



开发人员指南

AWS 网络安全经理



AWS 网络安全经理: 开发人员指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是 AWS 网络安全管理器？	1
操作方法 AWS 网络安全管理器工作原理一览	1
的特点 AWS 网络安全经理	1
使用案例	2
相关服务	2
访问 AWS 网络安全经理	3
定价	3
您是 新用户吗？	3
AWS 网络安全管理器的工作原理	5
AWS 网络安全管理器资源模型	5
AWS 网络安全管理器资源生命周期、合并和同步	6
草稿和活跃生命周期	6
版本控制	7
Priority-based 策略合并	7
利用资源发现 AWS Config	8
同步和修复	9
管理员和成员账户	10
Service-linked 角色	10
设置 AWS 网络安全管理器	11
选择你的组织模式	11
设置为单一账户使用	11
设置多账户使用 AWS Organizations	11
创建一个 AWS 网络安全管理器管理员帐户	12
使用创建 IAM 身份 AWS 网络安全管理员权限	14
注册获取 AWS 账户	15
使用 AWS 默认禁用的区域中的网络安全管理器	15
教程：部署您的第一个网络安全防护	16
先决条件	16
步骤 1：创建规则	16
步骤 2：创建模板	18
步骤 3：创建策略	18
步骤 4：创建作用域	19
步骤 5：创建和发布部署	20
步骤 6：监控同步状态	21

步骤 7：清除	21
后续步骤	22
管理防火墙和安全服务	24
管理 WAF 的网页 ACL AWS	24
AWS WAF 的概念	24
AWS WAF 快速创建	27
AWS WAF 的标准创建流程	31
管理 Shield 高级版的 DDoS AWS 防护	35
AWS Shield 高级版快速创建	36
AWS Shield Advanced 的标准创建流程	39
AWS 网络安全管理器和 Firewall Manager	42
与共存 AWS Firewall Manager	42
修复期间的优先级	42
计划迁移自 AWS Firewall Manager	42
安全性	43
数据保护	43
静态加密	44
传输中加密	44
密钥管理	44
Identity and access management	45
受众	45
使用身份进行身份验证	45
使用策略管理访问	46
操作方法 AWS 网络安全管理器可与 IAM 配合使用	48
Identity-based 策略示例	53
问题排查	56
Service-linked 角色	58
Service-linked 角色权限	58
创建服务相关角色	68
编辑服务相关角色	69
删除服务相关角色	69
支持的区域：	70
合规性验证	70
恢复能力	70
基础设施安全性	70
安全最佳实践	71

预防性控制机制	71
侦测性控制	71
监控 AWS 网络安全经理	72
监控同步状态	72
同步状态操作	72
了解同步状态值	72
了解评估时间戳	73
Cross-account 能见度	73
诊断不同步的资源	73
CloudTrail 日志	74
AWS 中的网络安全管理器信息 CloudTrail	74
示例：CreatePolicy 事件	75
配额	78
资源配额	78
资源构成配额	78
范围配置配额	79
管理员账户配额	79
API 分页配额	79
配额可调性	80
文档历史记录	81
.....	lxxxii

什么是 AWS 网络安全经理？

借助 AWS Network Security Manager，您可以为组织中的一个或多个账户和资源集中定义 AWS 和部署网络安全保护，例如 WAF 和 AWS Shield Advanced 规则。与其单独使用每种资源，不如定义一次可重复使用的策略对象（规则、模板和策略），然后大规模部署它们，并通过持续监控来检测和修复策略偏差。

操作方法 AWS 网络安全管理器工作原理一览

您可以定义一组分层策略对象并将其应用于目标范围。最低级别的策略对象是规则。您可以将规则分组为模板，然后将其组合成具有基于优先级的冲突解决方案的策略。然后，您可以选择要使用范围保护的账户和资源，并通过发布部署来强制执行您的策略。

部署后，AWS Network Security Manager 会持续监控范围内的环境和部署的策略，以检查它们是否符合预期的定义。否则，AWS 网络安全管理器可以选择修复偏离预期配置的资源。有关资源模型、生命周期和架构的完整详细信息，请参阅 [AWS 网络安全管理器的工作原理](#)。

的特点 AWS 网络安全经理

- 支持多种防火墙类型 — AWS Net AWS work Security Manager 支持 Web ACL 配置和规则组的 WAF。受保护的资源类型包括亚马逊 CloudFront 分配、应用程序负载均衡器和 Amazon API Gateway 阶段。AWS Network Security Manager 还支持 AWS Shield Advanced，为亚马逊 CloudFront 分发、应用程序负载均衡器、经典负载均衡器和弹性 IP 地址提供 DDoS 保护。
- 可重复使用的安全配置-将策略对象定义为规则，将其分组为模板，然后创建目标资源的范围。在多个策略和部署中重复使用规则、模板和范围。
- Priority-based 策略合并 — 当多个策略保护同一个资源时，AWS Network Security Manager 会根据策略优先级合并其配置，从而提供可预测的冲突解决方案。
- Single-account 和多管理员支持 — 在单个帐户中使用 AWS Network Security Manager 或指定多个管理员帐户，每个帐户都有优先级。当管理员的策略重叠时，AWS Network Security Manager 会先按管理员优先级解决冲突，然后按每个帐户内的策略优先级来解决冲突。
- 草稿和活动状态 — 每个 AWS Network Security Manager 资源，包括规则、模板、策略、范围和部署，都支持“草稿”和“活动”状态。在不影响实时保护的情况下将资源另存为“草稿”，然后在准备好强制执行时发布。
- 版本化快照 — 每个 AWS Network Security Manager 资源，包括规则、模板、策略、范围和部署，都支持不可变的版本号快照。使用版本控制来保留已知良好的 AWS 网络安全管理器资源配置。

- Protected-resource 同步诊断-对于每个范围内的资源，准确查看哪些设置不同步以及原因，以及每个配置字段的预期设置与实际值的比较。
- 自动修复- (可选) 启用 AWS Network Security Manager 自动修复不同步的资源，使其与预期配置保持一致，无需手动干预。
- Natural-language 规则生成 — 使用该GenerateRuleConfiguration操作以通俗易懂的语言描述规则，并接收由 Amazon Bedrock 提供支持的相应配置 JSON。

使用案例

以下是 AWS 网络安全管理器的常见用例：

- 在所有账户中强制执行基准 AWS WAF 规则 — 定义一组 AWS WAF 规则组，每个面向互联网的应用程序都必须使用这些规则组，然后将其部署到整个组织中。AWS 当新的范围内的资源进入范围时，网络安全管理器会自动将这些规则应用于这些资源。
- 跨特定资源创建特定的自定义或例外 AWS WAF 规则-定义一组仅适用于特定资源的 WAF 规则。该集合可以是您通过 AWS 账户 ID、OU、标签或 Amazon 资源名称 (ARN) 标识的特定业务部门或应用程序。
- 在@@ 面向互联网的资源上验证 DDoS 保护 — 创建适用于公共资源类型的 AWS Shield Advanced 策略，并在组织范围内部署，以便关键资源启用 DDoS 保护。
- 检测和修复配置偏差-使用同步状态监控来识别防火墙配置已偏离预期状态的资源，并可选择启用自动修复以使其恢复合规性。
- 将安全管理委托给多个团队-指定多个管理员帐户，这些帐户具有不同的优先级别，并对特定帐户、组织单位或防火墙类型进行限定访问权限，从而允许团队在定义的边界内管理自己的安全策略。

相关服务

- AWS WAF — 使用 AWS WAF 保护您的 Web 应用程序和 API 免受可能影响可用性、危及安全性或消耗过多资源的常见 Web 漏洞和机器人的侵害。AWS Network Security Manager 使用 WAF 为组织中的单个账户或多个账户中的资源创建和管理 Web ACL 和规则组。
- AWS Shield Advanced — 一项托管 DDoS 保护服务，可为您的应用程序提供扩展保护。AWS Network Security Manager 使用 Shield Advanced 为组织中的单个账户或多个账户中的资源提供 DDoS 保护。
- AWS Organizations — 随着 AWS 资源的增长和扩展，帮助您集中管理和治理环境。AWS Network Security Manager 要求 AWS 组织管理跨成员账户的保护。

- AWS Config — 一项使您能够评估、审核和评估 AWS 资源配置的服务。AWS Network Security Manager 使用与服务关联的 AWS Config 记录器来发现您的成员账户中的资源。

访问 AWS 网络安全经理

您可以通过以下接口访问 AWS 网络安全管理器：

AWS 管理控制台

用于管理 AWS 网络安全管理器资源的基于 Web 的界面。

打开 AWS 网络安全管理器控制台，网址为 <https://console.aws.amazon.com/network-security-manager/>。

AWS 命令行界面 (AWS CLI)

提供 AWS 网络安全管理器操作命令。有关更多信息，请参阅 [AWS CLI 命令参考](#)。

AWS 软件开发工具包

AWS 提供由适用于各种编程语言和平台的库和示例代码组成的 SDK。软件开发工具包提供了一种便捷的方式来创建对 AWS 网络安全管理器的编程访问权限。有关更多信息，请参阅[用于 Amazon Web Services 的工具](#)。

AWS 网络安全管理器 API

通过 HTTPS 使用 JSON 的 REST API。API 端点格式为 `network-security-manager.{region}.api.aws`。有关更多信息，请参阅[AWS 网络安全管理器 API 参考](#)。

要开始使用 AWS 网络安全管理器，请参阅[设置 AWS 网络安全管理器](#)和[教程：部署您的第一个网络安全防护](#)。

定价

您需要为 AWS 网络安全管理器监控和保护的每个范围内资源付费。您部署的底层安全服务（例如 AWS WAF 和 AWS Shield Advanced）需要支付额外费用。有关详细定价信息，请参阅 AWS 网站上的[AWS 网络安全管理器定价](#)。

您是新用户吗？

如果您是首次使用 AWS 网络安全管理器，我们建议您按顺序阅读以下主题：

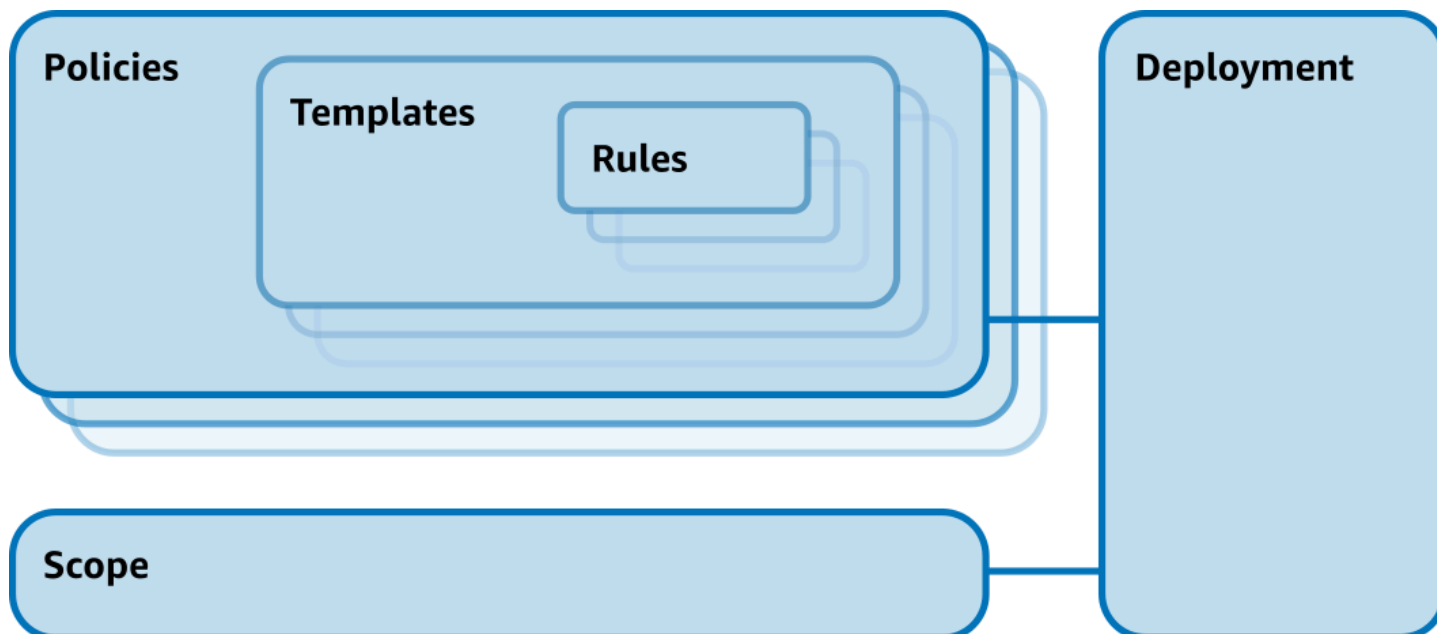
1. [AWS 网络安全管理器的工作原理](#)— 了解资源模型、生命周期状态、策略合并和同步。
2. [设置 AWS 网络安全管理器](#)— 完成使用 AWS 网络安全管理器的先决条件。
3. [教程：部署您的第一个网络安全防护](#)— 浏览创建您的第一个部署的端到端教程。

操作方法 AWS 网络安全管理器起作用

使用 AWS Network Security Manager 资源模型为组织中单个账户或多个账户中的资源设计和管理网络安全保护。本章介绍五种资源类型、它们如何形成层次结构以及控制其行为的关键概念。

AWS 网络安全管理器资源模型

AWS 网络安全管理器使用按组成层次结构排列的五种资源类型：



资源在层次结构中相互向上引用。规则用于模板和策略。策略中使用@@ 模板、规则或两者兼而有之。范围是指策略在部署中保护的资源。

以下各节描述了层次结构中的每种资源类型。

规则-网络安全配置的原子单位。有两种类型的规则：流量检查规则和防火墙配置规则。交通检查侧重于安全服务如何处理流量。配置规则指定流量检查之外的系统操作。规则的结构因防火墙类型而异。

模板-针对单一防火墙类型的一组有序、可重复使用的规则。使用模板将相关规则打包在一起，并在多个策略之间共享。模板是可选的。

策略-将一组有序的模板和规则与防火墙类型的强制设置相结合。每个策略都有一个优先级（数字越小表示优先级越高）。当多个策略保护同一个资源时，优先级决定如何解决冲突。对于流量检查规则，优先级决定规则的聚合顺序。对于防火墙配置规则，优先级决定了哪种配置适用于每种资源及其范围内的策略。

范围 — 保护适用范围的声明性选择。范围指定要保护的资源类型，您可以选择按标签或配置属性筛选资源。在多账户模式下，范围还会指定要包含或排除哪些账户或 OU。在单账户模式下，范围适用于账户本身。创建示波器时，其模式是固定的。您不能在多账户模式和单账户模式之间朝任何方向切换范围，因此多账户范围永远不会变成单账户范围，反之亦然。

部署-将一个或多个策略绑定到作用域。发布部署会激活强制执行。AWS Network Security Manager 会发现范围内的资源，计算预期的配置，并有选择地修复不同步的资源。

有关资源构成限制，请参阅[配额](#)。

AWS 网络安全管理器资源生命周期、合并和同步

以下各节说明了控制 AWS 网络安全管理器资源在创建后如何运行的行为和机制。

草稿和活跃生命周期

每个 AWS Network Security Manager 资源（包括规则、模板、策略、范围和部署）的状态都是“草稿”或“活动”：

- **活动**-默认状态。该资源已发布并可供使用。其他资源可以引用它，而包含它的部署会强制执行其配置。
- **草稿**-资源已保存但尚未激活。草稿资源不强制执行，也不能被其他资源引用。创建或更新资源时，请选择保存草稿以使其保持草稿状态。

默认情况下，AWS 网络安全管理器将资源创建为“活动”。要使用 API 将资源创建为草稿，请在创建或更新操作false中将isPublished参数设置为。

更新资源时，以下情况适用：

当前状态	处理建议	结果
草稿	选择“保存草稿”	更新草稿（仍为草稿）
草稿	选择“发布”	发布草稿（变为“激活”）
活动	选择“发布”	更新并保持活动状态（激活）
活动	选择“保存草稿”	创建草稿叠加层（变为草稿，下方有活动资源）

该 `hasPublishedVersion` 字段出现在列表中并获得回复。此字段告诉您草稿下方是否存在已发布的活动资源。当资源处于草稿状态时 `hasPublishedVersion: true`，待处理的草稿位于已发布的活动资源之上。

您无法删除其他活动资源引用的活动资源。

版本控制

每个 AWS Network Security Manager 资源（包括规则、模板、策略、范围和部署）都可以进行版本控制。要创建活动资源的版本，请选择该资源，选择操作，然后选择创建版本化快照。并非每次更新时都会自动创建版本。

AWS CLI 替代方案

您也可以使用 `Create{Resource}Snapshot` API 操作在活动资源上创建版本。

关键版本属性：

- 每个版本都有一个唯一的数字（一个连续整数）和一个版本限定的 ARN（例如）。`arn:aws:network-security-manager:us-east-1:123456789012:rule:abc123:3`
- 版本是不可变的。它们无法更新。
- 每个资源最多可以创建 10 个版本。
- 版本是可标记的。

使用版本来保留所需的配置变体。要回滚资源，请读取一个版本，然后使用版本所需的配置更新实时资源。

Priority-based 策略合并

当多个策略保护同一个资源时，AWS 网络安全管理器会将其配置合并为一个结果。优先级数字越低表示优先级越高（优先级 1 优先于优先级 2）。当 AWS Network Security Manager 合并包含流量检查规则的策略时，优先级决定规则的聚合顺序。对于防火墙配置规则，优先级较高的策略决定应用哪种配置。

AWS 网络安全管理器按以下顺序评估两个级别的优先级：

1. 管理员优先级- AWS 网络安全管理器首先评估管理员优先级。为每个组织管理员分配优先级，如中所述[the section called “管理员和成员账户”](#)。当 AWS Network Security Manager 合并策略时，它对管理员策略的排名要高于成员账户自己的单账户策略。如果管理员策略和成员账户的单账户策略都适用于资源并且存在冲突，则管理员策略的配置将获胜。成员账户不能选择退出、覆盖或免除管理员政策。
2. 策略优先级 — 然后，在每个帐户中，AWS 网络安全管理员使用策略优先级来解决剩余的冲突。策略优先级值是从 1 开始的整数，并且每个账户必须是唯一的。

您可以使用 PutAdminAccount 操作的必填 priority 字段（介于 1 到 10 之间的整数）来设置管理员优先级。优先级值是唯一的，因此两个管理员永远不会共享一个优先级，也不需要打破平局。有关更多信息，请参阅[AWS 网络安全管理器 API 参考](#)。

资源的所有适用策略的合并结果是有效的防火墙配置。AWS Network Security Manager 计算此配置，将其与资源的实际配置进行比较，并将任何差异报告为同步状态。

当策略发生冲突时，AWS 网络安全管理器会比较每个属性并应用优先级较高的策略中的值。如果优先级较高的策略未定义属性，则优先级较低的策略值适用。与有效配置相匹配的资源是 IN_SYNC。对于优先级较低的部署，受低优先级策略保护且其设置被较高优先级策略覆盖的资源报告为 OUT_OF_SYNC。这是预期的行为，而不是失败。

利用资源发现 AWS Config

AWS Network Security Manager 使用与服务关联的 Config AWS 配置记录器发现您账户中的受保护资源。当每个账户进入部署范围时，该记录器会自动在每个账户中创建。与 Fi AWS rewall Manager 不同，您无需执行任何其他设置。AWS AWS 网络安全管理器的 Config 使用量不向 AWS 网络安全管理器客户收费。

服务关联录制器的主要特征：

- 它被命名为 AWSConfigurationRecorderForNetworkSecurityManager。
- 它与账户中的任何客户管理的配置记录器是分开的。
- 它仅记录与您的活动范围和部署相关的资源类型。
- 您无需设置 AWS Config 或创建配置记录器。AWS 网络安全管理器会自动对此进行管理。AWS Network Security Manager 的 Config 使用量不向客户收费。
- 在使用录音机期间，您无法对其进行修改或删除。AWS 网络安全管理器自动管理其生命周期。

您无需手动启用或配置 AWS Config 即可让 AWS 网络安全管理器正常运行。发布部署后，该服务会自动处理资源发现。

同步和修复

AWS 网络安全管理器中的强制执行是异步的，并且最终是一致的。发布部署后，或者当资源发生变化时，会出现以下阶段：

1. 资源发现 — AWS 网络安全管理器使用与服务关联的 Config 记录器发现范围内的资源。
2. 配置计算-对于每个发现的资源，AWS Network Security Manager 通过按优先级合并所有适用的策略来计算有效的防火墙配置。
3. 同步评估 — AWS Network Security Manager 将有效配置与资源的实际配置进行比较，并记录同步状态。
4. 补救（可选）-如果您在策略remediationEnabled上进行了设置，则 AWS 网络安全管理器会更正不同步的资源以匹配有效的配置。

每个阶段都是异步的。对您的工作流程的影响：

- 在发布部署和资源受到保护之间会有一段延迟。
- 在范围内创建新资源 and 对其进行保护之间存在延迟。
- 同步状态条目上的Last Checked时间戳告诉你 AWS 网络安全管理器上次评估资源的时间。

补救和资源清理是策略级别的设置。您可以为policyConfiguration对象中的每个策略配置每个策略。

remediationEnabled

指定 AWS 网络安全管理器是否自动修复不合规的资源。启用此设置后，AWS 网络安全管理器会更正不同步的资源以匹配有效的配置。

resourcesCleanUp

指定 AWS 网络安全管理器是否在不再需要其创建的资源时自动删除这些资源。AWS 当您移除部署或帐户或资源超出范围时，Network Security Manager 会删除它创建的防火墙。

remediationEnabled和resourcesCleanUp设置均默认为false。AWS 在启用这些设置之前，网络安全管理器不会修复或清理资源。该policyConfiguration对象也成立wafConfig，这适用于AWS WAF 策略。有关更多信息，请参阅[AWS 网络安全管理器 API 参考](#)。

当资源不同步时，同步状态包括不同步的原因，每个设置的详细信息显示预期值与实际值的比较。原因分为以下几类：

- `missingFirewall`— 没有与资源关联的防火墙保护。
- `invalidFirewall`— 存在防火墙，但其配置与有效配置不同。这包括六个详细信息桶：`incorrectSingleValueConfigurations`、`missingAppendableConfigurationValues`、`unexpectedMergeableConfigurationValues` 和 `unexpectedMergeableConfigurationValues`。

如果启用了修复功能，但 AWS Network Security Manager 无法修复资源 `issueType`，则该 `remediationIssues` 字段会提供 `message` 描述问题并 `correctiveAction` 建议如何解决问题。

AWS 网络安全管理器不评估它不管理的设置。如果某个字段未出现在任何参与规则中，则在同步评估期间，AWS 网络安全管理器会忽略该字段。

管理员和成员账户

AWS Network Security Manager 使用基于以下 AWS 组织构建的跨账户管理模型：

- 管理员帐户-用于创建和管理 AWS 网络安全管理器资源（规则、模板、策略、范围和部署）的帐户。您可以指定一个或多个管理员帐户，每个帐户的优先级介于 1 到 10 之间。
- 成员帐户- AWS 网络安全管理员在其中发现资源、评估同步状态并选择性地修复不同步配置的帐户。AWS 网络安全管理员通过与服务相关的角色在成员账户中执行操作。有关更多信息，请参阅 [the section called “Service-linked 角色”](#)。

您可以选择将每个管理员的范围限定为帐户、OU 和防火墙类型的子集。使用此功能将特定领域的管理委托给不同的团队。

AWS 网络安全管理器是一项区域性服务。您可以按区域创建资源和部署，不存在跨区域依赖关系。

Service-linked 角色

AWS Network Security Manager 使用名为 `AWSServiceRoleForNetworkSecurityManager` 的 IAM 服务相关角色代表您在组织的成员账户中执行操作。此角色信任 `network-security-manager.amazonaws.com` 服务主体。它使用 `NetworkSecurityManagerServiceRolePolicy` AWS 托管策略。

AWS 当您启用该服务时，网络安全管理器会自动创建此角色，因此无需手动设置。该角色允许 AWS 网络安全管理员管理 AWS WAF 和 AWS Shield 高级保护，通过 AWS Config 发现受保护的资源，并执行跨账户操作。有关更多信息，请参阅 [the section called “Service-linked 角色”](#)。

设置 AWS 网络安全经理

使用 AWS 网络安全管理器，您可以在两种组织模式下工作。可以直接在单个账户中使用，也可以将其与 AWS Organizations 一起使用，以管理多个账户的保护。设置步骤取决于您选择的型号。

主题

- [选择你的组织模式](#)
- [设置为单一账户使用](#)
- [设置多账户使用 AWS Organizations](#)
- [创建一个 AWS 网络安全管理器管理员帐户](#)
- [使用创建 IAM 身份 AWS 网络安全管理员权限](#)
- [使用 AWS 默认禁用的区域中的网络安全管理器](#)

选择你的组织模式

从以下组织模式中进行选择：

- Single-account— 使用 AWS 网络安全管理器保护一个账户中的资源。您不需要 AWS Organizations 或管理员帐户。创建具有 AWS 网络安全管理员权限的 IAM 身份，然后直接开始使用该服务。AWS 网络安全管理器会自动在您的账户中创建服务相关角色。
- Multi-account— 使用 AWS Network Security Manager 和 AWS Organizations 来保护多个账户。此模式需要设置 AWS Organizations、启用可信访问和创建管理员帐户。

设置为单一账户使用

要在单个账户中使用 AWS Network Security Manager，请创建具有相应权限的 IAM 身份，然后直接开始使用该服务。您无需创建管理员帐户。AWS 网络安全管理器会在后台自动在您的账户中创建服务相关角色。跳至[the section called “使用创建 IAM 身份 AWS 网络安全管理员权限”](#)。

设置多账户使用 AWS Organizations

要管理多个账户的保护，请建立所需的 AWS Organizations 成员资格和配置。

1. 选择要用作组织 AWS 网络安全管理器管理员的帐户 — 这是您创建和管理 AWS 网络安全管理器资源的帐户。

2. 验证组织成员资格-如果您选择的帐户还不是该组织的成员，请将其加入。按照《[Organizations 用户指南](#)》中[邀请 AWS 账户加入您的AWS 组织](#)中的指导进行操作。
3. 启用组织中的所有功能 — Organizations 有两个可用的功能集：整合账单功能和所有功能。要使用 AWS 网络安全管理器，您的组织必须启用所有功能。如果您的组织仅配置为使用整合账单，请按照《Organizations 用户指南》中[启用AWS 组织中的所有功能](#)中的指导进行操作。
4. 为 AWS 网络安全管理器启用可信访问-在 Organizations 中为 AWS 网络安全管理员启用可 AWS 信访问。启用可信访问权限后，AWS Network Security Manager 可以在成员账户中创建服务相关角色并代表他们管理资源。
5. 注册委派管理员帐户-在 Organizations 中将您选择的账户注册为 AWS Network Security Manager 的委托 AWS 管理员。使用 Organizations 管理账户完成此步骤。

Multi-account 关闭可信访问时禁用保护

如果您在 Organizations 中 AWS 关闭 AWS Network Security Manager 的可信访问权限，或者取消注册委派的管理员帐户，AWS Network Security Manager 会将多账户范围和部署设置为 DISABLED 状态并清理其管理的保护。

创建一个 AWS 网络安全管理器管理员帐户

此步骤仅适用于多账户模式。只有组织的管理帐户才能创建 AWS 网络安全管理员帐户。

完成 Organizations 设置后，将您的帐户注册为 AWS Network Security Manager 管理员。您可以通过控制台或 AWS 命令行界面 (AWS CLI) 执行此操作。

当您创建管理员帐户时，AWS 网络安全管理器会自动在您组织中的所有帐户中创建一个服务相关角色。使用此角色，AWS 网络安全管理员可以发现资源并管理成员账户中的保护。

使用 AWS Network Security Manager，您可以有多个管理员来管理组织的防火墙资源。如果要在组织中使用多个管理员，则可以对每个管理员应用管理范围条件来定义他们可以管理的资源。这使您可以灵活地在组织中使用不同的管理员角色，并帮助您保持最低权限访问的原则。例如，一个管理员可以管理一组组织单位 (OU)。其他管理员只能管理特定的策略类型。

有关每个组织可以拥有的最大管理员人数，请参阅 [配额](#)。

地区注册

您在单个 AWS 区域中注册 AWS 网络安全管理员帐户。要在其他区域使用 AWS 网络安全管理器，请在每个区域重复此步骤。

使用控制台创建管理员帐户

1. 打开 AWS 网络安全管理器控制台，网址为<https://console.aws.amazon.com/network-security-manager/>。
2. 在导航窗格中，选择设置。
3. 选择添加管理员。
4. 选择账户并输入优先级值（1 到 10）。
5. 选择添加管理员进行确认。

要创建管理员帐户，请使用 AWS CLI

调用 PutAdminAccount 操作。您必须提供优先级值（1 到 10）。

以下 AWS CLI 示例将一个帐户注册为优先级 1 的 AWS 网络安全管理员管理员：

```
aws network-security-manager put-admin-account \  
  --account-id 123456789012 \  
  --priority 1
```

您可以指定多个管理员帐户，每个帐户的优先级不同。或者，您可以通过提供adminScope参数将每个管理员限制为特定的帐户、OU 或防火墙类型。

使用控制台删除管理员帐户

Multi-account 移除管理员时禁用保护

当您删除管理员帐户时，AWS Network Security Manager 会将多帐户范围和部署设置为DISABLED状态，并清理其管理的保护。

1. 打开 AWS 网络安全管理器控制台，网址为<https://console.aws.amazon.com/network-security-manager/>。
2. 在导航窗格中，选择设置。
3. 选择要删除的管理员帐户。
4. 选择删除管理员。
5. 要进行确认，请选择确认管理员删除。

使用创建 IAM 身份 AWS 网络安全管理员权限

要使用 AWS 网络安全管理器，您需要具有调用 AWS 网络安全管理器操作权限的 IAM 身份（用户或角色）。IAM 操作使用前缀 `network-security-manager`。

以下示例 IAM 策略包含三个语句。第一条语句授予对所有 AWS 网络安全管理器操作的完全访问权限。第二条语句授予 AWS 网络安全管理员所需的其 AWS 其他 Or AWS ganizations 和 WAF 权限。AWS Network Security Manager 使用这些权限来识别组织中的账户和组织单位 (OU)，并列出可用的 WAF 规则组和被管理产品。这些权限还允许 AWS Network Security Manager 启用可信访问权限并在 AWS 组织中注册委托管理员。第三条语句授予 AWS Network Security Manager 创建其服务相关角色所需的 `iam:CreateServiceLinkedRole` 权限，单账户和多账户使用都需要该权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "network-security-manager:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "wafv2:ListRuleGroups",
        "wafv2:ListAvailableManagedRuleGroups",
```

```
        "wafv2:DescribeAllManagedProducts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*"
    }
  ]
}
```

对于生产用途，我们建议您仅授予所需的最低权限。有关更多信息，请参阅 [the section called “Identity and access management”](#)。

注册获取 AWS 账户

要开始使用 AWS，你需要一个 AWS 账户。有关创建的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》AWS 账户中的[入门](#)指南。

使用 AWS 默认禁用的区域中的网络安全管理器

要在默认禁用的区域中使用 AWS 网络安全管理器，必须同时为组织的管理帐户和 AWS 网络安全管理员帐户启用该区域。有关默认情况下禁用的区域以及如何启用这些区域的信息，请参阅AWS 一般参考中的[管理 AWS 区域](#)。

启用或禁用区域

对于 Organizations 管理帐户和 AWS Network Security Manager 管理员帐户，请按照AWS 一般参考中的[启用区域](#)中的指导进行操作。

部署您的第一个网络安全防护

本教程将指导您使用 AWS 网络安全管理器控制台部署 AWS WAF Web ACL。您完成以下步骤：

1. 创建规则
2. 创建模板
3. 创建策略
4. 创建范围
5. 创建和发布部署
6. 监控同步状态

在本教程中，您将创建一个 AWS WAF Web ACL，用于保护所选账户中的应用程序负载均衡器。对于 AWS 网络安全管理器支持的所有安全服务和防火墙，此过程基本相同。

完成时间：大约 10 分钟

费用：本教程使用的 AWS 服务可能会产生费用。有关当前定价，请参阅 AWS 网站上的[AWS 网络安全管理器定价](#)。

先决条件

在开始之前，请确认您满足以下要求：

- 已完成安装步骤，如中所述[设置 AWS 网络安全管理器](#)。
- 具有网络安全管理员权限的 AWS 身份和访问管理 (IAM) Access Management AWS 身份。
- 一个启用了所有功能并具有指定的 AWS Network Security Manager 管理员帐户（多账户部署所必需的）的 Organizations AWS 组织。
- 访问 AWS 网络安全管理器控制台。

步骤 1：创建规则

规则是安全配置的基石。在此步骤中，您将创建两个 AWS WAF 规则：一个用于设置默认操作，另一个用于设置可见性配置。默认操作和 VisibilityConfig 是 AWS WAF Web ACL 的必填字段。

要创建默认操作规则，请执行以下步骤：

1. 打开 AWS 网络安全管理器控制台，网址为<https://console.aws.amazon.com/network-security-manager/>。
2. 在导航窗格中，选择概述。
3. 在概述页面上，选择创建规则。
4. 在规则名称中，输入描述性名称，例如my-default-action-rule。
5. 在“规则定义”部分中，对于防火墙类型，选择 AWS WAF。
6. 在“选择规则类型”中，选择“配置”。
7. 选择“插入配置类型”，然后选择“默认操作”。此时会出现一个带有默认配置的 JSON 编辑器。
8. 在 JSON 编辑器中，删除该Block分区并仅保留该Allow分区。
9. 选择 Create rule (创建规则) 。

要创建 VisibilityConfig 规则，请执行以下步骤：

1. 在导航窗格中，选择概述。
2. 在概述页面上，选择创建规则。
3. 在规则名称中，输入描述性名称，例如my-visibility-config-rule。
4. 在“规则定义”部分中，对于防火墙类型，选择 AWS WAF。
5. 在“选择规则类型”中，选择“配置”。
6. 选择“插入配置类型”，然后选择VisibilityConfig。此时会出现一个带有默认配置的 JSON 编辑器。
7. 选择 Create rule (创建规则) 。

AWS CLI 替代方案

您也可以使用 AWS CLI 创建规则：

```
aws network-security-manager create-rule \  
  --rule-name "my-default-action-rule" \  
  --firewall-type WAF \  
  --rule-type CONFIGURATION \  
  --configuration '{"DefaultAction": {"Allow": {}}}' \  
  --is-published true  
  
aws network-security-manager create-rule \  
  --rule-name "my-visibility-config-rule" \  
  --firewall-type WAF \  
  --rule-type VISIBILITY_CONFIG
```

```
--rule-type CONFIGURATION \  
--configuration '{"VisibilityConfig": {"SampledRequestsEnabled": true,  
"CloudWatchMetricsEnabled": true, "MetricName": "my-web-acl-metric"}}' \  
--is-published true
```

步骤 2：创建模板

模板对一条或多条规则进行分组，以便在策略之间重复使用。在此步骤中，您将创建一个包含步骤 1 中的规则的模板：

1. 在导航窗格中，选择概述。
2. 在概述页面上，选择创建模板。
3. 在模板名称中，输入描述性名称，例如 my-waf-template。
4. 对于防火墙类型，请选择 AWS WAF。
5. 在规则部分，选择添加规则，然后选择您在步骤 1 中创建的规则。
6. 选择创建模板。

AWS CLI 替代方案

您也可以使用 AWS CLI 创建模板：

```
aws network-security-manager create-template \  
--template-name "my-waf-template" \  
--firewall-type WAF \  
--associated-rule-list '["ruleIdentifier": "rule-arn-from-step-1"]' \  
--is-published true
```

步骤 3：创建策略

策略将模板与强制设置相结合。在此步骤中，您将创建一个引用您的模板并启用自动修复的策略：

1. 在导航窗格中，选择概述。
2. 在概述页面上，选择创建策略。
3. 对于策略名称，输入一个描述性名称，例如 my-waf-policy。

4. 对于防火墙类型，请选择 AWS WAF。
5. 在“策略优先级”部分中，将显示现有策略及其优先级。查看新政策的优先级。如果需要对其进行调整，请选择优先级字段并将该值更改为1或任何未使用的优先级数字。
6. 在模板和规则部分，选择添加模板，然后选择您在步骤 2 中创建的模板。
7. 对于“修复”，选择“启用”。
8. 对于现有客户 Web ACL 解析，请选择无补救。
9. 选择创建策略。

AWS CLI 替代方案

您也可以使用 AWS CLI 创建策略：

```
aws network-security-manager create-policy \  
  --policy-name "my-waf-policy" \  
  --firewall-type WAF \  
  --priority 1 \  
  --associated-template-and-rule-list '["templateIdentifier": "template-arn-  
from-step-2"]]' \  
  --policy-configuration '{"remediationEnabled": true, "resourcesCleanUp":  
false, "wafConfig": {"existingCustomerWebACLResolution": "NO_REMEDIATION"}}' \  
  --is-published true
```

步骤 4：创建作用域

范围定义了您的保护措施的范围。在此步骤中，您将创建一个以账户中的应用程序负载均衡器为目标的范围：

1. 在导航窗格中，选择概述。
2. 在“概述”页面上，选择“创建范围”。
3. 在“作用域名称”中，输入描述性名称，例如my-alb-scope。
4. (可选) 在“账户和组织单位选择”部分中，在“选择控制管理范围的方法”中，选择“范围至整个 AWS 组织 (所有 OU 和帐户)”。对于单账户部署，请跳过此步骤。
5. 在资源部分中，对于资源类型，选择 Application Load Balancer。
6. 选择 Create scope (创建范围)。

AWS CLI 替代方案

您也可以使用 AWS CLI 创建作用域：

```
aws network-security-manager create-scope \
--scope-name "my-alb-scope" \
--scope-configuration '{
    "accountFilter": {"includeAll": {}},
    "resourceScopes": {
        "AWS::ElasticLoadBalancingV2::LoadBalancer::application": {
            "includeAll": true
        }
    }
}' \
--is-published true
```

步骤 5：创建和发布部署

部署将策略绑定到范围并激活强制执行。要创建和发布部署，请执行以下操作：

1. 在导航窗格中，选择概述。
2. 在概述页面上，选择创建部署。
3. 在部署名称中，输入描述性名称，例如my-first-deployment。
4. 在策略部分，选择添加策略，然后选择您在步骤 3 中创建的策略。
5. 在“范围”部分中，选择“添加范围”，然后选择您在步骤 4 中创建的范围。
6. 选择创建部署。

AWS 网络安全管理器开始发现资源并应用保护。此过程是异步的，可能需要几分钟才能完成。

AWS CLI 替代方案

您还可以使用 AWS CLI 创建和发布部署：

```
aws network-security-manager create-deployment \
--deployment-name "my-first-deployment" \
--associated-policy-list '["policyIdentifier": "policy-arn-from-step-3"]]' \
```

```
--associated-scope-list '["scopeIdentifier": "scope-arn-from-step-4"]]' \
--deployment-configuration '{"enableCrossAccountVisibility": true}' \
--is-published true
```

步骤 6：监控同步状态

发布部署后，AWS 网络安全管理器会发现资源并同步其配置。要监控每种资源的状态，请执行以下操作：

1. 在导航窗格中，选择概述。
2. 选择部署选项卡。
3. 选择您在步骤 5 中创建的部署。
4. 选择“同步”选项卡。
5. 查看每种资源的同步状态：
 - IN_SYNC — 资源配置与您的预期保护设置相匹配。
 - OUT_OF_SYNC — 资源配置不匹配。AWS 启用修复后，网络安全管理器会自动修复此问题。
 - NOT_APPLICABLE — 资源在范围内，但无法通过此部署进行评估。

AWS CLI 替代方案

您还可以使用 AWS CLI 检查同步状态：

```
aws network-security-manager list-resource-synchronization-statuses \
--deployment-identifier "deployment-arn-from-step-5"
```

步骤 7：清除

如果您不再需要您创建的资源，请按相反的顺序将其删除，以停止强制执行并移除对范围内资源的保护：

反向顺序很重要，因为这些资源相互引用。要在删除资源之前查看与其关联的内容，请致电 `ListResourceAssociations` 该资源的 ARN。它返回每个关联资源的 ARN 和资源类型。有关更多信息，请参阅 [AWS 网络安全管理器 API 参考](#)。

1. 在导航窗格中，选择概述。选择部署选项卡。选择您的部署，选择操作，然后选择删除。
2. 选择“范围”选项卡。选择您的范围，选择操作，然后选择删除。
3. 选择策略选项卡。选择您的策略，选择操作，然后选择删除。
4. 选择 Templates 选项卡。选择您的模板，选择操作，然后选择删除。
5. 选择规则选项卡。选择您的规则，选择操作，然后选择删除。

AWS CLI 替代方案

在删除资源之前，请检查其关联以计划删除顺序：

```
aws network-security-manager list-resource-associations \  
  --resource-arn "resource-arn"
```

如果资源仍有关联，请先移除或删除关联的资源。

您可以使用 AWS CLI 按相反顺序删除资源：

```
aws network-security-manager delete-deployment \  
  --deployment-identifier "deployment-arn"  
  
aws network-security-manager delete-scope \  
  --scope-identifier "scope-arn"  
  
aws network-security-manager delete-policy \  
  --policy-identifier "policy-arn"  
  
aws network-security-manager delete-template \  
  --template-identifier "template-arn"  
  
aws network-security-manager delete-rule \  
  --rule-identifier "rule-arn"
```

后续步骤

现在您已经有了有效的部署，请探索以下方法来扩展您的网络安全保护：

- 在中了解资源模型和生命周期 [AWS 网络安全管理器的工作原理](#)。

- 使用 draft/publish 工作流程在更改生效之前对其进行暂存。有关更多信息，请参阅 [the section called “草稿和活跃生命周期”](#)。
- 创建快照以保留已知良好的配置。有关更多信息，请参阅 [the section called “版本控制”](#)。
- 用于GenerateRuleConfiguration根据自然语言描述创建规则。有关更多信息，请参阅[AWS 网络安全管理器 API 参考](#)。
- 探索在整个组织中管理 AWS WAF 和 AWS Shield 高级保护。有关更多信息，请参阅 [管理防火墙和安全服务](#)。

管理防火墙和安全服务

使用 AWS 网络安全管理器，您可以为多个防火墙和安全服务定义和部署安全策略。尽管 AWS 网络安全产品组合中有一些常见元素，但需要在 AWS 网络安全管理器中解决一些重要的差异。

对于每种支持的网络安全服务，以下小节描述了快速创建和标准详细创建过程的独特元素和步骤。

管理以下项的 Web ACL AWS WAF

使用 AWS 网络安全管理器，您可以跨组织中的账户和资源集中配置和部署 AWS WAF Web 访问控制列表 (Web ACL)。您可以为 AWS WAF 定义 AWS 网络安全管理器规则，将它们分组到保护模板中，然后通过 AWS 网络安全管理器策略和部署大规模实施这些规则。

AWS WAF 的概念

以下概念特定于将 AWS 网络安全管理器与 AWS WAF 配合使用。有关 AWS 网络安全管理器工作原理的更多信息，请参阅 [AWS 网络安全管理器的工作原理](#)。

AWS WAF 规则类型

对于 AWS WAF，规则是以下两种类型之一：

- 检查-包含使用 `PreProcessFirewallManagerRuleGroups` (在客户定义的规则之前运行的规则) 或 `PostProcessFirewallManagerRuleGroups` (之后运行的规则) 的规则组定义。
- 配置-包含单个 Web ACL 配置设置。配置 JSON 必须包含一个与支持的设置 (例如、`DefaultAction`、`VisibilityConfig`、`LoggingConfiguration` 或 `MonetizationConfig`) 匹配的顶级密钥。

大多数 Web ACL 配置设置与 AWS WAF `CreateWebACL` 操作的参数相对应。有关这些设置及其定义的更多信息，请参阅 AWS WAF API 参考中的 [CreateWebACL](#)。

唯一的例外是 `LoggingConfiguration`，您可以单独配置。有关更多信息，请参阅 [the section called “日志记录”](#)。

AWS WAF 策略合并

对于 AWS WAF，每个配置设置都使用以下合并策略之一：

SingleValue

只能有一个值的设置。优先级最高的策略获胜。优先级值是唯一的，因此两个策略不能在相同的优先级下定义不同的值。有关 AWS 网络安全管理器如何解析优先级的更多信息，请参阅[the section called “Priority-based 策略合并”](#)。以下设置使用 SingleValue : DefaultAction、VisibilityConfig、CaptchaConfig、ChallengeConfig、OnS 和Description。

附加 (和 AppendAndSort)

所有策略中的条目按优先顺序附加到列表中。

TokenDomains并DataProtectionConfig.DataProtections使用追加。

PreProcessFirewallManagerRuleGroups和

PostProcessFirewallManagerRuleGroups use AppendAndSort，它会从所有策略中追加规则组并按优先级对它们进行排序。顺序很重要，因为 AWS WAF 会按顺序评估规则组。

合并

无论优先级如何，来自所有策略的条目都合并为一个集合。CustomResponseBodies然后AssociationConfig.RequestBody使用“合并”。

追加 AppendAndSort、和合并策略会移除重复的条目。当两个策略提供相同的配置时，AWS 网络安全管理器会保留优先级较高的策略中的条目。因此，有效配置包含该条目的一个副本，而不是每个贡献策略的一个副本。

现有 Web ACL 分辨率

使用 AWS WAF 策略的existingCustomerWebACLResolution设置来指定 AWS 网络安全管理器如何处理已有客户管理的 Web ACL 的资源：

- RETROFIT— 更新现有的 Web ACL 以使其与有效配置保持一致。
- OVERRIDE_ASSOCIATION— 改为将 AWS 网络安全管理器管理的 Web ACL 与资源相关联。
- NO_REMEDIATION— 如果您的 Web ACL 存在，请不要进行修复。

记录 Web ACL 流量

您可以使用策略上的LoggingConfiguration设置来控制 Web ACL 日志记录。AWS 网络安全管理器使用 AWS WAF PutLoggingConfiguration 操作应用此设置。您可以为每个 Web ACL 定义一个日志记录目标。有关更多信息，请参阅 AWS WAF API 参考[PutLoggingConfiguration](#)中的。

策略管理的每个范围内 Web ACL 都会将其日志发送到策略指定的目标。这使您可以集中记录组织中的帐户。使用它来获取有关您的 Web ACL 在组织范围内分析的流量的详细信息。

要实现跨多个账户的集中日志记录，您可以将日志发送到 Amazon S3 存储桶或 Amazon Data Firehose 传输流。每种目标类型都需要额外的配置，您必须先完成这些配置，然后 AWS 网络安全管理器才能在您的范围内资源和账户中管理 AWS WAF 日志记录。目标名称必须以开头 `aws-waf-logs-`。

Amazon Data Firehose

创建具有以下特征的传送流：

- 使用您的 AWS 网络安全管理员帐户创建
- 例如，一个以开头 `aws-waf-logs-` 的名字 `aws-waf-logs-network-security-manager-central`
- 一个 PUT 消息来源
- 在您运营的地区创建，或者如果您为 Amazon 捕获日志，则在美国东部（弗吉尼亚北部）地区创建 CloudFront

在使用传输流之前，请对其进行测试，以确认其吞吐量是否足以容纳组织的日志。有关更多信息，请参阅 [《亚马逊数据 Firehose 开发者指南》中的创建亚马逊数据 Firehose 传输流](#)。

Amazon S3

按照 AWS WAF 开发者指南中的 Amazon S3 指南创建存储桶。您还必须为存储桶配置允许日志传输向其写入的权限。以下存储桶策略授予这些权限。

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryForNetworkSecurityManager",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheckNetworkSecurityManager",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-bucket-suffix"
    },
    {
```

```

        "Sid": "AWSLogDeliveryWriteNetworkSecurityManager",
        "Effect": "Allow",
        "Principal": {
            "Service": "delivery.logs.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3::aws-waf-logs-bucket-suffix/policy-id/AWSLogs/
    *",
        "Condition": {
            "StringEquals": {
                "s3:x-amz-acl": "bucket-owner-full-control"
            }
        }
    }
}
]
}

```

bucket-suffix 替换为您自己的存储桶名称后缀，并 *policy-id* 替换为您的策略的 ID。

CloudWatch 日志仅支持单账号使用

如果您在多个账户中使用 AWS 网络安全管理器，则不能使用 Amazon Log CloudWatch s 日志组作为日志目标。日志组必须与 Web ACL 位于同一个 AWS 账户和相同区域。对于多账户部署，请改用 Amazon S3 存储桶或 Amazon Data Firehose 传输流。

快速创建 AWS WAF

借助 Quick Create，您可以在单个指导式工作流程中定义和部署 AWS WAF 保护。如果要在一个会话中设置从规则到部署的完整 Web ACL 保护，请使用 Quick Create。

要使用 Quick Create 定义和部署 AWS WAF 保护，请按顺序完成以下步骤。

创建策略并添加保护

1. 打开 AWS 网络安全管理器控制台，网址为 <https://console.aws.amazon.com/network-security-manager/>。
2. 在导航窗格中，选择概述。
3. 在“概述”页面的右上角，选择“快速创建和部署”。“快速创建和部署”页面将显示多个窗格。

4. 在策略详细信息窗格中，为名称输入策略名称。（可选）对于描述，输入描述。
5. 在“定义保护”窗格中，选择要使用的防火墙类型。选择 AWS WAF。将出现“模板和规则”子窗格，您可以在其中添加规则或模板。
6. 要添加规则，请选择添加或管理规则。在出现的窗口中，对于“选择规则类型”，选择以下选项之一：
 - AWS 托管规则-该表显示了 AWS WAF 支持的所有 AWS 托管规则。
 - 规则-该表显示了您拥有的 AWS WAF 规则组（AWS 托管规则除外）。选中要添加到策略中的规则对应的复选框。然后选择添加规则。
7. 要添加模板，请选择添加模板。在出现的“添加模板”窗口中，该表格显示了所有可用的模板。选择所需的模板以及要包含在策略中的版本。然后选择“添加模板”。

配置策略

1. 在“模板和规则”表格中查看您的选择。位置列中的整数决定了规则和模板的评估顺序。要更改评估顺序，请在“位置”列中选择位置值。使用箭头更改值。要接受更改，请选择确认。要恢复更改，请选择“取消”。
2. 在“定义保护”窗格的“策略配置”下，决定 AWS 网络安全管理器在目标范围内自动执行的操作：
 - 修复会将定义的策略应用于其安全状态与 AWS 网络安全管理器中描述的所需状态不同步的所有资源。
 - 资源清理会在删除部署或帐户或资源超出范围时删除 AWS Network Security Manager 为该资源创建的防火墙。
 - 现有客户 WebACL 解决方案决定了如何解决您正在定义的策略与可能已部署的策略之间的冲突。从菜单中选择以下选项之一：
 - 任何补救措施都不会跳过对任何已有 Web ACL 的资源的修复。
 - 覆盖关联将现有的 Web ACL 替换为 AWS 网络安全管理员创建的 Web ACL。
 - Retrofit 将其规则改造到每个现有的 Web ACL 上，并保持 Web ACL 与资源相关联。
3. 在策略优先级窗格中，设置优先级。AWS 网络安全管理器根据策略的优先级评估策略以解决冲突。位置越低（整数越低）的优先级越高。要编辑优先级，请选择位置值。然后用箭头将其递增，或者直接输入一个值。要确认选择，请选择确认。要放弃更改，请选择“取消”。

要设置范围

1. 在设置范围窗格中，定义策略适用的资产集。在范围名称中，输入一个名称。（可选）对于描述，输入描述。

2.

 Multi-account 仅限模式

此步骤仅适用于多账户模式。在多账户模式下，使用账户和组织单位选择子窗格来选择要包含或排除哪些账户或组织单位。在单账户模式下，此子窗格不会出现在控制台中，因此请跳过此步骤。

在账户和组织单位选择子窗格中，选择以下选项之一：

- 范围涵盖整个 AWS 组织。无需进一步定义。
 - 范围涵盖整个 AWS 组织，但不包括特定的 OU 和账户。将出现“组织单位”子窗格和“帐户”子窗格。要排除组织单位，请选择添加 OU。在组织树中选择组织单位，然后选择添加 OU。要排除个人账户，请选择添加账户。在组织树中选择帐户，然后选择添加帐户。
 - 不要将范围扩大到整个 AWS 组织，而只包括特定的 OU 和账户。使用相同的“添加 OU”和“添加帐户”机制来包含所需的组织单位和帐户。
3. 在资源子窗格中，对于资源类型，选择所有或特定的 AWS WAF 资源类型。这些选项是以下一个或多个选项：
- 应用程序负载均衡器
 - 亚马逊 API Gateway REST API
 - CloudFront 分配

 CloudFront 区域要求

要保护 CloudFront 分销资源，请使用美国东部（弗吉尼亚北部）区域 (us-east-1)。

 全球和区域资源类型

您可以选择全球资源类型（CloudFront 分配）或区域资源类型（Application Load Balancer 和 Amazon API Gateway REST API），但不能同时选择两者。选择资源类型后，更新配置时无法在 CloudFront 分发资源类型和区域资源类型之间切换。

非托管资源 CloudFront

AWS Network Security Manager 不管理使用 CloudFront 统一费率定价计划或 CloudFront 分期分配的 CloudFront 分配。这些资源显示为不同步。

4. 对于每种选定的资源类型，请选择以下互斥选项之一：

- 包含所有资源
- 包括特定资源
- 排除特定资源

5. 如果您选择“包括特定资源”，请选择以下表达式类型之一，然后构建适当的标签或 ARN 组合：

- 单一标准
- 匹配所有条件 (AND)
- 匹配任何标准 (OR)
- 不是

所有资源类型都有标签和 ARN 包含标准。如果选择“标签”，请输入密钥和可选值。您可以识别多个标签。如果您的资源类型是 Application Load Balancer，则会显示其他配置标准。在“配置”中，选择一个方案，其中包含选项 Internet-facing 或“内部”。

查看和部署策略

1. 在查看和部署窗格中，在部署名称中输入名称。（可选）对于描述，输入描述。要确定您的部署内容是否对组织中的其他账户可见，请选择为此部署启用跨账户可见性。
2. （可选）要向资源添加标签，请选择添加新标签，然后输入密钥和可选值组合。
3. 要运行您定义的内容，请选择创建并部署。该过程完成后，将出现“部署”页面，您可以在其中查看已创建内容的详细信息。

部署可能会产生费用

部署创建网络安全服务并将其附加到受保护的资源。AWS 网络安全管理器对受保护的资源收费。安全服务本身会保护资源，这会产生额外费用。在部署之前，请查看[AWS 网络安全管理器定价页面](#)和[AWS WAF 定价页面](#)。

的标准创建流程 AWS WAF

使用标准创建流程，您可以单独创建每个 AWS WAF 组件（规则、模板、策略、范围和部署），以实现完全控制。如果要创建可重复使用的组件并根据需要组合它们，请使用此方法。

AWS 网络安全管理器 AWS WAF 策略可以包含规则和模板。当您应用策略时，AWS 网络安全管理器会在每个范围内帐户中创建一个 Web ACL。

创建规则（控制台）

1. 使用您的 AWS 网络安全管理员帐户登录 AWS 管理控制台，然后打开 AWS 网络安全管理器控制台，网址为 <https://console.aws.amazon.com/network-security-manager/>。

管理员账户设置

有关设置 AWS 网络安全管理员帐户的信息，请参阅 [设置 AWS 网络安全管理器](#)。

2. 在导航窗格中，选择 AWS 网络安全管理器，然后选择概述。
3. 在概述窗格中，选择创建规则。输入描述性名称，然后输入可选的描述。
4. 在规则定义窗格中，对于防火墙类型，选择 AWS WAF。
5. 对于规则类型，选择检查或配置。

如果您选择“检查”，则会出现一个名为“定义规则组引用”的 JSON 编辑器窗格，其中包含以下选项：

- 插入模板-为第一个（预处理）规则或最后一个（后处理）规则选择 JSON 模板。当您做出选择时，AWS 网络安全管理器会将相应的 JSON 以及警告图标插入编辑器中（如果需要输入才能完成模板）。
- 插入规则组-显示由三个选项驱动的选择列表：
 - AWS 托管规则 (AMR) 规则组
 - 现有的自定义规则组
 - M AWS marketplace 规则组

AWS Network Security Manager 会显示与您的选择关联的规则组，您可以选择一个要包含的实例。做出选择后，选择选择规则组。AWS 网络安全管理器使用正确的语法将对检查规则的引用插入到 JSON 编辑器中。

- 使用 AI 插入-打开名为 AI 配置生成器的叠加窗口。使用此工具用通俗易懂的语言描述您的规则，AWS 网络安全管理器会在编辑器中生成关联的 JSON。然后，您可以查看生成的代码并选择接受、修改或删除输出。
6. (可选) 完成 JSON 规则定义后，您可以将标签与规则相关联。选择 Add new tag (添加新标签)，然后输入 Key (键) 和可选 Value (值)。
 7. 完成定义后，选择“保存草稿”以保存非活动的、可能不完整的对象，或者选择“创建规则”。

Web ACL 名称是永久性的

创建 Web ACL 名称后，您就无法对其进行更改。如果您更新策略的名称，AWS 网络安全管理器不会更新关联的 Web ACL 名称。要让 AWS Network Security Manager 创建具有不同名称的 Web ACL，必须创建一个新策略。

创建模板 (控制台)

模板按优先级顺序汇编规则，以便在策略中进行评估。您可以将规则类型组织成与您的安全目标一致的分组。您还可以让不同的团队制定与其职责和技能相一致的安全控制声明。

1. 在概述页面的概述窗格中，选择创建模板。在创建模板页面上，输入模板名称，输入可选描述，然后选择防火墙类型 (在本例中为 AWS WAF)。
2. 选择防火墙类型后，将出现“规则”窗格。选择两个“添加规则”按钮之一，打开可用规则列表。选中规则名称左侧的复选框将其添加到模板中。要选择规则的特定版本，请选择该规则的“版本”字段。如果有多个版本可用，请选择所需的版本，然后选择“确认”。
3. (可选) 为模板创建标签。完成后，选择“保存草稿”或“创建模板”。要继续创建策略，请选择创建模板。

创建策略 (控制台)

这是策略定义和部署准备的最后一步。

1. 在概述页面的概述窗格中，选择创建策略。在创建策略页面上，输入名称和可选描述，然后选择防火墙类型 (在本例中为 AWS WAF)。
2. 在策略优先级窗格中，设置优先级。AWS 网络安全管理器根据策略的优先级评估策略以解决冲突。位置越低 (整数越低) 的优先级越高。要编辑优先级，请选择位置值。然后用箭头将其递增，或者直接输入一个值。要确认选择，请选择确认。要放弃更改，请选择“取消”。

3. 在策略配置窗格中，决定 AWS 网络安全管理器在目标范围内执行的自动操作：

- 修复会将定义的策略应用于安全状态与 AWS 网络安全管理器中描述的所需状态不同步的所有资源。
- 资源清理会在删除部署或帐户或资源超出范围时删除 AWS Network Security Manager 为该资源创建的防火墙。
- 现有客户 WebACL 解决方案决定了如何解决您正在定义的策略与可能已部署的策略之间的冲突。从菜单中选择以下选项之一：
 - 任何补救措施都不会跳过对任何已有 Web ACL 的资源的修复。
 - 覆盖关联将现有的 Web ACL 替换为 AWS 网络安全管理员创建的 Web ACL。
 - Retrofit 将其规则改造到每个现有的 Web ACL 上，并保持 Web ACL 与资源相关联。

4. 完成这些配置设置后，选择要添加到策略中的规则和模板。在模板和规则窗格中，选择添加规则或添加模板以填充策略。这两个进程都会打开一个窗口，其操作方式与本节前面描述的规则选择过程相同。

创建作用域（控制台）

1. 您可以从“概述”页面或工具内的其他区域开始此步骤。在范围详细信息窗格中，输入范围名称和可选的描述。

2.

Multi-account 仅限模式

此步骤仅适用于多账户模式。在多账户模式下，使用账户和组织单位选择子窗格来选择要包含或排除哪些账户或组织单位。在单账户模式下，此子窗格不会出现在控制台中，因此请跳过此步骤。

在账户和组织单位选择窗格中，选择控制管理范围的三种方法之一：

- 范围涵盖整个 AWS 组织（所有 OU 和账户）— 无需进一步定义。
- 范围涵盖整个 AWS 组织，但不包括特定的 OU 和帐户 — 出现两个子窗格，一个用于组织部门，一个用于帐户。选择“添加 OU”打开“添加 OU”窗口，从组织树中选择所需的组织单位，然后选择“添加 OU”。要添加个人帐户，请在“帐户”子窗格中选择“添加帐户”，从组织树中选择帐户，然后选择“添加帐户”。
- 不要将范围扩大到整个 AWS 组织，只包括特定的 OU 和账户 — 使用相同的子窗格来添加 OU 或帐户，其机制与上述选项中描述的机制相同。

3. 接下来，在“资源”子窗格中选择资源。在资源类型选择框中，选择所有或特定的 AWS WAF 资源类型。对于 AWS WAF，选项包括以下任意或全部：

- 应用程序负载均衡器
- 亚马逊 API Gateway REST API
- CloudFront 分配

CloudFront 区域要求

要保护 CloudFront 分销资源，请使用美国东部（弗吉尼亚北部）区域 (us-east-1)。

全球和区域资源类型

您可以选择全球资源类型（CloudFront 分配）或区域资源类型（Application Load Balancer 和 Amazon API Gateway REST API），但不能同时选择两者。选择资源类型后，更新配置时无法在 CloudFront 分发资源类型和区域资源类型之间切换。

非托管资源 CloudFront

AWS Network Security Manager 不管理使用 CloudFront 统一费率定价计划或 CloudFront 分期分配的 CloudFront 分配。这些资源显示为不同步。

4. 对于每种选定的资源类型，请选择以下互斥选项之一：

- 包含所有资源
- 包括特定资源
- 排除特定资源

5. 如果选择“包括特定资源”，请选择以下表达式类型之一：

- 单一标准
- 匹配所有条件 (AND)
- 匹配任何标准 (OR)
- 不是

6. 每种表达式类型都支持单个或多个包含条件和 ARN，因此您可以构建标签或 ARN 的组合。所有资源类型都支持标签和 ARN 包含标准。如果选择“标签”，请标识密钥和可选值。您可以识别多个标签。

7. 对于 Application Load Balancer，会出现一个额外的配置标准。在“配置”中，您可以使用选项 Internet-facing 或内部来设置架构。

创建部署（控制台）

部署会将您的策略绑定到范围并激活强制执行，从而使 AWS 网络安全管理器将您的 AWS WAF 规则应用于范围内的资源。

1. 在概述页面的概述窗格中，选择创建部署。您也可以从工具中的其他区域开始此步骤。
2. 选择要部署的策略。
3. 选择定义 AWS 网络安全管理器应用策略的账户和资源的范围。
4. 在部署名称中，输入一个名称。（可选）对于描述，输入描述。
5. （可选）要使该部署对组织中的其他账户可见，请选择为此部署启用跨账户可见性。
6. （可选）要添加标签，请选择添加新标签，然后输入密钥和可选值组合。
7. 选择创建和部署。将出现“部署”页面，您可以在其中查看 AWS 网络安全管理器创建内容的详细信息。

部署可能会产生费用

部署创建网络安全服务并将其附加到受保护的资源。AWS 网络安全管理器对受保护的资源收费。安全服务本身会保护资源，这会产生额外费用。部署之前，请查看[AWS 网络安全管理器定价页面](#)和[AWS WAF 定价页面](#)。

管理 DDoS 保护 AWS Shield Advanced

使用 AWS Network Security Manager，您可以跨组织中的账户和资源集中配置和部署 AWS Shield 高级保护。您可以定义 DDoS 保护策略，并通过 AWS 网络安全管理器策略和部署大规模实施这些策略。

AWS 网络安全管理器单独计费

AWS 网络安全管理器不是 AWS Shield Advanced 优惠的一部分。有关定价的更多信息，请参阅[AWS 网络安全管理器定价](#)和[AWS Shield Advanced 定价](#)。

AWS Shield 高级订阅

当活动部署的范围内包含一个账户时，AWS 网络安全管理器会将该账户订阅到 AWS Shield Advanced。AWS 当帐户离开作用域或您删除部署时，网络安全管理器不会取消订阅。要取消 AWS Shield Advanced 订阅，请参阅 [AWS WAF 开发者指南中的订阅 AWS Shield Advanced](#)。

快速创建 AWS Shield Advanced

使用 Quick Create，您可以在单个指导式工作流程中定义和部署 AWS Shield 高级保护。如果要在一个会话中设置从策略到部署的 DDoS 防护，请使用 Quick Create。

要使用快速创建定义和部署 AWS Shield 高级保护，请按顺序完成以下步骤。

创建策略和配置保护

完成以下步骤：

1. 打开 AWS 网络安全管理器控制台，网址为 <https://console.aws.amazon.com/network-security-manager/>。
2. 在导航窗格中，选择概述。
3. 在概述页面上，选择快速创建和部署。“快速创建和部署”页面将显示多个窗格。
4. 在策略详细信息窗格中，为名称输入策略名称。（可选）对于描述，输入描述。
5. 在“定义保护”窗格中，选择要使用的防火墙类型。选择 AWS Shield 高级版。
6. 在“定义保护”窗格的“策略配置”下，决定 AWS 网络安全管理器在目标范围内自动执行的操作：
 - 修复会将定义的策略应用于安全状态与 AWS 网络安全管理器描述的所需状态不匹配的任何资源。
 - 资源清理会在部署被移除或账户或资源超出范围时删除 AWS 网络安全管理器为该资源创建的 DDoS 保护。
 - 现有的客户 DDoS 解决方案决定了如何解决您正在定义的策略与可能已部署的策略之间的冲突。从菜单中选择以下选项之一：
 - 任何补救措施都不会跳过对任何已有 DDoS 保护的资源的修复。
 - 覆盖关联将现有的 DDoS 保护替换为 AWS 网络安全管理员创建的 DDoS 保护。
 - Retrofit 将其规则改造到每种现有 DDoS 保护上，并保持 DDoS 保护与资源相关联。

- 在策略优先级窗格中，设置优先级。AWS 网络安全管理器根据策略的优先级评估策略以解决冲突。位置越低（整数越低）的优先级越高。

要编辑优先级，请选择位置值。然后用箭头将其递增，或者直接输入一个值。要确认选择，请选择确认。要放弃更改，请选择“取消”。

要设置范围

完成以下步骤：

- 在“设置范围”窗格中，定义策略适用的资产集。在“作用域名称”中，输入一个名称。（可选）对于描述，输入描述。

2.

Multi-account 仅限模式

此步骤仅适用于多账户模式。在多账户模式下，使用账户和组织单位选择子窗格来选择要包含或排除哪些账户或组织单位。在单账户模式下，此子窗格不会出现在控制台中，因此请跳过此步骤。

在账户和组织单位选择子窗格中，选择以下选项之一：

- 范围涵盖整个 AWS 组织。无需进一步定义。
 - 范围涵盖整个 AWS 组织，但不包括特定的 OU 和账户。将出现“组织单位”子窗格和“帐户”子窗格。要排除组织单位，请选择添加 OU。在组织树中选择组织单位，然后选择添加 OU。要排除个人账户，请选择添加账户。在组织树中选择帐户，然后选择添加帐户。
 - 不要将范围扩大到整个 AWS 组织，而只包括特定的 OU 和账户。使用相同的“添加 OU”和“添加帐户”机制来包含所需的组织单位和帐户。
- 在资源子窗格中，对于资源类型，选择所有或特定的 AWS Shield Advanced 资源类型。这些选项是以下一个或多个选项：
 - 应用程序负载均衡器
 - CloudFront 分配
 - 经典负载均衡器
 - 弹性 IP 地址
 - 对于每种选定的资源类型，请选择以下互斥选项之一：
 - 包含所有资源

- 包括特定资源
- 排除特定资源

5. 如果您选择“包括特定资源”，请选择以下表达式类型之一，然后构建适当的标签或 ARN 组合：

- 单一标准
- 匹配所有条件 (AND)
- 匹配任何标准 (OR)
- 不是

所有资源类型都有标签和 ARN 包含标准。如果选择“标签”，请输入密钥和可选值。您可以识别多个标签。

CloudFront 区域要求

要保护 CloudFront 分销资源，请使用美国东部（弗吉尼亚北部）区域 (us-east-1)。

查看和部署策略

完成以下步骤：

1. 在查看和部署窗格中，在部署名称中输入名称。（可选）对于描述，输入描述。要确定您的部署内容是否对组织中的其他账户可见，请选择为此部署启用跨账户可见性。
2. （可选）要向资源添加标签，请选择添加新标签，然后输入密钥和可选值组合。
3. 要创建和部署策略和范围，请选择创建并部署。该过程完成后，将出现“部署”页面，您可以在其中查看 AWS 网络安全管理器创建内容的详细信息。

部署可能会产生费用

部署创建网络安全服务并将其附加到受保护的资源。AWS 网络安全管理器对受保护的资源收费。安全服务本身会保护资源，这会产生额外费用。在部署之前，请查看[AWS 网络安全管理器定价页面](#)和 [AWS Shield Advanced 定价页面](#)。

的标准创建流程 AWS Shield Advanced

通过标准创建流程，您可以单独设置每个 AWS Shield Advanced 组件（策略、范围和部署），以实现完全控制。如果要创建可重复使用的组件并根据需要组合它们，请使用此方法。

AWS Shield Advanced 策略很简单，不包含规则、规则组或模板。当你应用该策略时，AWS 网络安全管理器会在每个范围内账户中创建 AWS Shield Advanced DDoS 防护。有关 AWS 网络安全管理器工作原理的信息，请参阅 [AWS 网络安全管理器的工作原理](#)。

创建 策略（控制台）

完成以下步骤：

1. 使用您的 AWS 网络安全管理员帐户登录 AWS 管理控制台，然后打开 AWS 网络安全管理器控制台，网址为 <https://console.aws.amazon.com/network-security-manager/>。

管理员账户设置

有关设置 AWS 网络安全管理器管理员帐户的信息，请参阅 [设置 AWS 网络安全管理器](#)。

2. 在导航窗格中，选择 AWS 网络安全管理器，然后选择概述。
3. 在概述窗格中，选择创建策略。输入名称和可选描述，然后选择防火墙类型（在本例中为 AWS Shield Advanced）。
4. 在策略优先级窗格中，设置优先级。AWS 网络安全管理器根据策略的优先级评估策略以解决冲突。位置越低（整数越低）的优先级越高。

要编辑优先级，请选择位置值。然后用箭头将其递增，或者直接输入一个值。要确认选择，请选择确认。要放弃更改，请选择“取消”。

5. 在策略配置窗格中，决定 AWS 网络安全管理器在目标范围内执行的自动操作：
 - 修复会将定义的策略应用于安全状态与 AWS 网络安全管理器描述的所需状态不匹配的任何资源。
 - 资源清理会在部署被移除或账户或资源超出范围时删除 AWS 网络安全管理器为该资源创建的 DDoS 保护。
 - 现有的客户 DDoS 解决方案决定了如何解决您正在定义的策略与可能已部署的策略之间的冲突。从菜单中选择以下选项之一：
 - 任何补救措施都不会跳过对任何已有 DDoS 保护的资源的修复。
 - 覆盖关联将现有的 DDoS 保护替换为 AWS 网络安全管理员创建的 DDoS 保护。

- Retrofit 将其规则改造到每种现有 DDoS 保护上，并保持 DDoS 保护与资源相关联。

创建作用域（控制台）

完成以下步骤：

1. 在范围详细信息窗格中，输入范围名称和可选的描述。

2.  Multi-account 仅限模式

此步骤仅适用于多账户模式。在多账户模式下，使用账户和组织单位选择子窗格来选择要包含或排除哪些账户或组织单位。在单账户模式下，此子窗格不会出现在控制台中，因此请跳过此步骤。

在账户和组织单位选择窗格中，选择控制管理范围的三种方法之一：

- 范围涵盖整个 AWS 组织（所有 OU 和账户）— 无需进一步定义。
 - 范围涵盖整个 AWS 组织，但不包括特定的 OU 和帐户 — 出现两个子窗格，一个用于组织部门，一个用于帐户。选择“添加 OU”打开“添加 OU”窗口，选择所需的组织单位，然后选择“添加 OU”。要添加个人账户，请在帐户子窗格中选择添加账户，选择帐户，然后选择添加账户。
 - 不要将范围扩大到整个 AWS 组织，只包括特定的 OU 和帐户 — 使用相同的子窗格来添加 OU 或帐户。
3. 接下来，在“资源”子窗格中选择资源。在资源类型选择框中，选择所有或特定的 AWS Shield 高级资源类型。对于 AWS Shield Advanced，选项为以下任意或全部：
 - 应用程序负载均衡器
 - CloudFront 分配
 - 经典负载均衡器
 - 弹性 IP 地址
 4. 对于每种选定的资源类型，请选择以下互斥选项之一：
 - 包含所有资源
 - 包括特定资源
 - 排除特定资源
 5. 如果选择“包括特定资源”，请选择以下表达式类型之一：
 - 单一标准

- 匹配所有条件 (AND)
 - 匹配任何标准 (OR)
 - 不是
6. 每种表达式类型都支持单个或多个包含条件和 ARN，因此您可以构建标签或 ARN 的组合。所有资源类型都支持标签和 ARN 包含标准。如果选择“标签”，请标识密钥和可选值。您可以识别多个标签。

CloudFront 区域要求

要保护 CloudFront 分销资源，请使用美国东部（弗吉尼亚北部）区域 (us-east-1)。

创建部署（控制台）

部署会将您的策略绑定到范围并激活强制执行。AWS 然后，网络安全管理器会将您的 AWS Shield Advanced DDoS 保护应用于范围内的资源。

完成以下步骤：

1. 在概述页面的概述窗格中，选择创建部署。
2. 选择要部署的策略。
3. 选择定义 AWS 网络安全管理器应用策略的账户和资源的范围。
4. 在部署名称中，输入一个名称。（可选）对于描述，输入描述。
5. （可选）要使该部署对组织中的其他账户可见，请选择为此部署启用跨账户可见性。
6. （可选）要添加标签，请选择添加新标签，然后输入密钥和可选值组合。
7. 选择创建和部署。将出现“部署”页面，您可以在其中查看 AWS 网络安全管理器创建内容的详细信息。

部署可能会产生费用

部署创建网络安全服务并将其附加到受保护的资源。AWS 网络安全管理器对受保护的资源收费。安全服务本身会保护资源，这会产生额外费用。在部署之前，请查看[AWS 网络安全管理器定价页面](#)和 [AWS Shield Advanced 定价页面](#)。

AWS 网络安全管理器和 AWS Firewall Manager

AWS 网络安全管理器是取代 Fi AWS rewall Manager 的服务。两者是完全独立的服务，每种服务都具有独特的功能和不同的定价模式。如果您当前使用 Fire AWS wall Manager，则无需采取任何操作，因为您现有的防火墙和策略可以继续使用。本章介绍这两个服务是如何共存的，当你同时使用这两个服务时，优先级是如何运作的，以及迁移在可用时将如何运作。

AWS Network Security Manager 和 Fi AWS rewall Manager 并肩运行，相互独立。在某个时候，Fi AWS rewall Manager 将停止出售，然后停止运行。

与共存 AWS Firewall Manager

AWS 除非您启动更改防火墙的操作，否则网络安全管理器不会对您使用 Firewal AWS I Manager 创建的防火墙。除非您将其终止，否则使用 Firewal AWS I Manager 创建的防火墙和策略将继续运行。即使在 Fi AWS rewall Manager 停用后也是如此。

修复期间的优先级

当这两项服务都运行时，您可以采取影响使用 Firewal AWS I Manager 创建的防火墙的操作。在创建 AWS Network Security Manager 策略时，可以将其应用于一个范围，即一组目标资源。如果该范围包括 Fi AWS rewall Manager 策略已经处理的资源，则 AWS 网络安全管理器在修复期间优先考虑。在这种情况下，AWS 网络安全管理器的策略和范围将覆盖现有的 Firewal AWS I Manager 防火墙和策略。具体行为取决于您选择的分辨率选项。

计划迁移自 AWS Firewall Manager

从 Firew AWS all Manager 迁移到 AWS Network Security Manager 可以将您的防火墙管理整合到一项服务中，并允许您使用其功能。已计划迁移，但尚未可用。当迁移可用时，您可以将 Fi AWS rewall Manager 策略移至 AWS 网络安全管理器。迁移需要在这两个服务中执行尚未到位的新操作。

计划的过程将从 Fi AWS rewall Manager 中复制选定的策略，将其传输到 AWS 网络安全管理器，然后将其转换为新的策略结构。此过程不会影响您的原始策略或其在 Firewal AWS I Manager 中的关联防火墙。

中的安全性 AWS 网络安全经理

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。[责任共担模型](#)将此描述为云的安全性与云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。AWS 还为您提供可以安全使用的服务。Third-party 作为[AWS 合规计划合规计划合规计划](#)的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Network Security Manager 的合规性计划，请参阅[AWS 按合规计划划分的范围内AWS](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您的要求以及适用的法律法规。

本文档可帮助您了解在使用 AWS 网络安全管理器时如何应用分担责任模型。以下主题向您介绍如何配置 AWS 网络安全管理器以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS 网络安全管理器资源。

主题

- [中的数据保护 AWS 网络安全经理](#)
- [的身份和访问管理 AWS 网络安全经理](#)
- [将服务相关角色用于 AWS 网络安全经理](#)
- [的合规性验证 AWS 网络安全经理](#)
- [韧性在 AWS 网络安全经理](#)
- [中的基础设施安全 AWS 网络安全经理](#)
- [以下方面的安全最佳实践 AWS 网络安全经理](#)

中的数据保护 AWS 网络安全经理

[责任 AWS 共担模型](#)适用于 AWS 网络安全管理器中的数据保护。如本模型所述 AWS，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题解答AWS](#)条款。有关欧洲数据保护的信息，请参阅[通用数据保护条例 \(GDPR\) 中心](#)。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的[使用跟 CloudTrail 踪](#)。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-3 版》<https://aws.amazon.com/compliance/fips/>。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括 AWS 服务使用控制台、API 或 AWS SDK 与 AWS 网络安全管理器或其他人合作时。AWS CLI 在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

AWS 网络安全管理器使用密 AWS 钥管理服务 (AWS KMS) 密钥加密所有静态数据。Service-managed KMS 密钥可保护您的资源配置、部署状态和同步数据。您无需配置或管理这些密钥。

传输中加密

AWS 网络安全管理器使用传输层安全 (TLS) 对传输中的所有数据进行加密。所有 API 请求都需要 TLS 1.2 或更高版本。与 AWS 网络安全管理器 API 端点的连接仅使用 HTTPS。

密钥管理

AWS 网络安全管理器使用服务管理的 AWS KMS 密钥进行静态加密。您目前无法提供自己的 KMS 密钥。

的身份和访问管理 AWS 网络安全经理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS 网络安全管理器资源。您可以使用 IAM AWS 服务，无需支付额外费用。

主题

- [受众](#)
- [使用身份进行身份验证](#)
- [使用策略管理访问](#)
- [操作方法 AWS 网络安全管理器可与 IAM 配合使用](#)
- [Identity-based 的策略示例 AWS 网络安全经理](#)
- [问题排查 AWS 网络安全管理器身份和访问权限](#)

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅[问题排查 AWS 网络安全管理器身份和访问权限](#)）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅[操作方法 AWS 网络安全管理器可与 IAM 配合使用](#)）
- IAM 管理员：编写用于管理访问权限的策略（请参阅[Identity-based 的策略示例 AWS 网络安全经理](#)）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的[如何登录您的 AWS 账户](#)。

对于编程访问，AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的[适用于 API 请求的 AWS 签名版本 4](#)。

AWS 账户 根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的[需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。AWS IAM Identity Center 有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的[什么是 IAM Identity Center？](#)。

IAM 用户和群组

[IAM 用户](#)是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南[中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问](#)。

[IAM 组](#)指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的[IAM 用户使用案例](#)。

IAM 角色

[IAM 角色](#)是具有特定权限的身份，可提供临时凭证。您可以通过[从用户切换到 IAM 角色（控制台）](#)或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的[担任角色的方法](#)。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的[JSON 策略概述](#)。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的[在托管策略与内联策略之间进行选择](#)。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中[指定主体](#)。

Resource-based 策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《IAM 用户指南》中的[IAM 实体的权限边界](#)。
- 服务控制策略（SCP）– 指定 AWS Organizations 中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的[服务控制策略](#)。
- 资源控制策略（RCP）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的[资源控制策略（RCP）](#)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

操作方法 AWS 网络安全管理器可与 IAM 配合使用

在使用 IAM 管理 AWS 网络安全管理器的访问权限之前，请先了解 AWS 网络安全管理器可以使用哪些 IAM 功能。

IAM 功能	AWS 网络安全管理器支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	是
策略条件键	是
ACL	否
ABAC (策略中的标签)	是
临时凭证	是
主体权限	是
服务角色	是
Service-linked 角色	是

要全面了解 AWS 网络安全管理器和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM [配合使用的AWS 服务](#)。

Identity-based 的政策 AWS 网络安全经理

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

Resource-based 内部的策略 AWS 网络安全经理

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

AWS 网络安全管理器不支持基于资源的策略。

的政策行动 AWS 网络安全经理

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 AWS 网络安全管理器操作列表，请参阅《服务授权参考》中的[AWS 网络安全管理器定义的操作](#)。

AWS 网络安全管理器中的策略操作在操作前使用以下前缀：

```
network-security-manager
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
```

```
"network-security-manager:action1",  
"network-security-manager:action2"  
]
```

AWS 网络安全管理器跨其资源类型定义 IAM 操作。其中包括规则、模板、策略、作用域和部署的创建、读取、更新和删除 (CRUD) 操作，以及快照、标记、管理、同步状态和资源关联操作。

的政策资源 AWS 网络安全经理

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*" 
```

要查看 AWS 网络安全管理器资源类型及其 ARN 的列表，请参阅《服务授权参考》中的“[AWS 网络安全管理器定义的资源](#)”。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅[AWS 网络安全管理员定义的操作](#)。

AWS Network Security Manager 为其每种资源（规则、模板、策略、范围和部署）定义一个 IAM 资源类型，并为每个资源定义一个快照类型（例如 rule-snapshot）。ARN 格式为：

```
arn:aws:network-security-manager:{region}:{account}:{resource-type}:{resource-id}
```

草稿 ARN 会附加:DRAFT，快照 ARN 会附加版本号（例如）。:3

草稿不是单独的 IAM 资源类型。为了获得授权，草稿被视为其活动资源（即父资源）的子资源。:DRAFT 符合条件的 ARN 对活跃资源进行授权，因此对草稿采取行动的权限来自于对该活动资源执行操作的许可。

快照与草稿不同。每个快照都有自己的 IAM 资源类型，因此版本限定的 ARN 会直接针对该快照资源类型进行授权，而不是针对父活跃资源进行授权。

的策略条件键 AWS 网络安全经理

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

要查看 AWS 网络安全管理器条件密钥列表，请参阅《服务授权参考》中的[AWS 网络安全管理器条件密钥](#)。要了解可以使用条件键的操作和资源，请参阅[AWS 网络安全管理器定义的操作](#)。

AWS 网络安全管理器支持基于属性的访问控制 (ABAC) 的以下 AWS 全局标签条件密钥：

- `aws:ResourceTag/${TagKey}`
- `aws:RequestTag/${TagKey}`
- `aws:TagKeys`

Tag-based 条件键适用于活动资源和快照。草稿资源不可标记，也不支持 `aws:ResourceTag` 条件。

输入的 ACL AWS 网络安全经理

支持 ACL：否

访问控制列表 (ACL) 控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

AWS 网络安全管理器不支持访问控制列表 (ACL)。

ABAC with AWS 网络安全经理

支持 ABAC（策略中的标签）：是

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的[条件元素](#)中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的[使用 ABAC 授权定义权限](#)。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的[使用基于属性的访问权限控制 \(ABAC \)](#)。

AWS Network Security Manager 支持使用所有三个 AWS 全局标签条件键进行基于属性的访问控制。您可以根据附加到 AWS 网络安全管理器资源的标签来限制对这些资源的访问。

将临时证书与 AWS 网络安全经理

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的[IAM 中的临时安全凭证](#)和[使用 IAM 的 AWS 服务](#)

Cross-service 的委托人权限 AWS 网络安全经理

支持转发访问会话 (FAS)：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

的服务角色 AWS 网络安全经理

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 [IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的[创建向 AWS 服务委派权限的角色](#)。

Warning

更改服务角色的权限可能会中断 AWS 网络安全管理器的功能。只有在 AWS 网络安全管理器提供指导时才编辑服务角色。

Service-linked 的角色 AWS 网络安全经理

支持服务关联角色：是

服务相关角色是一种链接到的服务角色。AWS 服务该服务可以代替您执行操作。Service-linked 角色出现在您的，AWS 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

AWS 网络安全管理员使用服务相关角色在贵组织的成员帐户中进行操作。AWS 当您启用服务时，网络安全管理器会自动创建服务相关角色。该角色授予 AWS 网络安全管理员管理 AWS WAF 和 AWS Shield 高级资源的权限。该角色还授予访问 AWS Config 以进行资源发现和执行跨账户操作的权限。

有关创建和管理 AWS 网络安全管理器服务相关角色的详细信息，请参阅[the section called “Service-linked 角色”](#)。

Identity-based 的策略示例 AWS 网络安全经理

默认情况下，用户和角色无权创建或修改 AWS 网络安全管理器资源。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM 策略（控制台）](#)。

有关 N AWS etwork Security Manager 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的[“AWS 网络安全管理器的操作、资源和条件密钥”](#)。

主题

- [策略最佳实践](#)
- [使用 AWS 网络安全管理器控制台](#)
- [允许用户查看他们自己的权限](#)
- [Read-only 访问 AWS 网络安全经理](#)
- [仅管理规则和模板](#)

策略最佳实践

Identity-based 策略决定是否有人可以在您的帐户中创建、访问或删除 AWS 网络安全管理器资源。这些操作可能会使 AWS 帐户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的 AWS 托管策略。它们在你的版本中可用 AWS 帐户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的[AWS 托管策略](#)或[工作职能的 AWS 托管策略](#)。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的[IAM 中的策略和权限](#)。

- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [使用 IAM Access Analyzer 验证策略](#)。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 [使用 MFA 保护 API 访问](#)。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

使用 AWS 网络安全管理器控制台

要访问 AWS 网络安全管理器控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 AWS 网络安全管理器资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

要访问 AWS 网络安全管理器控制台，委托人需要拥有 `network-security-manager:List*` 和 `network-security-manager:Get*` 操作的最低权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
```

```

        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

Read-only 访问 AWS 网络安全经理

以下策略授予委托人对所有 AWS 网络安全管理器资源的只读访问权限。这对于需要在不进行更改的情况下查看配置和同步状态的审计员或监视角色非常有用。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "network-security-manager:Get*",
                "network-security-manager:List*"
            ],
            "Resource": "*"
        }
    ]
}

```

仅管理规则和模板

以下策略允许委托人创建、更新和删除规则和模板，而无需授予对策略、范围或部署的访问权限。这对于编写安全配置但不控制强制执行的团队很有用。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "network-security-manager:CreateRule",
        "network-security-manager:GetRule",
        "network-security-manager:UpdateRule",
        "network-security-manager>DeleteRule",
        "network-security-manager:ListRules",
        "network-security-manager:CreateRuleSnapshot",
        "network-security-manager:ListRuleSnapshots",
        "network-security-manager:CreateTemplate",
        "network-security-manager:GetTemplate",
        "network-security-manager:UpdateTemplate",
        "network-security-manager>DeleteTemplate",
        "network-security-manager:ListTemplates",
        "network-security-manager:CreateTemplateSnapshot",
        "network-security-manager:ListTemplateSnapshots",
        "network-security-manager:TagResource",
        "network-security-manager:UntagResource",
        "network-security-manager:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

问题排查 AWS 网络安全管理器身份和访问权限

使用以下信息来帮助您诊断和修复在使用 AWS 网络安全管理器和 IAM 时可能遇到的常见问题。

主题

- [我无权在以下位置执行操作 AWS 网络安全经理](#)
- [我无权执行 iam : PassRole](#)

- [我想允许我以外的人进入 AWS 账户 访问我的 AWS 网络安全管理器资源](#)

我无权在以下位置执行操作 AWS 网络安全经理

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 network-security-manager:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
network-security-manager:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 network-security-manager:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam : PassRole

如果您收到错误消息，说您无权执行该 iam:PassRole 操作，则必须更新您的策略以允许您将角色传递给 AWS 网络安全管理器。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户 marymajor 尝试使用控制台在 AWS Network Security Manager 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人进入 AWS 账户 访问我的 AWS 网络安全管理器资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 AWS 网络安全管理器是否支持这些功能，请参阅[操作方法 AWS 网络安全管理器可与 IAM 配合使用](#)。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户，请参阅[IAM 用户指南中的向您拥有 AWS 账户的另一个 IAM 用户提供访问权限](#)。
- 要了解如何向第三方提供对您的资源的访问[权限 AWS 账户](#)，请参阅[IAM 用户指南中的向第三方提供访问权限](#)。AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的[为经过外部身份验证的用户（身份联合验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的[IAM 中的跨账户资源访问](#)。

将服务相关角色用于 AWS 网络安全经理

AWS 网络安全管理器使用 IAM [服务相关角色](#)。服务相关角色是一种独特的 IAM 角色，直接链接到 AWS 网络安全管理器。Service-linked 角色由 AWS Network Security Manager 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

与服务相关的角色可以更轻松地设置 AWS 网络安全管理器，因为您不必手动添加必要的权限。AWS 网络安全管理器定义其服务相关角色的权限。除非另有定义，否则只有 AWS 网络安全管理员可以担任其角色。定义的权限包括信任策略和权限策略。您不能将该权限策略附加到任何其他 IAM 实体。

只有在首次删除相关资源后，才能删除服务相关角色。这样可以保护您的 AWS 网络安全管理器资源，因为您不能无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅与[IAM 配合使用的 AWS 服务](#)，并查找 Service-linked 角色列中包含“是”的服务。选择是链接以查看该服务的服务相关角色文档。

Service-linked 的角色权限 AWS 网络安全经理

AWS 网络安全管理器使用名为 `AWSServiceRoleForNetworkSecurityManager` 为的服务相关角色。此服务相关角色信任 `network-security-manager.amazonaws.com` 服务主体代入该角色。

名为的角色权限策略 `NetworkSecurityManagerServiceRolePolicy` 是一个 AWS 托管策略，允许 AWS 网络安全管理员完成对指定资源的操作。

以下信任策略允许 `network-security-manager.amazonaws.com` 服务主体担任该角色。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "network-security-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Note

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅 IAM 用户指南中的[Service-linked 角色权限](#)。

权限详细信息

AWS Network Security Manager 需要每组权限才能保护和发现您的账户和组织中的资源。NetworkSecurityManagerServiceRolePolicy 托管策略授予按服务分组的以下权限：

- **wafv2**— 创建、读取、更新和删除 Web ACL 和 Firewall Manager 规则组。将 Web ACL 与受保护的资源关联和解除关联。管理 Web ACL 日志记录配置和规则组权限策略。标记和取消标记资源。验证 AWS 网络安全管理器 Web ACL 和规则配置。
- **shield**— 创建、描述、列出和删除 AWS Shield 高级保护。创建并描述 AWS Shield 高级版订阅。
- **elasticloadbalancing**— 描述应用程序负载均衡器和标签。在应用程序负载均衡器上创建、删除和设置 Web ACL 关联。
- **cloudfront**— 获取并列出 Amazon 的 CloudFront 发行版、配置和标签。关联和取消关联分发 Web ACL。阅读 VPC 来源。
- **apigateway**— 阅读 Amazon API Gateway REST API、阶段和标签。在 API 阶段设置网页 ACL。
- **ec2**— 阅读 Amazon EC2 已验证访问实例 Web ACL 和关联。描述 Shi AWS eld 高级防护的弹性 IP 地址。
- **cognito-idp**、**apprunnerappsyncamplify**、和 **bedrock-agentcore** — 读取 Amazon Cognito 用户池、AWS App Runner 服务、GraphQL API、应用程序和 Amazon Bedrock

AgentCore 网关的 Web AC AWS AppSync L 关联 AWS Amplify ，以便 AWS 网络安全管理员可以发现受保护的资源。

- **config**— 选择资源配置并管理与服务相关的 AWS Config 配置记录器，AWS 网络安全管理器使用该记录器来发现范围内的资源。
- **organizations**— 读取您的组织、帐户、根目录、组织单位和委派的管理员，这样 AWS Network Security Manager 就可以在您的组织中运行。
- **logs**— 创建、读取、更新、删除和列出 Web ACL 日志记录的日志传送。
- **s3**— 在名称以开头的 Amazon S3 存储桶上获取并放置存储桶策略，aws-waf-logs-以便可以传送 Web ACL 日志。
- **iam**— 创建 AWS Shield Advanced 和 AWS WAF 所需的服务相关角色，其范围由条件键限制。
AWS Configiam:AWSServiceName

以下 JSON 显示了完整的NetworkSecurityManagerServiceRolePolicy权限策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LogsGeneral",
      "Effect": "Allow",
      "Action": [
        "logs:ListLogDeliveries",
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3LogBucketGeneral",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy"
      ],
      "Resource": "arn:aws:s3:::aws-waf-logs-*"
    },
    {
      "Sid": "CloudfrontVpcOriginAccess",
```

```

    "Effect": "Allow",
    "Action": [
        "cloudfront:GetVpcOrigin"
    ],
    "Resource": "arn:aws:cloudfront::*:vpcorigin/*"
},
{
    "Sid": "ConfigUnscoped",
    "Effect": "Allow",
    "Action": [
        "config:SelectResourceConfig"
    ],
    "Resource": "*"
},
{
    "Sid": "DescribeOrganizationUnScoped",
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListChildren",
        "organizations:ListRoots",
        "organizations:ListParents",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAWSServiceAccessForOrganization"
    ],
    "Resource": "*"
},
{
    "Sid": "DescribeAccountScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeAccount",
    "Resource": "arn:aws:organizations::*:account/o-*/*"
},
{
    "Sid": "DescribeOrganizationUnitScoped",
    "Effect": "Allow",
    "Action": "organizations:DescribeOrganizationalUnit",
    "Resource": "arn:aws:organizations::*:ou/o-*/ou-*"
},
{
    "Sid": "ListDelegatedAdministratorsScoped",
    "Effect": "Allow",
    "Action": "organizations:ListDelegatedAdministrators",

```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "network-security-manager.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "LoadBalancerNonMutationApiAccess",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeTags",
      "elasticloadbalancing:DescribeWebACLAssociation"
    ],
    "Resource": "*"
  },
  {
    "Sid": "LoadBalancerGetWebACLScoped",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:GetLoadBalancerWebACL",
    "Resource": "arn:aws:elasticloadbalancing:*:*:loadbalancer/app/*/*"
  },
  {
    "Sid": "CloudFrontDistributionNonMutationApiAccess",
    "Effect": "Allow",
    "Action": [
      "cloudfront:GetDistribution",
      "cloudfront:GetDistributionConfig",
      "cloudfront:ListTagsForResource"
    ],
    "Resource": "arn:aws:cloudfront:*:*:distribution/*"
  },
  {
    "Sid": "ApiGatewayStageNonMutationApiAccess",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
      "arn:aws:apigateway:*:*/restapis",
      "arn:aws:apigateway:*:*/restapis/*/stages",
      "arn:aws:apigateway:*:*/restapis/*/stages/*",
      "arn:aws:apigateway:*:*/tags/*"
    ]
  }

```

```

    ]
  },
  {
    "Sid": "Wafv2General",
    "Effect": "Allow",
    "Action": [
      "wafv2:TagResource",
      "wafv2:ListResourcesForWebACL",
      "wafv2:AssociateWebACL",
      "wafv2:ListTagsForResource",
      "wafv2:UntagResource",
      "wafv2:GetWebACL",
      "wafv2:DisassociateFirewallManager",
      "wafv2>DeleteWebACL",
      "wafv2:DisassociateWebACL",
      "wafv2:ValidateNetworkSecurityManagerWebACLConfiguration",
      "wafv2:ValidateNetworkSecurityManagerRuleConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
  },
  {
    "Sid": "Wafv2WebAclAndRuleGroupMutation",
    "Effect": "Allow",
    "Action": [
      "wafv2:UpdateWebACL",
      "wafv2:CreateWebACL",
      "wafv2>DeleteFirewallManagerRuleGroups",
      "wafv2:PutFirewallManagerRuleGroups"
    ],
    "Resource": [
      "arn:aws:wafv2:*:*:*/*webacl/*",
      "arn:aws:wafv2:*:*:*global/rulegroup/*",
      "arn:aws:wafv2:*:*:*regional/rulegroup/*",
      "arn:aws:wafv2:*:*:*global/managedruleset/*",
      "arn:aws:wafv2:*:*:*regional/managedruleset/*",
      "arn:aws:wafv2:*:*:*global/ipset/*",
      "arn:aws:wafv2:*:*:*regional/ipset/*",
      "arn:aws:wafv2:*:*:*global/regexpatternset/*",
      "arn:aws:wafv2:*:*:*regional/regexpatternset/*"
    ]
  },
  {
    "Sid": "Wafv2Logging",
    "Effect": "Allow",

```

```

    "Action": [
      "wafv2:PutLoggingConfiguration",
      "wafv2:GetLoggingConfiguration",
      "wafv2>DeleteLoggingConfiguration"
    ],
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
  },
  {
    "Sid": "Wafv2ListLogging",
    "Effect": "Allow",
    "Action": "wafv2:ListLoggingConfigurations",
    "Resource": "*"
  },
  {
    "Sid": "Wafv2ListWebACLs",
    "Effect": "Allow",
    "Action": "wafv2:ListWebACLs",
    "Resource": "*"
  },
  {
    "Sid": "Wafv2PermissionPolicy",
    "Effect": "Allow",
    "Action": [
      "wafv2:PutPermissionPolicy",
      "wafv2:GetPermissionPolicy",
      "wafv2>DeletePermissionPolicy"
    ],
    "Resource": [
      "arn:aws:wafv2:*:*:global/rulegroup/*",
      "arn:aws:wafv2:*:*:regional/rulegroup/*"
    ]
  },
  {
    "Sid": "Wafv2WebaclDescribe",
    "Effect": "Allow",
    "Action": "wafv2:GetWebACLForResource",
    "Resource": "arn:aws:wafv2:*:*:*/*webacl/*"
  },
  {
    "Sid": "CloudFrontListDistributions",
    "Effect": "Allow",
    "Action": [
      "cloudfront:ListDistributionsByWebACLId",
      "cloudfront:ListDistributions"
    ]
  }

```

```

    ],
    "Resource": "*"
  },
  {
    "Sid": "CloudFrontDistributionMutation",
    "Effect": "Allow",
    "Action": [
      "cloudfront:AssociateDistributionWebACL",
      "cloudfront:DisassociateDistributionWebACL"
    ],
    "Resource": "arn:aws:cloudfront::*:distribution/*"
  },
  {
    "Sid": "ElbWebAclRemediationScoped",
    "Effect": "Allow",
    "Action": [
      "elasticloadbalancing:CreateWebACLAssociation",
      "elasticloadbalancing>DeleteWebACLAssociation"
    ],
    "Resource": "arn:aws:elasticloadbalancing::*:loadbalancer/app/*/*"
  },
  {
    "Sid": "ElbSetWebAcl",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:SetWebACL",
    "Resource": "*"
  },
  {
    "Sid": "ApiGatewayWebAclRemediation",
    "Effect": "Allow",
    "Action": "apigateway:SetWebACL",
    "Resource": "arn:aws:apigateway::*/restapis/*/stages/*"
  },
  {
    "Sid": "CognitoWebAclIntegration",
    "Effect": "Allow",
    "Action": [
      "cognito-idp:GetWebACLForResource",
      "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AppRunnerWebAclIntegration",

```

```

    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService",
        "apprunner:ListAssociatedServicesForWebAcl"
    ],
    "Resource": "*"
},
{
    "Sid": "VerifiedAccessWebAclIntegration",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl",
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": "*"
},
{
    "Sid": "AppSyncWebAclIntegration",
    "Effect": "Allow",
    "Action": [
        "appsync:GetWebACLForResource",
        "appsync:ListResourcesForWebACL"
    ],
    "Resource": "*"
},
{
    "Sid": "AmplifyWebAclIntegration",
    "Effect": "Allow",
    "Action": [
        "amplify:GetWebACLForResource",
        "amplify:ListResourcesForWebACL"
    ],
    "Resource": "*"
},
{
    "Sid": "ShieldGeneral",
    "Effect": "Allow",
    "Action": [
        "shield:CreateProtection",
        "shield:DeleteProtection",
        "shield:DescribeProtection",
        "shield:ListProtections",
        "shield:CreateSubscription",
        "shield:DescribeSubscription",

```

```

        "shield:GetSubscriptionState",
        "ec2:DescribeAddresses",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTags"
    ],
    "Resource": "*"
},
{
    "Sid": "ShieldSlrCreation",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/shield.amazonaws.com/*",
    "Condition": {
        "StringEquals": {
            "iam:AWSServiceName": "shield.amazonaws.com"
        }
    }
},
{
    "Sid": "AllowConfigRecorderList",
    "Effect": "Allow",
    "Action": "config:ListConfigurationRecorders",
    "Resource": "*"
},
{
    "Sid": "AllowPutServiceLinkedConfigRecorder",
    "Effect": "Allow",
    "Action": "config:PutServiceLinkedConfigurationRecorder",
    "Resource": "*"
},
{
    "Sid": "AllowConfigRecorderScopedAccess",
    "Effect": "Allow",
    "Action": [
        "config:DescribeConfigurationRecorders",
        "config:DescribeConfigurationRecorderStatus",
        "config:DeleteServiceLinkedConfigurationRecorder",
        "config:AssociateResourceTypes",
        "config:DisassociateResourceTypes"
    ],
    "Resource": "arn:aws:config:*:*:configuration-recorder/*"
},
{
    "Sid": "AllowCreateConfigServiceLinkedRole",

```

```

    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/config.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "config.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowListActionsForAgentCoreGateway",
    "Effect": "Allow",
    "Action": [
      "bedrock-agentcore:GatewayListResourcesForWebACL"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowGetActionForAgentCoreGateway",
    "Effect": "Allow",
    "Action": [
      "bedrock-agentcore:GatewayGetWebACLForResource"
    ],
    "Resource": "arn:aws:bedrock-agentcore::*:gateway/*"
  },
  {
    "Sid": "WafV2LoggingSlrCreation",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/wafv2.amazonaws.com/*",
    "Condition": {
      "StringEquals": {
        "iam:AWSServiceName": "wafv2.amazonaws.com"
      }
    }
  }
]
}

```

为 创建服务相关角色 AWS 网络安全经理

您无需手动创建服务关联角色。启用 AWS 网络安全管理器后，AWS 网络安全管理器会为您创建服务相关角色。无需手动执行任何步骤。

如果您删除了此服务相关角色，然后需要重新创建它，则 AWS 网络安全管理器会在您下次使用该服务时重新创建该角色。你不必采取任何行动。

有关更多信息，请参阅 IAM 用户指南 中的[创建服务相关角色](#)。

为 编辑服务相关角色 AWS 网络安全经理

您无法更改AWSServiceRoleForNetworkSecurityManager服务相关角色的权限。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。

有关更多信息，请参阅《IAM 用户指南》中的[编辑服务关联角色](#)。

删除 的服务相关角色 AWS 网络安全经理

如果您不再需要使用 AWS 网络安全管理器，我们建议您删除AWSServiceRoleForNetworkSecurityManager服务相关角色。

在删除服务相关角色之前，请清理 AWS 网络安全管理器管理的资源。禁用 AWS 网络安全管理器并移除策略和范围，这样您的账户中就不会保留 AWS 网络安全管理器管理的资源。然后，您可以手动删除该角色。

Note

如果您尝试删除资源时 AWS 网络安全管理员正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 手动删除服务关联角色

1. 使用 <https://console.aws.amazon.com/iam/> 打开 IAM 控制台。
2. 在导航窗格中，选择角色。
3. 在搜索框中输入AWSServiceRoleForNetworkSecurityManager，然后选择角色。
4. 选择删除。
5. 要确认删除，请输入角色名称，然后选择删除。

有关更多信息，请参阅《IAM 用户指南》中的[删除服务相关角色](#)。

支持的区域 AWS 网络安全管理器服务相关角色

AWS 网络安全管理器支持在所有提供 AWS 网络安全管理器的 AWS 区域中使用服务相关角色。

的合规性验证 AWS 网络安全经理

我们全新的 AWS 注册体验不是为受监管的工作负载而设计的。如果您正在使用我们的全新 AWS 注册体验，但又想 AWS 用于受监管的工作负载，则可以[注册 AWS（高级）](#)或[激活适合您 AWS 环境的高级功能](#)。

要了解是否属于特定合规计划的范围，请参阅AWS 服务“[按合规计划划分的范围](#)”，然后选择您感兴趣的合规计划。AWS 服务 有关一般信息，请参阅[AWS 合规计划AWS](#)。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的“[下载报告](#)”中的“[AWS Artifact](#)”。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅[AWS 安全文档](#)。

韧性在 AWS 网络安全经理

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。AWS 区域 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

除了 AWS 全球基础架构外，AWS Network Security Manager 还提供多项功能来帮助支持您的数据弹性和备份需求。

中的基础设施安全 AWS 网络安全经理

作为一项托管服务，AWS 网络安全管理器受 [Amazon Web Services：安全流程概述白皮书中描述的 AWS 全球网络安全](#)程序的保护。

您可以使用 AWS 已发布的 API 调用通过 AWS 网络访问网络安全管理器。客户端必须支持传输层安全性协议（TLS）1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保

密 (PFS) 的密码套件，例如 DHE (短暂的) 或 ECDHE (椭圆曲线短暂的 Diffie-Hellman)。Diffie-Hellman 大多数现代系统 (如 Java 7 及更高版本) 都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 生成临时安全凭证来对请求进行签名。

以下方面的安全最佳实践 AWS 网络安全经理

以下最佳实践可帮助您维护安全的 AWS 网络安全管理器配置。

预防性控制机制

- 使用 IAM 最低权限--仅授予每个用户或角色执行其 AWS 网络安全管理员任务所需的权限。尽可能使用 IAM 条件密钥限制对特定资源的访问。
- 使用服务相关角色- AWS 网络安全管理器使用服务相关角色代表您执行操作。这些角色具有预定义的权限，其范围仅限于所需的最低访问权限。
- 谨慎配置范围--定义仅针对需要保护的账户和资源类型的范围配置。范围过宽可能导致意外执法。

侦测性控制

- 启用 AWS CloudTrail 日志记录-- CloudTrail 记录所有 AWS 网络安全管理器 API 调用。查看这些日志，以审核谁对您的安全配置进行了更改以及何时进行了更改。
- 监控同步状态--定期检查部署的同步状态，以确定哪些资源与您的预期安全状况不同步。

监控 AWS 网络安全经理

监控 AWS 网络安全管理器可帮助您了解您的资源是否按预期受到保护。AWS 网络安全管理器提供以下监控功能：

- 同步状态 API--查询部署中各个资源的保护状态。
- AWS CloudTrail--记录所有 AWS Network Security Manager API 调用以进行审计、合规和操作故障排除。

监控同步状态

监控您的资源是否受到保护的主要方法是通过同步状态 API。AWS Network Security Manager 会评估每个范围内的资源，并记录其实际防火墙配置是否与预期配置相匹配。

同步状态操作

AWS 网络安全管理器提供两个用于查询同步状态的操作：

`ListResourceSynchronizationStatuses`

返回特定部署的每个资源的状态。需要 `deploymentIdentifier` 参数。（可选）筛选依据 `synchronizationStatus`（`IN_SYNC`、`OUT_OF_SYNC` 或 `NOT_APPLICABLE`）。

`ListAggregateResourceSynchronizationStatuses`

返回所有部署中每种资源的汇总状态。（可选）筛选依据 `synchronizationStatus`。此操作显示适用于每种资源的所有策略的组合结果。

这两个操作都支持使用 `maxResults`（1 到 100）和 `nextToken` 进行分页。

了解同步状态值

`IN_SYNC`

资源的实际防火墙配置与根据所有适用策略计算出的有效配置相匹配。

不同步

资源的实际配置与有效配置不同。该 `outOfSyncReasons` 字段提供每个设置的详细信息，显示预期值与实际值。

不适用

资源的账户和资源类型在范围内，但资源本身与范围过滤器不匹配（例如，标签过滤器将其排除在外）。无需任何操作。

如果某个资源根本没有出现在结果中，则该账户或资源类型不在部署范围内。检查您的范围配置。

了解评估时间戳

每个同步状态条目都包含两个时间戳：

- `evaluatedAt`-- AWS 网络安全管理员上次评估资源配置的时间。过时的`evaluatedAt`值表示尚未对最近的更改进行评估。
- `updatedAt`--同步状态记录本身上次更改的时间。如果早`updatedAt`于`evaluatedAt`，则状态自上次评估以来一直保持稳定。

Cross-account 能见度

当多个管理员保护同一个资源时，聚合同步状态的可见性取决于每个部署的`enableCrossAccountVisibility`设置。

- 如果涵盖某个资源的所有部署都启用了跨账户可见性，则任何管理员都可以看到完整的聚合状态和不同步的原因。
- 如果任何部署禁用了跨账户可见性，则其他管理员会看到`NOT_VISIBLE`标记而不是详细原因。这表示另一位管理员也在保护资源，但没有共享可见性。

诊断不同步的资源

当资源报告 `OUT_OF_SYNC` 时，该`outOfSyncReasons`字段会标识特定的配置差异。最重要的原因是：

- `missingFirewall`--资源未关联任何防火墙保护。
- `invalidFirewall`--存在防火墙，但其配置与预期不符。具体差异列在已分类的存储桶中。

如果已启用修复但无法修复资源，则该`remediationIssues`字段将提供有关如何手动解决问题的指导。`correctiveAction`修正是一种策略级别的设置，默认情况下处于关闭状态。有关更多信息，请参阅 [the section called “同步和修复”](#)。

具有不同配置的多个部署可以针对同一个资源。在这种情况下，每个部署的同步状态可以是 OUT_OF_SYNC，而聚合同步状态为 IN_SYNC。这是预期行为，而不是失败。合并过程中，优先级较高的策略的设置优先。因此，该资源与有效配置相匹配，尽管它与优先级较低的部署的配置不匹配。

日志记录 AWS 网络安全管理器 API 调用 AWS CloudTrail

AWS Network Security Manager 与一项服务集成，该服务提供用户、角色或 AWS 服务所采取的操作的记录。CloudTrail 将 AWS 网络安全管理器的所有 API 调用捕获为管理事件。捕获的呼叫包括来自 AWS 网络安全管理器控制台的调用和对 AWS 网络安全管理器 API 操作的编程调用。

如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 AWS 网络安全管理器的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。有关更多信息，请参阅 [AWS CloudTrail 《用户指南》](#)。

AWS 中的网络安全管理器信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 AWS Network Security Manager 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅[使用事件历史记录查看 CloudTrail 事件](#)。

要持续记录您的事件 AWS 账户，包括 AWS 网络安全管理器的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录来自 AWS 分区中所有区域的事件。它会将日志文件传送到您指定的 Amazon S3 存储桶。您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- [创建跟踪记录概述](#)
- [CloudTrail 支持的服务和集成](#)
- [配置 Amazon SNS 通知 CloudTrail](#)

所有 AWS 网络安全管理器操作都由记录 CloudTrail。公共行动包括以下内容：

- 为规则、模板、策略、范围和部署创建、读取、更新和删除 (CRUD) 操作
- 快照操作
- 标记操作
- 管理员账号操作

- 同步状态操作
- 资源关联操作
- 规则生成操作

每个活动条目都包含以下信息：

- 事件源：network-security-manager.amazonaws.com
- 事件名称，即 API 操作名称（例如，CreatePolicy或ListDeployments）
- 受影响的资源，由 ARN 和资源类型标识

Read-only 操作（例如GetPolicyListRules、和ListResourceSynchronizationStatuses）使用响应元素进行记录readOnly: true，但不包括响应元素。变异操作包括请求参数和响应元素。

Note

CloudTrail 编辑事件记录中的敏感字段。例如，在GenerateRuleConfiguration操作中 CloudTrail 对prompt参数进行密文。

示例：CreatePolicy 事件

以下示例显示了该CreatePolicy操作的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROEXAMPLEID:my-session",
    "arn": "arn:aws:sts::123456789012:assumed-role/AdminRole/my-session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEID",
        "arn": "arn:aws:iam::123456789012:role/AdminRole",
        "accountId": "123456789012",
        "userName": "AdminRole"
      }
    }
  },
```

```

        "attributes": {
            "creationDate": "2026-08-10T18:22:41Z",
            "mfaAuthenticated": "false"
        }
    },
    "eventTime": "2026-08-10T18:24:03Z",
    "eventSource": "network-security-manager.amazonaws.com",
    "eventName": "CreatePolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.44",
    "userAgent": "aws-cli/2.17.0 Python/3.12.4 Darwin/24.6.0",
    "requestParameters": {
        "clientToken": "550e8400-e29b-41d4-a716-446655440001",
        "policyName": "production-web-acl-policy",
        "firewallType": "WAF",
        "priority": 1,
        "associatedTemplateAndRuleList": [
            {
                "templateIdentifier": "arn:aws:network-security-manager:us-
east-1:123456789012:template:t1a2b3c4d5"
            }
        ],
        "policyConfiguration": {
            "remediationEnabled": true,
            "resourcesCleanUp": false,
            "wafConfig": {
                "existingCustomerWebACLResolution": "RETROFIT",
                "conflictResolution": "MERGE_WHERE_APPLICABLE"
            }
        },
        "isPublished": true
    },
    "responseElements": {
        "policyId": "p9z8y7x6w5v4u3t2",
        "policyArn": "arn:aws:network-security-manager:us-
east-1:123456789012:policy:p9z8y7x6w5v4u3t2",
        "policyName": "production-web-acl-policy",
        "status": "ACTIVE",
        "version": "1"
    },
    "requestID": "b1c2d3e4-5f67-4890-a1b2-c3d4e5f6a7b8",
    "eventID": "f0e1d2c3-b4a5-4968-8776-5a4b3c2d1e0f",
    "readOnly": false,

```

```
"resources": [  
  {  
    "accountId": "123456789012",  
    "type": "AWS::NetworkSecurityManager::Policy",  
    "ARN": "arn:aws:network-security-manager:us-  
east-1:123456789012:policy:p9z8y7x6w5v4u3t2"  
  }  
],  
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "123456789012",  
"eventCategory": "Management"  
}
```

AWS 网络安全管理器配额

您的 AWS 网络安全管理器 AWS 账户 具有以下默认配额。除非另有说明，否则每个配额均为每个账户、每个区域。

资源配额

下表列出了您在每个区域中每个账户可以创建的最大 AWS 网络安全管理器资源数量。

资源	默认配额	可调整
每个 账户的规则数	200	否
每个账户的模板数	100	否
每个账户的策略数	100	否
每个账户的范围	100	否
每个账户的部署量	100	否
每种资源的快照	10	否

资源构成配额

下表列出了 AWS 网络安全管理器资源在资源层次结构中如何相互引用的配额。

配额	值
每个模板的规则	1 到 50
每个 AWS WAF 策略的模板	1 到 2
按照 AWS WAF 策略组合的规则和模板	1 到 100
每个 AWS Shield Advanced 策略的模板或规则	0 (必须为空)

配额	值
每次部署的策略	1 到 2
每个部署的范围	1 (正好一个)

范围配置配额

下表列出了作用域配置表达式的配额。

配额	值
每个范围的资源类型范围	20
作用域表达式深度 (嵌套级别)	2
作用域表达式宽度 (每个级别的标准)	20

管理员账户配额

下表列出了 AWS 网络安全管理器管理员帐户优先级的配额。

配额	值
管理员优先级	1 到 10

API 分页配额

下表列出了 List 操作的分页限制。

配额	值
每页的最大结果数 (maxResults)	100
每页最少搜索结果 (maxResults)	1

配额可调性

前面各节中列出的配额是固定的，目前无法增加。

的文档历史记录 AWS 网络安全管理器开发者指南

下表描述了 AWS 网络安全管理器的文档版本。

变更	说明	日期
初始版本	《AWS 网络安全管理器开发者指南》的初始版本。	2026年8月1日

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。