Amazon WAF Security Automations

部署手册

汤哲

版本：v1.0.0

最后更新时间: 2021 年 5 月

Copyright (c) 2021 by Amazon.com, Inc. or its affiliates.

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

目　录

目　录 **2**

背景 **3**

解决方案描述 **4**

使用场景 **4**

系统架构 **5**

架构图 5

组件 5

功能 6

部署说明 **7**

部署前提 7

快速部署 **8**

启动 CLOUDFORMATION 堆栈 8

指定堆栈详细信息 8

配置堆栈选项 11

审核堆栈 11

关联要保护的资源 12

（可选）手动配置允许或拒绝 IP 列表 **15**

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

背景

在所有线上业务中，安全永远是最重要的话题。亚马逊云科技提供 Amazon WAF 服务来允许客户创建规则过滤 Web 流量，从而阻止尝试利用 Web 应用程序漏洞的攻击。Web 攻击的规模和类型也不断升级，对 WAF 规则的复杂性、更新的及时性提出了更高的要求，也给安全团队带来了大量的人工工作。为了减轻安全团队的负担，用自动化、数据驱动的方式轻松抵御常见的 Web 攻击并及时升级安全策略，亚马逊云科技推出了 Amazon WAF Security Automations 解决方案。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

解决方案描述

本解决方案可用于自动部署一系列 Amazon WAF 规则，以过滤常见的基于 Web 的攻击。用户可以从预先配置的保护性功能中进行选择，这些功能用于定义 Amazon WAF Web 访问控制列表中包含的规则。部署完成后，Amazon WAF 可通过检查 Web 请求来保护 Application Load Balancers。

您可以使用 Amazon WAF 创建自定义的、应用程序特定的规则，以阻止各种攻击模式，确保应用程序可用性、资源安全性，并防止过度消耗资源。

使用场景

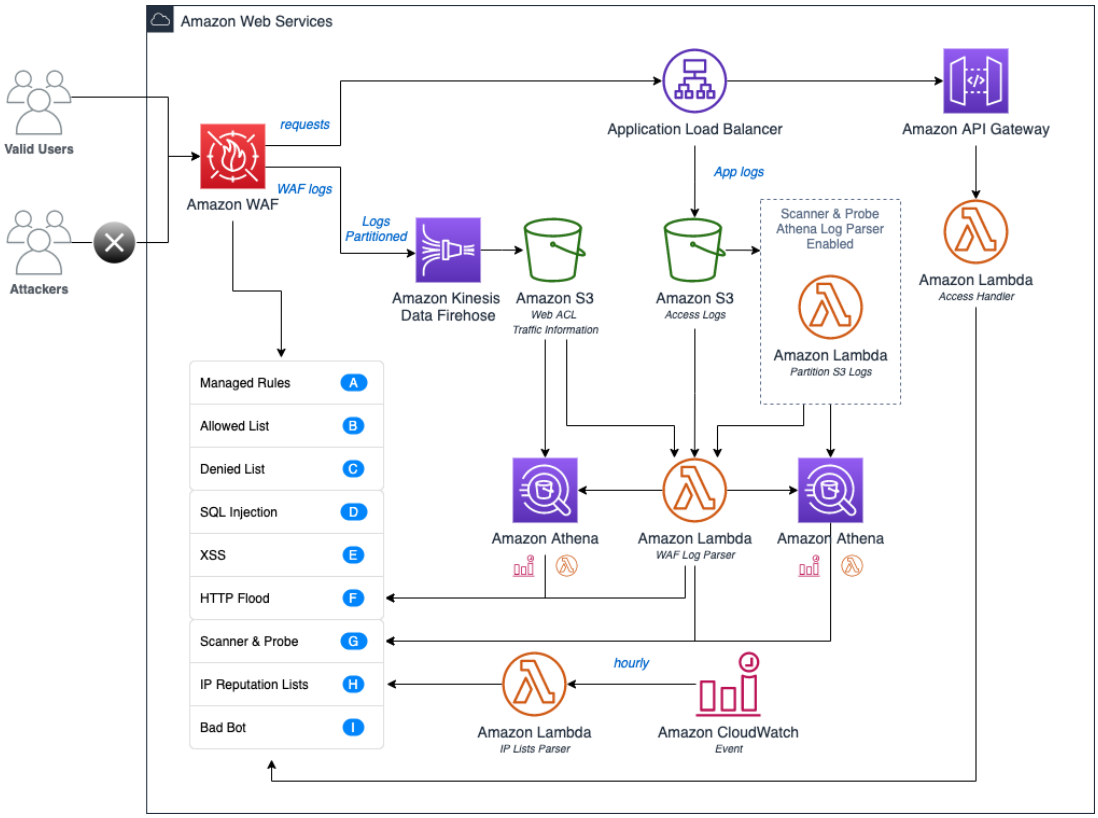
Amazon WAF Security Automations 适用于所有需要使用 WAF 来为 Application Load Balancer 过滤常见 Web 攻击的业务场景，尤其是当客户需要自动部署常见的安全策略，从而轻松提高安全防护和节约时间时。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

系统架构

架构图

此解决方案可在由西云数据运营的亚马逊云科技（宁夏）区域或由光环新网运营的亚马逊云科技（北京）区域中部署。



组件

这个解决方案会部署一组 WAF Web ACL 规则，包含 IP 规则、XSS 规则、SQL 注入规则等，来过滤基于 Web 的攻击。解决方案还会部署多个 Lambda 函数，或在分析 S3 中存储的访问日志后触发，或通过 CloudWatch 周期性触发，来及时更新这些 Web ACL 规则。除此之外，如果客户启用 Bat Bot 功能，解决方案还会部署一个 API Gateway 和一个 Lambda 函数，作为蜜罐引诱并转移机器人试图进行的攻击。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

功能

Amazon 托管规则 (A)：此 Amazon 托管核心规则组合提供保护，避免各种常见的应用程序漏洞被利用或出现其他不必要的流量。

手动 IP 列表（B 和 C）：此组件可创建两个特定的 Amazon WAF 规则，从而使您可以手动插入您想阻止或允许的 IP 地址。

SQL 注入 (D) 和 XSS (E)：此解决方案可配置两个本机 Amazon WAF 规则，这些规则旨在防止 URI、查询字符串或请求正文中的常见 SQL 注入或跨站点脚本 (XSS) 模式。

HTTP 泛洪攻击 (F)：此组件有助于防止由来自特定 IP 地址的大量请求组成的攻击，如 Web 层 DDoS 攻击或暴力登录尝试。此功能的支持阈值是 5 分钟之内少于 100 个请求。

扫描程序和探测器 (G)：此组件可解析应用程序访问日志，以搜索可疑行为，例如源生成的异常错误量。然后，它将在客户定义的时间段内阻止这些可疑的源 IP 地址。

IP 声誉列表 (H)：此组件是 IP 列表解析器 Amazon Lambda 函数，可每小时检查第三方 IP 声誉列表，以获取要阻止的新范围。

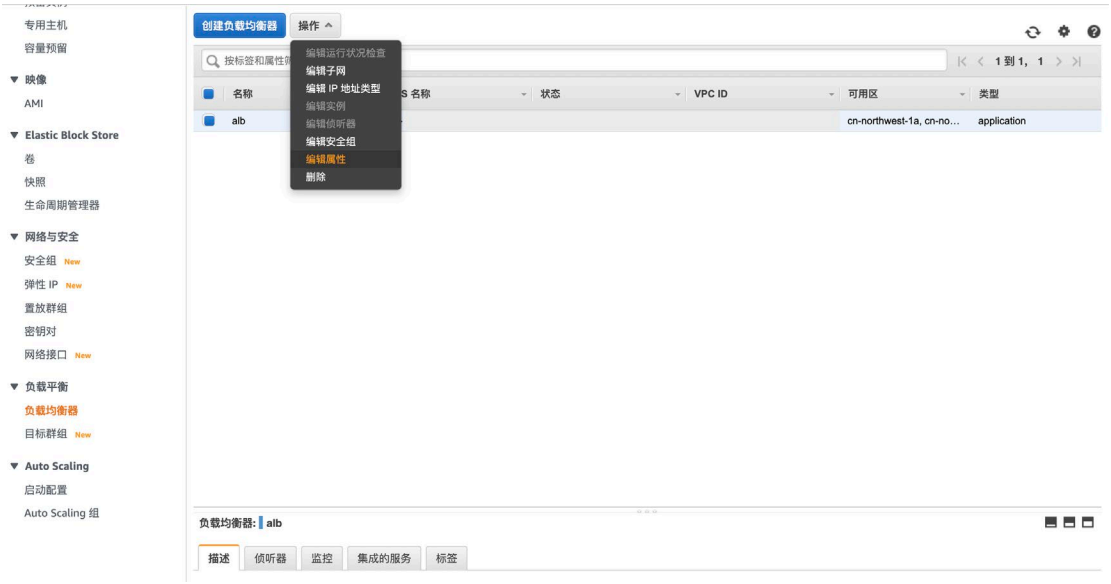
不良 Bot (I)：此组件可自动设置蜜罐，它是一种安全机制，旨在引诱并转移试图进行的攻击。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

部署说明

部署前提

1. 确保您已经拥有激活的亚马逊云科技中国区账户，如果还没有，可以通过注册亚马逊云科技中国区 进行注册。
2. 为您账户中计划保护的 ALB 启用日志功能，并记录日志的 S3 存储桶名称。



打开亚马逊云科技管理控制台，选择 EC2 服务，跳转到 EC2 服务页面。点击左边栏的【负载均衡器】标签，在其中选中您要保护的应用程序负载均衡器，点击【操作】->【编辑属性】，启用【访问日志】并设置 S3 存储桶位置。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

快速部署

本文的步骤针对在运行在由西云数据运营的亚马逊云科技（宁夏）区域或由光环新网运营的亚马逊云科技（北京）区域中部署该解决方案，您可以选择对应的启动模板，快速启动一个 CloudFormation 堆栈来部署和管理整个方案。

启动 CloudFormation 堆栈

点击宁夏和北京区域链接，打开亚马逊云科技管理控制台（如果还没登录会先跳转到登录页面，登录后进入模板启动页面）。默认情况下，此模板在宁夏区域启动，您同时可以使用控制台右上方的区域选择链接，以在其他区域部署该方案。然后单击下面的按钮以启动 CloudFormation 模板。

Launch Stack

指定堆栈详细信息

点击【下一步】，进入参数设置页面，如下图所示。

根据您的需求调整以下参数。

参数类型	参数	值	释义
Protection List	Activate Managed Rules Protection	从下拉框选择，默认为 no	是否启用托管规则功能，yes 为启用，no 为不启用
Protection List	Activate SQL Injection Protection	从下拉框选择，默认为 yes	是否启用 SQL 注入功能，yes 为启用，no 为不启用
Protection List	Activate Cross-site Scripting Protection	从下拉框选择，默认为 yes	是否启用 XSS 功能，yes 为启用，no 为不启用
Protection List	Activate HTTP Flood Protection	从下拉框选择，默认为 yes – WAF rate based rule	是否启用 HTTP 泛洪攻击功能，yes 为启用，no 为不启用，不同选项代表不同更新策略
Protection List	Activate Scanner & Probe Protection	从下拉框选择，默认为 yes – Lambda log parser	是否启用扫描程序和探测器功能，yes 为启用，no 为不启用，不同选项代表不同更新策略
Protection List	Activate Reputation List Protection	从下拉框选择，默认为 yes	是否启用 IP 声誉列表功能，yes 为启用，no 为不启用
Protection List	Activate Bad Bot Protection	从下拉框选择，默认为 yes	是否启用不良 Bot 功能，yes 为启用，no 为不启用

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

Settings	Endpoint Type	从下拉框选择，默认为 ALB	保护的资源类型，目前只支持 ALB
Settings	Application Access Log Bucket Name	输入 String 类型值，S3 存储桶名称，无默认值	存储 ALB 日志的 S3 存储桶名称，当启用了扫描程序和探测器功能时才需要输入此项
Advanced Settings	Error Threshold	输入整数值，默认为 50	每分钟每个 IP 允许的最大攻击请求数，当启用了扫描程序和探测器功能时才需要输入此项
Advanced Settings	Request Threshold	输入整数值，默认为 100	每 5 分钟每个 IP 允许的最大请求数，当启用了 HTTP 泛洪攻击功能时才需要输入此项
Advanced Settings	WAF Block Period	输入整数值，默认为 240	针对识别出的恶意 IP 的 block 周期，单位为分钟，当启用了扫描程序和探测器功能或 HTTP 泛洪攻击功能时才需要输入此项
Advanced Settings	Keep Data in Original s3 location	从下拉框选择，默认为 No	选择是否要将原始的日志文件保留一份在原始 S3 存储桶中，当启用了使用 Athena 日志解析器的扫描程序和探测器功能时才需要设置此项

调整好参数后，点击 【下一步】。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

配置堆栈选项

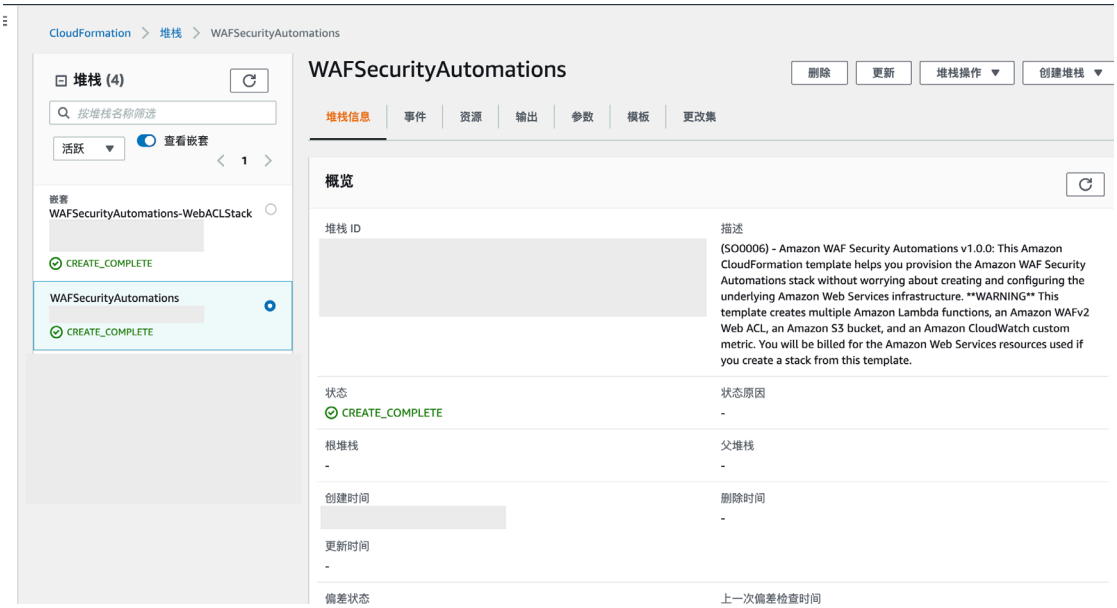
保持默认值，点击【下一步】。

审核堆栈

保持默认值，请勾选 “ 我确认，CloudFormation 可能创建具有自定义名称的 IAM 资源。” 的单选框，点击 【创建堆栈】。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

等待大概 20 分钟，直至堆栈状态为 Complete，创建完成。

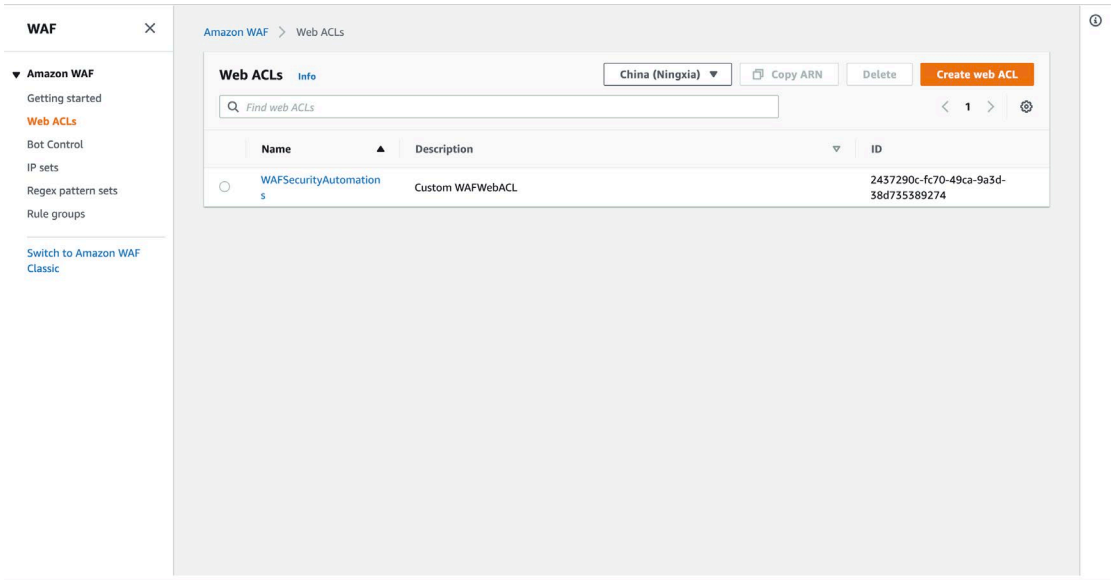


至此，解决方案部署完成，您可以到 WAF 服务中查看自动更新的 Web ACL 规则，它们已经开始帮您过滤流量，应对各种基于 Web 的攻击。

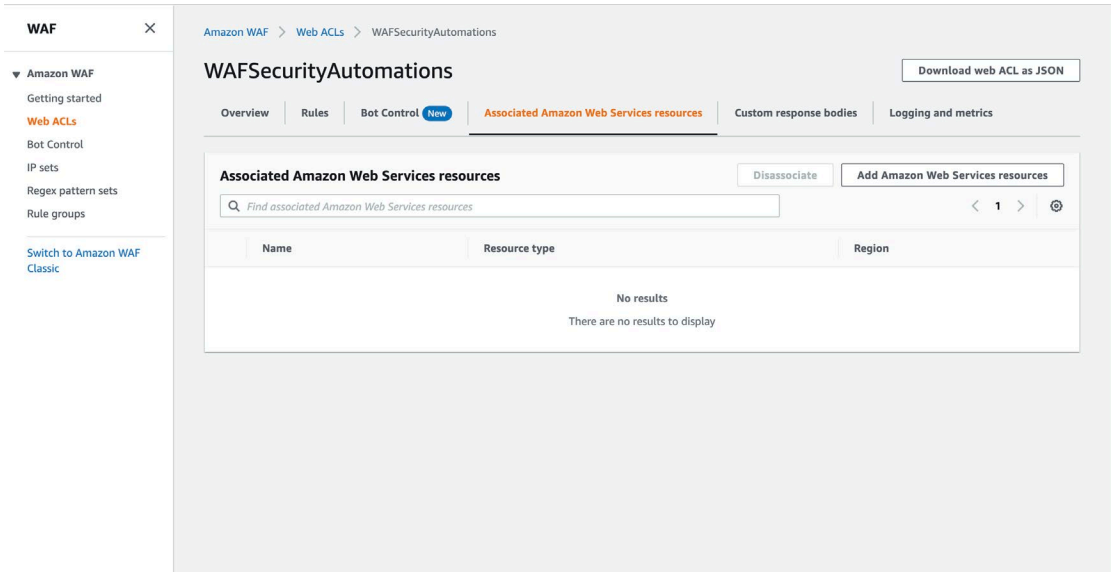
关联要保护的资源

打开亚马逊云科技管理控制台，选择 Amazon WAF 服务，跳转到 WAF 服务页面。然后在左边栏选择【Web ACLs】标签，此时您会看到自动化方案已经为您创建了一组名为 **WAFSecurityAutomations** 的 Web ACL 规则。（您可以通过中上方的按钮调整区域）

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

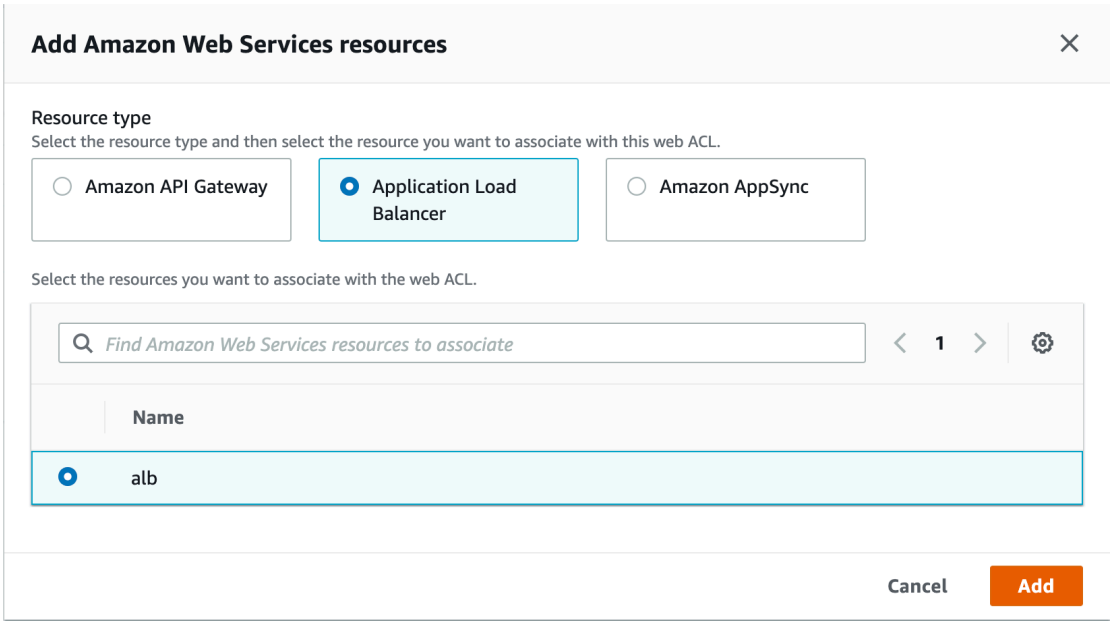


点击这个 ACL 规则，进入详细信息页面；点击【Associated Amazon Web Services resources】标签，设置资源关联。



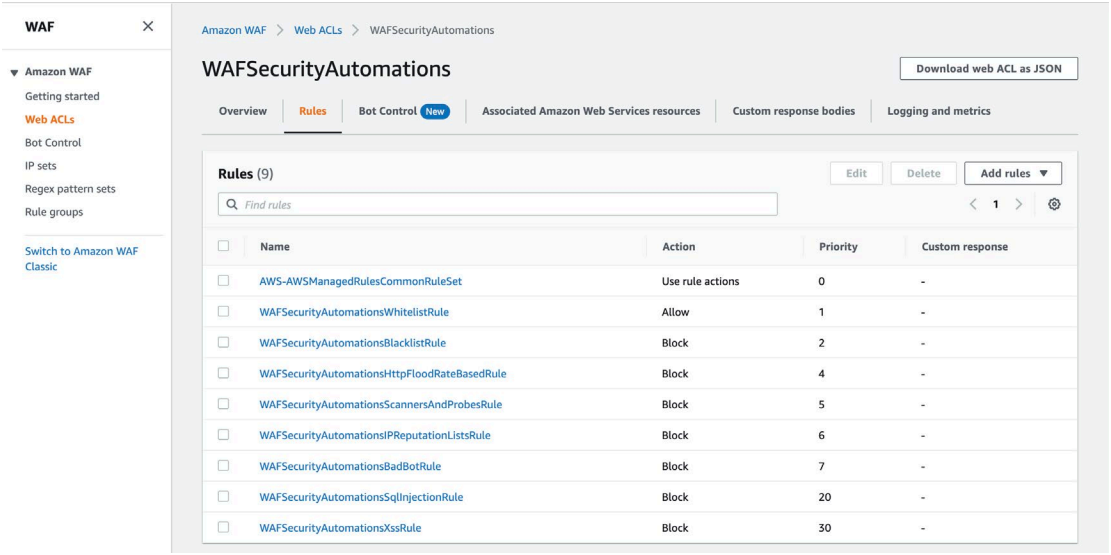
点击右侧的【Add Amazon Web Services resources】按钮，在其中选择您要保护的资源（如某一个负载均衡器），点击右下方的添加按钮，完成关联。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域



此时您关联的这个资源开始受到方案创建的 WAF Web ACL 规则的保护，而且方案会根据日志进行分析，自动更新这些 Web ACL 规则，使它们能够应对实时的安全攻击。

此时您可以在旁边的【Rules】标签页中浏览方案自动为您创建的所有 Web ACL 规则，并查看每个规则的具体功能。

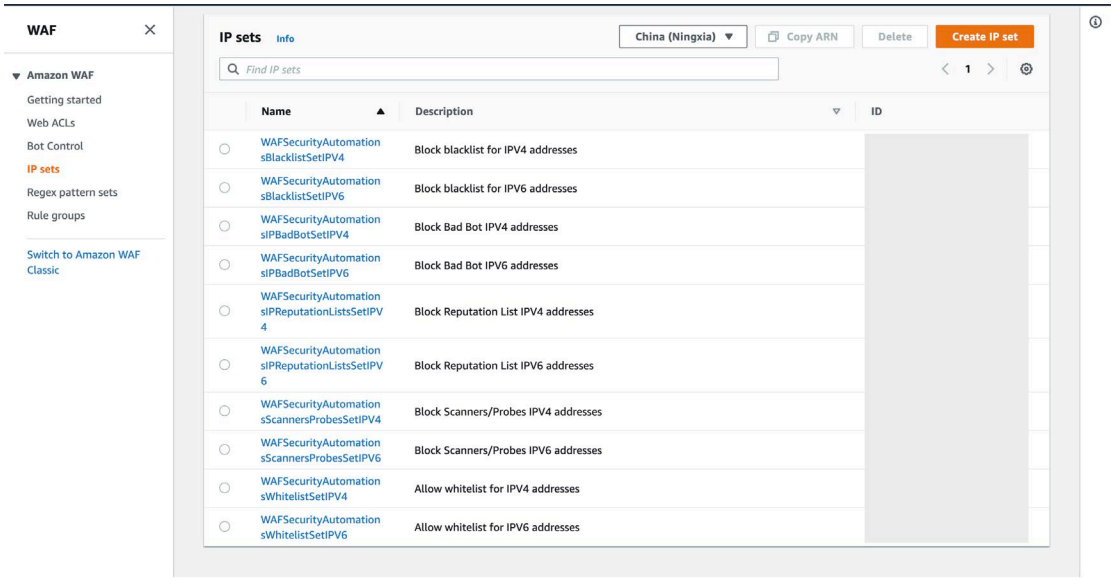


亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域

（可选）手动配置允许或拒绝 IP 列表

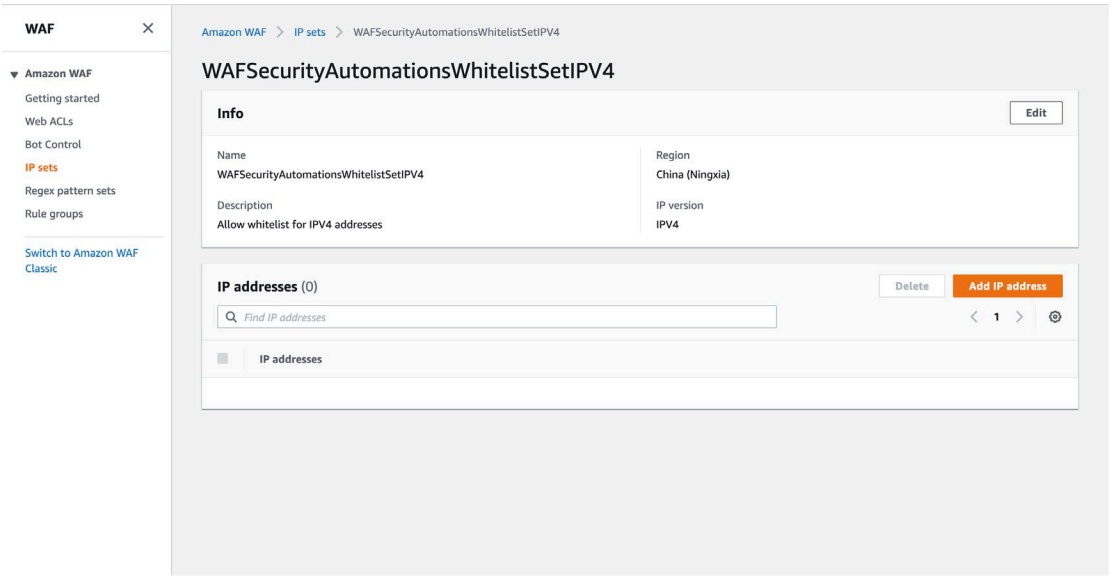
如果您需要在默认规则之外将一些特定的 IP 加入允许或拒绝列表，例如将已知的攻击来源 IP 加入黑名单，或将内部管理 IP 加入白名单等，您可以通过以下步骤进行操作。

打开 WAF 服务页面，点击左边栏的【IP sets】标签，进入 IP 设置功能。在其中寻找您计划修改的 IP set 名称，进入添加或修改。



例如您想为所有功能添加 IPV4 地址段 x.x.x.x/24 进白名单，就打开 **WAFSecurityAutomationsWhitelistSetIPV4** 这个 IP set，点击【Add IP address】按钮，将 x.x.x.x/24 这个地址段添加进去，点击【Add】按钮完成。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域



之后这个 IP 地址段的 IP 就进入白名单，不会触发 WAF 规则的阻挡。对其他功能的允许/拒绝列表也是类似的设置方式。

亚马逊 amazon web services
西云数据运营宁夏区域
光环新网运营北京区域