实施指南

AWS WAF 的安全自动化

AWS WAF 的安全自动化: 实施指南

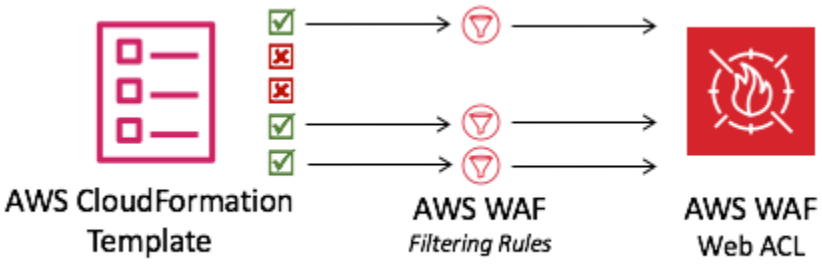
Table of Contents

在 AWS WAF 上使用安全自动化功能自动部署单个 Web 访问控制列表，过滤基于 Web 的攻击

AWS WAF 安全自动化解决方案部署了一组预配置的规则，以帮助您保护应用程序免受常见 Web 漏洞的侵害。该解决方案的核心服务 AWS WAF 可帮助保护 Web 应用程序免受可能影响应用程序可用性、危及安全性或消耗过多资源的攻击技术的侵害。您可以使用 AWS WAF 来定义可自定义的 Web 安全规则。这些规则控制允许或阻止部署在 A mazon CloudFront、Application Loa d Balancer (ALBAPIs) 等 AWS 资源上的 Web 应用程序和应用程序编程接口 () 的流量。有关更多支持的资源类型，请参阅 AWS WAF、AWS Fi rewall Manager 和 AWS Shield 高级开发人员指南中的 AWS WAF。

配置 AWS WAF 规则对大型和小型组织来说都可能具有挑战性和负担，特别是对于那些没有专门安全团队的组织而言。为了简化此过程，AWS WAF 安全自动化解决方案会自动部署一个 Web 访问控制列表 (ACL)，其中包含一组旨在过滤常见基于 Web 的攻击的 AWS WAF 规则。在初始配置此解决方案的 AWS CloudFormation 模板时，您可以指定要包括哪些保护功能。部署此解决方案后，AWS WAF 会检查向其现有 CloudFront 分配或 ALB 发出的网络请求，并在适用时将其阻止。

CloudFormation 模板部署带有 AWS WAF 筛选规则的 Web ACL。



本实施指南讨论了在 Amazon Web Services (AWS) 云中部署此解决方案的架构注意事项、配置步骤和最佳操作实践。它包括指向 CloudFormation 模板的链接，这些模板使用 AWS 在安全和可用性方面的最佳实践，启动、配置和运行在 AWS 上部署此解决方案所需的 AWS 安全、计算、存储和其他服务。

本指南中的信息假设您熟悉 AWS 服务，例如 AWS WAF、 CloudFront ALBs、和 AWS Lamb da。它还需要对常见的基于 Web 的攻击和缓解策略有基本的了解。

> **Note**
>
> 从版本 3.0.0 开始，此解决方案支持最新版本的 AWS WAF 服务 API (AWS)。 WAFV2

本指南适用于 IT 经理、安全工程师、 DevOps 工程师、开发人员、解决方案架构师和网站管理员。

> **Note**
>
> 我们建议使用此解决方案作为实施 AWS WAF 规则的起点。您可以根据需要自定义源代码、添加新的自定义规则并利用更多 AWS WAF 托管规则。

使用以下导航表可快速找到这些问题的答案：

如果您想. . .	阅读. . .
了解运行此解决方案的成本。运行此解决方案的总成本取决于激活的保护以及摄取、存储和处理的数据量。	成本
了解此解决方案的安全注意事项。	安全性
了解此解决方案支持哪些 AWS 区域。	支持的 AWS 区域
查看或下载此解决方案中包含的 CloudFormation 模板，以自动部署此解决方案的基础架构资源（“堆栈”）。	AWS CloudFormation 模板
使用 Support 来帮助您部署、使用解决方案或对其进行故障排除。	支持
访问源代码并选择使用 AWS Cloud Development Kit (AWS CDK) 来部署解决方案	GitHub 存储库

功能和优势

AWS WAF 安全自动化解决方案提供以下功能和优势。

使用 AWS 托管规则规则组保护您的 Web 应用程序

适用@@ 于 AWS WAF 的 AWS 托管规则提供针对常见应用程序漏洞或其他有害流量的保护。该解决方案包括 AWS 托管 IP 信誉规则组、AWS 托管基准规则组和 AWS 托管用例特定规则组。您可以选择为 Web ACL 选择一个或多个规则组，最高不超过 Web ACL 容量单位 (WCU) 的最大配额。

使用预定义的 HTTP Flood 自定义规则提供第 7 层洪水防护

HTTP Floo d 自定义规则可在客户定义的时间段内防御 Web 层分布式 Denial-of-Service (DDoS) 攻击。您可以选择以下选项之一来激活此规则：

- AWS WAF 基于费率的规则
- Lambda 日志解析器
- 亚马逊 Athena 日志解析器

Lambda 日志解析器或 Athena 日志解析器选项允许您定义小于 100 的请求配额。这种方法可以帮助您不达到 AWS WAF 基于费率的规则所要求的配额。有关更多信息，请参阅日志解析器选项。

您还可以通过在筛选条件中添加国家/地区和统一资源标识符 (URI) 来增强 Athena 日志解析器。这种方法可以识别并阻止具有不可预测的 URI 模式的 HTTP 洪水攻击。有关更多信息，请参阅在 HTTP Flood Athena 日志解析器中使用国家/地区和 URI。

使用预定义的扫描器和探测器自定义规则阻止对漏洞的利用

S canners & Probes 自定义规则解析应用程序访问日志，搜索可疑行为，例如源生成的异常错误。然后，它会在客户定义的一段时间内屏蔽这些可疑的源 IP 地址。您可以选择以下选项之一来激活此规则：Lambda 日志解析器或 Athena 日志解析器。有关更多信息，请参阅日志解析器选项。

使用预定义的 Bad Bot 自定义规则检测和转移入侵

Ba d Bot 自定义规则设置了 honeypot 端点，这是一种旨在引诱和转移未遂攻击的安全机制。您可以在网站中插入端点，以检测来自内容抓取工具和恶意机器人的入站请求。一旦检测到，来自相同来源的任何后续请求都将被阻止。有关更多信息，请参阅在您的 Web 应用程序中嵌入 Honeypot 链接。

使用预定义 IP 信誉屏蔽恶意 IP 地址列表自定义规则

IP 信誉列表自定义规则每小时都会检查第三方 IP 信誉列表，寻找要屏蔽的新 IP 范围。这些列表包括 Spamhaus Don't Route Or Peer (DROP) 和 Extended DROP (EDROP) 列表、Proofpoint 新兴威胁 IP 列表和 Tor 退出节点列表。

使用预定义的允许和拒绝 IP 列表自定义规则，提供手动 IP 配置

允许和拒绝的 IP 列表自定义规则允许您手动插入要允许或拒绝的 IP 地址。您还可以将 “允许” 和 “拒绝 IP” 列表上的 IP 保留配置为 IPs 在设定的时间过期。

创建自己的监控控制面板

此解决方案会发布 Amazon CloudWatch 指标，例如允许的请求、已阻止的请求和其他相关指标。您可以构建自定义控制面板来可视化这些指标，并深入了解 AWS WAF 提供的攻击模式和保护。有关更多信息，请参阅生成监控面板。

使用案例

以下是使用此解决方案的示例用例。您可以通过创新的方式自定义此解决方案，而不仅限于此列表。

自动设置 AWS WAF 规则

AWS WAF 可保护您的 Web 应用程序免受常见攻击；但是，设置 AWS WAF 规则可能既复杂又耗时。为了帮助您，此解决方案会自动使用模板将一组 AWS WAF 规则部署到您的账户。 CloudFormation 这样，您就无需自己配置 AWS WAF 规则，而且可以更快地开始使用 AWS WAF。

自定义第 7 层 HTTP 洪水防护

此解决方案提供了三个激活 HTTP 洪水防护的选项。您可以选择适合自己需求的选项，以获得防御 DDo S 攻击的保护。有关更多信息，请参阅 “功能和优势” 中的 “使用预定义的 HTTP Flood 自定义规则提供第 7 层洪水防护”。

利用源代码来应用自定义或构建自己的安全自动化

此解决方案提供了一个示例，说明如何使用 AWS WAF 和其他服务在 AWS 云上构建安全自动化。它的开源代码 GitHub使您可以方便地应用自定义设置或构建适合自己需求的安全自动化。

概念和定义

本节介绍关键概念，并定义了该解决方案特有的术语。

ALB 日志

此解决方案使用 ALB 资源的日志。此解决方案中的扫描仪和探测器保护规则会检查这些日志。

Athena 日志解析器

Amazon Athena 是一项基于开源框架的无服务器交互式分析服务，支持开放表和文件格式。此解决方案运行定时的 Athena 查询，以检查 AWS W CloudFront AF 或 ALB 日志（如果用户在激活 HTTP 洪

水防护规则或扫描器和探测器保护规则时yes - Amazon Athena log parser选择），并且可用于通过结构化逻辑链运行的检测来激活恶意机器人防护。

AWS WAF 规则

AWS WAF 规则定义了：

- 如何检查 HTTP (S) 网络请求
- 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。

CloudFront 日志

此解决方案使用 CloudFront 资源日志。此解决方案中的扫描仪和探测器保护规则会检查这些日志。

IP 套装

IP 集提供您要使用的 IP 地址和 IP 地址范围的集合

一起写在规则声明中。IP 集是 AWS 资源。

Lambda 日志解析器

此解决方案运行由亚马逊简单存储服务 (Ama zon S3) 对象创建事件调用的 Lambda 函数。如果用户在激活 HTTP 洪水防护、扫描器和探测器保护**yes - AWS Lambda log parser**时选择 CloudFront，Lambda 函数会启动对 AWS WAF 或 ALB 日志的检查，并且可以通过通过结构化逻辑链运行的检测来执行恶意机器人保护规则。

托管规则组

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

资源/端点类型

您可以将 AWS 资源与 Web 关联 ACLs 以保护它们。这些资源是 ALB、AWS CloudFront、AWS AppSync、A mazon Cognito、AWS App Runner 和 AWS 验证访问资源。目前，Amazon 支持该解决方案 CloudFront 和 ALB。

WAF 日志

此解决方案使用 AWS WAF 生成的日志来存储与 Web ACL 关联的资源。此解决方案的 HTTP 洪水防护、扫描器和探测器保护以及激活恶意机器人保护规则会检查这些日志。

WCU

AWS WAF 使用 Web 访问控制列表 (ACLWCUs) 容量单位 () 来计算和控制运行规则、规则组和 Web 所需的操作资源。 ACLs当您配置规则组和网络时，AWS WAF 会强制执行 WCU 配额。 ACLs WCUs 不影响 AWS WAF 检查网络流量的方式。

Web ACL

Web ACL 可让您精细控制受保护资源响应的 HTTP (S) Web 请求。

> **Note**
>
> 有关 AWS 术语的一般参考，请参阅 AWS 术语表。

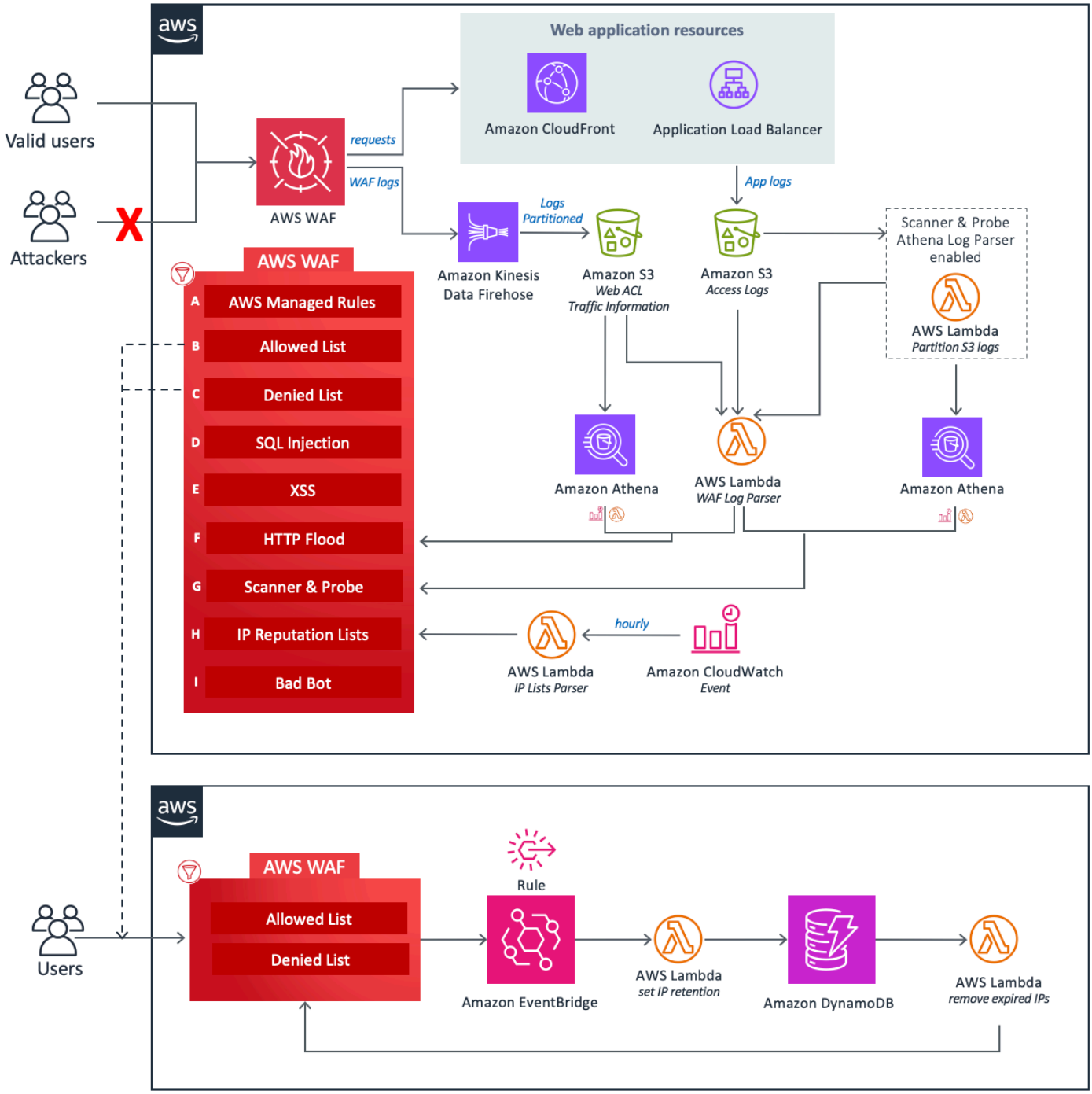
架构概述

本节提供了此解决方案所部署组件的参考实施架构图。

架构图

使用默认参数部署此解决方案将在您的 AWS 账户中部署以下组件。

CloudFormation 模板部署 AWS WAF 和其他 AWS 资源来保护您的 Web 应用程序免受常见攻击。



设计的核心是 AWS WAF Web ACL，它充当 Web 应用程序所有传入请求的中心检查和决策点。在 CloudFormation 堆栈的初始配置过程中，用户定义要激活哪些保护组件。每个组件独立运行，并向 Web ACL 添加不同的规则。

该解决方案的组件可以分为以下保护区域。

> **Note**
>
> 群组标签不反映 WAF 规则的优先级。

- AWS 托管规则 (A)-此组件包含 AWS 托管规则 IP 信誉规则组、基准规则组和特定于用例的规则组。这些规则组可以防止对常见应用程序漏洞或其他有害流量的利用，包括 OWASP 出版物中描述的漏洞，而无需自己编写规则。
- 手动 IP 列表（B 和 C）-这些组件创建了两个 AWS WAF 规则。使用这些规则，您可以手动插入要允许或拒绝的 IP 地址。您可以使用亚马逊 EventBridge规则和 Amazon DynamoD B 配置 IP 保留并删除允许或拒绝的 IP 集上的过期 IP 地址。有关更多信息，请参阅在允许和拒绝的 AWS WAF IP 集上配置 IP 保留。
- SQL 注入 (D) 和 XSS (E)-这些组件配置了两个 AWS WAF 规则，这些规则旨在防止 URI、查询字符串或请求正文中常见的 SQL 注入或跨站脚本 (XSS) 模式。
- HTTP Flood (F)-此组件可防范由来自特定 IP 地址的大量请求构成的攻击，例如 Web 层 DDo S 攻击或暴力登录尝试。使用此规则，您可以设置配额，该配额定义了在默认五分钟内允许来自单个 IP 地址的最大传入请求数（可使用 Athena Query 运行时间计划参数进行配置）。突破此阈值后，将暂时阻止来自该 IP 地址的其他请求。您可以通过使用基于 AWS WAF 速率的规则来实现此规则，也可以使用 Lambda 函数或 Athena 查询处理 AWS WAF 日志。有关与 HTTP 洪水缓解选项相关的权衡的更多信息，请参阅日志解析器选项。
- S@@ canner and Probe (G)-此组件解析应用程序访问日志，搜索可疑行为，例如源生成的异常数量错误。然后，它会在客户定义的一段时间内屏蔽这些可疑的源 IP 地址。您可以使用 Lambda 函数或 Athena 查询来实现此规则。有关与扫描器和探测器缓解选项相关的权衡的更多信息，请参阅日志解析器选项。
- IP 信誉列表 (H)-此组件是 `IP Lists Parser` Lambda 函数，它每小时检查第三方 IP 信誉列表，寻找要屏蔽的新范围。这些列表包括 Spamhaus Don't Route Or Peer (DROP) 和 Extended DROP (EDROP) 列表、Proofpoint 新兴威胁 IP 列表和 Tor 退出节点列表。
- Ba@@ d Bot (I)-除了蜜罐机制外，此组件还通过监控与应用程序负载均衡器 (ALB) 或 Amazon CloudFront 的直接连接来增强恶意机器人的检测。如果机器人绕过蜜罐尝试与 ALB 或交互 CloudFront，则系统会分析请求模式和日志以识别恶意活动。当检测到恶意机器人时，系统会提取其 IP 地址并将其添加到 AWS WAF 阻止列表中，以防止进一步访问。恶意机器人检测通过结构化的逻辑链运行，确保全面的威胁覆盖：
  - HTTP Flood Protection Lambda 日志解析器 — 在洪水分析期间 IPs 从日志条目中收集恶意机器人。

- Scanner & Probe Protection Lambda 日志解析器 — IPs 从与扫描仪相关的日志条目中识别不良机器人。
- HTTP Flood Protection Athena 日志解析器 — 使用跨查询运行的分区 IPs 从 Athena 日志中提取恶意机器人。
- Scanner & Probe Protection Athena 日志解析器 — 使用相同的分区策略 IPs 从与扫描仪相关的 Athena 日志中检索恶意机器人。
- 回退检测-如果同时禁用 HTTP 洪水防护和扫描器和探测器保护，则系统将依赖日志 Lambda 解析器，该解析器基于 WAF 标签筛选器记录机器人活动。

此解决方案中的三个自定义 Lambda 函数均向发布运行时指标。 CloudWatch有关这些 Lambda 函数的更多信息，请参阅组件详细信息。

AWS Well-Architected 设计注意事项

该解决方案采用 AWS Well-Architected Fram ework 中的最佳实践，可帮助客户在云中设计和运行可靠、安全、高效且经济实惠的工作负载。

本节介绍 Well-Architected Framework 的设计原则和最佳实践如何使该解决方案受益。

卓越运营

本节介绍我们是如何使用卓越运营支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案将指标推送 CloudWatch 到基础设施、Lambda 函数、Amazon D ata Firehose、A mazon S3 存储桶和其他解决方案组件中，以提供可观察性。
- 我们通过 AWS 持续集成和持续交付 (CI/CD) 管道开发、测试和发布解决方案。这可以帮助开发人员始终如一地获得高质量的结果。
- 您可以使用模板安装解决方案，该 CloudFormation 模板可在您的账户中预置所有必需的资源。要更新或删除解决方案，您只需要更新或删除模板即可。

安全性

本节介绍我们是如何使用安全性支柱的原则和最佳实践来设计此解决方案的。

- 所有服务间通信都使用 AWS Identity and Access Managem ent (IAM) 角色。

- 该解决方案使用的所有角色都遵循最低权限访问权限。换句话说，它们仅包含服务正常运行所需的最低权限。
- 所有数据存储，包括 Amazon S3 存储桶和 DynamoDB，都处于静态加密状态。

可靠性

本节介绍我们是如何使用可靠性支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案尽可能使用 AWS 无服务器服务（例如 Lambda、Firehose、Amazon S3 和 Athena）来确保高可用性并从服务故障中恢复。
- 我们对解决方案进行自动测试，以快速检测和修复错误。
- 该解决方案使用 Lambda 函数进行数据处理。该解决方案将数据存储在 Amazon S3 和 DynamoDB 中，并且默认保留在多个可用区域中。

性能效率

本节介绍我们是如何使用性能效率支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案使用无服务器架构，以较低的成本确保高可扩展性和可用性。
- 该解决方案通过对数据进行分区和优化查询来减少数据扫描量并更快地获得结果，从而提高数据库性能。
- 该解决方案每天都会自动测试和部署。我们的解决方案架构师和主题专家对解决方案进行审核，寻找需要实验和改进的领域。

成本优化

本节介绍我们是如何使用成本优化支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案使用无服务器架构，客户只需为其实际使用量付费。
- 解决方案的计算层默认为 Lambda，它使用模型。 pay-per-use
- Athena 数据库和查询经过优化，可减少数据扫描量，从而降低成本。

可持续性

本节介绍我们是如何使用可持续性支柱的原则和最佳实践来设计此解决方案的。

- 该解决方案使用托管和无服务器服务来最大限度地减少后端服务对环境的影响。
- 与持续运行本地服务器的足迹相比，该解决方案的无服务器设计旨在减少碳足迹。

架构详情

本节介绍构成此解决方案的组件和 AWS 服务，以及这些组件如何协同工作的架构详情。

此解决方案中的 AWS 服务

AWS 服务	描述
AWS WAF	核心。部署 AWS WAF Web ACL、AWS 托管规则规则组、自定义规则和 IP 集。发出 AWS WAF API 调用以阻止常见攻击和保护 Web 应用程序。
Amazon Data Firehose	核心。将 AWS WAF 日志传送到亚马逊 S3 存储桶。
Amazon S3	核心。存储 AWS WAF CloudFront、和 ALB 日志。
AWS Lambda	核心。部署多个 Lambda 函数以支持自定义规则。
Amazon EventBridge	核心。创建事件规则以调用 Lambda。
Amazon Athena	支持。创建 Athena 查询和工作组以支持 Athena 日志解析器。
AWS Glue	支持。创建数据库和表以支持 Athena 日志解析器。
Amazon SNS	支持。发送亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 电子邮件通知，以支持在允许和拒绝的名单上保留 IP。
AWS Systems Manager	支持。提供应用程序级资源监控，并可视化资源操作和成本数据。

日志解析器选项

如架构概述中所述，有三个选项可以处理 HTTP 泛洪以及扫描器和探测器保护。以下各节将更详细地解释这些选项。

AWS WAF 基于费率的规则

基于速率的规则可用于 HTTP 洪水防护。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。此解决方案允许您指定客户端 IP 在随后、持续更新的五分钟内允许的 Web 请求数量。如果某个 IP 地址违反了配置的配额，AWS WAF 会阻止新的请求，直到请求速率低于配置的配额。

如果请求配额为每五分钟超过 2,000 个请求，并且您无需进行自定义，我们建议您选择基于速率的规则选项。例如，在计算请求数时不考虑静态资源访问权限。

您可以进一步配置规则，使其使用其他各种聚合键和密钥组合。有关更多信息，请参阅聚合选项和密钥。

亚马逊 Athena 日志解析器

HTTP Flood Protec tion 和 Scanner & Prob e Prot ec tion 模板参数都提供 Athena 日志解析器选项。激活后，预 CloudFormation 置 Athena 查询和计划的 Lambda 函数，负责编排 Athena 的运行、处理结果输出和更新 AWS WAF。此 Lambda 函数由配置为每五分钟运行一次 CloudWatch 的事件调用。可以使用 Athena 查询运行时间计划参数对其进行配置。

如果您无法使用基于 AWS WAF 费率的规则，并且熟悉 SQL 来实现自定义，我们建议您选择此选项。有关如何更改默认查询的更多信息，请参阅查看 Amazon Athena 查询。

HTTP 洪水防护基于 AWS WAF 访问日志处理并使用 WAF 日志文件。与 ALB 日志的传输时间相比，WAF 访问日志类型的延迟时间更短，您可以使用它来更快地识别 HTTP 洪水来源。 CloudFront 但是，您必须在 “激活扫描仪和探测器保护” 模板参数中选择 CloudFront 或 ALB 日志类型才能接收响应状态代码。

> **Note**
>
> 如果恶意机器人绕过蜜罐直接与 ALB 交互，则系统会通过日志分析检测恶意行为 CloudFront，除非 HTTP 洪水防护和扫描器和探测器保护都未使用 Lambda 日志解析器。

AWS Lambda 日志解析器

HTTP 洪水防护和扫描器和探测器保护模板参数提供了 AWS Lambda 日志解析器选项。仅当基于速率的 AWS WAF 规则和 Amazon Athena 日志解析器选项不可用时，才使用 Lambda 日志解析器。此选项的一个已知局限性是，信息是在正在处理的文件上下文中处理的。例如，一个 IP 生成的请求或错误可能超过定义的配额，但是由于这些信息被拆分为不同的文件，因此每个文件存储的数据不足以超过配额。

> **Note**
>
> 此外，如果恶意机器人绕过蜜罐直接与 ALB 或交互 CloudFront，则检测依赖于所选的日志解析器选项来有效识别和阻止恶意活动。

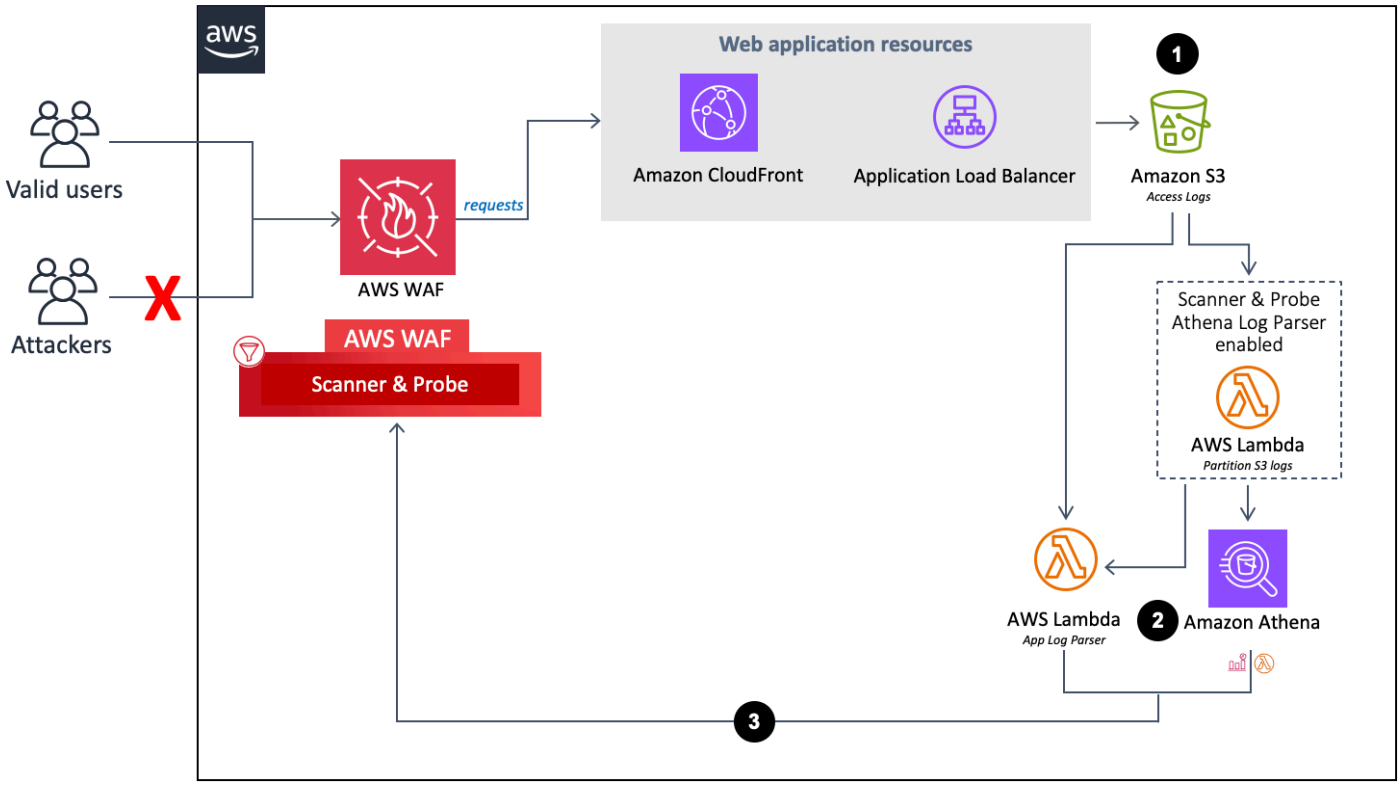
组件详细信息

如架构图所述，该解决方案的四个组件使用自动化来检查 IP 地址并将其添加到 AWS WAF 阻止列表中。以下各节将更详细地解释其中的每一个组件。

日志解析器-应用程序

应用程序日志解析器有助于防范扫描器和探测器。

应用程序日志解析器流程。



1. 当 CloudFront 或 ALB 代表您的 Web 应用程序收到请求时，它会将访问日志发送到 Amazon S3 存储桶。

   a. （可选）如果您`Yes - Amazon Athena log parser`为模板参数选择“激活 HTTP 防洪保护”和“激活扫描器和探测器保护”，Lambda 函数会在访问日志到达 Amazon S3 后将其从其原始文件夹`<customer-bucket>`/AWSLogs移动到新分区的文件夹 `<customer-bucket>` /AWSLogs-partitioned/ `<optional-prefix>` /year= `<YYYY>` /month= `<MM>` /day= `<DD>` /hour= `<HH>` /中。

   b. （可选）如果您选择`yes`将数据保留在原始 S3 位置模板参数，则日志将保留在原始位置并复制到其分区文件夹，从而复制您的日志存储。

   > **Note**
   >
   > 对于 Athena 日志解析器，此解决方案仅在您部署此解决方案后对到达您的 Amazon S3 存储桶的新日志进行分区。如果您要对现有日志进行分区，则必须在部署此解决方案后手动将这些日志上传到 Amazon S3。

2. 根据您选择的模板参数“激活 HTTP 防洪保护”和“激活扫描仪和探测器保护”，此解决方案使用以下方法之一来处理日志：

a. Lambda-每次在 Amazon S3 存储桶中存储新的访问日志时，都会启动 Lambda Log Parser 函数。

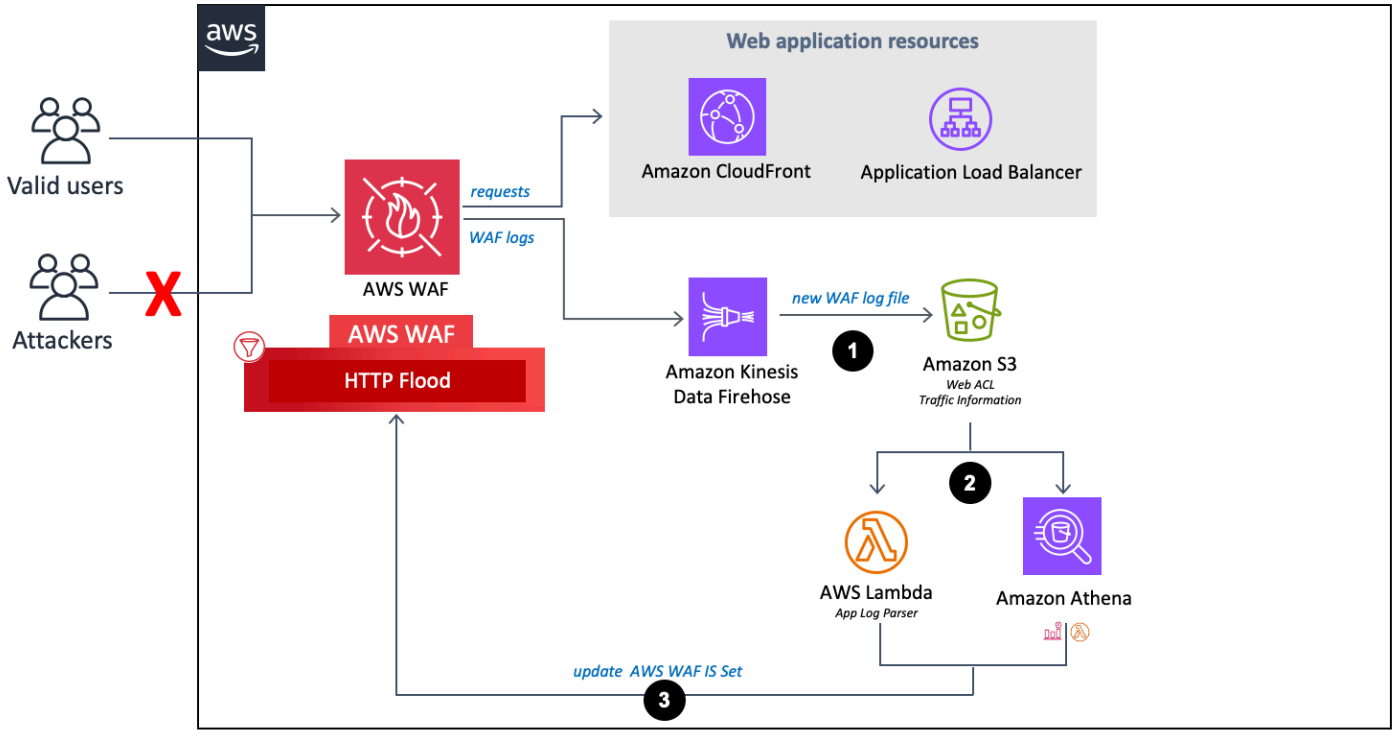
b. Athena-默认情况下，扫描器和探测保护 Athena 查询每五分钟运行一次，输出将推送到 AWS WAF。此过程由事件启动，该 CloudWatch 事件启动负责运行 Athena 查询的 Lambda 函数，并将结果推送到 AWS WAF。

3. 该解决方案分析日志数据，以确定产生比定义配额更多的错误的 IP 地址。然后，该解决方案会更新 AWS WAF IP 设置条件，以便在客户定义的时间段内屏蔽这些 IP 地址。

日志解析器-AWS WAF

如果您yes - Amazon Athena log parser为 “激活 HTTP 防洪保护” 选择yes - AWS Lambda log parser或，则此解决方案会预配置以下组件，这些组件会解析 AWS WAF 日志，以识别和阻止请求速率大于您定义的配额的终端节点的来源。

AWS WAF 日志解析器流程。



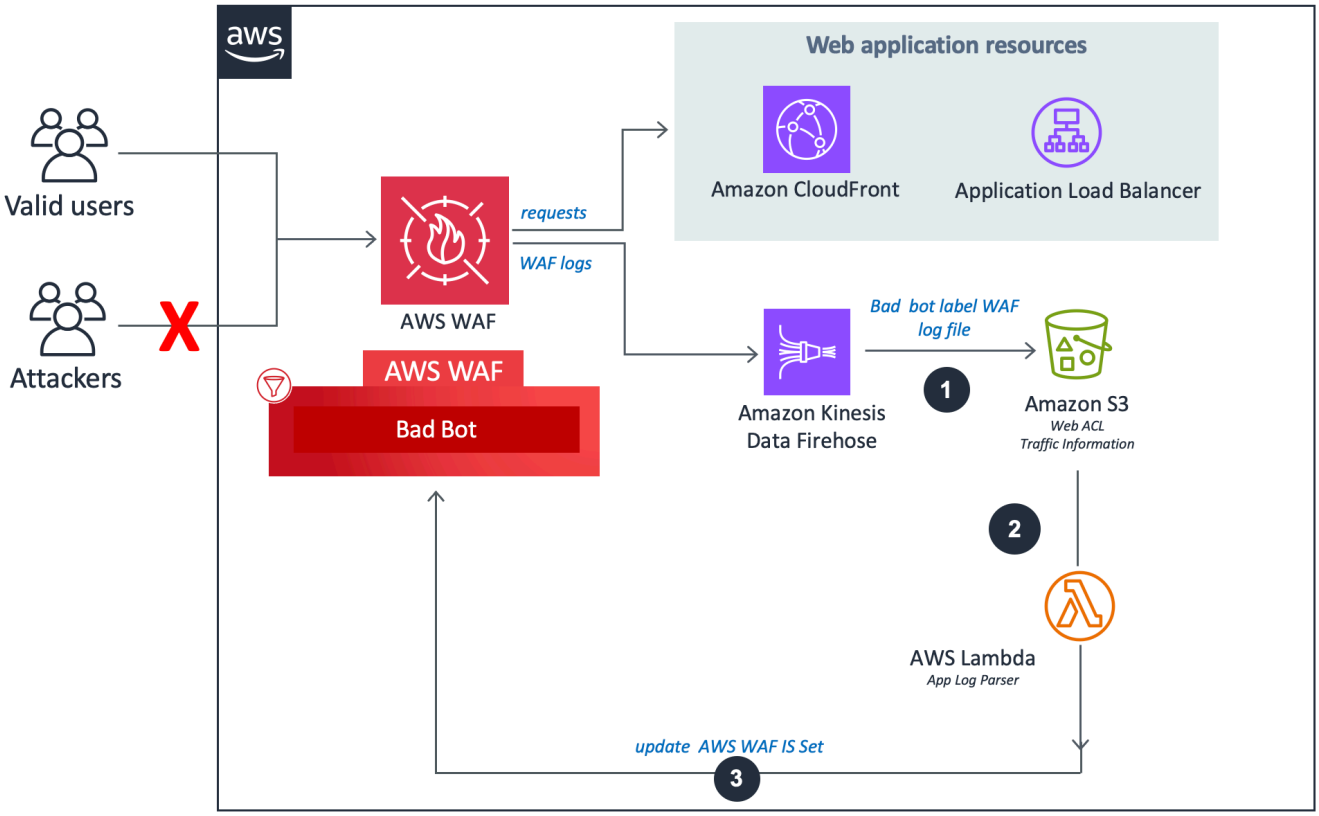
1. 当 AWS WAF 收到访问日志时，它会将日志发送到 Firehose 终端节点。然后 Firehose 将日志传送到亚马逊 S3 中名为的分区存储桶 *<customer-bucket>* /AWSLogs/ *<optional-prefix>* / year= *<YYYY>* /month= *<MM>* /day= *<DD>* /hour= *<HH>* /

2. 根据您选择的模板参数 “激活 HTTP 防洪保护” 和 “激活扫描仪和探测器保护”，此解决方案使用以下方法之一来处理日志：
   a. Lambda：每次在 Amazon S3 存储桶中存储新的访问日志时，都会启动 Lambda `Log Parser` 函数。
   b. Athena：默认情况下，每五分钟运行一次扫描器和探测器 Athena 查询，并将输出推送到 AWS WAF。此过程由亚马逊 CloudWatch 事件启动，然后启动负责执行亚马逊 Athena 查询的 Lambda 函数，并将结果推送到 AWS WAF。
3. 该解决方案分析日志数据，以确定发送的请求数超过定义配额的 IP 地址。然后，该解决方案会更新 AWS WAF IP 设置条件，以便在客户定义的时间段内屏蔽这些 IP 地址。

日志解析器-Bad bot

Bad bot 日志解析器会检查向 honeypot 端点发出的请求以提取其源 IP 地址。

机器人日志解析器流程不正确。



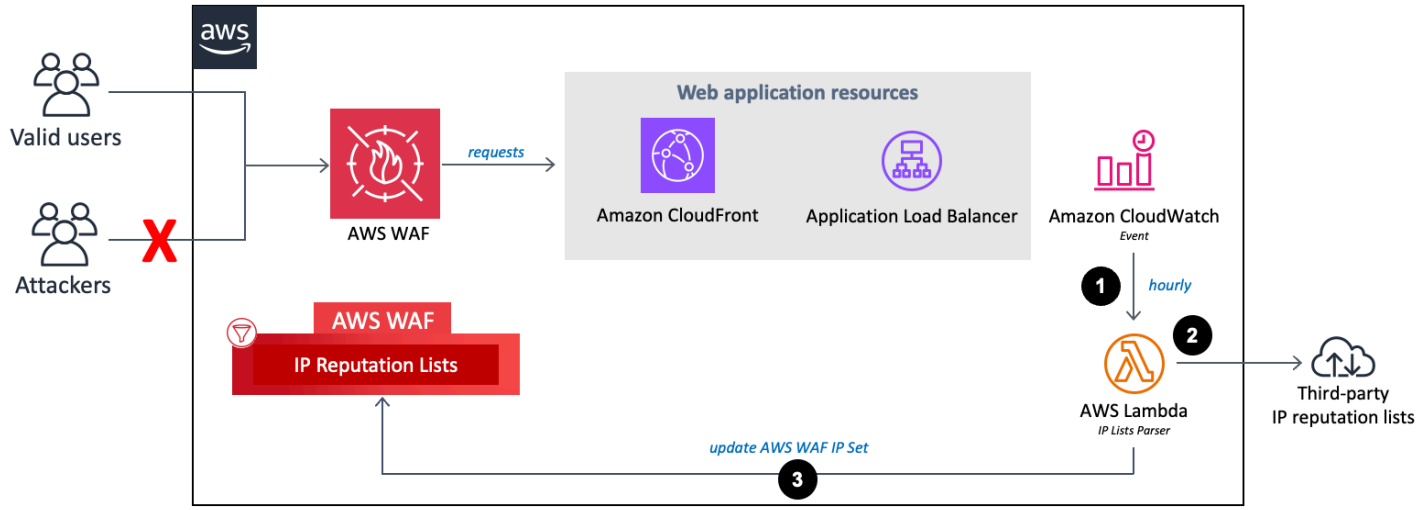
1. 如果`Bad Bot Protection`已激活并禁用 HTTP 洪水防护和扫描器和探测器保护功能：系统将使用 Log Lambda 解析器，该解析器基于 WA F 标签筛选器仅记录错误的机器人请求。

2. Lambda 函数拦截并检查请求标头，以提取访问陷阱端点的源的 IP 地址。
3. 该解决方案分析日志数据，以确定发送的请求数超过定义配额的 IP 地址。然后，该解决方案会更新 AWS WAF IP 设置条件，以便在客户定义的时间段内屏蔽这些 IP 地址。

IP 列表解析器

`IP Lists Parser`Lambda 函数有助于抵御第三方 IP 信誉列表中识别的已知攻击者。

IP 声誉列出了解析器流程。



1. 每小时一次的亚马逊 CloudWatch 事件会调用 Lambda 函数`IP Lists Parser`。
2. Lambda 函数从三个来源收集和解析数据：
   - Spamhaus DROP 和 EDROP 列表
   - Proofpoint 新兴威胁 IP 列表
   - Tor 退出节点列表
3. Lambda 函数使用当前 IP 地址更新 AWS WAF 阻止列表。

规划您的部署

本节介绍部署解决方案之前的成本、安全性、配额和其他注意事项。

支持的 AWS 区域

根据您定义的模板输入参数值，此解决方案需要不同的资源。这些资源（在下表中列出）可能并非在所有 AWS 区域都可用。因此，您必须在提供这些服务的 AWS 地区启动此解决方案。要了解按地区划分的 AWS 服务的最新可用性，请参阅 AWS 区域服务列表。

	AWS WAF Web ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
端点类型				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
激活 HTTP 洪水防护				
是的——AWS Lambda 日志解析器				✓
是的——亚马逊 Athena 日志解析器		✓	✓	✓
激活扫描仪和探头保护				
是的——亚马逊 Athena 日志解析器		✓	✓	

> **Note**
>
> 如果您选择CloudFront作为终端节点，则必须将解决方案部署在美国东部（弗吉尼亚北部）区域 (us-east-1)。

成本

运行适用于 AWS WAF 的安全自动化解决方案时使用的 AWS 服务的费用由您承担。运行此解决方案的总成本取决于激活的保护以及摄取、存储和处理的数据量。

我们建议通过 AWS Cost Explorer 创建预算，以帮助管理成本。有关完整详情，请参阅您在本解决方案中使用的每项 AWS 服务的定价网页。

下表是在美国东部（弗吉尼亚北部）区域（不包括 AWS 免费套餐）运行此解决方案的费用明细示例。价格可能会发生变化。

示例 1：激活信誉列表保护、恶意机器人保护、用于 HTTP 洪水防护的 AWS Lambda 日志解析器以及扫描器和探测器保护

AWS 服务	尺寸/月	成本 [美元]
Amazon Data Firehose	100 GB	大约 2.90 美元
Amazon S3	100 GB	大约 2.30 美元
AWS Lambda	128 MB：3 个函数，100 万次调用，每次 Lambda 运行的平均持续时间为 500 毫秒 512 MB：2 个函数，100 万次调用，每次 Lambda 运行的平均持续时间为 500 毫秒	大约 5.40 美元
AWS WAF 网络 ACL	1	5.00 美元
AWS WAF 规则	4	4.00 美元
AWS WAF 请求	1M	0.60 美元

AWS 服务	尺寸/月	成本 [美元]
总计		每月大约 20.60 美元

示例 2：激活信誉列表保护、恶意机器人防护、用于 HTTP 洪水防护的 Amazon Athena 日志解析器以及扫描器和探测器保护

AWS 服务	尺寸/月	成本 [美元]
Amazon Data Firehose	100 GB	大约 2.90 美元
Amazon S3	100 GB	大约 2.30 美元
AWS Lambda	128 MB：3 个函数，100 万次调用，每次 Lambda 运行的平均持续时间为 500 毫秒 512 MB：2 个函数，7560 次调用，每次 Lambda 运行的平均持续时间为 500 毫秒	大约 1.26 美元
Amazon Athena	每天有 120 万个 CloudFront 对象命中或 120 万个 ALB 请求，每次命中或请求都会生成大约 500 字节的日志记录	大约 4.32 美元
AWS WAF 网络 ACL	1	5.00 美元
AWS WAF 规则	4	4.00 美元
AWS WAF 请求	1M	0.60 美元
总计		每月大约 20.38 美元

示例 3：为允许和拒绝的 IP 集激活 IP 保留

AWS 服务	尺寸/月	成本 [美元]
Amazon DynamoDB	1 千次写入和 1 MB 的数据存储空间	大约 0.00 美元
AWS Lambda	128 MB：1 个函数，2K 次调用，每次 Lambda 运行的平均持续时间为 500 毫秒 512 MB：1 个函数，2K 次调用，每次 Lambda 运行的平均持续时间为 500 毫秒	大约 0.01 美元
Amazon CloudWatch	2K 赛事	大约 0.00 美元
AWS WAF Web ACL	1	5.00 美元
AWS WAF 规则	2	2.00 美元
WAS WAF 请求	1M	0.60 美元
总计		每月大约 7.61 美元

CloudWatch 日志的成本估算

此解决方案中使用的某些 AWS 服务（例如 Lambda）会生成 CloudWatch 日志。这些日志会产生费用。我们建议删除或存档日志以降低成本。有关日志存档的详细信息，请参阅 Amazon 日志用户指南中的将日志数据导出到 Amazon CloudWatch S3。

如果您选择在安装时使用 Athena 日志解析器，则此解决方案会根据配置安排对您的 Amazon S3 存储桶中的 AWS WAF 或应用程序访问日志运行查询。根据每次查询扫描的数据量向您收费。该解决方案将分区应用于日志和查询，以最大限度地降低成本。默认情况下，该解决方案会将应用程序访问日志从其原始 Amazon S3 位置移动到分区文件夹结构。您也可以保留原始日志，但您需要为重复的日志存储付费。此解决方案使用工作组对工作负载进行细分，您可以对两者进行配置以管理查询访问权限和成本。有关成本估算计算的示例，请参阅 Athena 的成本估算。有关更多信息，请参阅亚马逊 Athena 定价。

Athena 的成本估算

如果您在运行 HTTP 洪水防护、扫描器和探测器保护或恶意机器人保护规则时使用 Athena 日志解析器选项，则需要支付使用 Athena 的费用。默认情况下，每个 Athena 查询每五分钟运行一次，并扫描过去四个小时的数据。该解决方案将分区应用于日志和 Athena 查询，以最大限度地降低成本。您可以通过更改 WAF 封禁周期模板参数的值来配置查询扫描的数据小时数。但是，增加扫描的数据量可能会增加 Athena 的成本。

> **Tip**
>
> 以下是 CloudFront 日志成本计算示例：
> 平均而言，每次 CloudFront 命中可能生成大约 500 字节的数据。
> 如果每天有 120 万个 CloudFront 物体被命中，则假设以稳定的速度摄取数据，则每四小时将有 20 万次（120 万/6）次命中。在计算费用时，请考虑您的实际流量模式。
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena 每扫描一TB的数据收取5.00美元的费用。
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Athena 查询每五分钟运行一次，即每小时 12 次运行。
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> 实际成本因应用程序的流量模式而异。有关更多信息，请参阅亚马逊 Athena 定价。

安全性

当您在 AWS 基础设施上构建系统时，AWS 和您如何共同分担安全责任。此责任共担模式能够减轻您的运营负担，因为 AWS 负责运行、管理和控制各种组件，包括主机操作系统、虚拟化层和服务运行所在设施的物理安全性。有关 AWS 安全性的更多信息，请访问 AWS 云安全性。

IAM 角色

借助 IAM 角色，您可以向 AWS 云上的服务和用户分配精细的访问权限、策略和权限。此解决方案创建权限最低的 IAM 角色，这些角色为解决方案的资源授予所需的权限。

数据

存储在 Amazon S3 存储桶和 DynamoDB 表中的所有数据都处于静态加密状态。通过 Firehose 传输的数据也会经过加密。

保护能力

Web 应用程序容易受到各种攻击。这些攻击包括旨在利用漏洞或控制服务器的特制请求；旨在关闭网站的容量攻击；或者编程为抓取和窃取网页内容的不良机器人和抓取工具。

此解决方案 CloudFormation 用于配置 AWS WAF 规则，包括 AWS 托管规则组和自定义规则，以阻止以下常见攻击：

- AWS 托管规则-此托管服务提供针对常见应用程序漏洞或其他有害流量的保护。该解决方案包括 AWS 托管 IP 信誉规则组、AWS 托管基准规则组和 AWS 托管用例特定规则组。您可以选择为 Web ACL 选择一个或多个规则组，最高不超过 Web ACL 容量单位 (WCU) 的最大配额。
- SQL 注入-攻击者在 Web 请求中插入恶意 SQL 代码，以从您的数据库中提取数据。我们设计此解决方案是为了阻止包含潜在恶意 SQL 代码的 Web 请求。
- XSS-攻击者利用良性网站中的漏洞作为工具，将恶意客户端脚本注入合法用户的网络浏览器。我们设计它来检查传入请求中常见探索的元素，以识别和阻止 XSS 攻击。
- HTTP 洪水-Web 服务器和其他后端资源面临遭受 DDo S 攻击的风险，例如 HTTP 洪水。当来自客户端的 Web 请求超过可配置配额时，此解决方案会自动调用基于速率的规则。或者，您可以通过使用 Lambda 函数或 Athena 查询处理 AWS WAF 日志来强制执行此配额。
- 扫描仪和探测器-恶意来源通过发送一系列生成 HTTP 4xx 错误代码的请求来扫描和探测面向互联网的 Web 应用程序是否存在漏洞。您可以使用此历史记录来帮助识别和阻止恶意来源 IP 地址。此解决方案创建 Lambda 函数或 Athena 查询，用于自动解析 CloudFront 或 ALB 访问日志，计算每分钟来自唯一源 IP 地址的不良请求数量，并更新 AWS WAF 以阻止对达到定义的错误配额的地址进行进一步扫描。
- 已知的攻击者来源（IP 信誉列表）-许多组织都维护着由已知攻击者（例如垃圾邮件发送者、恶意软件分发者和僵尸网络）运营的 IP 地址的信誉列表。此解决方案利用这些信誉列表中的信息来帮助您阻止来自恶意 IP 地址的请求。此外，该解决方案还会根据 Amazon 内部威胁情报阻止由 IP 信誉规则组识别的攻击者。
- 机器人和抓取器-可公开访问的 Web 应用程序的运营商需要相信访问其内容的客户可以准确识别自己的身份，并且他们按预期使用服务。但是，一些自动化客户端，例如内容抓取工具或恶意机器人，为了绕过限制，会歪曲自己的陈述。此解决方案可帮助您识别和阻止恶意机器人和抓取程序。

配额

服务配额（也称为限制）是您的 AWS 账户使用的服务资源或操作的最大数量。

此解决方案中的 AWS 服务的配额

请确保此解决方案中实施的每项服务都有足够的配额。有关更多信息，请参阅 AWS 服务配额。要在不切换页面的情况下查看文档中所有 AWS 服务的服务配额，请改为查看 PDF 中服务终端节点和配额页面中的信息。

AWS WAF 配额

每个 IP 匹配条件，AWS WAF 最多可以屏蔽 10,000 个 IP 地址范围，采用无类域间路由 (CIDR) 表示法。此解决方案创建的每个列表都受此配额的约束。有关更多信息，请参阅 AWS WAF 配额。从 3.0 版本开始，此解决方案创建了两个 IP 集来附加到每个规则，一个用于 IPv4 ，一个用于 IPv6。

AWS WAF 允许在每个 AWS 区域的每个账户每秒向任何个人`Create`或`Update`操作发出 API 调用最多一个请求。`Put`如果您在解决方案之外进行这些 API 调用，则可能会遇到 API 限制问题。为防止出现此问题，我们建议避免在部署此解决方案的同一账户和区域中运行其他调用这些 API 的应用程序。

部署注意事项

以下各节提供了实施此解决方案的限制和注意事项。

AWS WAF 规则

此解决方案生成的 Web ACL 旨在为 Web 应用程序提供全面保护。该解决方案提供了一组 AWS 托管规则和自定义规则，您可以将其添加到 Web ACL 中。要包含规则，请在启动 CloudFormation 堆栈时选择`yes`相关参数。参见步骤 1。启动堆栈以获取参数列表。

> **Note**
>
> 该 out-of-box解决方案不支持 AWS Firewall Manager。如果要使用 Firewall Manager 中的规则，我们建议您对其源代码进行自定义。

Web ACL 流量记录

如果您在美国东部（弗吉尼亚北部）以外的 AWS 区域创建堆栈并将终端节点设置为`CloudFront`，则必须将 “激活 HTTP 防洪保护” 设置为`no`或`yes - AWS WAF rate based rule`。

其他两个选项（`yes - AWS Lambda log parser`和`yes - Amazon Athena log parser`）需要在所有 AWS 边缘站点上运行的 Web ACL 上激活 AWS WAF 日志，但美国东部（弗吉尼亚北部）以外地区不支持此操作。有关记录 Web ACL 流量的更多信息，请参阅 AWS WAF 开发人员指南。

对请求组件进行超大处理

AWS WAF 不支持检查网络请求组件的正文、标头或 Cookie 中的超大内容。当您编写检查其中一种请求组件类型的规则语句时，您可以选择以下选项之一来告诉 AWS WAF 如何处理这些请求：

- `yes`（继续）-根据规则检查标准正常检查请求组件。AWS WAF 会检查大小限制范围内的请求组件内容。这是解决方案中使用的默认选项。
- `yes - MATCH` – 将 Web 请求视为与规则语句匹配。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。对于带有`Block`操作的规则，这会阻止带有超大组件的请求。
- `yes - NO_MATCH`-将 Web 请求视为与规则声明不匹配，而不根据规则的检查标准对其进行评估。AWS WAF 继续使用网络 ACL 中的其余规则来检查 Web 请求，就像它对待任何不匹配的规则一样。

有关更多信息，请参阅在 AWS WAF 中处理超大的 Web 请求组件。

多种解决方案部署

您可以在同一个账户和区域中多次部署该解决方案。您必须为每个部署使用唯一的 CloudFormation 堆栈名称和 Amazon S3 存储桶名称。每次单独部署都会产生额外费用，并且受每个区域每个账户的 AWS WAF 配额限制。

部署的最低角色权限（可选）

客户可以手动创建具有部署所需最低权限的 IAM 角色：

- WAF 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:UpdateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:GetWebACL",
                "wafv2:ListWebACLs",
```

```
                "wafv2:CreateIPSet",
                "wafv2:UpdateIPSet",
                "wafv2:DeleteIPSet",
                "wafv2:GetIPSet",
                "wafv2:AssociateWebACL",
                "wafv2:DisassociateWebACL",
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration",
                "wafv2:ListWebACLs",
                "wafv2:ListIPSets",
                "wafv2:ListTagsForResource"
            ],
            "Resource": [
                "arn:aws:wafv2:*:*:regional/webacl/*",
                "arn:aws:wafv2:*:*:regional/ipset/*",
                "arn:aws:wafv2:*:*:global/webacl/*",
                "arn:aws:wafv2:*:*:global/ipset/*"
            ]
        }
```

- Lambda 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*"
        }
```

- Firehose 权限

```
        {
```

```
            "Effect": "Allow",
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- S3 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:PutBucketLogging",
                "s3:GetBucketLogging"
            ],
            "Resource": "arn:aws:s3:::*"
        }
```

- Athena 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "athena:CreateWorkGroup",
                "athena:DeleteWorkGroup",
                "athena:GetWorkGroup",
                "athena:UpdateWorkGroup",
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution"
            ],
            "Resource": "arn:aws:athena:*:*:workgroup/WAF*"
        }
```

- Glue 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch 日志权限

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream",
                "logs:PutRetentionPolicy",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/*",
                "arn:aws:logs:*:*:log-group:*",
                "arn:aws:logs:*:*:log-group:/aws/kinesisfirehose/*"
            ]
        }
```

- CloudWatch 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DeleteDashboards",
                "cloudwatch:GetDashboard",
                "cloudwatch:ListDashboards",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        }
```

- SNS 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:Subscribe",
```

```
                "sns:Unsubscribe",
                "sns:SetTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*"
        }
```

- DynamoDB 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeTable",
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/*"
        }
```

- CloudFormation 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "cloudformation:ListStacks"
            ],
            "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
        }
```

- Service Catalog 应用程序注册表权限

```
        {
```

```
            "Effect": "Allow",
            "Action": [
                "servicecatalog:CreateApplication",
                "servicecatalog:DeleteApplication",
                "servicecatalog:GetApplication",
                "servicecatalog:TagResource",
                "servicecatalog:CreateAttributeGroup",
                "servicecatalog:DeleteAttributeGroup",
                "servicecatalog:GetAttributeGroup",
                "servicecatalog:AssociateAttributeGroup",
                "servicecatalog:DisassociateAttributeGroup",
                "servicecatalog:AssociateResource",
                "servicecatalog:DisassociateResource"
            ],
            "Resource": "arn:aws:servicecatalog:*:*:*"
        }
```

- X-Ray 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords"
            ],
            "Resource": "*"
        }
```

- IAM 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
```

```
                "iam:GetRolePolicy",
                "iam:ListRoles",
                "iam:PassRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/*"
        }
```

- EventBridge 权限

```
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:DescribeRule",
                "events:EnableRule",
                "events:ListRules",
                "events:PutRule",
                "events:DeleteRule",
                "events:ListEventSources",
                "events:DescribeEventSource",
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

部署解决方案

该解决方案使用 AWS CloudFormation 模板和堆栈来自动部署。这些 CloudFormation 模板指定了此解决方案中包含的 AWS 资源及其属性。 CloudFormation 堆栈提供模板中描述的资源。

部署流程概述

在启动 CloudFormation 模板之前，请查看本指南中讨论的架构和配置注意事项。按照本节中的 step-by-step说明配置解决方案并将其部署到您的账户。

部署时间：大约 15 分钟。

> **Note**
>
> 如果您之前部署过此解决方案，请参阅更新解决方案以获取更新说明。

先决条件

- 配置 CloudFront 发行版
- 配置 ALB

第 1 步：启动堆栈

- 将 CloudFormation 模板启动到您的 AWS 账户。
- 输入所需参数的值：堆栈名称和应用程序访问日志存储桶名称。
- 查看其他模板参数，并根据需要进行调整。

第 2 步：将 Web ACL 与您的 Web 应用程序关联

- 将您 CloudFront 的 Web 发行版或 ALB 与该解决方案生成的网络 ACL 相关联。您可以根据需要关联任意数量的分配或负载均衡器。

第 3 步：配置 Web 访问日志

- 为您的网络分配或 ALB 开启 CloudFront 网络访问日志记录，并将日志文件发送到相应的 Amazon S3 存储桶。将日志保存在与用户定义前缀匹配的文件夹中。如果未使用用户定义的前缀，请将日志

保存到 AWSLogs（默认日志前缀AWSLogs/）。请参阅步骤 1 中的应用程序访问日志存储桶前缀参数。启动堆栈以获取更多信息。

AWS CloudFormation 模板

该解决方案包括一个主要 AWS CloudFormation 模板和两个嵌套模板。您可以在部署解决方案之前下载 CloudFormation 模板。

主堆栈

View template

aws-waf-security-automations.template-使用此模板作为切入点，在您的账户中启动解决方案。默认配置部署带有预配置规则的 AWS WAF Web ACL。您可以根据需要自定义模板。

WebACL 堆栈

View template

aws-waf-security-automations-webacl.template-此嵌套模板预配置 AWS WAF 资源，包括 Web ACL、IP、集合和其他相关资源。

Firehose Athena 堆栈

View template

aws-waf-security-automations-firehose-athena.template-此嵌套模板提供与 AWS Glue 、 Athena 和 Firehose 相关的资源。它是在你选择 S canner & Pro be Athena 日志解析器或 HTTP Flood Lambda 或 Athena 日志解析器时创建的。

> **Note**
>
> AWS CloudFormation 资源是基于 AWS Cloud Development Kit (AWS CDK) 结构创建的。

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

先决条件

此解决方案专为使用 CloudFront 或 ALB 部署的 Web 应用程序而设计。如果您尚未配置这些资源之一，请在启动此解决方案之前完成相应的任务。

配置 CloudFront 发行版

完成以下步骤，为 Web 应用程序的静态和动态内容配置 CloudFront 分发。有关详细说明，请参阅 Amazon CloudFront 开发者指南。

1. 创建 CloudFront Web 应用程序分发。请参阅创建分配。
2. 配置静态和动态来源。请参阅在 CloudFront 分布中使用各种原点。
3. 指定分配的行为。请参阅您在创建或更新分配时指定的值。

> **Note**
>
> 如果您选择`CloudFront`作为终端节点，则必须在美国东部（弗吉尼亚北部）地区创建 WAFV2 资源。

配置 ALB

要配置 ALB 以将传入流量分发到您的 Web 应用程序，请参阅应用程序负载均衡器用户指南中的创建应用程序负载均衡器。

第 1 步：启动 堆栈

此自动化 AWS CloudFormation 模板将该解决方案部署在 AWS 云上。

1. 登录 AWS 管理控制台并选择启动解决方案以启动`waf-automation-on-aws.template` CloudFormation 模板。

   Launch solution

2. 默认情况下，该模板在美国东部（弗吉尼亚州北部）区域启动。要在不同的 AWS 区域启动此解决方案，请使用控制台导航栏中的区域选择器。如果您选择`CloudFront`作为终端节点，则必须将解决方案部署在美国东部（弗吉尼亚北部）(`us-east-1`) 区域。

> **Note**
>
> 根据您定义的输入参数值，此解决方案需要不同的资源。这些资源目前仅在特定的 AWS 区域可用。因此，您必须在提供这些服务的 AWS 地区启动此解决方案。有关更多信息，请参阅支持的 AWS 区域。

3. 在 “指定模板” 页面上，验证您选择的模板是否正确，然后选择 “下一步”。
4. 在指定堆栈详细信息页面上，在堆栈名称字段中为您的 AWS WAF 配置分配一个名称。这也是模板创建的 Web ACL 的名称。
5. 在参数下，检查模板的参数，并根据需要进行修改。要选择退出某项特定功能，请选择none或no（如果适用）。该解决方案使用以下默认值。

参数	默认值	描述
堆栈名称	`[.red]#<requires input>`	堆栈名称不能包含空格。此名称在您的 AWS 账户中必须是唯一的，并且是模板创建的 Web ACL 的名称。
资源类型		
Endpoint	`CloudFront`	选择正在使用的资源类型。注意：如果您选择`CloudFront` 作为终端节点，则必须启动该解决方案才能在美国东部（弗吉尼亚北部）区域创建 WAF 资源 (`us-east-1`)。
AWS 托管 IP 信誉规则组		
激活 Amazon IP 信誉列表托管规则组保护	no	选择打开`yes`旨在将 Amazon IP 信誉列表托管规则组添加到 Web ACL 的组件。 该规则组基于 Amazon 内部威胁情报。如果您想屏蔽通常与机器人或其他威胁相关的 IP

参数	默认值	描述
		地址，则此功能非常有用。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。 所需的 WCU 为 25。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。
激活匿名 IP 列表托管规则组保护	no	选择打开yes旨在向 Web ACL 添加匿名 IP 列表托管规则组的组件。 此规则组阻止来自允许混淆查看者身份的服务的请求。其中包括来自代理 VPNs、Tor 节点和托管提供商的请求。如果要筛选出可能试图从应用程序中隐藏其身份的查看者，则此规则组非常有用。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。 所需的 WCU 为 50。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。
AWS 托管基线规则组		

参数	默认值	描述
激活核心规则集托管规则组保护	no	选择打开yes旨在向 Web ACL 添加核心规则集托管规则组的组件。 该规则组提供保护，防止利用各种漏洞，包括一些高风险漏洞和常见漏洞。考虑将此规则组用于任何 AWS WAF 用例。 所需的 WCU 是 700。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。
激活管理员保护托管规则组保护	no	选择打开yes旨在向 Web ACL 添加管理员保护托管规则组的组件。 此规则组阻止外部访问公开的管理页面。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。 所需的 WCU 为 100。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活已知错误输入托管规则组保护	no	选择打开yes旨在将已知错误输入托管规则组添加到 Web ACL 的组件。 此规则组阻止外部访问公开的管理页面。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。 所需的 WCU 为 100。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。
AWS 托管用例特定规则组		

参数	默认值	描述
激活 SQL 数据库托管规则组保护	no	选择打开yes旨在将 SQL 数据库托管规则组添加到 Web ACL 的组件。 此规则组阻止与 SQL 数据库利用相关的请求模式，例如 SQL 注入攻击。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。如果您已经激活了 AWS 托管 SQL 规则组，则使用 SQL 注入自定义规则是可选的。 所需的 WCU 为 200。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活 Linux 操作系统托管规则组保护	no	选择打开yes旨在将 Linux 操作系统托管规则组添加到 Web ACL 的组件。 该规则组阻止与利用 Linux 特有的漏洞相关的请求模式，包括 Linux 特有的本地文件包含 (LFI) 攻击。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。如果您的应用程序的任何部分在 Linux 上运行，请评估此规则组。您应将此规则组与 POSIX 操作系统规则组配合使用。 所需的 WCU 为 200。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活 POSIX 操作系统托管规则组保护	no	选择打开yes旨在向 Web ACL 添加核心规则集托管规则组保护的组件。 该规则组阻止与利用 POSIX 和类似 POSIX 的操作系统特有的漏洞（包括 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。如果您的应用程序的任何部分在 POSIX 或类似 POSIX 的操作系统上运行，请评估此规则组。 所需的 WCU 为 100。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活 Windows 操作系统托管规则组保护	no	选择打开yes旨在将 Windows 操作系统托管规则组添加到 Web ACL 的组件。 此规则组阻止与利用 Windows 特有的漏洞相关的请求模式，例如远程执行 PowerShell 命令。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。 所需的 WCU 为 200。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活 PHP 应用程序托管规则组保护	no	选择打开yes旨在将 PHP 应用程序托管规则组添加到 Web ACL 的组件。 该规则组阻止与利用 PHP 编程语言特有的漏洞（包括注入不安全的 PHP 函数）相关的请求模式。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。 所需的 WCU 为 100。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。

参数	默认值	描述
激活 WordPress 应用程序托管规则组保护	no	选择打开yes旨在将WordPress 应用程序托管规则组添加到 Web ACL 的组件。 此规则组阻止与利用特定于 WordPress 网站的漏洞相关的请求模式。如果您正在运行，请评估此规则组 WordPress。此规则组应与 SQL 数据库和 PHP 应用程序规则组配合使用。 所需的 WCU 为 100。您的账户应有足够的 WCU 容量，以避免因超出容量限制而导致 Web ACL 堆栈部署失败。 有关更多信息，请参阅 AWS 托管规则组列表。
自定义规则-扫描仪和探测器		
激活扫描仪和探头保护	`yes - AWS Lambda log parser`	选择用于阻挡扫描仪和探测器的组件。有关与缓解选项相关的权衡的更多信息，请参阅日志解析器选项。

参数	默认值	描述
应用程序访问日志存储桶名称	[.red]<requires input>	如果您选择了 yes “激活扫描器和探测保护” 参数，请输入您要存储 CloudFront 分配或 ALB 访问日志的 Amazon S3 存储桶（新的或现有的）的名称。如果您使用的是现有 Amazon S3 存储桶，则该存储桶必须位于部署 CloudFormation 模板的同一 AWS 区域。您应该为每个解决方案部署使用不同的存储桶。 要停用此保护，请忽略此参数。注意：为您的网络分配或 ALB 开启 CloudFront 网络访问日志以将日志文件发送到此 Amazon S3 存储桶。使用堆栈中定义的相同前缀（默认前缀AWSLogs/）保存日志。有关更多信息，请参阅应用程序访问日志存储桶前缀参数。

参数	默认值	描述
应用程序访问日志存储桶前缀	AWSLogs/	如果您选择了 yes “激活扫描仪和探测保护” 参数，则可以为上面的应用程序访问日志存储桶输入可选的用户定义前缀。 如果您选择了 CloudFront E ndpoin t 参数，则可以输入任何前缀，例如yourprefix/ 。 如果您选择了 ALB Endpoin t 参数，则必须在前缀后面AWSLogs/追加，yourprefix/AWSLogs/ 例如。 如果没有用户定义的前缀，则使用AWSLogs/（默认）。 要停用此保护，请忽略此参数。
存储桶访问日志是否已开启？	no	yes如果您在应用程序访问日志存储桶名称参数中输入了现有 Amazon S3 存储桶名称，并且该存储桶的服务器访问日志已开启，请选择此选项。 如果您愿意no，该解决方案会为您的存储桶启用服务器访问日志记录。 如果您选择了 no “激活扫描仪和探针保护” 参数，请忽略此参数。

参数	默认值	描述
错误阈值	50	如果您选择了 yes “激活扫描仪和探测保护” 参数，请输入每个 IP 地址每分钟可接受的最大错误请求数。 如果您选择了 no “激活扫描仪和探针保护” 参数，请忽略此参数。
将数据保存在原始 S3 位置	no	如果您选择了 yes - Amazon Athena log parser “激活扫描器和探测保护” 参数，则解决方案会将分区应用于应用程序访问日志文件和 Athena 查询。默认情况下，该解决方案会将日志文件从其原始位置移动到 Amazon S3 中的分区文件夹结构中。 选择yes是否还要将日志的副本保存在其原始位置。这将复制您的日志存储。 如果您没有选择 “yes - Amazon Athena log parser激活扫描仪和探针保护” 参数，请忽略此参数。
自定义规则-HTTP 洪水		
激活 HTTP 洪水防护	yes - AWS WAF rate-based rule	选择用于阻止 HTTP 洪水攻击的组件。有关与缓解选项相关的权衡的更多信息，请参阅日志解析器选项。

参数	默认值	描述
默认请求阈值	100	如果您选择了 yes “激活 HTTP 防洪保护” 参数，请输入每个 IP 地址每五分钟可接受的最大请求数。 如果您选择了 yes - AWS WAF rate-based rule “激活 HTTP 防洪保护” 参数，则可接受的最小值为10。 如果为 “激活 HTTP 防洪保护” 参数选择yes - AWS Lambda log parser或yes - Amazon Athena log parser，则它可以是任何值。 要停用此保护，请忽略此参数。

参数	默认值	描述
按国家/地区划分的请求阈值	<optional input>	如果您选择了 `yes - Amazon Athena log parser` “激活 HTTP 防洪保护” 参数，则可以按照此 JSON 格式按国家/地区输入阈值`{"TR":50,"ER":150}` 。该解决方案对来自指定国家/地区的请求使用这些阈值。该解决方案对剩余的请求使用默认请求阈值参数。注意：如果您定义此参数，则国家/地区将自动包含在 Athena 查询组中，还会自动包含在 IP 和其他可选的分组依据字段中，您可以使用 HTTP Flood 中的请求分组 Athena 查询参数选择这些字段。 + 如果您选择停用此保护，请忽略此参数。
在 HTTP Flood Athena 查询中按请求分组	None	如果您选择了 `yes - Amazon Athena log parser` “激活 HTTP 洪水保护” 参数，则可以选择分组依据字段来计算每个 IP 的请求数，也可以选择选定的分组依据字段。例如，如果您选择URI，则解决方案会计算每个 IP 和 URI 的请求数。 如果您选择停用此保护，请忽略此参数。

参数	默认值	描述
WAF 封禁周期	240	如果您yes - Amazon Athena log parser为 “激活扫描仪和探测器保护” 或 “激活 HTTP 洪水防护” 参数选择yes - AWS Lambda log parser了或，请输入屏蔽适用的 IP 地址的时段（以分钟为单位）。 要停用日志解析，请忽略此参数。
Athena 查询运行时间安排（分钟）	5	如果您选择了 yes - Amazon Athena log parser “激活扫描器和探测器保护” 或 “激活 HTTP 洪水防护” 参数，则可以输入 Athena 查询运行的时间间隔（以分钟为单位）。默认情况下，Athena 查询每 5 分钟运行一次。 如果您选择停用这些保护，请忽略此参数。

参数	默认值	描述
规则密钥	IP	如果您选择了 yes - AWS WAF rate-based rule “激活 HTTP 防洪保护” 参数，请将此规则配置为使用各种其他聚合密钥组合。可用选项: IP（默认） IP+自定义标头（如果选择此选项，Rule Keys Custom Header则为必填项） IP+URI IP+HTTP 方法 有关更多信息，请参阅基于 WAF 规则速率的聚合选项。
规则密钥自定义标题	no	如果您选择了IP+Custom Header规则密钥参数，请输入用于请求聚合的自定义标头的名称。 有关更多信息，请参阅 WAF 规则语句类型基于速率的聚合选项。

参数	默认值	描述
时间窗阈值（分钟）	5	HTTP 洪水防护的时间窗口阈值（以分钟为单位）。适用于基于速率的规则和 lambda 日志解析器。可用选项：[1、2、5、10]。 如果您选择 `yes - AWS WAF rate-based rule` “激活 HTTP 防洪保护” 参数将用于评估时间窗口。有关更多信息，请参阅基于 WAF Web ACL 速率的语句。 如果您选择 `yes - AWS Lambda log parser` “激活 HTTP 防洪保护” 参数，则除了封锁期外，还将用于评估期。
自定义规则-Bad Bot		
激活恶意机器人防护	`yes`	选择开启`yes`旨在屏蔽恶意机器人和内容抓取器的组件。
对您的账户中的 CloudWatch 日志具有写入权限的 IAM 角色的 ARN	<optional input>	提供对您账户中 CloudWatch 日志具有写入权限的 IAM 角色的可选 ARN。 例如：`ARN: arn:aws:iam::account_id:role/myrolename` 。 如果将此参数留空（默认），则解决方案会为您创建一个新角色。

参数	默认值	描述
自定义规则-第三方 IP 信誉列表		
激活信誉列表保护	yes	选择yes阻止来自第三方信誉列表上的 IP 地址的请求（支持的列表包括 Spamhaus、新兴威胁和 Tor 退出节点）。
旧版自定义规则		
激活 SQL 注入保护	yes	选择打开yes旨在阻止常见 SQL 注入攻击的组件。如果您未使用 AWS 托管核心规则集或 AWS 托管 SQL 数据库规则组，请考虑将其激活。 您可以选择一个您希望 AWS WAF 处理超过 8 KByes（8192 字节yes - NO_MATCH）的超大请求的选项（（继续）yes - MATCH、或）。默认情况下，根据规则yes检查标准检查大小限制范围内的请求组件内容。有关更多信息，请参阅处理超大的 Web 请求组件。 选择停no用此功能。注意：CloudFormation 堆栈会将选定的超大处理选项添加到默认 SQL 注入保护规则中，并将其部署到您的 AWS 账户。如果您在之外自定义了规则 CloudFormation，则堆栈更新后您的更改将被覆盖。

参数	默认值	描述
SQL 注入保护的敏感度级别	LOW	选择您希望 AWS WAF 用来检查 SQL 注入攻击的敏感度级别。 HIGH检测到更多的攻击，但可能会产生更多的误报。 对于已经具有针对 SQL 注入攻击的其他保护或对误报具有低容忍度的资源，LOW 通常是更好的选择。 有关更多信息，请参阅 AWS CloudFormation 用户指南中的 AWS WAF 为 SQL 注入规则语句和SensitivityLevel 属性添加敏感级别。 如果您选择停用 SQL 注入保护，请忽略此参数。注意：CloudFormation 堆栈会将选定的敏感度级别添加到默认 SQL 注入保护规则中，并将其部署到您的 AWS 账户。如果您在之外自定义了规则 CloudFormation，则堆栈更新后您的更改将被覆盖。

参数	默认值	描述
激活跨站点脚本保护	yes	选择开启yes旨在阻止常见 XSS 攻击的组件。如果您不使用 AWS 托管核心规则集，请考虑将其激活。您也可以选择您希望 AWS WAF 处理超过 8 KByes（8192 字节yes - NO_MATCH）的超大请求的选项（（继续）yes - MATCH、或）。默认情况下，yes使用Continue选项，该选项根据规则检查标准检查大小限制范围内的请求组件内容。有关更多信息，请参阅请求组件的超大处理。 选择停no用此功能。注意：CloudFormation 堆栈会将选定的超大处理选项添加到默认的跨站点脚本规则中，并将其部署到您的 AWS 账户中。如果您在之外自定义了规则 CloudFormation，则堆栈更新后您的更改将被覆盖。
允许和拒绝的 IP 保留设置		

参数	默认值	描述
允许的 IP 集的保留期（分钟）	-1	如果要为允许的 IP 集激活 IP 保留，请输入一个数字（15或更大）作为保留期（分钟）。达到保留期的 IP 地址会过期，解决方案会将其从 IP 集中删除。该解决方案支持至少 15 分钟的保留期。如果您输入介于0和之间的数字15，则解决方案会将其视为15。 将其保留为-1（默认）以关闭 IP 保留。
被拒绝 IP 集的保留期（分钟）	-1	如果要激活 “被拒绝 IP” 集的 IP 保留，请输入一个数字（15或更大）作为保留期（分钟）。达到保留期的 IP 地址会过期，解决方案会将其从 IP 集中删除。该解决方案支持至少 15 分钟的保留期。如果您输入介于0和之间的数字15，则解决方案会将其视为15。 将其保留为-1（默认）以关闭 IP 保留。
用于在允许或拒绝的 IP 集到期时接收通知的电子邮件	<optional input>	如果您激活了 IP 保留期参数（参见前面的两个参数），并希望在 IP 地址到期时收到电子邮件通知，请输入有效的电子邮件地址。 如果您没有激活 IP 保留或想要关闭电子邮件通知，请将其留空（默认）。

参数	默认值	描述
高级设置		
日志组的保留期（天）	365	如果要激活 CloudWatch 日志组的保留期，请输入一个数字（1或更大）作为保留期（天）。您可以选择介于一天 (1) 和十年 (3650) 之间的保留期。默认情况下，日志将在一年后过期。 将其设置-1为可无限期保留日志。

6. 选择下一步。
7. 在配置堆栈选项页面上，您可以为堆栈中的资源指定标签（键值对），并设置其他选项。选择下一步。
8. 在 “查看并创建” 页面上，查看并确认设置。选中确认模板将创建 IAM 资源以及所需的任何其他功能的复选框。
9. 选择提交以部署堆栈。

   在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。你应该会在大约 15 分钟后收到 CREATE_COMPLETE 的状态。

> **Note**
>
> 除Log Parser和 IP Lists Parser AWS Lambda 函数外，此解决方案还包括和 helper Lamb custom-resource da 函数，它们仅在初始配置期间或更新或删除资源时运行。
> 使用此解决方案时，您将在 AWS Lambda 控制台中看到所有功能，但只有三个主要的解决方案功能定期处于活动状态。不要删除其他两个函数；它们是管理关联资源所必需的。

要查看堆栈资源的详细信息，请选择输出选项卡。这包括该BadBotHoneypotEndpoint值。请记住这个值，因为你将在 Web 应用程序的 “嵌入 Honeypot” 链接中使用它。

第 2 步：将 Web ACL 与您的 Web 应用程序关联

使用您在 CloudFront 步骤 1 中生成的资源更新您的分配或 ALB 以激活 AWS WAF 并进行日志记录。Launch the stack。

1. 登录 AWS WAF 控制台。
2. 选择要使用的网络 ACL。
3. 在关联的 AWS 资源选项卡上，选择添加 AWS 资源。
4. 在资源类型下，选择 CloudFront 分配或 ALB。
5. 从列表中选择一个资源，然后选择 “添加” 以保存您的更改。

第 3 步：配置 Web 访问日志记录

将 CloudFront 或您的 ALB 配置为将 Web 访问日志发送到相应的 Amazon S3 存储桶，以便日志解析器 Lambda 函数可以使用这些数据。

存储来自 CloudFront 分配的 Web 访问日志

1. 登录 Amazon CloudFront 控制台。
2. 选择 Web 应用程序的发行版，然后选择 “分发设置”。
3. 在 General 选项卡上，选择 Edit。
4. 对于 AWS WAF Web ACL，请选择创建的 Web ACL 解决方案（堆栈名称参数）。
5. 对于 Logging，选择 On。
6. 对于日志存储桶，请选择要用于存储 Web 访问日志的 S3 存储桶。这可以是在主堆栈中使用并有权写入日志的新的 S3 存储桶或现有的 CloudFront S3 存储桶。下拉列表列举了与当前 AWS 账户关联的存储桶。有关更多信息，请参阅《Amazon CloudFront 开发者指南》中的基本 CloudFront 发行版入门。
7. 将日志前缀设置为用于部署解决方案的前缀。你可以在主堆栈的 “参数” 选项卡中找到前缀 AppAccessLogBucketPrefixParam（默认`AWSLogs/`）。
8. 选择 Yes, edit 以保存所做更改。

有关更多信息，请参阅《Amazon CloudFront 开发者指南》中的配置和使用标准日志（访问日志）。

存储来自 Application Load Balancer 的 Web 访问日志

1. 登录亚马逊弹性计算云 (Amazon EC2) 控制台。
2. 在导航窗格中，选择负载均衡器。
3. 选择您的 Web 应用程序的 ALB。
4. 在说明选项卡上，选择编辑属性。
5. 选择 Enable access logs。
6. 对于 S3 位置，键入要用于存储 Web 访问日志的 S3 存储桶的名称。这可以是新的或现有的 S3 存储桶，用于主堆栈，并拥有 Application Load Balancer 写入日志的权限。
7. 将日志前缀设置为用于部署解决方案的前缀。你可以在主堆栈的 “参数” 选项卡中找到前缀 AppAccessLogBucketPrefixParam（默认`AWSLogs/`）。
8. 选择保存。

有关更多信息，请参阅 Ela stic Load Balancing 用户指南中的应用程序负载均衡器的访问日志。

更新此解决方案

如果您之前部署了该解决方案，请按照以下步骤更新解决方案 CloudFormation 堆栈以获取最新版本的解决方案框架。在更新堆栈之前，请仔细阅读更新注意事项。

1. 登录 A WS CloudFormation 控制台。
2. 在左侧导航菜单中选择 Stacks。
3. 选择您现有的`aws-waf-security-automations` CloudFormation 堆栈。
4. 选择更新。
5. 选择替换当前模板。
6. 在指定模板下：
   a. 选择 Amazon S3 URL。
   b. 复制 A `aws-waf-security-automations.template` WS 的链接 CloudFormation。
   c. 将链接粘贴到 Amazon S3 URL 框中。
   d. 确认 Amazon S3 网址文本框中显示的模板网址是否正确。
   e. 选择下一步。
   f. 再次选择下一步。
7. 在参数下，检查模板的参数，并根据需要进行修改。请参阅 Step 1. Launch the stack 以获取有关参数的详细信息。
8. 选择 Next(下一步)。
9. 在 配置堆栈选项 页面上，请选择 下一步。
10. 在 Review 页面上，审核并确认设置。
11. 选中确认模板可能创建 IAM 资源的复选框。
12. 选择查看更改集并验证更改。
13. 选择更新堆栈以部署堆栈。

您可以在 AWS CloudFormation 控制台的 “状态” 列中查看堆栈的状态。您应在大约 15 分钟后看到 UPDATE_COMPLETE 状态。

更新注意事项

以下各节提供了更新此解决方案的限制和注意事项。

资源类型更新

创建堆栈后，必须部署新的堆栈才能更新 Endpoin t 参数。更新堆栈时不要更改 Endpoin t 参数。

WAFV2 升级

从 3.0 版本开始，此解决方案支持 AWS WAFV2。我们将所有 AWS WAF C lassic API 调用替换为 AW WAFV2 S API 调用。这将移除对 Node.js 的依赖并使用最多的 up-to-date Python 运行时。要继续使用具有最新功能和改进的解决方案，必须将 3.0 或更高版本部署为新堆栈。

堆栈更新时的自定义

该 out-of-box解决方案使用堆栈将一组带有默认配置的 AWS WAF 规则部署到您的 AWS 账户中。CloudFormation 我们不建议对解决方案部署的规则进行自定义。堆栈更新会覆盖这些更改。如果您需要自定义规则，我们建议您在解决方案之外创建单独的规则。

Bad bot 保护升级

在 4.1.0 版本中，带有 API Gatew ay 的访问处理程序 Lambda 已被弃用，取而代之的是该功能中增强的日志功能。`Log parser - Bad bot`现在，该解决方案不再使用通过 API Gateway 的直接请求，而是重复使用日志流来检测恶意机器人。

之前的实现：

1. 必需的访问处理程序 Lambda 和 API Gateway。
2. 使用 honeypot 端点直接处理请求。
3. 需要在网站上嵌入 honeypot 端点。

新实现 (4.1.0+)：Ba d Bot Protection 日志解析器现已推出：

1. 通过日志检查对 honeypot 端点的请求。
2. 激活 Ba d Bot 保护后处理请求。
3. 使用 WAF 过滤器BadBotRuleFilter识别不良的机器人请求。
4. 分析日志数据以识别超出定义配额的 IP 地址。
5. 更新 AWS WAF IP 设置条件以屏蔽已识别的地址。

此更改通过消除重复功能并利用现有的日志处理功能来简化架构。

CDK 升级

从 v4.1.0 版本开始，CDK 支持此解决方案。如果从 v4.1.0 以下的版本迁移。在 Cloudformation 中使用新的模板并更新解决方案。然后你可以开始使用 cdk deploy 通过终端在本地更新解决方案（有关更多信息，请参阅自述文件）如果你尝试直接使用 cdk deploy，那么你可能会看到这个错误：流量收集中的缩进不足

更新解决方案的另一种方法是使用解决方案提供的模板，然后转到 AWS 控制台的 Cloudformation 部分，点击更新解决方案，然后将新模板粘贴到那里。

> **Note**
>
> 如果您要从本解决方案的 3.0 或 3.1 版本升级到 3.2 或更高版本，并且已手动将 IP 地址插入到允许或拒绝的 IP 集中，则将面临丢失这些 IP 地址的风险。为防止这种情况发生，请在升级解决方案之前，复制允许或拒绝的 IP 集中的 IP 地址。然后，在完成升级后，根据需要将 IP 地址重新添加到 IP 集中。请参阅get-ip-set和 C update-ip-setLI 命令。如果您已经在使用 3.2 或更高版本，请忽略此步骤。

卸载此解决方案

要卸载解决方案，请删除 CloudFormation 堆栈：

1. 登录 A WS CloudFormation 控制台。
2. 选择解决方案的父堆栈。所有其他解决方案堆栈将被自动删除。
3. 选择删除。

> **Note**
>
> 卸载该解决方案会删除该解决方案使用的所有 AWS 资源，但 Amazon S3 存储桶除外。如果由于 AWA WAF API 配额导致的超速限制问题导致某些 IP 集无法删除，请手动删除这些 IP 集，然后删除堆栈。

使用解决方案

本节提供部署解决方案后如何使用该解决方案的详细说明。

修改允许和拒绝的 IP 集（可选）

部署此解决方案的 CloudFormation 堆栈后，您可以根据需要手动修改允许和拒绝的 IP 集以添加或删除 IP 地址。

1. 登录 AWS WAF 控制台。
2. 在左侧导航窗格中，选择 IP 集。
3. 为允许列表选择 IP 设置，然后添加来自可信来源的 IP 地址。
4. 为拒绝列表选择设置的 IP，然后添加要阻止的 IP 地址。

在你的 Web 应用程序中嵌入 Honeypot 链接（可选）

如果您在步骤 1 中选择了 `yes` “激活恶意机器人保护” 参数。启动堆栈，CloudFormation 模板为低交互生产蜜罐创建陷阱端点。此陷阱旨在检测和转移来自内容抓取器和恶意机器人的入站请求。有效用户不会尝试访问此端点。

除了 honeypot 机制外，该组件还通过监控与 Application Load Balancer (ALB) 或 Amazon CloudFront 的直接连接来增强恶意机器人检测。如果机器人绕过蜜罐尝试与 ALB 或交互 CloudFront，则系统会分析请求模式和日志以识别恶意活动。当检测到恶意机器人时，系统会提取其 IP 地址并将其添加到 AWS WAF 阻止列表中，以防止进一步访问。恶意机器人检测通过结构化的逻辑链运行，确保全面的威胁覆盖：

- HTTP Flood Protection Lambda 日志解析器 — 在洪水分析期间 IPs 从日志条目中收集恶意机器人。
- Scanner & Probe Protection Lambda 日志解析器 — IPs 从与扫描仪相关的日志条目中识别不良机器人。
- HTTP Flood Protection Athena 日志解析器 — 使用跨查询运行的分区 IPs 从 Athena 日志中提取恶意机器人。
- Scanner & Probe Protection Athena 日志解析器 — 使用相同的分区策略 IPs 从与扫描仪相关的 Athena 日志中检索恶意机器人。
- 回退检测-如果同时禁用 HTTP 洪水防护和扫描器和探测器保护，则系统将依赖日志 Lambda 解析器，该解析器基于 WAF 标签筛选器记录机器人活动。

使用以下过程之一为来自任一 CloudFront 分配的请求嵌入 honeypot 链接。

为 Honeypot 端点创建 CloudFront 起源

对于使用 CloudFront 发行版部署的 Web 应用程序，请使用此过程。使用 CloudFront，您可以添加一个`robots.txt`文件来帮助识别忽略机器人排除标准的内容抓取者和机器人。完成以下步骤以嵌入隐藏链接，然后在您的`robots.txt`文件中明确禁止该链接。

1. 登录 A WS CloudFormation 控制台。
2. 选择您在步骤 1 中构建的堆栈。启动堆栈
3. 选择输出选项卡。
4. 从BadBotHoneypotEndpoint密钥中复制终端节点 URL。
   - 行为路径 (`/ProdStage`)
5. 在指向蜜罐的内容中嵌入此端点链接。向您的人类用户隐藏此链接。例如，请查看以下代码示例：`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`。
6. 修改网站根目录中的`robots.txt`文件以明确禁止 honeypot 链接，如下所示：

```
User-agent: <*>
        Disallow: /<behavior_path>
```

> **Important**
>
> 不需要在中注册路径，因为请求 CloudFront 是：被 WAF BadBotRuleFilter阻止。解决方案会自动收集到日志中。由日志解析器 lambda 处理。这种简化的方法直接使用 WAF 日志，无需进行额外的端点配置，从而通过日志分析提高了恶意机器人检测过程的效率

> **Note**
>
> 您有责任验证哪些标签值在您的网站环境中起作用。`rel="nofollow"`如果您的环境没有观察到它，请不要使用。有关机器人元标记配置的更多信息，请参阅 Google 开发者指南。修改网站根目录中的`robots.txt`文件以明确禁止 honeypot 链接，如下所示：

将 Honeypot 端点嵌入为外部链接

> **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。

对于 Web 应用程序，请使用此程序。

1. 登录 A WS CloudFormation 控制台。
2. 选择您在步骤 1 中构建的堆栈。Launch the stack。
3. 选择输出选项卡。
4. 从BadBotHoneypotEndpoint密钥中复制终端节点 URL。

```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-hidden="true"><honeypot link></a>
```

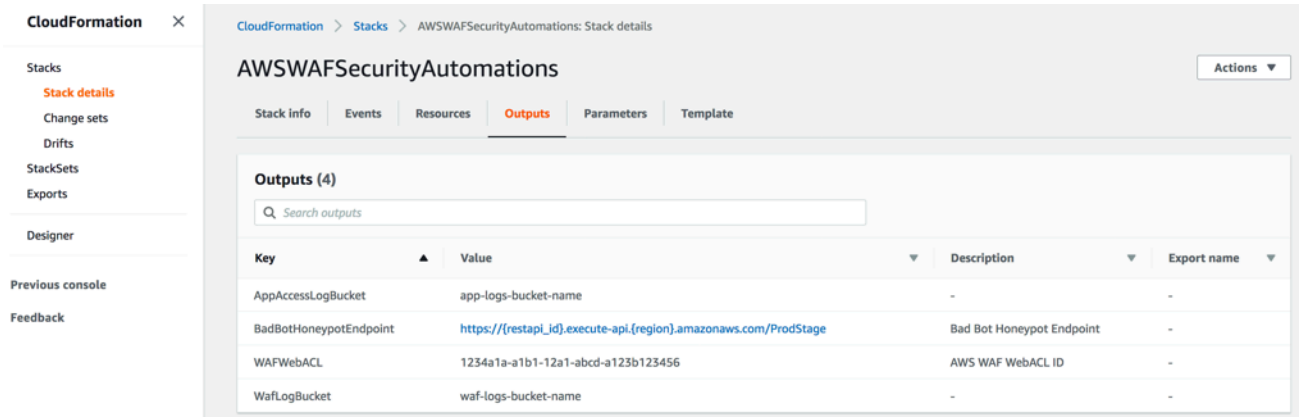
> **Note**
>
> 此过程`rel=nofollow`用于指示机器人不要访问蜜罐 URL。但是，由于链接是在外部嵌入的，因此您不能包含明确禁止该链接的`robots.txt`文件。您有责任验证哪些标签在您的网站环境中起作用。`rel="nofollow"`如果您的环境没有观察到它，请不要使用。

使用 Lambda 日志解析器 JSON 文件

使用 Lambda 日志解析器 JSON 文件进行 HTTP 洪水防护

如果您选择激活 HTTP 防洪模板参数，则此解决方案会创建一个名`Yes - AWS Lambda log parser`为的配置文件 `<stack_name>-waf_log_conf.json`并将其上传到用于存储 AWS WAF 日志文件的 Amazon S3 存储桶。要查找存储桶名称，请参阅 CloudFormation 输出中的WafLogBucket变量。下图显示了一个示例。

屏幕截图描绘了标有 “ AWSWAFSecurity自动化” 的屏幕并列出了四个输出



如果您在 Amazon S3 上编辑和覆盖该 `<stack_name>-waf_log_conf.json`文件，Lamb Log `Parser` da 函数在处理新的 AWS WAF 日志文件时会考虑新值。以下是一个示例代理配置文件：

示例配置文件的屏幕截图

```
{
 "general": {
    "requestThreshold": 2000,
    "blockPeriod": 240,
    "ignoredSufixes": [".css", ".js", ".jpg", "png", ".gif"]
  },
 "uriList": {
    "/search": {
        "requestThreshold": 500,
        "blockPeriod": 600
    }
  }
}
```

参数包括以下内容：

- 常规：
  - 请求阈值（必填）-每个 IP 地址每五分钟可接受的最大请求数。此解决方案使用您在配置或更新 CloudFormation 堆栈时定义的值。
  - 封禁期限（必填）-封锁适用 IP 地址的时间段（以分钟为单位）。此解决方案使用您在配置或更新 CloudFormation 堆栈时定义的值。
  - 忽略的后缀-访问此类资源的请求不计入请求阈值。默认情况下，此列表为空。
- URI 列表-使用它来定义自定义请求阈值和屏蔽期限，以了解具体情况 URLs。默认情况下，此列表为空。

当 WAF 日志到达时 WafLogBucket，Lambda 日志解析器函数将使用您的配置文件中的配置对其进行处理。该解决方案将结果写入同一个存储桶 `<stack_name>-waf_log_out.json`中名为的输出文件中。如果输出文件包含识别为攻击者的 IP 地址列表，则该解决方案会将其添加到 HTTP Floo d 的 WAF IP 集中，并阻止他们访问您的应用程序。如果输出文件没有 IP 地址，请根据配置文件检查您的配置文件是否有效或者是否已超过速率限制。

使用 Lambda 日志解析器 JSON 文件进行扫描和探测保护

如果您选择 “激活扫描器和探测保护” 模板参数，则此解决方案会创建一个名`Yes - AWS Lambda log parser`为的配置文件 `<stack_name>-app_log_conf.json`并将其上传到用于存储 CloudFront 或 Application Load Balancer 日志文件的已定义 Amazon S3 存储桶。

如果您在 Amazon S3 上进行编辑和覆盖，Lamb Log Parser da 函数 `<stack_name>-app_log_conf.json`在处理新的 AWS WAF 日志文件时会考虑新值。以下是一个示例代理配置文件：

配置文件屏幕截图

```
{
    "general": {
        "errorThreshold": 50,
        "blockPeriod": 240,
        "errorCodes": ["400", "401", "403", "404", "405"]
    },
    "uriList": {
        "/login": {
            "errorThreshold": 5,
            "blockPeriod": 600
        },
        "/api/feedback": {
            "errorThreshold": 10,
            "blockPeriod": 240
        }
    }
}
```

参数包括以下内容：

- 常规：
  - 错误阈值（必填）-每个 IP 地址每分钟可接受的最大错误请求数。此解决方案使用您在配置或更新 CloudFormation 堆栈时定义的值。
  - 封禁期限（必填）-封锁适用 IP 地址的时间段（以分钟为单位）。此解决方案使用您在配置或更新 CloudFormation 堆栈时定义的值。
  - 错误代码-返回状态码被视为错误。默认情况下，该列表将以下 HTTP 状态代码视为错误：`400 (Bad Request)401 (Unauthorized)`、`403 (Forbidden)`、`404 (Not Found)`、和`405 (Method Not Allowed)`。

- URI 列表-使用它来定义自定义请求阈值和屏蔽期限，以了解具体情况 URLs。默认情况下，此列表为空。

当应用程序访问日志到达时 AppAccessLogBucket，Log ParserLambda 函数会使用您的配置文件中的配置对其进行处理。该解决方案将结果写入同一个存储桶中名为 <stack_name>`-app_log_out.json` 的输出文件中。如果输出文件包含识别为攻击者的 IP 地址列表，则该解决方案会将其添加到 S canner & Prob e 的 WAF IP 集中，并阻止他们访问您的应用程序。如果输出文件没有 IP 地址，请根据配置文件检查您的配置文件是否有效或者是否已超过速率限制。

在 HTTP 洪水中使用国家/地区和 URI Athena 日志解析器

您可以在 Athena 查询中 IPs 按国家/地区和 URI 进行分组，以检测和阻止 URI 模式不可预测的 HTTP 洪水攻击。为此，请在启动堆栈时为 HTTP Flood 中的请求分组 Athena Query 参数选择一个选项（CountryURI、、Country and URI）。

您也可以使用 “按国家/地区划分的请求阈值” 参数按国家/地区输入请求阈值。例如 {"TR": 50,"ER":150}。该解决方案对来自这些特定国家/地区的请求使用这些阈值。该解决方案对来自其他国家/地区的请求使用默认阈值。

> **Note**
>
> 如果您按国家/地区定义阈值，则解决方案会自动将该国家/地区包含在 Athena 查询 group-by 子句中。有关更多信息，请参阅步骤 1 中的参数表。Launch the stack。

默认情况下，该解决方案会计算五分钟内的请求阈值。可以使用 Athena Query 运行时间计划（分钟）参数进行配置。

> **Note**
>
> Athena 查询通过将请求阈值除以时间段来计算每分钟的阈值。例如：
> 请求阈值（按国家/地区划分的默认阈值或阈值）：100
> Athena Query 运行时间安排：5
> 每分钟请求阈值：20 = 100/ 5

查看亚马逊 Athena 查询

如果您选择了 `Yes - Amazon Athena log parser` “激活 HTTP 洪水防护” 或 “激活扫描器和探测器保护” 模板参数，则此解决方案会 CloudFront 为或 ALB `ScannersProbesLogParser` () 或 AWS WAF 日志 `HTTPFloodLogParser` () 创建并运行 Athena 查询，解析输出并相应地更新 AWS WAF。

为了提高性能并降低成本，该解决方案根据文件名中的时间戳对日志进行分区。该解决方案动态生成使用分区键（年、月、日和小时）的 Athena 查询。默认情况下，查询每五分钟运行一次。您可以通过更改 Athena Query 运行时间计划（分钟）模板参数的值来配置他们的运行计划。默认情况下，每次查询运行都会扫描最近四到五个小时的数据。您可以通过更改 WAF 封禁周期模板参数的值来配置查询扫描的数据量。该解决方案还将查询放在单独的工作组中，以管理查询访问权限和成本。

> **Note**
>
> 验证 Athena 是否已配置为访问 AWS Glue 数据目录。此解决方案在 AWS Glue 中创建访问日志数据目录，并配置 Athena 查询来处理数据。如果 Athena 配置不正确，则查询将无法运行。有关更多信息，请参阅升级到最新的 AWSAWS Glue 数据目录 step-by-step。

使用以下步骤查看这些查询：

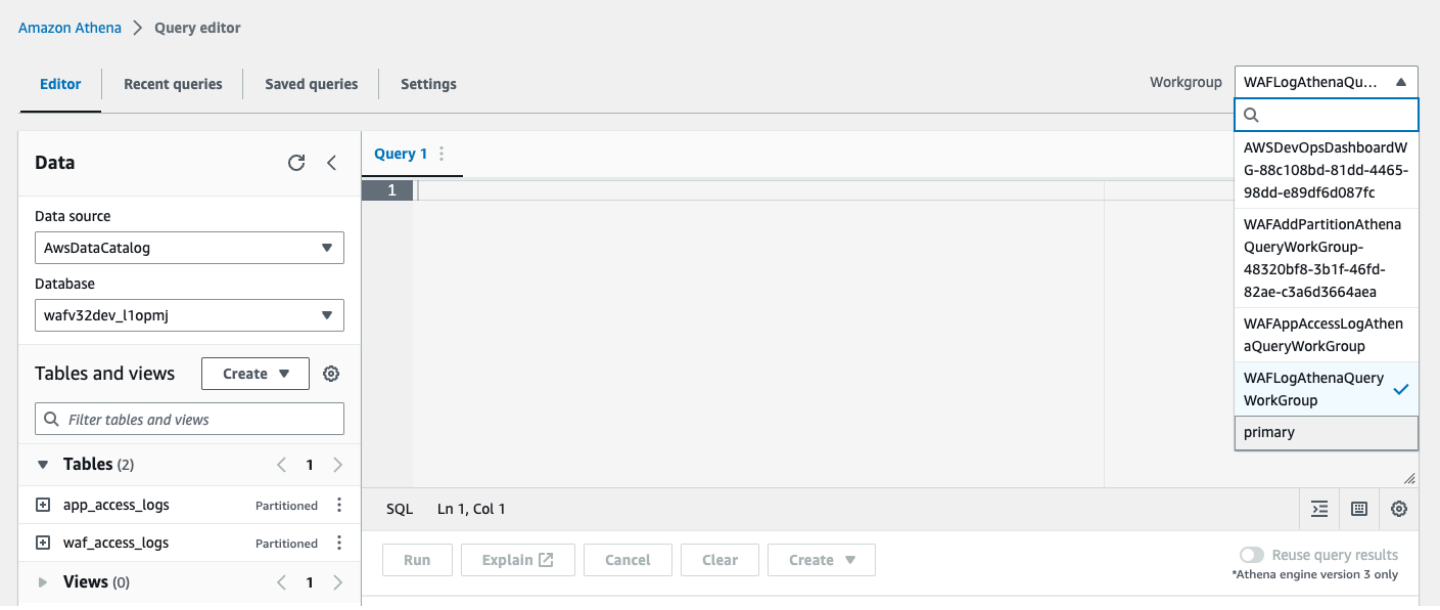
查看 WAF 日志查询

1. 登录亚马逊 Athena 控制台。
2. 选择启动查询编辑器。
3. 为此解决方案选择数据库。
4. WAFLogAthenaQueryWorkGroup从下拉列表中选择。

> **Note**
>
> 仅当您选择 `Yes - Amazon Athena log parser` “激活 HTTP 洪水防护” 模板参数时，此工作组才会存在。

5. 选择 “切换” 以切换工作组。

Athena 查询编辑器的屏幕截图未显示任何查询



1. 选择 “历史记录” 选项卡。
2. 从列表中选择并打开SELECT查询。

查看应用程序访问日志查询

1. 登录亚马逊 Athena 控制台。
2. 选择 “工作组” 选项卡。
3. 从列表中选择 WAFAppAccessLogAthenaQueryWorkGroup。

> **Note**
>
> 仅当您选择了 “激活扫描仪和探测**Yes - Amazon Athena log parser**器保护” 模板参数时，此工作组才存在。

4. 选择 “切换工作组”。
5. 选择 “最近的查询” 选项卡。
6. 从列表中选择并打开SELECT查询。

查看添加 Athena 分区查询

1. 登录亚马逊 Athena 控制台。

2. 选择 “工作组” 选项卡。
3. 从列表中选择 WAFAddPartitionAthenaQueryWorkGroup。

> **Note**
>
> 仅当您选择 `Yes - Amazon Athena log parser` “激活 HTTP 洪水保护 and/or 激活扫描仪和探测器保护” 模板参数时，此工作组才会存在。

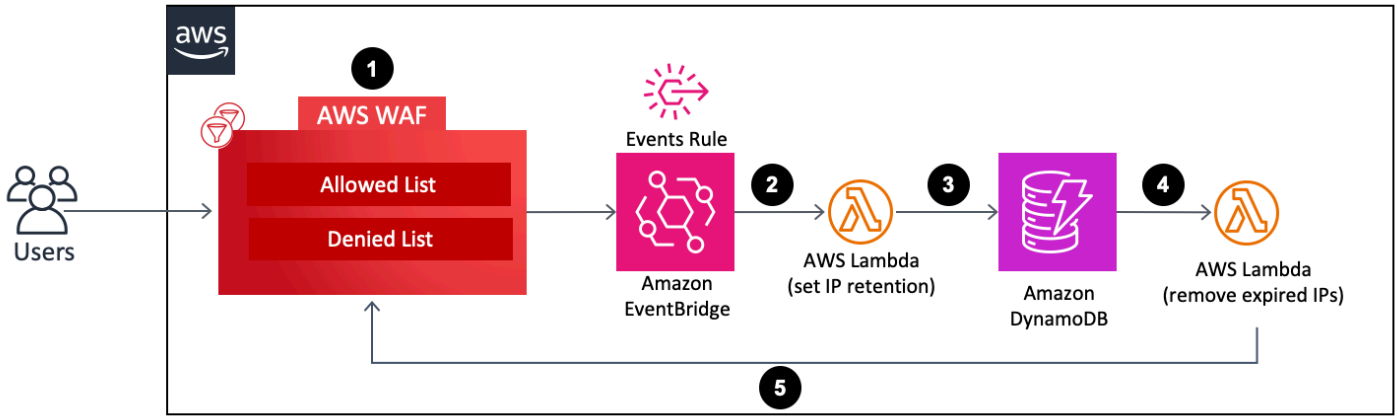
4. 选择 “切换工作组”。
5. 选择 “历史记录” 选项卡。
6. 从列表中选择并打开`ALTER TABLE`查询。这些查询每小时运行一次，以向 Athena 表中添加一个新的每小时分区。

在允许和拒绝的 AWS WAF IP 集上配置 IP 保留

您可以在解决方案创建的允许和拒绝的 AWS WAF IP 集上配置 IP 保留。以下各节说明了它的工作原理并提供了设置步骤。

工作原理

描述了 AWS WAF 允许和拒绝列表以及其他 AWS 资源的架构图



1. 当用户更新（添加或删除 IP 地址）允许或拒绝的 WAF IP 集时，此操作将调用 AWS WAF `UpdateIPSet` API 调用并创建事件。
2. A [mazon EventBridge] 事件规则根据预定义的事件模式检测事件，并调用 Lambda 函数来设置更新后存在于 IP 集中的所有 IP 地址的保留期。

3. Lambda 函数处理事件，提取与 IP 保留相关的数据（例如 IP 集名称、ID、范围、IP 地址），然后将其插入到 DynamoDB 表中。它还会为每个 DynamoDB 项目插入一个`ExpirationTime`属性。该解决方案通过在事件时间中添加用户定义的保留期来计算到期时间。该表已开启 DynamoDB Stream s 和 T ime to Live (TTL)。TTL 属性为。`ExpirationTime`
4. 当项目达到其过期时间时，将调用 TTL，DynamoDB 会在项目到期时间后将其从表中删除。删除该项目后，已删除的项目将添加到 DynamoDB 流中，DynamoDB 流会调用 Lambda 函数进行下游处理。
5. Lambda 函数从 DynamoDB 流中获取有关已删除项目的信息，然后调用 AWS WAF API，将项目中包含的过期 IP 地址从目标 AWS WAF IP 集中删除。

开启 IP 保留

请按照以下步骤开启 IP 保留：

1. 在您部署或更新的 Cloudformation 堆栈中，输入 “允许的 IP 集” 的 IP 保留期（分钟）和 “拒绝的 IP 集” 的 IP 保留期（分钟）。最短保留期为 15 分钟。该解决方案将介于`0`和之间的任意数字`15`视为`15`。有关部署配置的更多信息，请参阅步骤 1。Launch the stack。
2. 如果您想在从 AWS WAF IP 集中删除过期的 IP 地址时收到电子邮件通知，请输入电子邮件地址。如果您选择接收电子邮件通知，则必须使用解决方案成功部署后收到的电子邮件中的链接确认订阅。有关部署配置的更多信息，请参阅步骤 1。Launch the stack。
3. 通过添加或删除 IP 地址来更新 AWS WAF IP 集。这将启动 IP 保留流程并创建一个 DynamoDB 项目，包括 IP 过期列表。此过期列表由更新后存在于 AWS WAF IP 集中的 IP 地址组成。
4. 当 DynamoDB 项目达到其过期时间并从表中删除后，该解决方案将从 WAF IP 集中删除该项目 IP 过期列表中包含的 IP 地址。

> **Note**
>
> 根据 DynamoDB 删除按照 TTL 过期的项目的时间，从 AWS WAF IP 集中删除过期的 IP 地址的实际操作可能会有所不同。DynamoDB TTL 的删除主要取决于表的大小和活动级别。由于 DynamoDB 删除操作可能会延迟，因此 AWS WAF 删除操作可能会延迟。通常，该解决方案会在删除 DynamoDB TTL 后不久从 AWS WAF IP 集中删除过期的 IP 地址。有关更多信息，请参阅亚马逊 DynamoDB 开发者指南中的 DynamoDB 上线时间 (TTL)。

构建监控面板

AWS 建议您为每个关键终端节点配置自定义基准监控系统。有关创建和使用自定义指标视图的信息，请参阅CloudWatch 控制面板-创建和使用自定义指标视图和使用 Amazon CloudWatch 控制面板。

以下仪表板屏幕截图显示了自定义基准监控系统的示例。

CloudFront 仪表板屏幕截图

控制面板显示以下指标：

- 允许的请求与已阻止的请求-显示您收到的允许访问量激增（是正常访问峰值的两倍）还是被阻止的访问（任何识别出超过 1K 个被阻止请求的时段）。 CloudWatch 向 Slack 频道发送警报。您可以使用此指标来跟踪已知的 DDo S 攻击（当被阻止的请求增加时）或攻击的新版本（当允许请求访问系统时）。

> **Note**
>
> 注意：该解决方案提供了此指标。

- BytesDownloaded vs U ploaded-帮助识别 DDo S 攻击何时针对通常无法获得大量资源访问权限的服务（例如，搜索引擎组件为一个特定的请求参数集发送 MBs 信息）。

- ELB 溢出和队列长度-帮助验证 DDo S 攻击是否对基础设施造成损害，攻击者是否正在绕过 CloudFront AWS WAF 层，直接攻击未受保护的资源。
- ELB 请求计数-帮助识别基础设施损坏情况。此指标显示攻击者是否在绕过保护层，或者您是否应该查看 CloudFront 缓存规则以提高缓存命中率。
- ELB Healthy Host-您可以将其用作另一个系统运行状况检查指标。
- ASG CPU 利用率-帮助识别攻击者是否在绕过 CloudFront、AWS WAF 和 Elastic Load Balancing。您也可以使用此指标来识别攻击造成的伤害。

处理 XSS 误报

此解决方案配置了 AWS WAF 规则，该规则可检查传入请求中经常探索的元素，以识别和阻止 XSS 攻击。如果您的工作负载允许合法用户撰写和提交 HTML（例如，在内容管理系统中使用富文本编辑器），则这种检测模式的效果会降低。在这种情况下，可以考虑创建一个例外规则，绕过接受富文本输入的特定 URL 模式的默认 XSS 规则，并实施其他机制来保护那些被排除在外的网址。 URLs

此外，某些图像或自定义数据格式可能导致误报，因为它们包含指示 HTML 内容中可能存在 XSS 攻击的模式。例如，SVG 文件可能包含`<script>`标签。如果您希望合法用户提供此类内容，请严格调整您的 XSS 规则，以允许包含这些其他数据格式的 HTML 请求。

完成以下步骤以更新 XSS 规则以排除接受 HTML 作为输入 URLs 的规则。有关详细说明，请参阅 Amazon WAF 开发者指南。

1. 登录 AWS WAF 控制台。
2. 创建字符串匹配或正则表达式条件。
3. 根据 XSS 规则，配置筛选器设置以检查要接受的 URI 和列出要接受的值。
4. 编辑此解决方案的 XSS 规则并添加您创建的新条件。

   例如，要排除列表 URLs 中的所有内容，请在 “请求时” 中选择以下选项：

   - 不是
   - 匹配字符串匹配条件中的至少一个申报器
   - XSS 允许名单

问题排查

如果您需要有关此解决方案的帮助，请联系 Support 以打开此解决方案的支持案例。

联系 AWS Support

如果您有 AWS Business Support+、AWS Enterpris e Support 或统一运营，则可以使用 AWS 支持中心获取有关此解决方案的专家帮助。以下部分提供了说明。

创建工单

1. 打开 Supp ort Center。
2. 选择创建工单。

我们可提供哪些帮助？

1. 选择技术。
2. 对于服务，选择解决方案。
3. 对于类别，选择适用于 AWS WAF 的安全自动化。
4. 对于 “严重性”，是与您的用例最匹配的选项。
5. 当您输入 “服务”、“类别” 和 “严重性” 时，界面会填充常见疑难解答问题的链接。如果您无法通过这些链接解决问题，请选择下一步: 附加信息。

附加信息

1. 对于主题，输入可概括您的问题的文本。
2. 对于描述，请详细描述问题，包括此解决方案的名称和您使用的版本，例如以下示例：AWS WAF Vx.y.z 的安全自动化。
3. 选择附加文件。
4. 附加支持团队处理该请求所需的信息。

帮助我们更快地处理您的工单

1. 输入请求的信息。

2. 选择下一步：立即解决或联系我们。

立即解决或联系我们

1. 查看立即解决中的解决方案。
2. 如果您无法使用这些解决方案解决问题，请选择联系我们，输入请求的信息，然后选择提交。

开发人员指南

本节提供解决方案的源代码。

源代码

访问我们的GitHub 存储库，下载此解决方案的模板和脚本，并与其他人共享您的自定义设置。

此解决方案的模板是使用 AWS CDK 生成的。有关其他信息，请参阅 README.md 文件。

参考

本节包含有关用于收集该解决方案的独特指标的可选功能的信息、相关资源的指针以及为该解决方案做出贡献的构建者列表。

匿名数据收集

该解决方案包括向 AWS 发送运营指标的选项。我们使用这些数据来更好地了解客户如何使用此解决方案以及相关服务和产品。开启后，该解决方案会收集以下信息，并在 CloudFormation 模板的初始部署期间将其发送到 AWS：

- 解决方案 ID-AWS 解决方案标识符
- 唯一 ID (UUID)-为该解决方案的每个部署随机生成的唯一标识符
- 时间戳-数据收集时间戳
- 解决方案配置-在初始启动期间开启功能并设置参数
- 生命周期-客户使用此解决方案的时长（基于堆栈删除）
- 日志解析器数据：
  - 扫描器和探测器 IP 集、Ba d Bot IP 集和设置为屏蔽的 HTTP Floo d IP 中的 IP 地址数量
  - 已处理和阻止的请求数
- IP 列出解析器数据：
  - 信誉列表 IP 集中的 IP 地址数量
  - 已处理和阻止的请求数
- IP 保留数据-从“允许”或“拒绝 IP”集中删除的过期 IP 地址的数量

通过此调查收集的数据归 AWS 所有，数据收集受 AWS 隐私政策的约束。要选择退出此功能，请在启动 AWS CloudFormation 模板之前完成以下步骤。

1. 将 `aws-waf-security-automations.template` AWS 下载 CloudFormation到您的本地硬盘。
2. 使用文本编辑器打开 CloudFormation 模板。
3. 从以下位置修改 CloudFormation 模板映射部分：

```
Solution:
  Data:
```

```
    SendAnonymizedUsageData: "Yes"
```

更改为：

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. 登录 AWS CloudFormation 控制台。
5. 选择创建堆栈。
6. 在创建堆栈页面的指定模板部分，选择上传模板文件。
7. 在上传模板文件下，选择选择文件，然后从本地驱动器中选择编辑过的模板。
8. 选择 “下一步”，然后按照步骤 1 中的步骤进行操作。Launch the stack。

相关资源

相关的 AWS 白皮书

- AWS DDo S 弹性最佳实践

相关的 AWS 安全博客文章

- 如何使用 AWS WAF、A CloudFront mazon 和反向链接检查来防止盗链

第三方 IP 信誉列表

- Spamhaus DROP List 网站
- Proofpoint 新兴威胁 IP 列表
- Tor 退出节点列表

贡献者

- Heiter Vital
- 李·阿特金森

- 本·波特
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- 舒·杰克逊
- 权威廉
- Mykhailo Markhain

修订

访问我们 GitHub 存储库中的 Changelog.md，跟踪特定版本的改进和修复。

版权声明

本实施指南仅供参考。它代表了截至本文档发布之日当前 AWS 产品和实践，如有更改，恕不另行通知。客户有责任对本文档中的信息以及对 AWS 产品或服务的任何使用进行独立评估，每种产品或服务均按“原样”提供，不附带任何形式的明示或暗示担保。本文档不设定 AWS、其关联公司、供应商或许可方的任何担保、陈述、合同承诺、条件或保证。AWS 对其客户承担的责任和义务受 AWS 协议制约，本文档不是 AWS 与客户直接协议的一部分，也不构成对该协议的修改。

AWS WAF 安全自动化解决方案根据 A pache 许可版本 2.0 的条款进行许可。

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。