实施指南

的安全自动化 AWS WAF

的安全自动化 AWS WAF: 实施指南

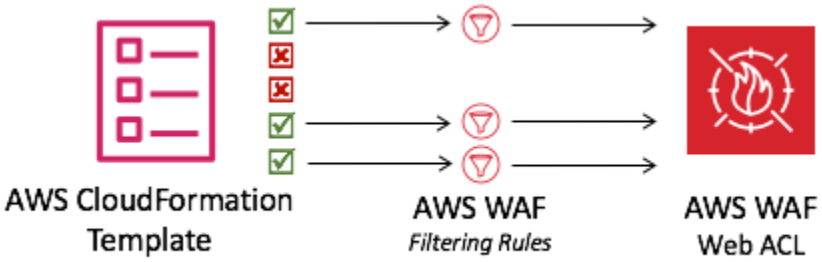
Table of Contents

自动部署单个 Web 访问控制列表，在安全自动化开启的情况下过滤基于 Web 的攻击 AWS WAF

发布日期：2016 年 9 月（最后更新时间：2024 年 12 月）

Security Automations AWS WAF 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有助于保护 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。AWS WAF您可以使用定义 AWS WAF可自定义的 Web 安全规则。这些规则控制允许或阻止部署在 Amazon CloudFront、Application Loa d Balancer (APIs) 和 Amazon APIGat eway 等 AWS 资源上的网络应用程序和应用程序编程接口 (ALB) 的流量。有关更多支持的资源类型，请参阅AWS WAF AWS Firewall Manager、和 AWS Shield Advanced 开发者指南AWS WAF中的。

对于大型和小型组织来说，配置 AWS WAF 规则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，“安全自动化” AWS WAF 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。在对该解决方案的AWS CloudFormation模板进行初始配置期间，您可以指定要包括哪些保护功能。部署此解决方案后， AWS WAF 会检查其现有 CloudFront 发行版的 Web 请求，并在适用时将其屏蔽。ALB



AWS WAF 网络配置 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 安全性和可用性 AWS 的最佳实践，启动、配置和运行部署此解决方案所需的安全 AWS、计算、存储和其他服务。

本指南中的信息假设您具备诸如 AWS WAF、 CloudFrontALBs、和之类的 AWS 服务的工作知识AWS Lambda。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 WAF V 2)。

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 AWS 区域 哪些解决方案。	支持 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
Support 用于帮助您部署、使用解决方案或对其进行故障排除。	Support
访问源代码，也可以使用 AWS Cloud Development Kit (AWS CDK) 来部署解决方案	GitHub存储库

功能和优势

“安全自动化” AWS WAF 解决方案提供以下功能和优点。

使用 AWS 托管式规则 规则组保护您的 Web 应用程序

AWS 托管式规则 f AWS WAF or 提供针对常见应用程序漏洞或其他有害流量的保护。此解决方案包括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 选择一个或多个规则组ACL，但不超过 Web ACL 容量单位的最大配额 (WCU)。

使用预定义的洪水自定义规则提供第 7 层HTTP防洪保护

F HTTPloo 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避免达到 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。

您还可以通过在过滤条件中添加国家/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URI模式的HTTP洪水攻击。有关更多信息，请参阅使用国家/地区和 FI HTTP ood Athena 日志解析器URI中的内容。

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。您可以构建自定义仪表板来可视化这些指标，并深入了解攻击模式和提供的保护 AWS WAF。有关更多信息，请参阅生成监控面板。

与 Service Catalog AppRegistry 和 AWS Systems Manager 应用程序管理器集成

此解决方案包括一个 S ervice Catalog AppRegistry 资源，用于在 Service Catalog 和 Sy AWS stems Manager Appl AWS icat AppRegistry ion Manager 应用程序管理器中将解决方案的 CloudFormation 模板及其底层资源注册为应用程序。通过这种集成，您可以集中管理解决方案的资源。

使用案例

发布日期：二零一六年九月（最后更新时间：2023 年 5 月）

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 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 CloudFormation 模板将一组 AWS WAF 规则部署到您的账户中。这样，您就无需自己配置 AWS WAF 规则，而且可以 AWS WAF 更快地开始使用。

自定义第 7 层HTTP防洪保护

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，以获得针对DDoS攻击的保护。有关更多信息，请参阅 “功能和优势” 中的 “使用预定义的洪HTTP水自定义规则提供第 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 和其他服务在上构建安全自动化。 AWS Cloud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。如果用户在激活HTTP防洪规则ALB或扫描器和探测器保护规则时**yes – Amazon Athena log parser**选择CloudFront，则此解决方案会运行定时的 Athena 查询 AWS WAF进行检查，或者记录日志。

AWS WAF 规则

AWS WAF 规则定义了：

- 如何检查 HTTP (S) Web 请求
- 当请求符合检查标准时要采取的操作

只能在规则组或 Web 的上下文中定义规则ACL。

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 集就是 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防洪规则或扫描器和探测器保护规则`yes - AWS Lambda log parser`时选择，Lamba 函数会启动检查 CloudFront、或ALB记录。 AWS WAF

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。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 API Gateway CloudFront、、ALBAWS AppSync、Amazon Cognito、A AWS pp Runner 和AWS 已验证访问资源。目前，Amazon 支持此解决方案 CloudFront ，并且ALB。

WAF 日志

此解决方案使用生成的日志来 AWS WAF 获取与 Web 关联的资源ACL。此解决方案的HTTP防洪规则会检查这些日志。

WCU

AWS WAF 使用 Web 访问控制列表 (ACL) 容量单位 (WCUs) 来计算和控制运行规则、规则组和 Web 所需的操作资源ACLs。 AWS WAF 在配置规则组和 Web ACLs 时强制WCU实施配额。 WCUs不影响 AWS WAF 检查网络流量的方式。

网页 ACL

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

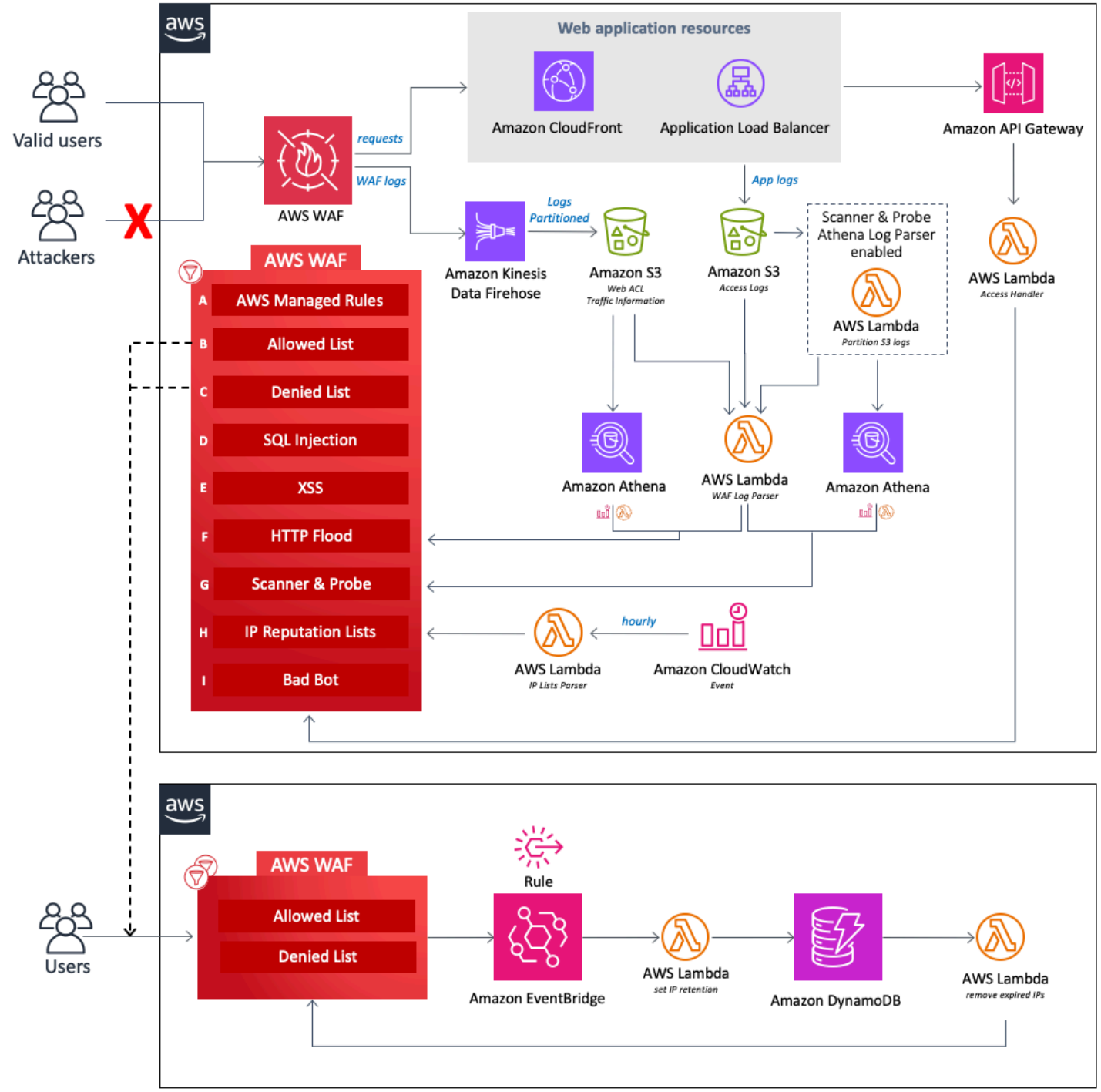
> **Note**
>
> 有关术语的一般参考，请参阅AWS 词汇表。 AWS

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中部署以下组件。 AWS 账户



适用于 AWS WAF 架构的安全自动化 AWS

设计的核心是一个 AWS WAFWebACL，它充当 Web 应用程序所有传入请求的中央检查和决策点。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，并向网络添加不同的规则ACL。

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 托管式规则 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规则和亚马逊 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 IP 集上配置 AWS WAF IP 保留。
- SQL注入 (D) 和 XSS (E) — 这些组件配置了两 AWS WAF 条规则，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。
- HTTPFlood (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DDoS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 AWS WAF 基于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 信誉列表以寻找要阻止的新范围。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) — 此组件会自动设置蜜罐，这是一种旨在引诱和转移未遂攻击的安全机制。此解决方案的 honeypot 是一个陷阱端点，您可以将其插入网站中，以检测来自内容抓取器和恶意机器人的入站请求。如果来源访问蜜罐，Lambda `Access Handler` 函数会拦截并检查请求以提取其 IP 地址，然后将其添加到阻止列表中。 AWS WAF

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 的设计注意事项

该解决方案使用了 AWS Well-Architected Framework 中的最佳实践，该框架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 Data Firehose、Gat eway API、Amazon 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 Management(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、Gateway API、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，默认情况下它会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，以及有关这些组件如何协同工作的架构详细信息。

AWS 此解决方案中的服务

AWS 服务	描述	
AWS WAF	核心。部署 AWS WAF Web ACL、 AWS 托管式规则 规则组、自定义规则和 IP 集。拨 AWS WAF API打电话以阻止常见攻击和保护 Web 应用程序。	
Amazon Data Firehose	核心。将 AWS WAF 日志传输到 Amazon 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。	
亚马逊API网关	支持。创建恶意的机器人蜜罐端点。	
Amazon SNS	支持。发送亚马逊简单通知服务 (AmazonSNS) 电子邮件通	

AWS 服务	描述	
	知，以支持在允许和拒绝的名单上保留 IP。	
AWS Systems Manager (系统管理员)	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洪水以及扫描器和探头保护。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，则会 AWS WAF 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

Fl HTTPood 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 AWS WAF 基于费率的规则，并且已经熟悉SQL如何实现自定义，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。WAF访问日志类型的延迟时间较短，与ALB日志传输时间相比，您可以使用它来 CloudFront 更快地识别HTTP洪水来源。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。

AWS Lambda 日志解析器

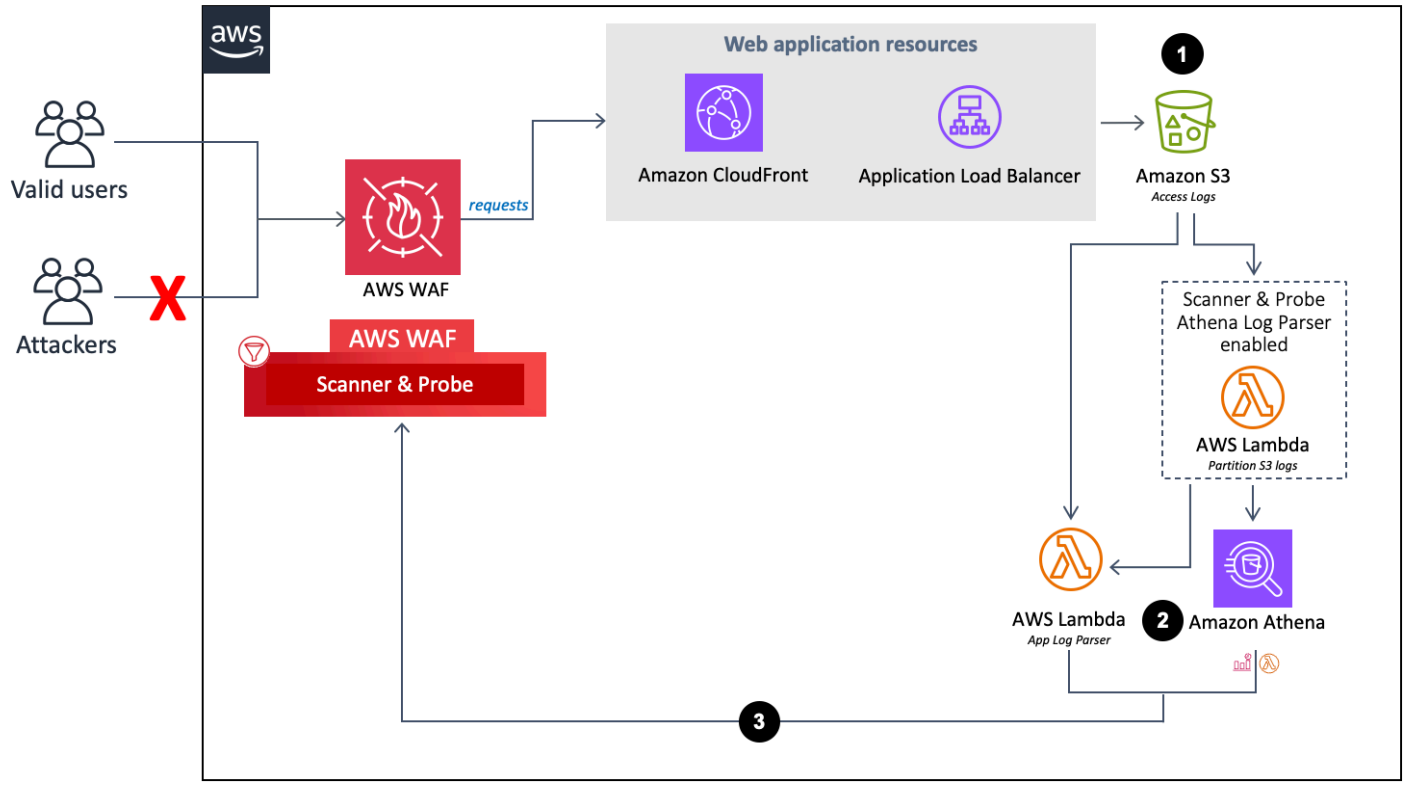
“HTTP洪水防护” 和 “扫描仪和探测器保护” 模板参数提供了 “AWS Lambda 日志解析器” 选项。仅当AWS WAF 基于速率的规则和 Amazon Athena 日志解析器选项不可用时，才使用 Lambda 日志解析器。此选项的一个已知限制是，信息是在正在处理的文件上下文中处理的。例如，一个 IP 生成的请求或错误可能超过定义的配额，但是由于这些信息被拆分为不同的文件，因此每个文件存储的数据不足以超过配额。

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仪和探测器。



应用程序日志解析器流程

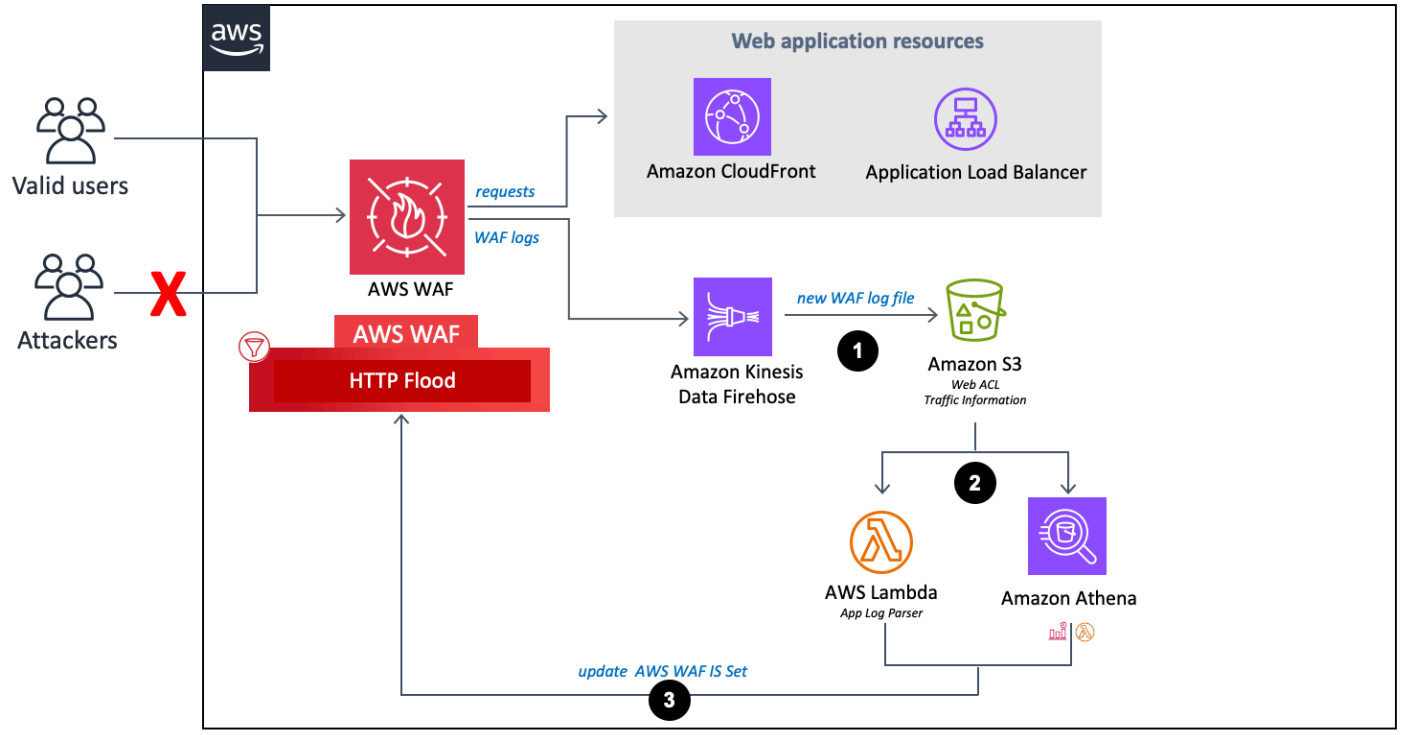
1. 当 CloudFront 或代表您的 Web 应用程序ALB接收请求时，它会将访问日志发送到 Amazon S3 存储桶。
   a. （可选）如果您`Yes - Amazon Athena log parser`为模板参数选择 “激活HTTP防洪保护” 和 “激活扫描器和探测器保护”，Lambda 函数会在访问日志到达 Amazon S3 *<customer-bucket>*/AWSLogs-partitioned/*<optional-prefix>* /year=*<YYYY>*/month=*<MM>* /day=*<DD>*/hour=*<HH>*/ 时将其从其原始文件夹*<customer-bucket>*/AWSLogs移动到新分区的文件夹。
   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，扫描仪和探针保护 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，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 Act ivate Fl HTTP ood Protec tion 选择`yes - AWS Lambda log parser`或，则此解决方案会配置以下组件，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。

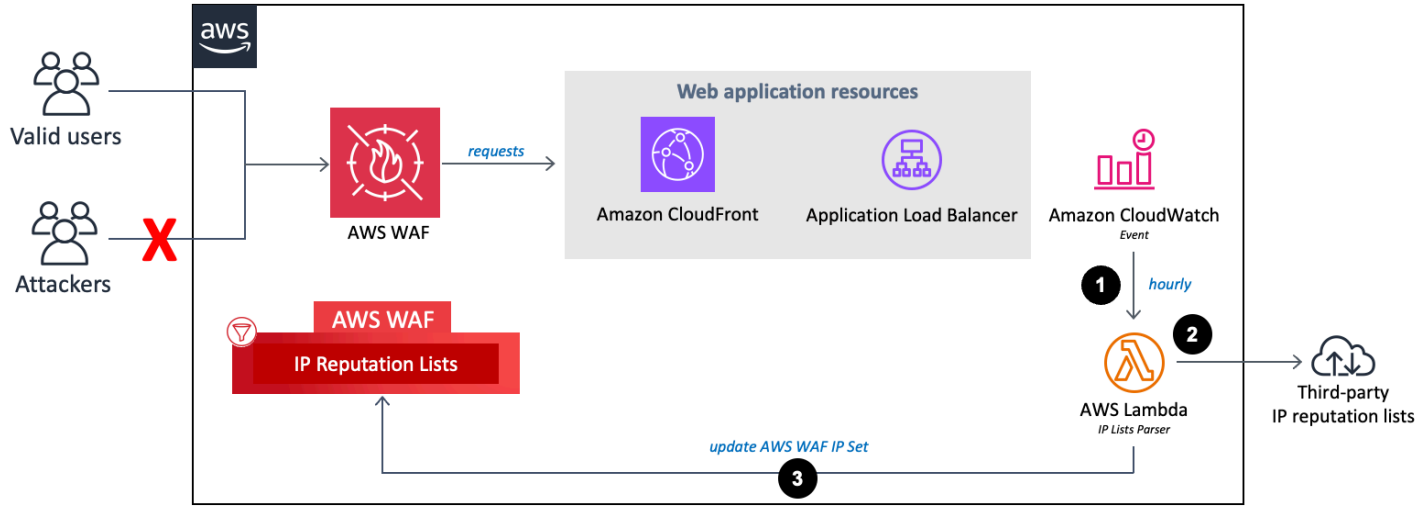


AWS WAF 日志解析器流程

1. 当 AWS WAF 收到访问日志时，它会将日志发送到 Firehose 端点。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 Amazon 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，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 ParserLambda 函数有助于抵御第三方 IP 信誉列表中识别的已知攻击者。

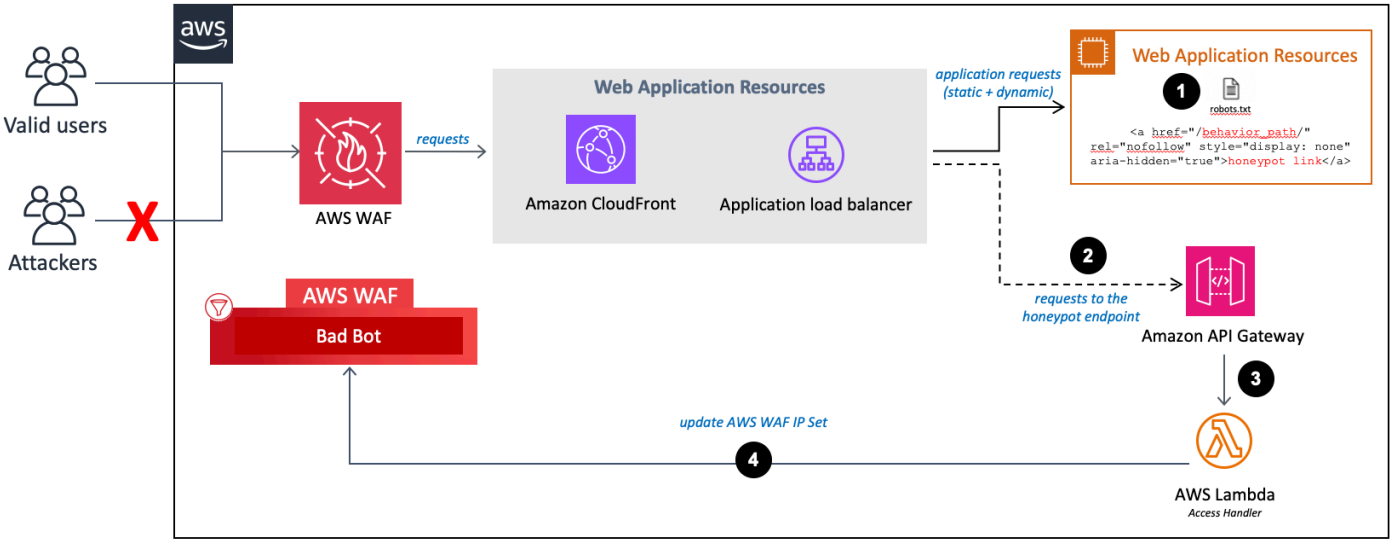


IP 信誉列表解析器流程

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：
   - 垃圾邮件地址和列表 DROP EDROP
   - 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。

访问处理器

`Access Handler`Lambda 函数检查向蜜罐终端节点发出的请求以提取其源 IP 地址。



访问处理程序和蜜罐端点

1. 在您的网站中嵌入 honeypot 端点并更新您的机器人排除标准，如在您的 Web 应用程序中嵌入 Honeypot 链接（可选）中所述。
2. 当内容抓取器或恶意机器人访问蜜罐端点时，它会调用 Lambda 函数。`Access Handler`
3. 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。
4. Lambda 函数会更新 AWS WAF IP 设置条件以屏蔽这些 IP 地址。

规划您的部署

本节介绍部署解决方案之前的成本the section called “限额”、安全性和其他注意事项。

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）可能并非全部可用 AWS 区域。因此，您必须在提供这些服务 AWS 区域 的地方启动此解决方案。有关按地区划分的最新 AWS 服务可用性，请参阅AWS 区域所有服务列表。

	AWS WAF 网页 ACL	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
端点类型				
CloudFront	✓			
Application Lood Balancer (ALB)	✓			
激活HTTP防洪功能				
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

运行安全自动化 AWS WAF 解决方案时使用的 AWS 服务费用由您承担。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。

我们建议通过创建预算AWS Cost Explorer来帮助管理成本。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）中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、恶意机器人防护、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 [USD]
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
亚马逊API网关	100 万个请求	大约 3.40 美元
AWS WAF 网页 ACL	1	5.00 美元
AWS WAF 规则	4	4.00 美元

AWS 服务	尺寸/月	成本 [USD]
AWS WAF 请求	1M	0.60 美元
总计		每月大约 23.60 美元

示例 2：激活信誉列表保护、Bad Bot 防护、HTTP用于防洪的 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 [USD]
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
亚马逊API网关	100 万个请求	大约 3.40 美元
Amazon Athena	每天有 120 万个 CloudFront 对象命中或 120 万个ALB请求，每次点击或请求生成大约 500 字节的日志记录	大约 4.32 美元
AWS WAF 网页 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 23.78 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 [USD]
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 网页 ACL	1	5.00 美元
AWS WAF 规则	2	2.00
WASWAF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 AWS WAF 中的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洪水防护或扫描器和探测器保护规则时使用 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区块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 基础架构上构建系统时，安全责任由您和共同承担 AWS。这种分担责任模式减轻了您的 AWS 运营负担，因为您可以操作、管理和控制包括主机操作系统、虚拟化层和服务运行设施的物理安全在内的组件。有关 AWS 安全的更多信息，请访问AWS Cloud 安全。

IAM 角色

通过IAM角色，您可以为上的服务和用户分配精细的访问权限、策略和权限。 AWS Cloud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 托管式规则 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。此解决方案包括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 选择一个或多个规则组ACL，但不超过 Web ACL 容量单位的最大配额 (WCU)。
- 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，将恶意的客户端脚本注入合法用户的网络浏览器。我们设计它是为了检查传入请求中经常探索的元素，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DDoS攻击（例如HTTP洪水）的风险。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，并进行更新 AWS WAF 以阻止从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。

限额

服务限额（也称为限制）是 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 服务配额

请确保此解决方案中实施的每项服务都有足够的限额。有关更多信息，。请参阅 AWS service quotas。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PDF改为查看服务终端节点和配额页面中的信息。

AWS WAF 配额

AWS WAF 每个 IP 匹配条件最多可以阻止 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 每个账户每秒最多允许向任何个人`CreatePut`、或任何`Update`操作API发出一个请求。AWS 区域 如果您在解决方案之外API拨打这些电话，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进行这些API调用的应用程序。

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

ACL此解决方案生成的网络旨在为 Web 应用程序提供全面保护。该解决方案提供了一组 AWS 托管式规则 自定义规则，您可以将其添加到 Web 中ACL。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。

网络ACL流量记录

如果您在美国东部（弗吉尼亚北部）以 AWS 区域 外的地方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）要求在所有 AWS 边缘站点运行的网络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 开发者指南。

对请求组件进行超大处理

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

- yes（继续）— 根据规则检查标准通常检查请求组件。 AWS WAF 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。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 继续使用网络中的其余规则来检查 Web 请求ACL，就像对待任何不匹配的规则一样。

有关更多信息，请参阅中的处理超大的 Web 请求组件。AWS WAF

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。每次独特的部署都会产生额外费用，并受每个地区每个账户的AWS WAF 配额限制。

部署解决方案

此解决方案使用 AWS CloudFormation 模板和堆栈来实现自动部署。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
- 配置一个 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 发行版与ACL该解决方案生成的网站相关联。ALB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

- 为您的网络分发开启 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。ALB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 AWS日志（默认日志前缀AWS Logs/）。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

此解决方案包括一个主 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-使用此模板作为在您的账户中启动解决方案的入口。默认配置使用预先配置的规则部署 AWS WAF Web ACL。您可以根据需要自定义模板。

网络ACL堆栈

View template

aws-waf-security-automations-webacl.tem plate — 此嵌套模板 AWS WAF 提供资源，包括网络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、Athena 和 Firehose 相关的资源。AWS Glue它是在你选择 S canner & Pro be Athena 日志解析器或 Flood HTTPLambda 或 Athena 日志解析器时创建的。

先决条件

此解决方案专为与 CloudFront 或一起部署的 Web 应用程序而设计ALB。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. 指定您的分配的行为。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。

配置一个 ALB

要将配置ALB为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 AWS CloudFormation 模板将解决方案部署在。 AWS Cloud

1. 登录AWS Management Console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。要以其他方式启动此解决方案 AWS 区域，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 AWS 区域 仅提供特定内容。因此，您必须在提供这些服务 AWS 区域 的地方启动此解决方案。有关更多信息，请参阅支持 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 配置指定一个名称。这也是模板创建的网站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	*<requires input>*	堆栈名称不能包含空格。此名称在您的内部必须是唯一的，AWS 账户 并且是模板创建ACL的网站的名称。
资源类型		
Endpoint	CloudFront	选择正在使用的资源类型。 **Note** 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		

参数	默认值	描述
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网络的组件ACL。 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 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。 必填项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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 规则组列表。

参数	默认值	描述
激活匿名 IP 列表托管规则组保护	no	选择打开yes旨在将匿名 IP 列表托管规则组添加到 Web 的组件ACL。 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。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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旨在将核心规则集托管规则组添加到 Web 的组件ACL。 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。 所需的值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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旨在将管理员保护托管规则组添加到 Web 的组件ACL。 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。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 的组件ACL。 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。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 规则组列表。
AWS 托管特定用例规则组		

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 的组件ACL。 此规则组阻止与利用SQL数据库相关的请求模式，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。评估此规则组，以便在您的应用程序与SQL数据库接口时使用。如果您已经激活了 AWS 托管规则组，则使用SQL注入自定义SQL规则是可选的。 所需的值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 的组件ACL。 此规则组阻止与利用 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。 所需的值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 添加核心规则集托管规则组保护的组件ACL。 此规则组阻止与利用特定于POSIX和POSIX类似操作系统的漏洞（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类似POSIX或的操作系统上运行，请评估此规则组。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 的组件ACL。 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。 所需的值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 的组件ACL。 该规则组阻止与利用PHP编程语言使用特有的漏洞相关的请求模式，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。评估此规则组PHP是否安装在与您的应用程序交互的任何服务器上。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS 托管式规则 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 的组件ACL。 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。 必填值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网络ACL堆栈部署失败。 有关更多信息，请参阅AWS托管式规则 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	*<requires input>*	如果您选择了 yes “激活扫描器和探测保护” 参数，请输入您要在其中存储 CloudFront 分配访问日志的 Amazon S3 存储桶（新的或ALB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您部署 CloudFormation 模板的同一 AWS 区域 位置。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。 **Note** 为您的网络分发开启 CloudFront 网络访问日志功能，将日志文件发送到此 Amazon S3 存储桶。ALB使用堆栈中定义的相同前缀（默认前缀AWS Logs/）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	AWS Logs/	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 Endp oin t 参数，则必须在前缀后面AWS Logs/追加，yourprefix/AWSLogs/ 例如。 如果没有用户定义的前缀，则使用AWS Logs/（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如果您为应用程序访问日志存储桶名称参数输入了现有 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 “激活扫描器和探测保护” 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防洪功能	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100。 如果您为 “激活HTTP防洪保护” 参数选择了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。 **Note** 如果您定义此参数，则国家/地区将自动包含在 Athena 查询组中，还有 IP 和其他可选的分组依据字段，您可以通过 Flood Athena 查询参数按请求分组进行选择。HTTP 如果您选择停用此保护，请忽略此参数。

参数	默认值	描述
在 Fl HTTP ood Athena 查询中按请求分组	None	如果您选择了 yes – Amazon Athena log parser “激活HTTP防洪保护” 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 的请求和URI。 如果您选择停用此保护，请忽略此参数。
WAF封锁期	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防洪保护” 参数选择了yes - AWS Lambda log parser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 “激活扫描仪和探测器保护” 或 “激活HTTP防洪保护” 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
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。
ARN拥有您账户中 CloudWatch日志的写入权限的IAM角色	<optional input>	提供一个可选ARNIAM角色，该角色对您的账户中的 CloudWatch 日志具有写入权限。例如：ARN: arn:aws:iam::account_id:role/myrolename 。有关如何创建角色的说明，请参阅RESTAPI在 API Gateway 中设置 CloudWatch 日志记录。 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
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 yes - AWS WAF rate-based rule “激活HTTP防洪保护” 参数，则可接受的最小值为 100。 如果您为 “激活HTTP防洪保护” 参数选择了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。
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		

参数	默认值	描述
激活SQL注射保护	yes	选择开启专yes为阻止常见SQL注入攻击而设计的组件。如果您没有使用 AWS 托管核心规则集或托 AWS 管SQL数据库规则组，请考虑将其激活。 您可以选择一个选项（yes（继续）yes - MATCH、或yes - NO_MATCH） AWS WAF 来处理超过 8 KB（8192 字节）的超大请求。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。 **Note** CloudFormation 堆栈会将选定的超大尺寸处理选项添加到默认的SQL注入保护规则中，并将其部署到您的中。 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注射保护的灵敏度等级	LOW	选择要 AWS WAF 用来检查SQL注射攻击的灵敏度级别。 HIGH检测到更多的攻击，但可能会产生更多的误报。 LOW对于已经具有针对SQL注入攻击的其他保护措施或对误报容忍度较低的资源来说，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 添加SQL注入规则语句和SensitivityLevel属性的敏感度级别。 如果您选择停用SQL注入保护，请忽略此参数。 **Note** 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 AWS 账户的。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	选择开启专yes为阻止常见XSS攻击而设计的组件。如果您没有使用 AWS 托管核心规则集，请考虑将其激活。您也可以选择要处理超过 8 KByes（8192 字节yes - NO_MATCH）的超大请求的选项（（继续）yes - MATCH、或）。 AWS WAF 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。 **Note** 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，并将其部署到您的脚本规则中。 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。
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资源和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。大约 15 分钟后，您应该会收到 CREATE COMPLETE _ 的状态。

> **Note**
>
> 除了`Log Parser`、和`Access Handler` AWS Lambda 函数外`IP Lists Parser`，此解决方案还包括`helper`和 `custom-resource` Lambda 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。

要查看有关堆栈资源的详细信息，请选择输出选项卡。这包括BadBotHoneypotEndpoint值，即 Gate API way 蜜罐终端节点。请记住此值，因为您将在 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

使用您在步骤 1 中生成的资源更新您的 CloudFront 发行版以激活 AWS WAF 和记录日志。ALB启动堆栈。

1. 登录 AWS WAF 控制台。
2. 选择您要ACL使用的网站。
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 分布或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

配置 CloudFront 或您的ALB以将 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，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存储桶关联的存储桶。 AWS 账户有关更多信息，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`AWS Logs/`）。
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 (AmazonEC2) 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AWS Logs/）。
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。

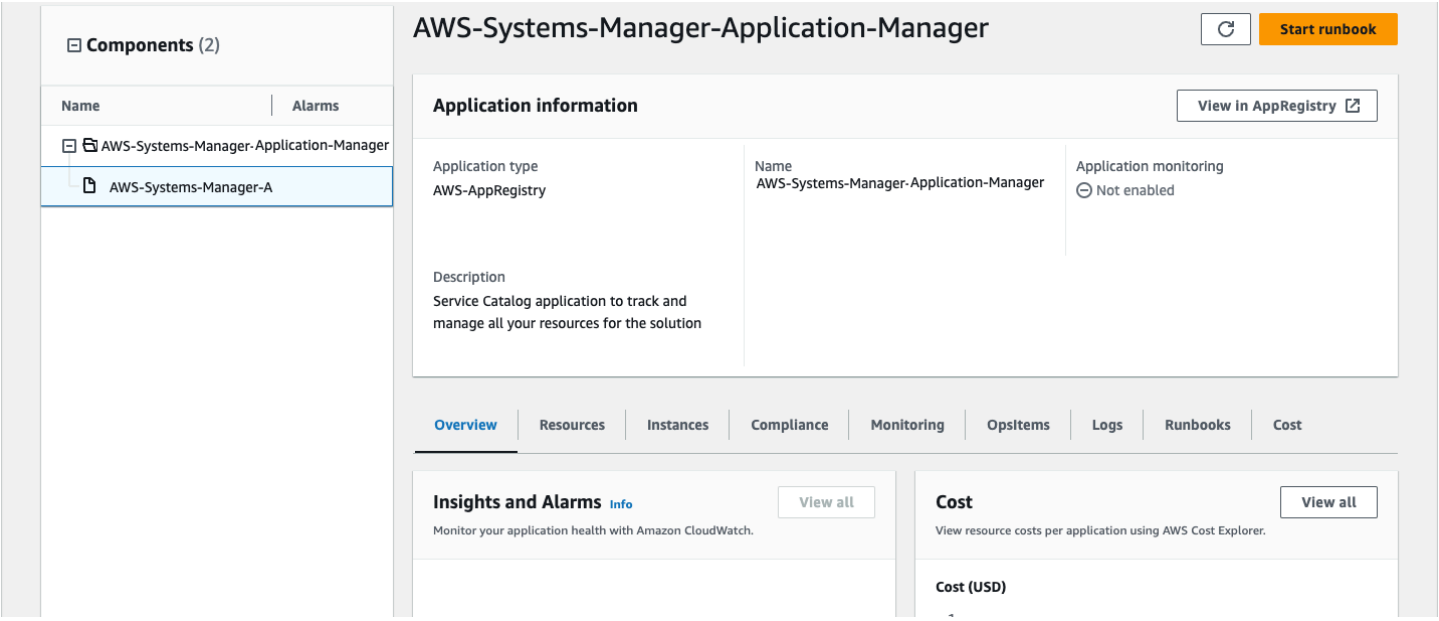
使用监控解决方案 AppRegistry

该解决方案包括服务目录 AppRegistry 资源，用于在 Service Catalog 和 S AWS ystems Manager Application Manager Application Manager 中将 CloudFormation 模板 AppRegistry 和底层资源注册为应用程序。

AWS Systems Manager Application Manager 为您提供了此解决方案及其资源的应用程序级视图，因此您可以：

- 从中心位置监控其资源、跨堆栈部署的资源的成本以及与此解决方案相关的日志。 AWS 账户
- 在应用程序的上下文中查看此解决方案资源的操作数据。例如，部署状态、 CloudWatch 警报、资源配置和操作问题。

下图描述了 Application Manager 中解决方案堆栈的应用程序视图示例。



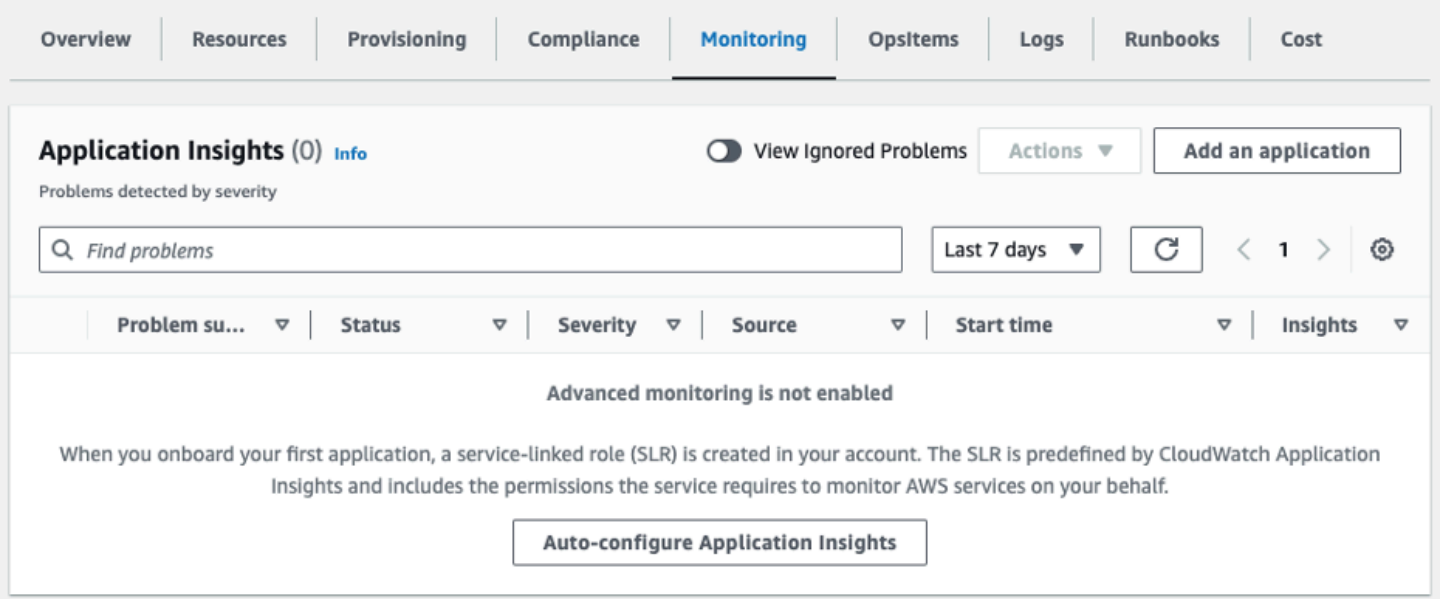
应用程序管理器中的解决方案堆栈

激活 CloudWatch 应用程序见解

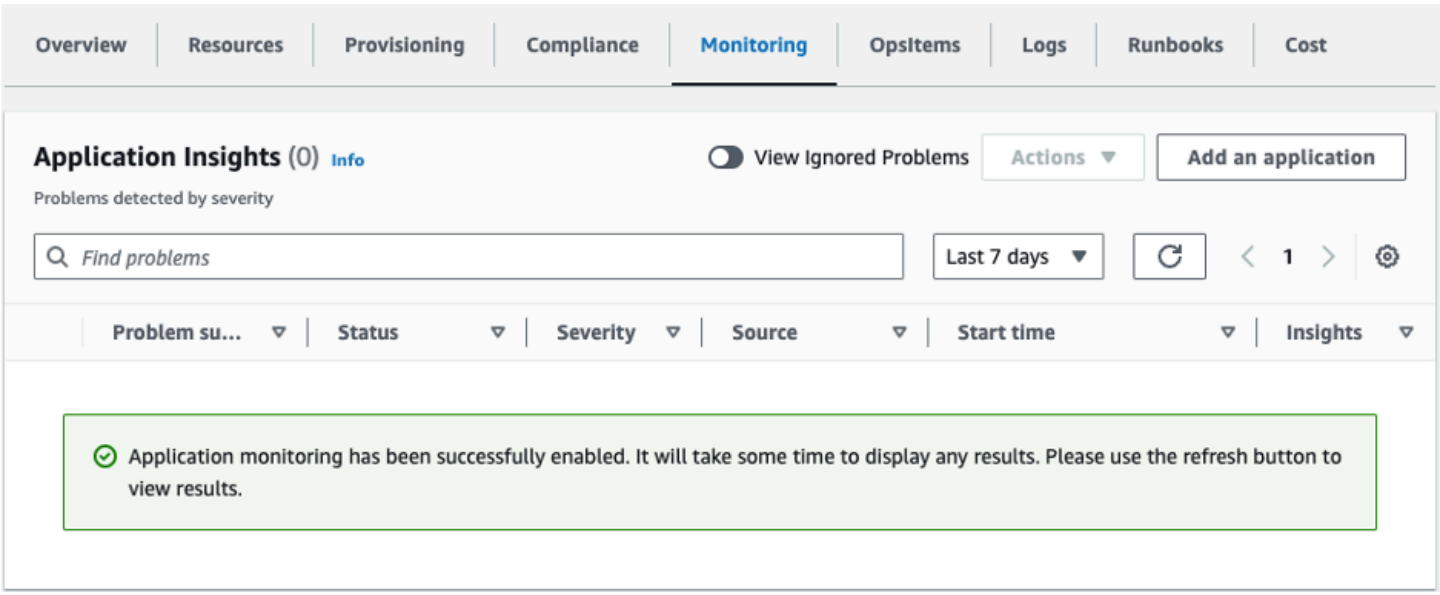
1. 登录 Systems Manager 控制台。
2. 在导航窗格中，选择 Application Manager。
3. 在 “应用程序” 中，搜索此解决方案的应用程序名称并将其选中。

应用程序名称的 “应用程序来源” 列中将包含 App Re gistry，并将包含解决方案名称、区域、账户 ID 或堆栈名称的组合。

4. 在组件树中，选择要激活的应用程序堆栈。
5. 在 “监控” 选项卡的 “应用程序见解” 中，选择 “自动配置应用程序见解”。



监控应用程序现已激活，系统显示以下状态框：

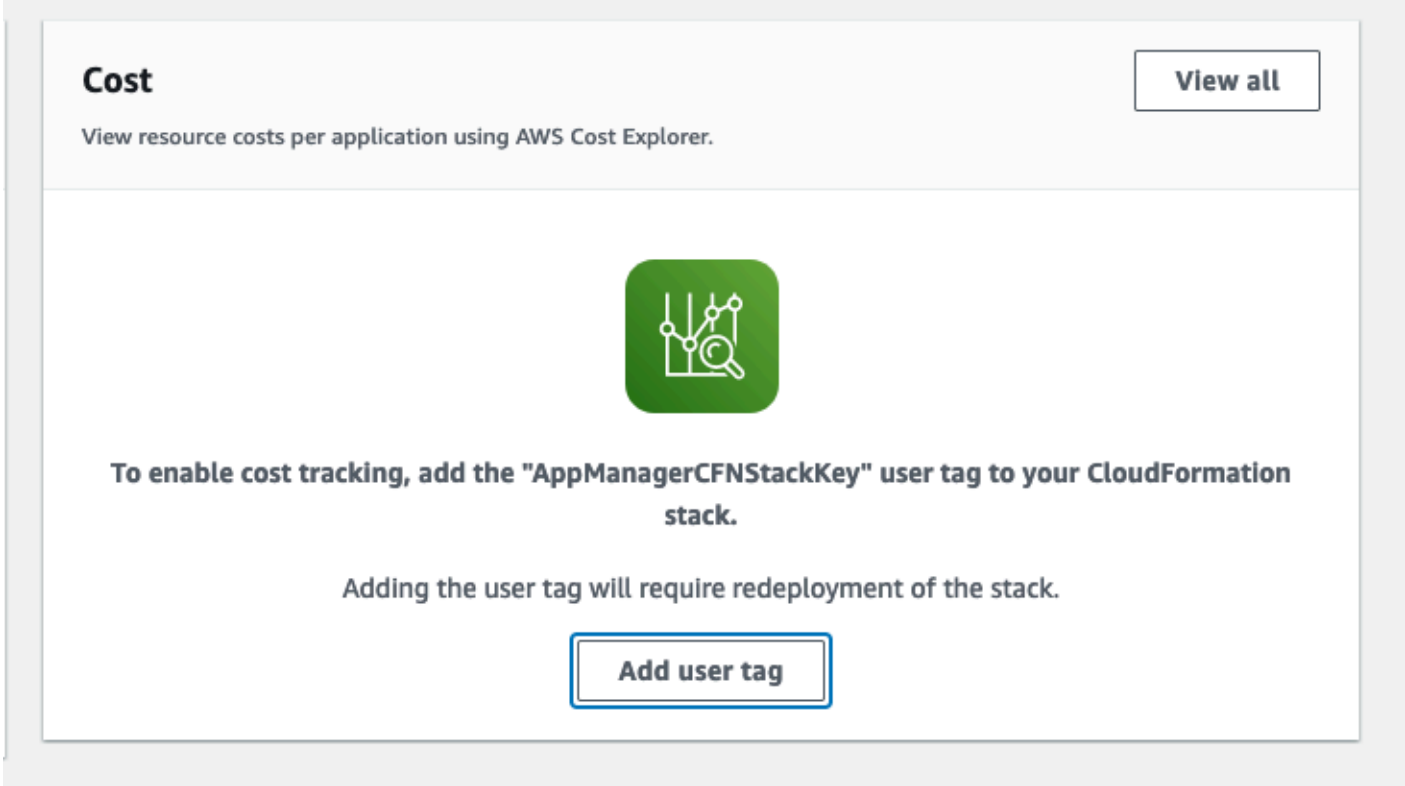


确认与此解决方案关联的成本标签

激活与此解决方案关联的成本分配标签后，您必须确认成本分配标签才能查看此解决方案的成本。要确认成本分配标签，请按以下步骤操作：

1. 登录 Systems Manager 控制台。
2. 在导航窗格中，选择 Application Manager。
3. 在应用程序中，选择此解决方案的应用程序名称并将其选中。

   应用程序名称的 “应用程序来源” 列中将包含 App Re gistry，并将包含解决方案名称、区域、账户 ID 或堆栈名称的组合。
4. 在概览选项卡的成本中，选择添加用户标签。



5. 在添加用户标签页面上，输入 `confirm`，然后选择添加用户标签。

激活过程可能需要长达 24 小时才能完成，显示标签数据。

激活与此解决方案关联的成本分配标签

激活 Cost Explorer 成本管理服务后，您必须激活与此解决方案关联的成本分配标签才能查看此解决方案的成本。成本分配标签只能在组织的管理账户中激活。要激活成本分配标签，请按以下步骤操作：

1. 登录AWS Billing and Cost Management 和成本管理控制台。
2. 在导航窗格中，选择成本分配标签。
3. 在成本分配标签页面上，筛选 AppManagerCFNStackKey 标签，然后从显示的结果中选择该标签。
4. 选择激活。

AWS Cost Explorer

通过与集成（必须先激活），您可以在 Application Manager 控制台中查看与 AWS Cost Explorer应用程序和应用程序组件相关的成本概览。Cost Explorer 成本管理服务通过提供一段时间内的 AWS 资源成本和使用情况视图，帮助您管理成本。要为此解决方案激活 Cost Explorer 成本管理服务，请按以下步骤操作：

1. 登录 AWS 成本管理控制台。
2. 在导航窗格中，选择 Cos t Explorer 以查看解决方案在一段时间内的成本和使用情况。

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 AWS 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 S3URL。
   b. 复制的链接 `aws-waf-security-automations.template` AWS CloudFormation.
   c. 将链接粘贴到 Amazon S3 URL 框中。
   d. 确认 Amazon S3 URL 文本框中URL显示的模板是否正确。
   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。请参阅步骤 1。启动堆栈以获取有关参数的详细信息。
8. 请选择 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. 选中确认模板可能会创建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。大约 15 分钟后，您应该会看到状态为 UPDATE _ COMPLETE。

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 WAF V2。我们用 AWS WAF V2 API 通话替换了所有AWS WAF 经典API通话。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解决方案将一组带有默认配置的 AWS WAF 规则部署到您的 AWS 账户 CloudFormation 堆栈中。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。

> **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update-ip-setCLI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 AWS 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。如果某些 IP 集由于AWAWAFAPI配额导致的速率超出限制问题而无法删除，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“IP 设置”，然后添加要屏蔽的 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。

但是，内容抓取器和机器人（例如扫描安全漏洞并抓取电子邮件地址的恶意软件）可能会尝试访问陷阱端点。在这种情况下，Access HandlerLambda 函数会检查请求以提取其来源，然后更新关联的 AWS WAF 规则以阻止来自该 IP 地址的后续请求。

使用以下过程之一为来自 CloudFront 分发或的请求嵌入 h ALB oneypot 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 AWS 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密钥中复制端点URL。它包含完成此过程所需的两个组件：
   - 端点主机名（例如，`xxxxxxxxxx.execute-api.region.amazonaws.com`）
   - 请求 URI (`/ProdStage`)
5. 登录 Amazon CloudFront 控制台。
6. 选择要使用的发行版。
7. 选择分配设置。
8. 在 Origins (源) 选项卡上，选择 Create Origin (创建源)。
9. 在 Origin Domain Nam e 字段中，粘贴您在步骤 2 中复制URL的端点的主机名组件。将 Web ACL 与您的 Web 应用程序关联。
10. 在 Origin Path 中URL，粘贴您在步骤 2 中也复制的请求。将 Web ACL 与您的 Web 应用程序关联。
11. 接受其他字段的默认值。
12. 选择创建。
13. 在 Behaviors (行为) 选项卡上，选择 Create Behavior (创建行为)。
14. 创建新的缓存行为并将其指向新的原点。您可以使用自定义域名，例如与 Web 应用程序中其他内容相似的虚假产品名称。
15. 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，查看以下代码示例：

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

> **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。

16. 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>
```

将 Honeypot 端点嵌入为外部链接

对于使用部署的 Web 应用程序，请使用此过程ALB。

1. 登录 AWS 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密钥中复制端点URL。
5. 在您的网页内容中嵌入此端点链接。使用您在步骤 2 中复制的完整URL内容。将 Web ACL 与您的 Web 应用程序关联。向您的人类用户隐藏此链接。例如，查看以下代码示例：

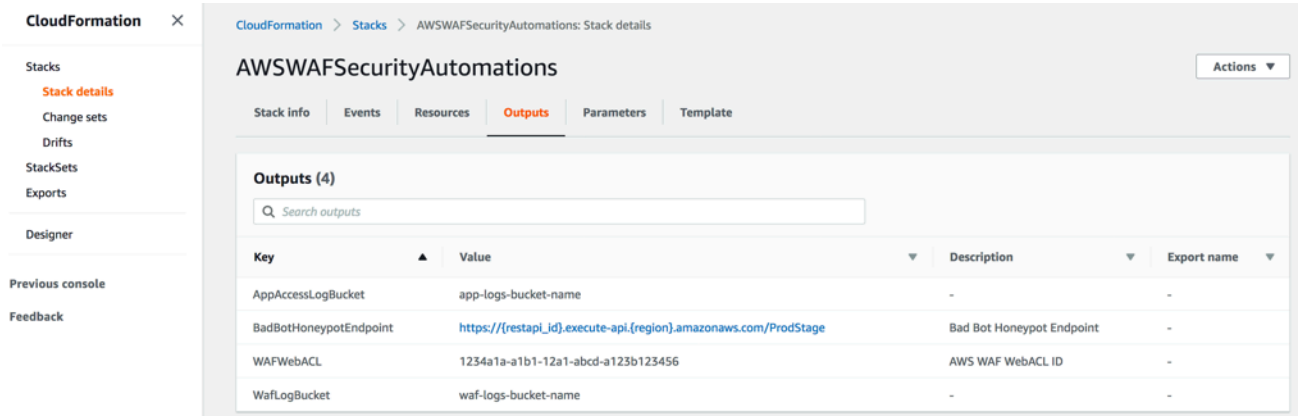
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-hidden="true"><honeypot link></a>
```

> **Note**
>
> 此过程rel=nofollow用于指示机器人不要访问蜜URL罐。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 日志解析器文件 JSON

使用 Lambda 日志解析器JSON文件进行洪水防护 HTTP

如果您选择 Yes - AWS Lambda log parser “激活HTTP防洪保护” 模板参数，则此解决方案会创建一个名为的配置文件*<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。



堆栈输出

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 函数在处理新的日志文件时会考虑 AWS WAF 新值。以下是一个示例代理配置文件：

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

HTTP洪水配置文件

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）-屏蔽适用 IP 地址的时间（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。
- URIlist — 使用它来定义自定义的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，则解决方案会将其添加到 FI HTTPoo d WAF 的 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 函数在处理新的日志文件时会考虑 AWS WAF 新值。*<stack_name>*-app_log_conf.json以下是一个示例代理配置文件：

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

扫描仪和探测器配置文件

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）-屏蔽适用 IP 地址的时间（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)。

- URIlist — 使用它来为具体信息URLs定义自定义请求阈值和封锁周期。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*<stack_name>*-app_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，则解决方案会将其添加到 S

canner & Prob e WAF 的 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。

使用国家和HTTP洪水URI中 Athena 日志解析器

您可以IPs按国家/地区和 URI Athena 查询进行分组，以检测和HTTP阻止具有不可预测模式的洪水攻击。URI为此，请在启动堆栈时为 Fl HTTPood Athena Query 中的请求分组参数选择一个选项（`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。启动堆栈。

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，则此解决方案会创建并运行 CloudFront 对ALB或 `ScannersProbesLogParser` () AWS WAF 或日志 `HTTPFloodLogParser` () 的 Athena 查询，解析输出并进行相应更新。 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小时的数据。您可以通过更改WAF区块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 是否已配置为可以访问。 AWS AWS Glue Data Catalog此解决方案在中创建访问日志数据目录， AWS Glue 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，请参阅升级到最新版本 AWSAWS Glue Data Catalog step-by-step。

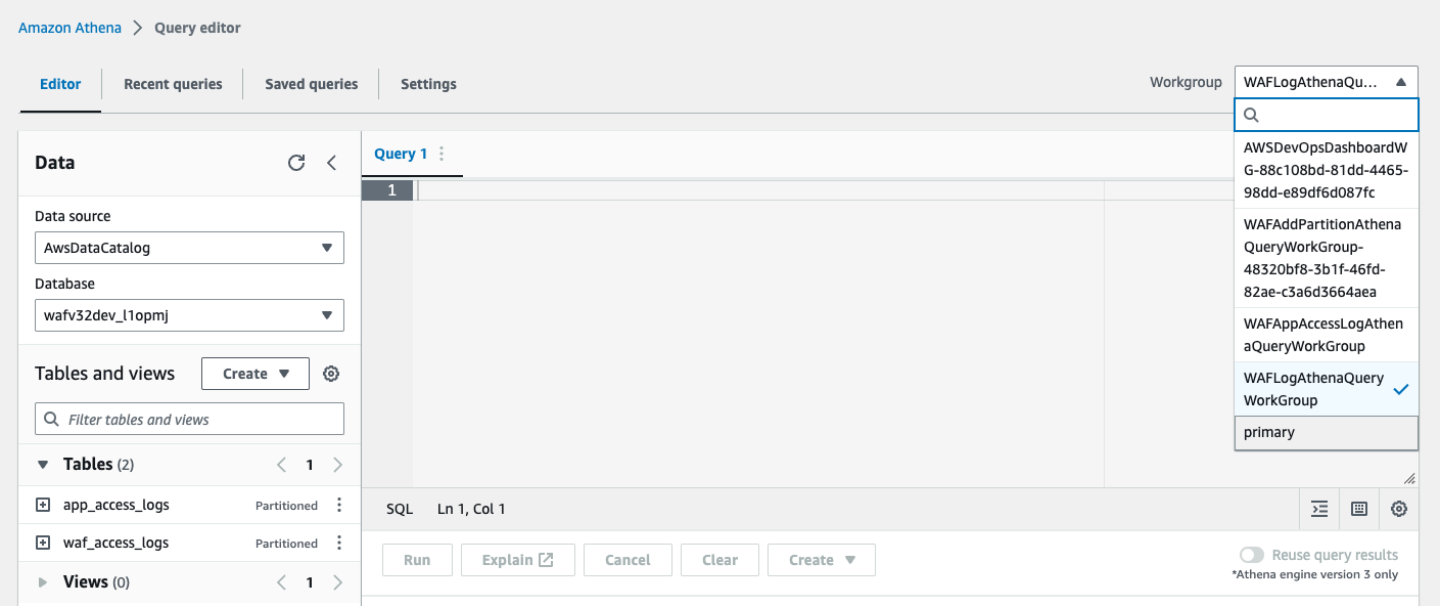
使用以下步骤查看这些查询：

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**
>
> 仅当您选择了 `Yes - Amazon Athena log parser` “激活HTTP防洪保护” 模板参数时，此工作组才会存在。

5. 选择 “切换” 以切换工作组。



6. 选择 “历史记录” 选项卡。
7. 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，此工作组才会存在。

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。

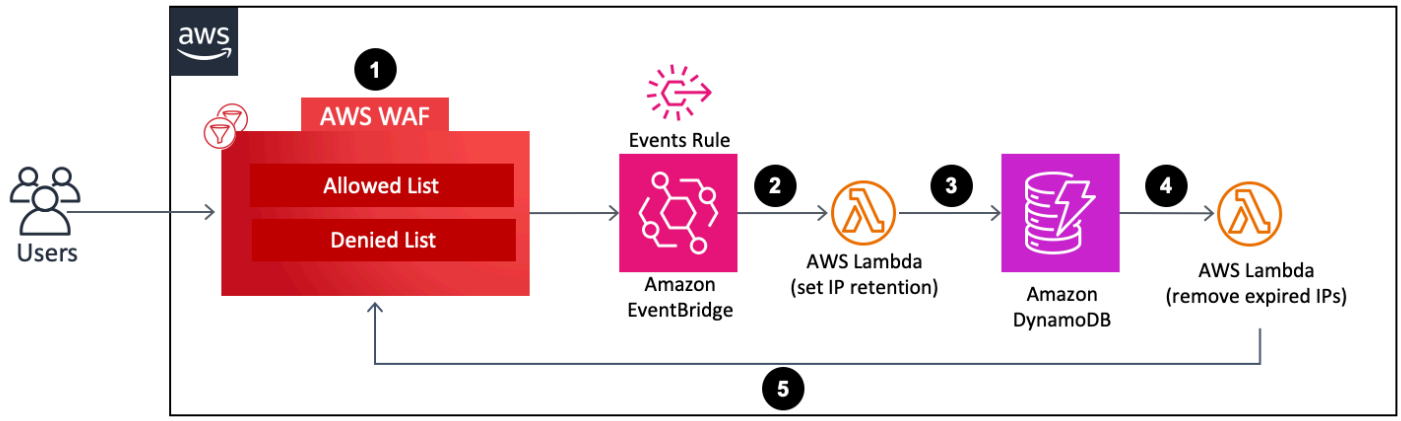
> **Note**
>
> 仅当您选择了 `Yes - Amazon Athena log parser` “激活HTTP防洪保护” 和/或 “激活扫描仪和探测器保护” 模板参数时，此工作组才会存在。

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 IP 集上配置 AWS WAF IP 保留

可以在解决方案创建的 “允许” 和 “拒绝” AWS WAF 的 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。

工作方式



允许和拒绝的 IP 集上WAF的 IP 保留

1. 当用户更新（添加或删除 IP 地址）允许或已拒绝 WAF IP 集时，此操作会调用 AWS WAF `UpdateIPSet`API呼叫并创建事件。
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。该表已打开 DynamoDB Stream s 和 T ime to Live () TTL。该TTL属性是`ExpirationTime`。
4. 当项目达到其过期时间时，会被调TTL用，DynamoDB 会在该项目到期时间后将其从表中删除。删除项目后，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，并 AWS WAF APIl调用从目标 IP 集中删除该项目中包含的过期 IP 地址。 AWS WAF

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。启动堆栈。
2. 如果您想在从 IP 集中删除过期的 IP 地址时收到电子邮件通知，请 AWS WAF 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。启动堆栈。
3. 通过添加或删除 AWS WAF IP 地址来更新 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。此到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，该解决方案就会从 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 删除已过期TTL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。Dy TTL namoDB 的删除主要取决于表的大小和活动级别。由于 DynamoDB AWS WAF 删除操作可能会延迟，因此预计删除操作会出现延迟。通常，该解决方案在 DynamoDB TTL 删除后不久就会从 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 Dynam oD B 上线时间 TTL ()。

构建监控面板

AWS 建议您为每个关键端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。

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DDoS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DDoS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DDoS攻击是否对基础设施造成损害，攻击者是否绕过 CloudFront 或该 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主机运行状况良好 — 您可以将其用作另一个系统运行状况检查指标。
- ASGCPU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

此解决方案配置了一 AWS WAF 条规则，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（例如HTML，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，并实施替代机制来保护那些被排除在外的URLs模式。

此外，某些图像或自定义数据格式可能会导致误报，因为它们包含表明HTML内容中存在潜在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XSS规则，以允许包含其他数据格式的HTML请求。

完成以下步骤以更新XSS规则以排除URLs该接受HTML作为输入。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. 配置筛选器设置以检查URI并列出要XSS根据规则接受的值。
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许可名单

故障排除

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。

联系我们 Support

如果您有AWS开发者支持、AWS商业支持或AWS企业支持，则可以使用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。

创建案例

1. 打开 Supp ort Center。
2. 选择创建案例。

我们能帮上什么忙？

1. 选择 “技术”。
2. 在 “服务” 中，选择WAF或AWS WAF。
3. 在 “类别” 中，选择 “WAF安全自动化” 或 “安全自动化”。 AWS WAF
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：其他信息。

其他信息

1. 在 “主题” 中，输入总结您的问题或问题的文本。
2. 在描述中，详细描述问题。
3. 选择 “附加文件”。
4. 附上处理请求 Support 所需的信息。

帮助我们更快地解决您的问题

1. 输入所需的信息。

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” 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”，输入所需信息，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。

参考

本节包括有关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

此解决方案包括向发送操作指标的选项 AWS。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 AWS 期间将其发送到：

- 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：
  - 扫描仪和探测器 IP 集中的 IP 地址数量以及设置为屏蔽的 FI HTTPoo d IP
  - 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
- 访问处理器数据：
  - Ba d Bot 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

AWS 拥有通过本次调查收集的数据。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. 将下载`aws-waf-security-automations.template`AWS 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。启动堆栈。

相关资源

相关 AWS 白皮书

- AWS DDoS弹性最佳实践

相关 AWS 安全博客文章

- 如何通过使用 AWS WAF、Amazon CloudFront 和推荐人检查来防止盗链

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

修订

Date	更改
2016 年 月 9 日	初始版本
2017 年 1 月	澄清了此解决方案中的 IP 地址限制。
2017 年 3 月 日	有关创建缓存行为的更多指南；已URLs针对 AWS 安全博客文章进行了更新。
2017 年 6 月	增加了ALB支持并更新了产品限制。
2017 年 11 月	增加了对HTTP洪水防护的基于速率的规则支持；增加了用于存储资源访问日志的链接。
2018 年 1 月	更新了有关应用程序负载均衡器区域可用性的 AWS WAF 内容。
2018 年 12 月	添加了 Su IPv6 pport，扩大了CIDR范围，并添加了监控面板。
2019 年 4 月	AWS WAF 日志集成、Amazon Athena 集成，并添加了可配置的日志解析器。
2019 年 12 月	添加了有关支持 Node.js 更新的信息。
2020 年 2 月	错误修复并更新了 RequestThreshold 参数。
2020 年 6 月	添加了使用分区的 Athena 成本优化；README 更新了指令；修复了 Bad Bots 标题中潜在的 DoS 问题。 X-Forward-For
2020 年 7 月	从 AWS WAF Classic 升级到 AWS WAF V2 服务API。
2020 年 11 月	版本3.1.0：澄清了特定区域的HTTP洪水保护以及扫描仪和探测器保护规则；将 S3 路径类型替换为虚拟托管样式；为所有区域添加了分区

Date	更改
	变量ARNs；有关更多信息，请参阅存储库中的 CHANGELOG.md 文件。 GitHub
2021 年 9 月	3.2.0 版本发布：在 “允许的 IP 集” 和 “拒绝的 IP 集” 中添加了 IP 保留支持；错误修复。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 8 月	发行版 3.2.1：增加了对请求组件WAF超大处理的支持；增加了对SQL注入规则语句WAF敏感度级别的支持。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 9 月	更新了在解决方案 CloudFormation堆栈之外进行自定义的文档。
2022 年 12 月	3.2.2 版本发布：增加了与 Service Catalog AppRegistry 和 S AWS ystems Manager 应用程序管理器的集成。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2022 年 12 月	版本3.2.3：在应用程序属性组名称中添加区域作为前缀，以避免与以开头的名称发生冲突。AWS有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 2 月	版本3.2.4：升级了 pytest 和缓解请求。CVE 有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 3 月	更新了允许或拒绝 IP 地址的解决方案从 3.0 或 3.1 版本升级到 3.2 或更高版本的文档。
2023 年 4 月	版本3.2.5：缓解了所有新的 Amazon S3 存储桶的 Amazon S3 对象所有权（ACLs已禁用）的新默认设置所造成的影响。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

Date	更改
2023 年 5 月	版本4.0.0：增加了对新 AWS 托管式规则 规则组和更新的自定义规则的支持。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 5 月	版本4.0.1：更新了`.gitignore` 文件以解决文件丢失的问题。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 9 月	版本4.0.2：重构代码以提高质量。已修补请求包漏洞。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 10 月	版本4.0.3：更新了软件包版本以解决安全漏洞。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2023 年 11 月	文档更新：添加了AWS开发者支持，并将 Contact S AWS upport 合并到故障排除部分。
2023 年 11 月	文档更新：在 “使用 S AWS ervice Catalog 监控解决方案” AppRegistry 部分添加了确认与解决方案关联的成本标签。
2024 年 4 月	文档更新：阐明了在部署步骤 3 中添加 S3 存储桶的说明。
2024 年 9 月	版本4.0.4：更新了软件包版本以解决安全漏洞。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。
2024 年 10 月	版本4.0.5：使用 Poetry 进行依赖关系管理。用 aws_lambda_powertools 记录器替换了原生 Python 记录器。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

Date	更改
2024 年 12 月	发布版本 4.0.6：将 lambda 更新为 python 3.12。有关更多信息，请参阅 GitHub 存储库中的 CHANGELOG.md 文件。

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的当前AWS产品和做法，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产品或服务的任何使用进行独立评估，每项AWS产品或服务均按 “原样” 提供，不提供任何形式的明示或暗示担保。本文件不设定其关联公司、供应商或许可方的任何担保、陈述AWS、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。

AWSWAF解决方案的安全自动化是根据 Apache 许可版本 2.0 的条款许可的。

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。