日志的命名已更改。	2021 年 5 月 26 日
更新了的 AWS 托管规则 AWS WAF	AWS 托管规则， AWS WAF 增加了对标记 IP 信誉列表的支持，并删除了 Amazon IP 信誉列表规则名称上的后缀。	2021 年 5 月 4 日
添加对 AWS Organizations 委派管理员的支持	在设置 AWS Firewall Manager 管理员帐户时，Firewall Manager 现在会将该帐户指定为防火墙管理器的 AWS Organizations 委派管理员。通过此更改，在设置 Firewall Manager 管理员账户时，必须提供组织管理账户以外的成员账户。此更改不会影响您的现有设置。	2021 年 4 月 30 日
更新了的 AWS 托管规则 AWS WAF	AWS AWS WAF 已添加 AWS WAF 机器人控制规则组的托管规则。	2021 年 4 月 1 日
将规则组中的单个规则操作设置为 Count	现在，您可以将规则组中的单个规则操作设置为 Count。规则组级别的现有覆盖信息已得到更正。	2021 年 4 月 1 日

托管规则组的范围缩小语句	现在，您可以像使用基于速率的语句一样对托管规则组使用范围缩小语句。	2021 年 4 月 1 日
日志筛选	现在，您可以根据规则操作和标签筛选记录的 Web ACL 流量。	2021 年 4 月 1 日
AWS WAF 网络请求上的标签	您可以配置规则，为匹配的 Web 请求添加标签，并匹配其他规则添加的标签。	2021 年 4 月 1 日
AWS WAF 机器人控制	您可以使用新的 Bot Control 功能监控和控制 AWS WAF 机器人流量，该功能将 Bot Control 托管规则组与 Web 请求标记、范围缩小语句和日志过滤相结合。	2021 年 4 月 1 日
Firewall Manager 支持 Amazon Route 53 Resolver DNS 防火墙策略	AWS Firewall Manager 支持集中管理您的 VPC 的 Amazon Route 53 Resolver DNS 防火墙出站 DNS 流量过滤。	2021 年 3 月 31 日
自定义请求和响应处理	您可以为 AWS WAF 不阻止的 Web 请求添加自定义标头，也可以为被 AWS WAF 阻止的 Web 请求发送自定义响应。这适用于 Web ACL 默认操作和规则操作设置。	2021 年 3 月 29 日
AWS Firewall Manager 托管策略变更	更新为 `FMSServiceRolePolicy` 。	2021 年 3 月 17 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新以下规则组的托管规则：核心规则集 (CRS)、管理员保护、已知的错误输入和 Linux 操作系统。	2021 年 3 月 3 日
AWS Shield 托管策略变更跟踪	Shield 开始跟踪其 AWS 托管策略的变更。	2021 年 3 月 3 日
AWS Firewall Manager 托管策略变更跟踪	Firewall Manager 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 2 日
AWS WAF 托管策略变更跟踪	AWS WAF 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 1 日
将 Web 请求正文作为解析后的 JSON 进行检查	添加了检查已解析和筛选的 JSON 的 Web 请求正文的选项。这是对以纯文本形式检查 Web 请求正文的现有选项的补充。	2021 年 2 月 12 日
Firewall Manager 支持 AWS Network Firewall 策略	AWS Firewall Manager 支持集中管理您的 VPC 的 AWS Network Firewall 网络流量过滤。	2020 年 11 月 17 日
添加对 AWS Shield Advanced 保护组的支持	现在，您可以将受保护的资源分组为逻辑组，并集体管理其保护。	2020 年 11 月 13 日
添加了对 AWS AppSync 的支持 AWS WAF	现在，您可以将 AWS WAF 网页 ACL 与 AWS AppSync GraphQL API 关联起来。此更改仅在最新版本的 CI AWS WAF assic 中可用。 AWS WAF	2020 年 10 月 1 日

更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新了 Windows 操作系统规则集的托管规则。	2020 年 9 月 23 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新的托管规则集 PHP 应用程序和 POSIX 操作系统。	2020 年 9 月 16 日
更新了 AWS Shield 控制台	AWS Shield 提供了新的控制台选项，改善了用户体验。文档中的控制台指南适用于新控制台。	2020 年 9 月 1 日
Firewall Manager 对常见安全组策略的更新	AWS Firewall Manager 现在，通过控制台实现，通用安全组策略支持应用程序负载均衡器和经典负载均衡器资源类型。新选项可在通用策略的策略范围设置中找到。	2020 年 8 月 11 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新核心规则集的托管规则。	2020 年 8 月 7 日
Firewall Manager 支持 AWS WAF 日志配置	AWS Firewall Manager 现在支持 AWS WAF 策略的集中日志配置。	2020 年 7 月 30 日
在 Web 请求中指定 IP 地址位置	添加了使用您指定的 HTTP 标头中的 IP 地址，而不使用 Web 请求源的选项。备用标头通常是 `X-Forwarded-For` (XFF)，但您可以指定任何标头名称。您可以将此选项用于 IP 集匹配、地理匹配和基于速率的规则计数聚合。	2020 年 7 月 9 日

Firewall Manager 对内容审核安全组策略的更新	AWS Firewall Manager 扩展了内容审计安全组策略的功能，包括使用托管应用程序和协议列表的托管规则选项，以及资源违规的详细信息。	2020 年 7 月 7 日
Firewall Manager 托管列表	AWS Firewall Manager 现在支持托管应用程序和协议列表。Firewall Manager 可以管理一些列表，您也可以创建和管理自己的列表。	2020 年 7 月 7 日
Firewall Manager 支持通用安全组策略中的共享 VPC	AWS Firewall Manager 现在支持在共享 VPC 中使用常见的安全组策略。除了在范围内账户拥有的 VPC 中使用这些策略之外，还可以执行该操作。	2020 年 5 月 26 日
更新了的 AWS 托管规则 AWS WAF	在的 AWS 托管规则中为每条规则添加了文档 AWS WAF。	2020 年 5 月 20 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新的 Linux 操作系统规则组的托管规则。	2020 年 5 月 19 日
添加对将 AWS WAF 经典资源迁移到 AWS WAF (v2) 的支持	现在，您可以使用控制台或 API 导出 AWS WAF Classic 资源以迁移到最新版本的 AWS WAF。	2020 年 4 月 27 日

在策略范围内添加对 AWS Organizations 组织单位的支持	AWS Firewall Manager 现在支持使用 AWS Organizations 组织单位 (OU) 来指定策略范围。除了包括或排除特定账户外，您还可以使用 OU 在范围中包括或排除账户。指定 OU 等同于指定 OU 及其任何子 OU 中的所有账户，包括之后添加的任何子 OU 和账户。	2020 年 4 月 6 日
将对 AWS WAF (v2) 的支持添加到 AWS Firewall Manager	AWS Firewall Manager 除了以前的版本外 AWS WAF，现在还支持最新版本的 AWS WAF Classic。	2020 年 3 月 31 日
更新 AWS Firewall Manager 常用安全组策略	AWS Firewall Manager 通用安全组策略现在可以选择将该策略应用于范围内的 Amazon EC2 实例中的所有弹性网络接口。您仍然可以选择仅将策略应用于默认弹性网络接口。	2020 年 3 月 11 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 添加规则组的托管`AWSManagedRulesAnonymousIpList` 规则。	2020 年 3 月 6 日
更新了的 AWS 托管规则 AWS WAF	AWS 用于 AWS WAF 更新 WordPress 应用程序和规则组的托管`AWSManagedRulesCommonRuleSet` 规则。	2020 年 3 月 3 日
在 AWS Shield Advanced 保护选项中添加了 Amazon Route 53 运行状况检查	Shield Advanced 现在支持使用 Amazon Route 53 运行状况检查关联，以提高威胁检测和缓解的准确性。	2020 年 2 月 14 日

更新了的 AWS 托管规则 AWS WAF	AWS 的托管规则 AWS WAF 已更新 SQL 数据库规则组，添加了对消息 URI 的检查。	2020 年 1 月 23 日
Firewall Manager 新增安全组使用情况审核策略选项	Firewall Manager 为安全组使用情况审核策略提供了一个新选项。现在，您可以设置安全组在被视为不合规之前必须保持未使用状态的最小分钟数。默认情况下，此分钟数设置为零。	2020 年 1 月 14 日
Firewall Manager 的新 AWS WAF 策略选项	Firewall Manager 有了新的 AWS WAF 策略选项。现在，您可以选择从范围内资源删除所有现有 Web ACL 关联，然后再将策略的新 Web ACL 与这些资源关联。	2020 年 1 月 14 日
更新了的 AWS 托管规则 AWS WAF	AWS 的托管规则更新 AWS WAF 了核心规则集和 SQL 数据库规则组中规则的文本转换。	2019 年 12 月 20 日
AWS Firewall Manager 与集成 AWS Security Hub	AWS Firewall Manager 现在可以为不合规的资源和攻击创建调查结果并将其发送到 AWS Security Hub。	2019 年 12 月 18 日

AWS WAF 版本 2 的发布	AWS WAF 开发者指南的新版本。您可以管理 JSON 格式的 Web ACL 或规则组。扩展的功能包括逻辑规则语句、规则语句嵌套以及对 IP 地址和地址范围的完整 CIDR 支持。规则不再是 AWS 资源，而只存在于 Web ACL 或规则组的上下文中。对于现有客户，该服务的先前版本现在称为 C AWS WAF lassic。在 API、SDK 和 CLI 中，Cl AWS WAF assic 保留了其命名方案，根据上下文的不同，此最新版本 AWS WAF 的 “V2” 或 “v2” 在引用时会加上 “V2” 或 “v2”。 AWS WAF 无法访问在 C AWS WAF lassic 中创建的 AWS 资源。要在中使用这些资源 AWS WAF，您需要将其迁移。	2019 年 11 月 25 日
AWS 的托管规则规则组 AWS WAF	添加了 AWS 托管规则规则组。这些对 AWS WAF 客户是免费的。	2019 年 11 月 25 日
AWS Firewall Manager 支持 Amazon Virtual Private Cloud 安全组	在 Firewall Manager 中添加了对 Amazon VPC 安全组的支持。	2019 年 10 月 10 日
AWS Firewall Manager 支持 AWS Shield Advanced	在 Firewall Manager 中添加了对 Shield Advanced 的支持。	2019 年 3 月 15 日
教程：创建分层策略	增加了有关在 AWS Firewall Manager中创建分层策略的教程。	2019 年 2 月 11 日

规则组中的规则级别控制	现在，您可以从 AWS Marketplace 规则组中排除单个规则，也可以从自己的规则组中排除。	2018 年 12 月 12 日
AWS Shield Advanced 支持 AWS Global Accelerator 标准加速器	Shield Advanced 现在可以保护 AWS Global Accelerator 标准加速器了。	2018 年 11 月 26 日
AWS WAF 支持 Amazon API Gateway	AWS WAF 现在可以保护 Amazon API Gateway API。	2018 年 10 月 25 日
扩展 AWS 盾牌高级入门向导	新向导提供了创建基于费率的规则和 Amazon Ev CloudWatch ents 的机会。	2018 年 8 月 31 日
AWS WAF 日志记录	启用日志记录，以获取有关 Web ACL 对流量进行分析的详细信息。	2018 年 8 月 31 日
在条件中支持查询参数	创建条件时，您现在可以在请求中搜索特定的参数。	2018 年 6 月 5 日
Shield Advanced 入门向导	引入了订阅 AWS Shield Advanced 的全新简化流程。	2018 年 6 月 5 日
扩展了允许的 CIDR 范围	创建 IP 匹配条件时， AWS WAF 现在支持 IPv4 地址范围：/8 以及介于 /16 到 /32 之间的任何范围。	2018 年 6 月 5 日

2018 年以前的更新

下表描述 2018 年之前发布的每个 AWS WAF 开发人员指南中的重要变化。

更改	API 版本	描述	发行日期
更新	2016-08-24	AWS Marketplace 规则组	2017 年 11 月
更新	2016-08-24	弹性 IP 地址的 Shield 高级支持	2017 年 11 月
更新	2016-08-24	全局威胁控制面板	2017 年 11 月
更新	2016-08-24	能够抵御 DDoS 的网站教程	2017 年 10 月
更新	2016-08-24	地理和正则表达式条件	2017 年 10 月
更新	2016-08-24	基于速率的规则	2017 年 6 月
更新	2016-08-24	重新企业	2017 年 4 月
更新	2016-08-24	添加了有关 DDOS 保护和 Application Load Balancer 支持的信息。	2016 年 11 月
新功能	2015-08-24	现在，您可以 AWS WAF 通过 AWS CloudTrail该 AWS 服务记录您账户的 API 调用并将日志文件传送到您的 S3 存储桶，从而记录您的所有 API 调用。 CloudTrail 日志可用于启用安全分析、跟踪 AWS 资源更改以及帮助进行合规性审计。集成 AWS WAF 并 CloudTrail 允许您确定向 AWS WAF API 发出了哪些请求、发出每个请求的源 IP 地址、谁发出了请求、何时发出请求等。 如果您已经在使用 AWS CloudTrail，则将在 CloudTrail 日志中开始看到 AWS WAF API 调用。如果您尚未 CloudTrail 为自己的账户启用该功能，则可以 CloudTrail 从中将其启用AWS Management Console。	2016 年 4 月 28 日

更改	API 版本	描述	发行日期
		启用无需支付额外费用 CloudTrail，但是 Amazon S3 和 Amazon SNS 的使用将适用标准费率。	
新功能	2015-08-24	现在，您可以使用 AWS WAF 允许、阻止或计算看似包含恶意脚本（称为跨站脚本或 XSS）的 Web 请求。攻击者有时会将恶意脚本插入到 Web 请求中，企图利用 Web 应用程序中的漏洞。有关更多信息，请参阅 跨站点脚本攻击规则语句。	2016 年 3 月 29 日
新功能	2015-08-24	在此版本中， AWS WAF 增加了以下功能： • 您可以根据请求的指定部分（例如查询字符串或 URI）的长度进行配置 AWS WAF ，以允许、阻止或计数 Web 请求。有关更多信息，请参阅 大小约束规则语句。 • 您可以根据请求正文中的内容进行配置， AWS WAF 以允许、阻止或计数 Web 请求。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 Web 请求组件规格和处理。	2016 年 1 月 27 日
新特征	2015-08-24	现在，您可以使用 AWS WAF 控制台选择要与 Web ACL 关联的 CloudFront 分配。有关更多信息，请参阅关联或取消关联 Web ACL 和分发。 CloudFront	2015 年 11 月 16 日
首次发布	2015-08-24	这是 AWS WAF 开发人员指南的首次发布。	2015 年 10 月 6 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。