AMS 加速概念和程序

AMS 加速用户指南

版本 October 3, 2025

AMS 加速用户指南: AMS 加速概念和程序

Table of Contents

什么是 AMS 加速？

欢迎使用亚马逊 Web Services 的 AMS Accelerate (AWS)。AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。无论您是刚刚开始涉足云端、想要扩大现有团队，还是需要长期运营解决方案，Accelerate 都能帮助您在云端实现运营目标。我们利用 AWS 服务 自动化、配置和运行手册库，为新环境和现有 AWS 环境提供 end-to-end操作解决方案。

Accelerate 服务利用一套原生 AWS 服务 和功能来提供一套全面的基础架构管理功能。在其中 AWS 服务，Accelerate创建和维护精心策划的监控控件、检测护栏、自动化和运行手册，以合规和安全的方式运营基础架构。

主题

AMS 作战计划

AWS Managed Services (AMS) 有两个运营计划可供选择：AMS Accelerate 和 AMS Advanced。运营计划提供一组特定的功能，并且具有不同的服务级别、技术能力、要求、价格和限制。我们的运营计划使您可以灵活地为每个 AWS 工作负载选择合适规模的运营能力。本节概述了与每个计划相关的功能和差异，以及与每个计划相关的责任、功能和好处，以便您可以了解哪种运营计划最适合您的客户。

有关两个运营计划的详细功能比较，请参阅 AWS Managed Services 功能。

AMS 加快运营计划

AMS Accelerate 是 AMS 运营计划，可帮助您对新环境或现有 AWS 环境进行 day-to-day基础设施管理。AMS Accelerate 提供运营服务，例如监控、事件管理和安全。AMS Accelerate 还为需要定期修补的 EC2基于 Amazon 的工作负载提供了可选的补丁插件。

使用 AMS Accelerate， AWS 账户 您可以决定希望 AMS Accelerate 运营哪个 AWS 区域、您希望 AMS Accelerate 运营的 AWS 区域、所需的附加组件以及所需的服务级别协议 (SLAs)。有关更多详细信息，请参阅使用 AMS Accelerate 运营计划和服务描述。

AMS 高级操作计划

AMS Advanced 提供全生命周期服务，用于配置、运行和支持您的基础架构。除了 AMS Accelerate 提供的运营服务外，AMS Advanced 还包括其他服务，例如着陆区管理、基础设施变更和配置、访问管理和端点安全。

AMS Advanced 会部署一个着陆区，您可以将 AWS 工作负载迁移到该着陆区并获得 AMS 运营服务。我们的托管多账户登录区域预先配置了基础设施，以促进身份验证、安全、联网和日志记录。

AMS Advanced 还包括变更和访问管理系统，该系统通过防止未经授权的访问或对您的 AWS 基础设施进行风险更改来保护您的工作负载。客户需要使用我们的变更管理系统创建变更申请 (RFC)，才能在您的 AMS Advanced 账户中实施大多数更改。您可以根据由我们的安全和运营团队预先审查的自动变更库进行创建 RFCs ，或者如果认为这些更改既安全又受到 AMS Advanced 支持，则可以申请手动更改，然后由我们的运营团队进行审查和实施。

使用 AMS 加速运营计划

AMS Accelerate 是 AMS 运营计划，可以运行支持工作负载的 AWS 基础设施。无论您的工作负载已在 AWS 账户中，还是计划迁移新工作负载，您都可以从 AMS Accelerate 运营服务（例如监控和警报、事件管理、安全管理和备份管理）中受益，而无需进行新的迁移、停机或更改使用 AWS 的方式。AMS Accelerate 还为需要定期修补的 EC2 基于工作负载提供了可选的补丁插件。

借助 AMS Accelerate，您可以自由地在本地或使用首选工具使用、配置和部署所有 AWS 服务。您可以继续使用现有的访问和变更机制，同时 AMS 始终如一地采用久经考验的实践，帮助您扩大团队规模、优化成本、提高安全性和效率并提高弹性。

虽然 AMS Accelerate 可以简化您的操作，但您仍需负责应用程序开发、部署、测试和调整以及管理。AMS Accelerate 仅会因事件、警报、补救措施和某些服务请求而对您的账户进行更改。AMS Accelerate 不会代表你在账户中配置资源。AMS Accelerate 为影响应用程序的基础设施问题提供故障排除帮助，但是 AMS Accelerate 不会在您不知情和未经您批准的情况下访问或验证您的应用程序配置。AMS Accelerate 服务和变更直接在 AWS 控制台中提供 APIs，因此，您可以继续利用现有账户 AWS 和可用的 AWS 市场解决方案。AMS Accelerate 不会修改 infrastructure-as-code模板中的代码（例如 CloudFormation 模板），但可以指导您的团队进行哪些更改以遵循最佳运营和安全实践。

AMS 关键术语

- AMS Advanced：AMS 高级文档的 “服务描述” 部分中描述的服务。参见服务说明。
- AMS 高级 AWS 账户：始终符合 AMS 高级入职要求中所有要求的账户。有关 AMS Advanced 权益、案例研究以及联系销售人员的信息，请参阅 AWS Managed Services。
- AMS 加速 AWS 账户：始终满足 AMS 加速入职要求中所有要求的账户。请参阅 AMS 加速入门。
- AWS Managed Services：AMS 和/或 AMS 加速。
- AWS Managed Services 账户：AMS 账户和/或 AMS Accelerate 账户。
- 关键建议： AWS 通过服务请求发布的建议，告知您必须采取行动来防范潜在的风险或资源中断或. AWS 服务如果您决定在指定日期之前不遵守关键建议，则您应对您的决定造成的任何损害承担全部责任。
- 客户请求的配置：以下文件中未标识的任何软件、服务或其他配置：
  - 加速：支持的配置或 AMS 加速；服务描述。
  - AMS 高级：支持的配置或 AMS 高级；服务描述。
- 事件沟通：AMS 通过在 AMS Accelerate 的 Support Center 和 AMS 控制台中创建的事件向您传达事件，或者您通过在 AMS Accelerate 的 AMS 控制台中创建的事件请求与 AMS 发生的事件。AMS Accelerate 控制台在控制面板上提供事件和服务请求摘要，并提供指向 Support Center 的链接以获取详细信息。
- 托管环境：由 AMS 运营的 AMS 高级账户和/或 AMS Accelerate 账户。

  对于 AMS Advanced，这些账户包括多账户着陆区 (MALZ) 和单账户着陆区 (SALZ) 账户。
- 账单开始日期： AWS 收到您在 AWS Managed Services 入职电子邮件中要求的信息后的下一个工作日。AWS Managed Services 入职电子邮件是指向您发送的电子邮件， AWS 用于收集在您的账户上激活 AWS Managed Services 所需的信息。

  对于您随后注册的账户，账单开始日期为 AWS Managed Services 为已注册账户发送 AWS Managed Services 激活通知后的第二天。AWS Managed Services 激活通知发生在以下情况下：

  1. 您授予对兼容 AWS 账户的访问权限并将其移交给 AWS Managed Services。
  2. AWS Managed Services 设计和建立 AWS 托管服务账户。
- 服务终止：您可以出于任何原因终止所有 AWS Managed Services 账户的 AWS Managed Services 账户的 AWS 托管服务，方法是通过服务请求提供至 AWS 少 30 天的通知。在服务终止日期，可以：

  1. AWS 将所有 AWS Managed Services 账户或指定的 AWS Managed Services 账户（如果适用）的控制权移交给您，或者

2. 双方删除 AWS 允许从所有 AWS Managed Services 账户或指定的 AWS Managed Services 账户进行访问的 AWS Identity and Access Management 角色（如果适用）。

- 服务终止日期：服务终止日期是必需的 30 天终止通知期结束后的日历月的最后一天。如果必要的终止通知期限在日历月的第20天之后，则服务终止日期为下一个日历月的最后一天。以下是终止日期的示例方案。
  - 如果终止通知是在4月12日提供的，则为期30天的通知将于5月12日结束。服务终止日期为5月31日。
  - 如果在4月29日发出终止通知，则为期30天的通知将于5月29日结束。服务终止日期为 6 月 30 日。
- 提供 AWS Manag AWS ed Services：从服务开始之日起，您可以访问和使用每个 AWS 托管服务账户的 AWS 托管服务。
- 终止指定的 AWS Managed Services 账户：您可以出于任何原因终止指定 AWS Managed Services 账户的 AWS 托管服务，方法是通过服务请求（“AMS 账户终止申请”） AWS 发出通知。

事件管理条款：

- 事件：您的 AMS 环境发生了变化。
- 警报：每当来自支持的事件 AWS 服务 超过阈值并触发警报时，系统就会创建警报并将通知发送到您的联系人列表。此外，还会在您的事件列表中创建事件。
- 事件：您的 AMS 环境或 AWS Managed Services 的计划外中断或性能降级，导致影响，如 AWS Managed Services 或您所报告的那样。
- 问题：一个或多个事件的共同根本原因。
- 事件解决或解决事件：
  - AMS 已将与该事件相关的所有不可用 AMS 服务或资源恢复到可用状态，或者
  - AMS 已确定不可用的堆栈或资源无法恢复到可用状态，或者
  - AMS 已启动经您授权的基础设施恢复。
- 事件响应时间：创建事件与 AMS 通过控制台、电子邮件、服务中心或电话提供初始响应之间的时间差。
- 事件解决时间：AMS 或您创建事件与事件解决时间之间的时间差。
- 事件优先级：AMS 或您如何将事件的优先级分为 “低”、“中” 或 “高”。
  - 低：您的 AMS 服务存在非严重问题。
  - 中：您的托管环境中的 AWS 服务可用，但未按预期运行（根据适用的服务描述）。

- 高：(1) AMS 控制台或托管环境 APIs 中的一个或多个 AMS 不可用；或 (2) 托管环境中的一个或多个 AMS 堆栈或资源不可用，且不可用会使您的应用程序无法执行其功能。

  AMS 可以根据上述指南对事件进行重新分类。
- 基础设施恢复：根据受影响堆栈的模板重新部署现有堆栈，并在无法解决事件时根据上次已知的还原点启动数据恢复，除非您另行指定。

基础设施条款：

- 托管生产环境：客户生产应用程序所在的客户帐户。
- 托管的非生产环境：仅包含非生产应用程序（例如用于开发和测试的应用程序）的客户帐户。
- AMS 堆栈：由 AMS 作为一个单元管理的一组或多个 AWS 资源。
- 不可变基础设施：Amazon A EC2 uto Scaling 组 (ASGs) 的典型基础设施维护模式，在这种模式中 AWS，每次部署都会替换更新的基础设施组件（在 AMI 中），而不是就地更新。不可变基础架构的优势在于，所有组件都保持同步状态，因为它们总是从同一个基础生成的。不可变性独立于任何用于构建 AMI 的工具或工作流程。
- 可变基础设施：一种典型的基础设施维护模型，适用于不是 Amazon A EC2 uto Scaling 组且包含单个实例或仅包含几个实例的堆栈。该模型最接近于传统的、基于硬件的系统部署，即在系统生命周期开始时部署系统，然后随着时间的推移将更新分层到该系统上。系统的任何更新都将单独应用于实例，并且可能由于应用程序或系统重启而导致系统停机（取决于堆栈配置）。
- 安全组：您的实例的虚拟防火墙，用于控制入站和出站流量。安全组在实例级别运行，而不是子网级别。因此，您的 VPC 子网中的每个实例都可以为其分配一组不同的安全组。
- 服务级别协议 (SLAs)：与您签订的 AMS 合同的一部分，其中定义了预期的服务级别。
- SLA 不可用和不可用：
  - 您提交的导致错误的 API 请求。
  - 您提交的控制台请求生成 5xx HTTP 响应（服务器无法执行请求）。
  - 如Service Health Dashboard所示，在 AMS 管理的基础设施中构成堆栈或资源的任何 AWS 服务产品都处于 “服务中断” 状态。
  - 在确定服务积分资格时，不考虑因AMS排除而直接或间接导致的不可用性。除非服务符合不可用标准，否则视为可用。
- 服务级别目标 (SLOs)：与您签订的 AMS 合同的一部分，其中定义了 AMS 服务的具体服务目标。

修补条款：

- 强制补丁：关键安全更新，用于解决可能危及您的环境或账户安全状态的问题。“关键安全更新” 是由 AMS 支持的操作系统的供应商评为 “严重” 的安全更新。
- 已发布补丁与已发布补丁：补丁通常按计划发布和发布。紧急补丁是在发现需要补丁时宣布的，通常不久之后，补丁就会发布。
- 补丁附加组件：针对 AMS 实例进行基于标签的修补，它利用 AWS Systems Manager (SSM) 功能，因此您可以使用基准和您配置的窗口标记实例并对这些实例进行修补。
- 补丁方法：
  - 就地修补：通过更改现有实例完成的修补。
  - AMI 替换补丁：通过更改现有 A EC2 uto Scaling 组启动配置的 AMI 参考参数来完成的修补。
- 补丁提供商（操作系统供应商、第三方）：补丁由应用程序的供应商或管理机构提供。
- 补丁类型：
  - 关键安全更新 (CSU)：被支持的操作系统的供应商评为 “严重” 的安全更新。
  - 重要更新 (IU)：被支持的操作系统的供应商评为 “重要” 的安全更新或评级为 “严重” 的非安全更新。
  - 其他更新 (OU)：供应商对不是 CSU 或 IU 的支持的操作系统的更新。
- 支持的补丁：AMS 支持操作系统级补丁。供应商发布升级是为了修复安全漏洞或其他错误或提高性能。有关当前支持的列表 OSs，请参阅 Supp ort 配置。

安全条款：

- Det@@ ective Contro ls：由 AMS 创建或启用的监控器组成的库，用于持续监督客户托管的环境和工作负载，以发现与安全、运营或客户控制不一致的配置，并通过通知所有者、主动修改或终止资源来采取行动。

服务请求条款：

- 服务请求：您请求采取行动，希望 AMS 代表您采取行动。
- 警报通知：AMS 在触发 AMS 警报时在您的服务请求列表页面上发布的通知。为您的账户配置的联系人也会通过配置的方法（例如电子邮件）收到通知。如果您的实例/资源上有联系人标签，并且已同意您的云服务交付经理 (CSDM) 接收基于标签的通知，则还会通知标签中的联系人信息（密钥值）以获取自动的 AMS 警报。
- 服务通知：AMS 发布到您的服务请求列表页面的通知。

其他术语：

- AWS Managed Services 接口：适用于 AMS：AWS Managed Services 高级控制台、AMS CM AP 支持 I 和 API。对于 AMS Accelerate： 支持 控制台和 支持 API。
- 客户满意度 (CSAT)：AMS CSAT 通过深入分析获得信息，包括每个案例或信件的案例信件评级（如果给出）、季度调查等。
- DevOps: DevOps 是一种开发方法，强烈倡导在所有步骤上实现自动化和监控。 DevOps 旨在通过在自动化基础上整合传统上独立的开发和运营功能，缩短开发周期，提高部署频率和更可靠的发布。当开发人员可以管理运营，运营为开发提供信息时，问题和问题就会更快地发现和解决，业务目标也更容易实现。
- ITIL：信息技术基础设施库（称为 ITIL）是一个 ITSM 框架，旨在标准化 IT 服务的生命周期。ITIL 分为五个阶段，涵盖了 IT 服务生命周期：服务策略、服务设计、服务过渡、服务运营和服务改进。
- IT 服务管理 (ITSM)：一套让 IT 服务与您的业务需求保持一致的实践。
- 托管监控服务 (MMS)：AMS 运营自己的监控系统，即托管监控服务 (MMS)，该系统使用 AWS 健康事件并汇总亚马逊数据 AWS 服务和其他数据，将通过 CloudWatch 亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题创建的任何警报通知AMS操作员（全天候在线）。
- 命名空间：在创建 IAM 策略或使用 Amazon 资源名称 (ARNs) 时，您可以使用命名空间来识别。AWS 服务 您可以使用命名空间来标识操作和资源。

服务描述

AMS Accelerate 是 AWS Managed Services 服务的一项运营计划，用于管理 AWS 基础设施的运营。

AWS Managed Services (AMS) AMS 加速运营计划功能

AMS Accelerate 提供以下功能：

- 事件管理：

  事件管理是 AMS 服务用来回应您报告的事件的流程。

  AMS Accelerate 会主动检测和响应事件，并协助您的团队解决问题。您可以使用 Support Center 全天候联系 AMS Accelerate 运营工程师，响应时间 SLAs 取决于您为账户选择的响应级别。 AWS
- Monitoring（监控）：

  监控是 AMS 服务用来跟踪您的资源的过程。

  注册 AMS Accelerate 的账户配置了 Amazon CloudWatch 事件和警报的基准部署，这些事件和警报已经过优化，可以降低噪音并识别可能即将发生的事件。收到警报后，AMS 团队使用自动补救措

施、人员和流程将资源恢复到健康状态，并在适当时与您的团队互动，以提供有关行为学习以及如何预防行为的见解。如果补救失败，AMS 将启动事件管理流程。您可以通过更新默认配置文件来更改基准。

- 安全性：

  安全管理是 AMS 服务用来保护您的资源的流程。AWS Managed Services 通过使用多种控制措施（包括 AWS Config 规则和亚马逊）来保护您的信息资产并帮助保持您的 AWS 基础设施的安全 GuardDuty。

  AMS Acceler AWS Config 规则 ate 维护着一个补救措施库，以确保您的所有账户都符合安全性和运营完整性的行业标准。 AWS Config 规则 持续跟踪您录制的资源之间的配置更改。如果更改违反了任何规则条件，AMS 会报告其调查结果，并允许您根据违规的严重程度自动或根据请求进行补救。AWS Config 规则 促进遵守互联网安全中心 (CIS)、美国国家标准与技术研究院 (NIST) 云安全框架 (CSF)、《健康保险便携性和责任法案》(HIPAA) 以及支付卡行业 (PCI) 数据安全标准 (DSS) 制定的标准。

  此外，AMS Accelerate 还利用 Amazon GuardDuty 来识别您的 AWS 环境中可能存在的未经授权或恶意的活动。 GuardDuty AMS 全天候监测调查结果。AMS 将与您合作，根据最佳实践建议了解调查结果和补救措施的影响。AMS 还支持 Amazon Macie 来保护您的敏感数据，例如个人健康信息 (PHI)、个人身份信息 (PII) 和财务数据。最后，AMS 会对托管账户中生成的所有 Amazon Route 53 Resolver 警报和屏蔽事件进行监控和分类，以进一步检查网络流量并增强其侦测能力。

- 补丁管理：

  补丁管理是 AMS 服务用来更新资源的流程。

  对于带有补丁附加组件的 AWS 账户，AWS Managed Services 会在您选择的维护时段内为支持的操作系统的亚马逊 EC2 实例应用并安装供应商更新。AMS 会在修补之前创建实例的快照，监控补丁安装情况，并将结果通知您。如果补丁失败，AMS 将调查失败并向您推荐修复问题的操作方案。或者，如果有请求，AMS 会将实例恢复为回滚状态。AMS 会提供补丁合规覆盖范围的报告，并向您建议适合您业务的行动方案。

- Backup 管理：

  AMS 使用备份管理来拍摄您的资源快照。

  AWS Managed Servic AWS es 为支持的服务创建、监控和存储快照 AWS Backup。您可以通过在注册账户和应用程序时创建 AWS Backup 计划来定义备份计划、频率和保留期。您可以将计划与资源关联。AMS 会跟踪所有备份任务，当备份任务失败时，会提醒我们的团队进行修复。如有必

要，AMS 会利用您的快照在事故期间执行恢复操作。AMS 为您提供备份覆盖率报告和备份状态报告。

- 问题管理：

  AMS 进行趋势分析以识别和调查问题并确定根本原因。问题可以通过变通方法或永久解决方案进行修复，以防止将来再次出现类似的 future 服务影响。任何 “高” 事件一经解决，均可要求提供事后报告 (PIR)。PIR捕捉了根本原因和所采取的预防措施，包括预防措施的实施。

- 指定专家：

  AMS Accelerate 还会指定一名云服务交付经理 (CSDM) 和一名云架构师 (CA) 与您的组织合作，推动卓越的运营和安全性。您的 CSDM 和 CA 会在配置期间和之后为您提供指导 AMS Accelerate，提供运营指标的月度报告，并与您合作，使用 AWS Cost Explorer、成本和使用情况报告等工具确定潜在的成本节约。 Trusted Advisor

- 操作工具：

  AMS Accelerate 可以为您在 AWS 中的工作负载基础设施提供持续运营。我们的补丁、备份、监控和事件管理服务依赖于对资源进行标记，并在您的亚马逊 EC2 实例上安装和配置 AWS Systems Manager (SSM) 和 CloudWatch 代理，并使用授权它们与 SSM 和 Amazon 服务交互的 IAM 实例配置文件。 CloudWatch AMS Accelerate 提供了诸如资源标记器之类的工具，可帮助您根据规则标记资源，以及用于在您的 Amazon 实例中安装所需代理的自动 EC2实例配置。如果您遵循不可变的基础架构实践，则可以直接在控制台或 infrastructure-as-code模板中完成先决条件。

- 成本优化：

  AMS 资源调度器可自动启动和停止亚马逊弹性计算云 (Amazon EC2) 实例、亚马逊关系数据库服务 (Amazon RDS) 实例和 Amazon A EC2 uto Scaling 组。AMS Resource Scheduler 可停止未使用的资源，并在需要容量时重新启动这些资源，从而帮助您降低运营成本。

- 日志和报告：

  AWS Managed Services 汇总并存储在 CloudWatch CloudTrail、和 Amazon VPC 流日志中操作后生成的日志。从 AMS 进行日志记录有助于更快地解决事件和进行系统审计。AMS Accelerate 还为您提供月度服务报告，其中汇总了 AMS 的关键绩效指标，包括执行摘要和见解、运营指标、托管资源、AMS 服务水平协议 (SLA) 遵守情况，以及有关支出、节省和成本优化的财务指标。报告由指定给您的 AMS 云服务交付经理 (CSDM) 交付。

- 服务请求管理：

要请求有关您的托管环境、AMS 或 AWS 服务产品的信息，请使用 AMS Accelerate 控制台提交服务请求。您可以提交服务申请，询问有关 AWS 服务和功能的 “操作方法” 问题，也可以申请其他 AMS 服务。

所有 AMS Accelerate 客户都从事件管理、监控、安全监控、日志记录、必备工具、备份管理和报告功能开始。您可以额外付费添加 AMS 补丁管理附加组件。

> **Note**
>
> 有关中不支持的功能列表 AWS GovCloud (US)，请参阅 AMS Accelerate 的不同之处 AWS GovCloud (US)

支持的配置

AMS 加速支持以下配置：

- 语言：英语。
- 区域：在 AWS 区域服务网页中查看 AWS Managed Ser AWS vices 支持的区域。

> **Note**
>
> 2019 年 3 月 20 日之前推出的 AWS 区域被视为 “原始” 区域，默认情况下处于启用状态。在此日期之后引入的区域是 “选择加入” 区域，默认情况下处于禁用状态。如果您的账户使用多个区域，并且您将 AMS Accelerate 加入的账户中已启用 “选择加入” 区域作为默认区域，则 AMS 报告功能仅在该区域可用。如果您未设置默认区域，则您上次访问的区域就是您的默认区域。
>
> 要启用区域，请参阅启用区域。要设置默认区域，请参阅选择区域。有关每个区域的选择加入状态列表，请参阅 Amazon Elastic Compute Cloud 用户指南中的可用区域。

- 操作系统架构（x86-64 或 ARM64）：S ystem s Manager 和。CloudWatch
- 支持的操作系统：
  - AlmaLinux 8.3-8.9、9.x（AlmaLinux 仅支持 x86 架构）
  - Amazon Linux 2023
  - 亚马逊 Linux 2（预计 AMS 支持截止日期为 2026 年 6 月 30 日）
  - 甲骨文 Linux 9.x、8.x

- 红帽企业 Linux (RHEL) 9.x、8.x
- SUSE Linux 企业服务器 15 SP6
- 适用于 SAP 15 SP3 及更高版本的 SUSE Linux 企业服务器
- 微软 Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

- 支持的终止支持 (EOS) 操作系统：

> **Note**
>
> End of Support (EOS) 操作系统不在操作系统制造商的一般支持期内，因此安全风险增加。只有当 AMS 要求的代理支持操作系统并且... 时，EOS 操作系统才被视为支持的配置
>
> 1. 您已获得操作系统供应商的扩展支持，允许您接收更新，或者
> 2. 任何使用 EOS 操作系统的实例都要遵守 AMS 在《加速用户指南》中指定的安全控制措施，或者
> 3. 您遵守 AMS 要求的任何其他补偿性安全控制措施。
>
> 如果 AMS 无法再支持 EOS 操作系统，AMS 会发布升级操作系统的关键建议。
> AMS 所需的代理可能包括但不限于： CloudWatch、 AWS Systems Manager亚马逊、端点安全 (EPS) 代理和 Active Directory (AD) Bridge（仅限 Linux）。

  - Ubuntu Linux 18.04
  - SUSE Linux 企业服务器 15 SP3 SP4、和 SP5
  - 适用于 SAP 的 SUSE Linux 企业服务器 15 SP2
  - SUSE Linux 企业服务器 12 SP5
  - 适用于 SAP 的 SUSE Linux 企业服务 12 SP5
  - 微软 Windows Server 2012/2012 R2
  - 红帽企业 Linux (RHEL): 7.x
  - 甲骨文 Linux 7.5-7.9
- 如果您使用 AWS Control Tower 管理多账户环境，请确保运行的是最新版本的，以便与 Accelerat AWS Control Tower e 兼容。不支持使用 2.7 之前 AWS Control Tower 版本（2021 年 4 月发布）的环境。有关如何更新的信息 AWS Control Tower，请参阅更新您的着陆区。

受支持的服务

AWS Managed Services 为以下服务提供运营管理支持 AWS 服务。每种 AWS 服务都是不同的，因此，AMS的运营管理支持水平因基础 AWS 服务的性质和特征而异。如果您请求 AWS Managed Services 为以下列表中未明确确定为支持的软件或服务提供服务，则根据服务条款，为此类客户请求的配置提供的任何 AWS Managed 服务都将被视为 “测试版服务”。

- 事件：所有 AWS 服务
- 服务请求：所有 AWS 服务
- 正在修补：Amazon EC2
- 备份和恢复：全部 AWS 服务 支持 AWS Backup。有关支持的服务的列表 AWS Backup，请参阅AWS Backup 支持的资源。
- 资源调度器：亚马逊弹性计算云 (Amazon EC2) 实例、亚马逊关系数据库服务 (Amazon RDS) 和亚马逊 A EC2 uto Scaling 组
- 针对运营事件监控的服务：支持的支票和 Trusted Advisor、应用程序负载均衡器、Aurora、亚马逊 EC2、Elastic Load Balancing、适用 FSx 于 NetApp ONTAP 的亚马逊、适用 FSx于 Windows 的文件服务器的亚马逊、NAT 网关（网络地址转换 (NAT) 服务）、、 OpenSearch Health Dashboard、Amazon Redshift、亚马逊关系数据库服务（Amazon RDS） Site-to-Site、VPN。要详细了解 AMS Accelerate 作为服务的一部分正在监控的内容，请参阅 AMS 基准监控发出的警报。
- 受安全配置规则监控的服务： AWS 账户、、Macie GuardDuty、Amazon API Gateway、、、、、、、 AWS Certificate Manager、、 AWS Config、、 CloudTrail、 CloudWatch AWS CodeBuild、亚马逊 DynamoDB AWS Database Migration Service、亚马逊、亚马 EC2 ElastiCache逊 Elastic Block Store (亚马逊 EBS)、亚马逊弹性文件系统 (亚马逊 EFS)、亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、Elastic Load Balancing、亚马逊服务、亚马逊 AWS Key Management Service EMR、(IAM)、、、 AWS Identity and Access Management 亚马逊 Redshift、亚马逊关系数据库服务 AWS Lambda、亚马逊 S3、亚马逊 AI、、 OpenSearch SageMaker AWS Secrets Manager 亚马逊简单通知服务 AWS Systems Manager、亚马逊 VPC（安全组、卷、弹性 IP 地址、VPN 连接、互联网网关）、亚马逊 VPC 流日志。有关更多详细信息，请参阅 加速中的配置合规性 和 “加速” 中的数据保护。您可以在我们的私有安全指南中找到其他 AMS 安全信息，可通过 AWS Artifact AWS Managed Services 的 “报告” 选项卡访问这些信息。

> **Note**
>
> 中东 (UAE) 地区的 AMS Accelerate 支持一系列范围内的功能，如下表所述。对该地区的 AMS 账户控制台和实例的访问完全由入站服务请求触发器驱动。有关 Accelerate 在中东 (UAE) 地区的可用性的更多信息，请咨询您的客户经理或 AWS 云服务交付经理 (CSDM)。

AMS 加速中东 (UAE) 地区的范围内的功能	功能描述
事件管理	AMS 提供事件响应和协助，以帮助您的团队解决问题。为了让 AMS 协助您进行事件管理，您需要提交服务请求。AMS 不会主动检测或响应该地区的事件。
监控	在收到您的服务请求后，AMS 可以协助进行资源修复。AMS 使用自动修复、人员和流程将您的资源恢复到健康状态。AMS 不在该区域配置基准 CloudWatch 事件和警报。如果您有现有的监控工具，则可以根据云架构师 (CA) 和 CSDM 评估主动跟踪您的资源。
安全性	在收到您的服务请求后，AMS 可以协助修复安全问题。AMS 不部署安全控制措施，例如 AWS Config 规则 和 GuardDuty /或监控该地区的安全发现。如果您有现有的安全工具，则可能会基于 CA 和 CSDM 评估提供主动安全监控。
补丁管理	AMS 可以在选定的维护时段内将供应商更新应用于支持的操作系统的 Amazon EC2 实例，并创建预修补快照。为了让 AMS 帮助您管理补丁，您需要提交服务请求。该地区不提供 AMS 补丁通知和报告。
Backup 管理	AMS 可以创建和存储 AWS 服务 支持的快照 AWS Backup，并协助进行备份修复。为了让 AMS 协助您管理备份，您需要提交服务请求。AMS 不跟踪该地区的备份任务。

AMS 加速中东 (UAE) 地区的范围内的功能	功能描述
指定专家	AMS 指定一名云架构师 (CA) 和一名云服务交付经理 (CSDM) 与客户组织合作，推动卓越的运营和安全性。
服务请求管理	要请求有关您的托管环境、AMS 或 AWS 服务产品/服务的信息，请通过 AMS Accelerate 控制台提交服务请求。您可以提交服务请求，询问有关 AWS 服务 和功能的 “操作方法” 问题，也可以申请该地区可用的 AMS 服务，如下表所述。

角色和责任

AMS Accelerate 负责任、负责、咨询和知情或 RACI 矩阵将各种活动的主要责任分配给客户或 AMS。下表描述了您（“客户”）的责任与我们（“AMS Accelerate”）的责任。

本AMS Accelerate 执行的变更范围节列出了 AMS 有权更改您的账户的具体情况；以及 AMS 从未做过的某些类型的更改。

AMS 加速 RACI 矩阵

AMS 加速管理您的 AWS 基础设施。下表概述了在托管环境中运行的应用程序生命周期中您和 AMS Accelerate 的角色和职责。

- R 代表负责完成任务的责任方。
- C 代表 C onsulted；通常作为主题专家征求意见的一方；与之进行双边沟通。
- I 代表 Inforded；该方通常只有在任务完成后才会被告知进展情况。

> **Note**
>
> 有些部分包含针对 AMS 和客户的 “R”。这是因为，在责任 AWS 共担模式中，AMS 和客户共同拥有应对基础设施和应用程序问题的所有权。

活动	Customer	AWS Managed Services (AMS)
AMS 模式		
创建新图案	我	R
部署和自定义模式	R	C，I
测试并移除图案	R	我
应用程序生命周期		
应用程序开发	R	我
应用程序基础架构需求、分析和设计	R	我
应用程序部署	R	我
AWS 资源部署	R	我
应用程序监控	R	我
应用程序测试/优化	R	我
对应用程序问题进行故障排除和解决	R	我
疑难解答和解决问题	R	我
AWS 基础设施支持监控	C	R
AWS 网络问题事件响应	C	R
AWS 资源问题事件响应	C	R
托管账户入门		
向 AMS 团队授予访问 AWS 托管账户和工具的权限	R	C

活动	Customer	AWS Managed Services (AMS)
在账户或环境中实施变更以允许在账户中部署工具。例如，服务控制策略的更改 (SCPs)	R	C
在实例中安装 SSM 代 EC2 理	R	C
安装和配置提供 AMS 服务所需的工具。例如， CloudWatch 代理、修补脚本、警报、日志等	我	R
管理 AMS 工程师的访问权限和身份生命周期	我	R
收集配置 AMS 服务所需的所有输入。例如，补丁维护时段、持续时间、时间表和目标	R	我
请求配置 AMS 服务并提供所有必需的输入	R	我
根据客户的要求配置 AMS 服务。例如，补丁维护窗口、资源标记器和警报管理器	C	R
管理用于访问 AWS 账户和实例的本地目录服务的用户的生命周期及其权限	R	我
推荐预留实例优化	我	R
向 Trusted Remediator 注册账户	C，I	R
补丁管理		
收集所有必需的输入以配置补丁维护窗口、补丁基准和目标	R	我
请求配置补丁维护窗口和基准，并提供所有必需的输入	R	我
根据客户的要求配置补丁维护窗口、补丁基准和目标	C	R
监控支持的操作系统的适用更新，以及预先安装了支持的操作系统的 EC2 软件	我	R

活动	Customer	AWS Managed Services (AMS)
报告支持的操作系统缺少更新和维护时段覆盖范围	我	R
在应用更新之前拍摄实例快照	我	R
根据客户配置对 EC2 实例进行更新	我	R
调查 EC2 实例更新失败	C	R
自动缩放群组的更新 AMIs 和堆栈 () ASGs	R	C
修补安装在操作系统上的 Windows 操作系统和受 Windows 更新控制的微软软件包	我	R
修补未由 Windows Update 管理的已安装的应用程序、软件或应用程序依赖关系	R	我
修补 Linux 操作系统和任何允许操作系统原生软件包管理器管理的软件包（例如 Yum、Apt、Zypper）	我	R
修补未由 Linux 操作系统的本机软件包管理器管理的已安装应用程序、软件或应用程序依赖项	R	我
备份		
收集所有必需的输入，以配置备份计划和目标资源	R	我
请求配置 Backup 计划并提供所有必需的输入	R	我
根据客户的要求配置备份计划和目标	C	R
指定备份时间表和目标资源	R	我
按计划执行备份	我	R
调查失败的备份作业	我	R

活动	Customer	AWS Managed Services (AMS)
报告备份任务状态和备份覆盖范围	我	R
验证备份	R	我
作为事件管理的一部分，请求对支持的 AWS 服务资源的资源进行备份恢复	R	我
为支持的 AWS 服务的资源执行备份恢复活动	我	R
恢复受影响的自定义应用程序或第三方应用程序	R	我
联网		
配置和配置托管账户 VPCs IGWs、直接连接和其他 AWS 联网服务	R	我
在托管账户Groups/NAT/NACL中配置和操作 AWS 安全	R	我
客户网络中的网络配置和实施（例如 DirectConnect）	R	我
在 AWS 网络中配置和实施网络	R	我
AMS 为网络安全定义的监控器，包括安全组	我	R
网络级日志配置和管理（VPC 流日志等）	我	R
日志系统		
记录所有应用程序更改日志	R	我
记录 AWS 基础设施变更日志	我	R
启用和汇总 AWS 审计跟踪	我	R
汇总来自 AWS 资源的日志	我	R
监控和修复		

活动	Customer	AWS Managed Services (AMS)
收集所有必需的输入以配置警报管理器、资源标记器和警报阈值	R	我
请求配置警报管理器并提供所有必需的输入	R	我
根据客户的要求配置警报管理器、资源标记器和警报阈值。	C	R
根据客户配置部署 AMS CloudWatch 基准指标和警报	我	R
使用基准 CloudWatch 指标和警报监控支持的 AWS 资源	我	R
调查来自 AWS 资源的警报	C	R
根据定义的配置修复警报，或创建事件	我	R
定义、监控和调查客户特定的监视器	R	我
调查来自应用程序监控的警报	R	C
配置补救 Trusted Advisor 检查	R	C
自动修复支持的检查 Trusted Advisor	我	R
手动修复支持的检查 Trusted Advisor	R	C
报告补救状态	我	R
修复失败疑难解答	R	C
安全架构		
查看 AMS 资源和代码，了解安全问题和潜在威胁	我	R
在 AMS 资源和代码中实施安全控制以降低安全风险	我	R
启用支持的 AWS 服务，以便对账户及其 AWS 资源进行安全管理	我	R
管理 AMS 工程师的账户特权凭证和操作系统访问权限	我	R

活动	Customer	AWS Managed Services (AMS)
安全风险管理		
监控支持的 AWS 服务以进行安全管理，例如 GuardDuty 和 Macie	我	R
定义并创建 AMS 定义的 Config 规则，以检测 AWS 资源是否符合互联网安全中心 (CIS) 和 NIST 安全最佳实践。	我	R
监控 AMS 定义的 Config 规则	我	R
报告 Config 规则的一致性状态	我	R
定义所需的 Config 规则列表并对其进行修正	我	R
评估修复 AMS 定义的 Config 规则的影响	R	我
在 AWS 账户中请求修正 AMS 定义的 Config 规则	R	我
追踪不受 AMS 定义的 Config 规则约束的资源	R	我
修复 AWS 账户中支持的 AMS 定义的 Config 规则	C	R
修复 AWS 账户中不支持的 AMS 定义的 Config 规则	R	我
定义、监控和调查特定于客户的 Config 规则	R	我
事件管理		
通知 AMS 在 AWS 资源中检测到的事件	我	R
通知 AWS 资源中的事件	R	我
根据监控通知 AWS 资源的事件	我	R
处理应用程序性能问题和中断	R	我
对事件优先级进行分类	我	R

活动	Customer	AWS Managed Services (AMS)
提供事件响应	我	R
利用可用备份为资源提供事件解决方案或基础架构恢复	C	R
安全事件响应-准备		
通讯		
提供并更新客户安全联系人详细信息，以便 AMS 在安全事件、通知和安全升级期间使用	R	我
存储和管理提供的客户安全联系人详细信息，以便在安全事件和安全升级期间使用	C	R
训练		
在事件响应过程中向客户提供支持 AMS 的文档	我	R
在安全比赛日的事故响应流程中实践责任共担	R	R
资源管理		
AWS 服务 为警报、警报关联、降噪和其他规则配置支持的安全管理	我	R
维护全面的 AWS 资源清单（Amazon EC2、Amazon S3 等），包括每项资产对业务的价值和重要性的详细信息。这些信息将有助于确定有效的遏制策略	R	C
使用 AWS 标签来识别资源和工作负载	R	C
定义和配置日志保留和存档	我	R
通过为 AWS 账户、服务和访问管理定义和实施组织的安全策略和配置，建立安全的基准	R	我
安全事件响应-检测		

活动	Customer	AWS Managed Services (AMS)
记录、指标和监控		
配置日志记录和监控以启用实例和账户的事件管理	我	R
支持显示安全警报 AWS 服务 的监视器	我	R
部署和管理端点安全工具	R	我
使用端点安全监控实例上的恶意软件	R	我
通过出站消息通知客户检测到的事件	我	R
协调内部利益相关者沟通和领导层最新消息，以缩短响应时间	R	我
定义、部署和维护 AMS 标准检测服务（例如 Amazon GuardDuty 和 AWS Config）	C	R
记录 AWS 基础设施变更日志	R	我
启用和配置日志记录、监控以启用应用程序的事件管理	R	C
在支持 AWS 的安全服务（例如 Amazon）上实施和维护允许名单、拒绝名单和自定义检测 GuardDuty	R	R
安全事件报告		
将可疑活动或正在进行的安全调查通知AMS	R	我
将检测到的安全事件和事件通知客户	我	R
通知可能触发安全事件响应流程的计划事件	R	我
安全事件响应-分析		
调查和分析		

活动	Customer	AWS Managed Services (AMS)
对支持的检测源生成的支持安全警报执行初始响应	我	R
使用现有数据评估 false/true 阳性	R	R
生成受影响实例的快照，以便在需要时与客户共享	我	R
执行取证任务，例如监管链、文件系统分析、内存取证和二进制分析	R	C
收集应用程序日志以帮助调查	R	我
收集数据和日志，以帮助调查安全警报	R	R
SMEs 参与 AWS 服务 安全调查	C	R
在调查期间与客户共享支持 AWS 服务 人员的调查日志	我	R
沟通		
从 AMS 检测源为托管资源发送警报和通知	我	R
管理应用程序安全事件的警报和通知	R	我
在安全事件调查期间与客户安全联系人接触	R	我
安全事件响应-包含		
遏制策略和执行		
评估风险并确定遏制策略，确认潜在的服务影响	R	C
备份受影响的系统以供进一步分析	我	R
包含应用程序和工作负载（通过应用程序特定的配置或响应活动）	R	C
根据安全事件和受影响的资源定义遏制策略	我	R
启用受影响系统的时间点备份的加密和安全存储	C	R

活动	Customer	AWS Managed Services (AMS)
对 AWS 资源（包括 EC2 实例、网络和 IAM）执行支持的遏制操作	我	R
安全事件响应-根除		
根除策略和执行		
根据安全事件和客户应用程序工作负载上受影响的资源来定义清除选项	C	R
决定商定的根除战略、执行根除的时间和后果	R	我
根据安全事件和 AMS 托管工作负载上受影响的资源定义根除步骤	C	R
消除威胁并强化 AWS 资源，包括 EC2 实例、网络和 IAM 根除	R	C
消除威胁并强化应用程序和工作负载（通过应用程序特定的配置或响应活动）	R	我
安全事件响应-恢复		
恢复准备和执行		
根据客户的要求配置备份计划和目标	我	R
查看备份计划以恢复 AMS 托管的工作负载	R	我
对支持的资源执行备份恢复活动 AWS 服务	我	R
备份客户应用程序、应用程序配置和部署设置，并查看备份计划，以便在事后恢复客户应用程序和工作负载	R	我
恢复应用程序和客户工作负载（通过应用程序特定的恢复步骤）	R	我
安全事件响应-事后报告		
事后报告		

活动	Customer	AWS Managed Services (AMS)
根据需要与客户在事后分享适当的经验教训和行动项目	我	R
问题管理		
关联事件以识别问题	我	R
对问题进行根本原因分析 (RCA)	我	R
修复问题	我	R
识别和修复应用程序问题	R	我
服务管理		
使用服务请求请求信息	R	我
回复服务请求	我	R
提供成本优化建议	我	R
准备并提交月度服务报告	我	R
变更管理		
用于在托管环境中配置和更新资源的变更管理流程和工具	R	我
维护应用程序变更日历	R	我
关于即将到来的维护窗口的通知	R	我
记录 AMS 运营部门所做的更改	我	R
成本优化		
收集所有必需的输入以配置资源调度器	R	我
申请资源调度器的入职和配置并提供所有必需的输入	R	我

活动	Customer	AWS Managed Services (AMS)
根据客户配置部署资源调度器	C，I	R
在客户账户上禁用和启用资源调度器	R	C
创建、删除、描述和更新计划	C	R
创建、删除、描述和更新时段	C	R
使用资源调度器调查和解决问题	我	R
请求下线资源调度器	R	我
从账户中移除资源调度器	C，I	R

AMS Accelerate 执行的变更范围

AMS Accelerate 仅针对下文所述的特定目的和情况进行更改。AMS 仅在基础设施级别进行更改，使用控制台或 APIs。AMS 永远不会更改您的应用程序、控件或域层。您可以使用我们的预建查询集查看 AMS（或其他用户）所做的任何更改；要执行此操作，请参阅跟踪您的 AMS Accelerate 账户中的更改。

AWS resources

AMS Accelerate 仅在以下情况下部署或更新 AWS 资源：

- 部署和更新 AMS 所需的工具和资源。
- 作为 AMS 监控的一部分，用于响应事件和警报。
- 作为修复安全问题的一部分对 “加速” 中违规行为的回应（使不合规的资源符合安全最佳实践）。
- 在修复和恢复期间，作为事件响应的一部分。
- 在回应客户配置 AMS 功能的请求时，例如：
  - 警报管理器
  - 资源标记器
  - 补丁基准和维护窗口

- 资源调度器
- 备份计划

在这些情况之外，AMS Accelerate 不会部署或更新资源。如果您需要 AMS 的帮助才能在其他情况下进行更改，请考虑使用按需操作。

操作系统软件

AMS Accelerate 可以在无法使用时通过我们的服务等级协议中定义的事件解决方案对您的操作系统软件进行更改。AMS 还可以对您的操作系统进行更改，作为其中的一部分AMS Accelerate 中的自动实例配置。

应用程序代码和配置

AMS Accelerate 从不修改您的代码（例如 AWS CloudFormation infrastructure-as-code 模板、其他模板或 Lambda 函数），但可以指导您的团队进行哪些更改才能遵循最佳运营和安全实践。AMS Accelerate 为影响应用程序的基础设施问题提供故障排除帮助，但是 AMS Accelerate 无法访问或验证您的应用程序配置。

Accelerate 中针对不支持的操作系统的功能

不支持的操作系统是指未在中列出的任何操作系统。支持的配置AMS 将操作系统不支持的实例视为“客户请求的配置”，受测试版和预览版服务AWS 条款的约束。

以下有限的 AMS 功能适用于操作系统不支持的实例：

功能	备注
事件管理	AMS 提供事件响应。
服务请求管理	AMS 会对服务请求做出回应。
监控	AMS 监控并响应 Amazon EC2 系统状态检查和实例状态检查。系统状态检查包括：网络连接中断、系统电源中断、物理主机上的软件问题以及影响网络可访问性的物理主机上的硬件问题。 实例状态检查包括：网络或启动配置不正确、内存耗尽、文件系统损坏以及内核不兼容。

功能	备注
安全管理	AMS 监控并回应 Amazon 的 EC2 GuardDuty 调查结果和AWS Config 规则。
备份管理	AMS 在 Accelerate 中为 EC2 使用 AMS 定制的 AWS Backup 计划和保管库提供连续性管理。

联系和升级

您有指定的云服务交付经理 (CSDM)，负责在 AMS Accelerate 中提供咨询帮助，并详细了解托管环境的用例和技术架构。 CSDMs 与客户经理、技术客户经理、AWS Managed Services 云架构师 (SAs) 和 AWS 解决方案架构师 () 合作（如适用），以帮助启动新项目，并在整个软件开发和运营过程中提供最佳实践建议。CAsCSDM 是 AMS 的主要联系点。您的 CSDM 的主要职责是：

- 组织并主持与客户的月度服务审查会议。
- 提供有关安全性、环境软件更新和优化机会的详细信息。
- 支持您的要求，包括 AMS Accelerate 的功能请求。
- 回应并解决账单和服务报告请求。
- 为财务和容量优化建议提供见解。

联系时间

您可以出于不同的原因在不同的时间联系 AMS Accelerate。

功能	AMS Accelerate
	高级等级
服务请求	全天候
事件管理 (P2-P3)	全天候
备份和恢复	全天候
补丁管理	全天候

功能	AMS Accelerate
	高级等级
监控和提醒	全天候
云服务交付管理器 (CSDM)	周一至周五：08:00 — 17:00，当地工作时间

营业时间

功能	AMS Accelerate
	高级等级
服务请求	全天候
事件管理 (P1)	全天候
事件管理 (P2-P3)	全天候
备份和恢复	全天候
补丁管理	全天候
监控和提醒	全天候
云服务交付管理器 (CSDM)	周一至周五：09:00 — 17:00，当地工作时间

升级路径

AMS 根据适用于账户的 AMS 服务等级协议，为客户提供全年 365 天、每天 24 小时、每周 7 天、每天 24 小时的事件管理和服务请求管理支持。

要报告影响您的托管环境的 AWS 或 AMS 服务性能问题，请使用 AMS 控制台并提交事件案例。有关更多信息，请参阅 为 Accelerate 提交事件。有关 AMS 事件管理的一般信息，请参阅AMS Accerate 中的事件管理。

要向 AMS 询问信息或建议，或请求其他服务，请使用 AMS 控制台并提交服务请求。有关更多信息，请参阅 在 Accelerate 中创建服务请求。有关 AMS 服务请求的一般信息，请参阅Accelerate 中的服务请求管理。

用于加速的资源清单

AMS Accelerate 部署到您的 AWS 账户 或账户的所有资源都列在resource_inventory.zip文件 resource_inventory.xlsx 电子表格（压缩）中。

> **Note**
>
> 在资源名称列中，前缀 CFN: 表示 CloudFormation 逻辑 ID 而不是资源名称。这些是针对未命名的资源（例如 S3 存储桶策略）显示的。

AMS 部署了一组服务，如中所服务描述述。部署到空账户时，部署它们的成本很低，但是随着利用率的增长，成本也会增加。例如，创建日志，并在资源更改时调用配置规则。

当对配置规则进行多次更改时，可能会触发多个配置合规性调用，从而导致更高的成本。同样的可能性也适用于 CloudWatch 用于监控实例的 Amazon，您的监控越精细，服务成本就越高。 AWS Backup 是另一个例子。如果您存储了多个备份，或者保留期更长，则表示您使用的存储空间越多，成本也会更高。

这些数字很难预测。在与云服务交付经理 (CSDM) 进行的每月业务评估中，跟踪变化并努力确定降低成本的机会领域。

AMS 入门加速

如果您还没有 AWS Managed Services (AMS) 运营账户，请先使用我们的 AWS Managed Services-联系销售页面联系亚马逊网络服务 (AWS) 销售代表。

在您注册 AMS 后，AMS Accelerate 团队将指导您完成每个 AMS 的以下入职流程。 AWS 账户

在此处查看功能集：AWS Managed Services 功能

> **Note**
>
> AMS 加速支持 GovCloud 区域。如果您的服务将驻留在中 AWS GovCloud (US) Region，另请参阅入门 AWS GovCloud (US)。

Accelerate 的账户注册流程

将账户注册到 AMS Accelerate 分为四个阶段。

1. 第 1 步：在 “加速” 中发现账户评估您账户的当前状态，并确定登录账户所需的技术障碍。
2. 第 2 步：Accelerate 中的入职管理资源要求您接受条款和条件；并为 AMS Accelerate 云架构师 (CAs) 创建一个入职职位，该架构师将协助您设置安全基准并根据需要解决问题。
3. 第 3 步：使用默认策略加载 AMS 功能用于加速功能，例如监控、修补和备份。
4. 第 4 步：在 “加速” 中自定义功能确保为您的应用程序正确配置资源（包括 EC2 实例）。

加快入职先决条件

在开始入门流程之前，请务必了解 Accelerate 组件所依赖的技术依赖关系。

> **Note**
>
> 要使用 AMS Accelerate，您必须使用两个支持的 支持 计划之一：企业版入口或企业版。开发人员和商业计划没有资格获得 AMS Accelerate 资格。要了解有关不同套餐的更多信息，请参阅比较 支持 套餐。

AMS 加速 VPC 终端节点

VPC 终端节点可在您的 VPC 与支持的 AWS 服务以及由提供支持的 VPC 终端节点服务之间建立私有连接 AWS。如果您需要筛选出站互联网连接，请配置以下 VPC 服务终端节点，以确保 AMS Accelerate 与其服务依赖项建立连接。

> **Note**
>
> 在以下列表中，*region*代表 AWS 区域的标识符，例如us-east-2美国东部（俄亥俄州）地区的标识符。

```
com.amazonaws.region.logs
com.amazonaws.region.monitoring
com.amazonaws.region.ec2
com.amazonaws.region.ec2messages
com.amazonaws.region.ssm
com.amazonaws.region.ssmmessages
com.amazonaws.region.s3
com.amazonaws.region.events
```

有关如何配置 AWS VPC 终端节点的信息，请参阅 V PC 终端节点。

> **Note**
>
> 如果您要在账户中为上述所有服务创建 VPC 终端节点，请查看此示例 CloudFormation 模板。您可以根据自己的用例更新此模板并删除或添加 VPC 终端节点定义。

加速中的出站互联网连接

1. 下载 egressMgmt.zip。
2. 打开 **ams-egress.json**文件。
3. 在 JSON 属性 URLs 下找到：
   - `WindowsPatching`
   - `RedHatPatching`
   - `AmazonLinuxPatching`

- EPELRepository

4. 允许访问这些 URLs。

在 “加速” 中测试出站连接

使用以下方法之一测试出站连接。

> **Note**
>
> 在运行脚本/命令之前，请将红色*region*替换为您的区域标识符，例如。us-east-1

Windows PowerShell 脚本

```
$region = 'region'
@('logs','monitoring','ec2','ec2messages','ssm','ssmmessages','s3','events') | `
ForEach-Object { `
Test-NetConnection ("$_" + '.' + "$region" + '.amazonaws.com') -Port 443 } | `
Format-Table ComputerName,RemotePort,RemoteAddress,PingSucceeded,TcpTestSucceeded -
AutoSize
```

Linux 命令

```
for endpoint in logs monitoring ec2 ec2messages ssm ssmmessages s3 events; do nc -zv
 $endpoint.region.amazonaws.com 443; done
```

加速中的 Amazon EC2 Systems Manager

您必须在希望 AMS 管理的所有 EC2 实例上安装代 AWS Systems Manager 理（SSM 代理）。您还需要添加 SSM 代理所需的存储桶权限。有关包括 Amazon 的概述 EC2，请参阅第 3 步：使用默认策略加载 AMS 功能。

加速中的 IAM

要允许您的用户读取和配置 AMS Accelerate 功能，例如访问 AMS 控制台或配置备份，您必须在 AWS Identity and Access Management (IAM) 中授予执行这些操作的明确权限。有关 IAM 策略的示例，请参阅使用 AMS 功能的权限。

第 1 步：在 “加速” 中发现账户

在账户发现期间，AMS 会与您合作，评估您账户的当前状态，并找出登录账户所需的技术屏障。AMS 不在账户发现阶段提供运营服务。AMS 使用AWSServiceRoleForSupport服务相关角色来识别技术屏障，然后与您合作进行补救，然后进入账户级入门阶段。

Accelerate 中的账户发现流程

为了帮助您分析和发现您的账户，AMS 会执行操作检查，通过只读 API 调用识别技术拦截器。在您的账户加入 AMS 后，这些检查将按需执行，以保持账户状态。在需要时，AMS 会与您合作，对与这些检查相关的任何发现进行补救。AMS 使用以下操作检查和只读 API 操作作为账户发现的一部分：

操作检查	用途	AWS 使用的 API 调用
AWS Control Tower 版本评估	标识 AWS Control Tower 版本以确保它是入门支持的最低版本。 AWS 账户	• ControlTower:GetLandingZone • ControlTower:ListEnabledControls • ControlTower:ListLandingZones
AWS CloudTrail 评估	确定您的入职 AWS CloudTrail 跟踪及其配置， AWS 账户 以最大限度地降低 CloudTrail 跟踪成本。	• CloudTrail:GetTrail • CloudTrail:ListTrails • S3:GetBucketOwnershipControls • S3:GetBucketPolicy • KMS:GetKeyPolicy • CloudTrail:GetEventSelectors • S3:GetBucketLogging • S3: GetBucketLifecycleConfiguration

操作检查	用途	AWS 使用的 API 调用
		• S3: GetBucketEncryption
CloudFormation 挂钩评估	识别您的入职 AWS 账户 中阻碍在您 AWS 账户中部署 AMS 服务的 CloudFormation 挂钩。	• CloudFormation:ListTypes
Amazon EC2 实例评估	识别您 AWS 账户 中未运行 AWS Systems Manager 代理（SSM 代理）和 AMS 不支持的 EC2 实例。	• EC2:DescribeInstances • EC2:DescribeImages • SSM:DescribeInstanceInformation

AMS Accelerate 遵循行业最佳实践，以满足并保持合规资格。AMS Accelerate Discovery 对您账户的访问权限是 AWS CloudTrail 通过AWSServiceRoleForSupport 服务相关角色记录的。这有助于满足监控和审计要求。有关的信息 AWS CloudTrail，请参阅《AWS CloudTrail 用户指南》。

第 2 步：Accelerate 中的入职管理资源

这是入职管理资源流程的概述。

您接受条款

您的云服务交付经理 (CSDM) 将指导您完成验收流程。您需要接受条款和条件 AWS 区域，选择附加组件和服务等级协议 (SLA)。

您向 AMS 角色授予权限

您需要授予对 AMS 流程和云架构师的访问权限。为此，您可以为每个角色创建一个 CloudFormation 堆栈。创建 AMS 角色的模板然后看为加速aws_managedservices_onboarding_roleCloudFormation 而创作。有关更多详细信息，请参阅AMS 中的访问管理加速。

AMS 会审查您的配置

您的云架构师 (CA) 还会查找您的账户中可能存在的配置问题，例如服务控制策略 (SCPs)，以及可能阻止 AMS 部署 AMS 所需的工具和资源的安全发现。您的 CA 会与您合作，帮助您补救发现并移除 AMS 工具和资源部署的所有障碍。

AMS 会审查您的 AWS CloudTrail 跟踪配置

您的云架构师 (CA) 将审查您的 CloudTrail 跟踪配置，并确认您是希望 AMS 部署全球 CloudTrail 跟踪，还是将 Accelerate 与您的 CloudTrail 账户或组织跟踪资源集成。如果您选择将 Accelerate 与您的 CloudTrail 跟踪集成，则您的 CA 将指导您完成对 CloudTrail 跟踪资源配置的必要更新。

AMS 部署管理资源

AMS 团队部署工具和 AWS 资源来提供 AMS Accelerate 的不同服务。完成后，AMS 已建立 AWS Managed Services 账户，AMS 会通知您您的账户已激活。

入职管理资源阶段到此结束。您可以直接进入入职流程的下一步:第 3 步：使用默认策略加载 AMS 功能.

> **Note**
>
> 现在您的账户已激活，您可以选择执行以下任一任务：
>
> - 使用 Support Center 控制台为 AWS 基础设施创建事件和服务请求。请参阅AMS Accelerate 中的事件报告、服务请求和账单问题。
> - 在您的账户中查看 AMS 部署的 AWS Config 规则的一致性状态。加速中的配置合规性
> - 定位和分析 GuardDuty 以及 Macie（可选）调查结果。请参阅使用监视器 GuardDuty。
> - 访问和审核 CloudTrail 日志
> - 追踪您的 AMS Accelerate 账户中的变化。请参阅跟踪您的 AMS Accelerate 账户中的更改。
> - 使用资源标记器创建标签。请参阅加速资源标记器。
> - 申请 Patch、Backup 和 AWS Config 报告。请参阅报告和选项。

查看并更新您的配置，让 AMS Accelerate 能够使用您的 CloudTrail 跟踪

AMS Acc AWS CloudTrail elerate 依靠登录来管理您账户中所有资源的审计和合规性。在入职期间，您可以选择 Accelerate 是在您的主要 AWS 区域部署 CloudTrail 跟踪，还是使用现有 CloudTrail 账户或组织跟踪生成的事件。如果您的账户未配置跟踪，则 Accelerate 将在入职期间部署托管 CloudTrail 跟踪。

> **Important**
>
> CloudTrail 只有当您选择将 AMS Accelerate 与您的 CloudTrail 账户或组织跟踪集成时，才需要进行日志管理配置。

与您的云架构师 (CA) 一起查看您的 CloudTrail 跟踪配置、Amazon S3 存储桶策略和 CloudTrail 活动交付目的地的 AWS KMS 密钥策略

在 Accelerate 可以使用您的 CloudTrail 跟踪之前，您必须与您的云架构师 (CA) 合作审查和更新您的配置以满足 Accelerate 的要求。如果您选择将 Accelerate 与您的 CloudTrail 组织跟踪集成，则您的 CA 会与您合作更新您的 CloudTrail 事件交付目标 Amazon S3 存储桶和 AWS KMS 密钥策略，以允许从您的 Accelerate 账户进行跨账户查询。您的 Amazon S3 存储桶可以位于由 Accelerate 管理的账户中，也可以位于您管理的账户中。在入职期间，Accelerate 会验证是否可以向您的 CloudTrail 组织跟踪事件交付目的地进行查询，如果查询失败，则会暂停入门。您与您的 CA 合作更正这些配置，以便可以恢复入职流程。

查看并更新您的 CloudTrail 账户或组织跟踪配置

要集成加速 CloudTrail 日志管理您的 CloudTrail 账户或组织跟踪资源，需要进行以下配置：

- 您的 CloudTrail 跟踪已配置为记录所有事件 AWS 区域。
- 您的 CloudTrail 跟踪已启用全局服务事件。
- 您的 CloudTrail 账户或组织跟踪记录所有管理事件，包括读取和写入事件， AWS KMS 并且 Amazon RDS Data API 事件日志已启用。
- 您的 CloudTrail 跟踪已启用日志文件完整性验证。
- 您的 CloudTrail 跟踪的 Amazon S3 存储桶使用 SSE-S3 或 SS E-KMS 加密来传输事件以加密事件。
- 您的 CloudTrail 跟踪向其发送事件的 Amazon S3 存储桶已启用服务器访问日志记录。
- 您的 CloudTrail 跟踪发送事件的 Amazon S3 存储桶的生命周期配置可将您的 CloudTrail 跟踪数据保留至少 18 个月。
- 您的 CloudTrail 跟踪向其发送事件的 Amazon S3 存储桶已将对象所有权设置为强制存储桶所有者。
- Accelerate 可以访问您的 CloudTrail 跟踪向其发送事件的 Amazon S3 存储桶。

查看并更新您的 CloudTrail 活动交付目的地的 Amazon S3 存储桶政策

在入职期间，您需要与您的云架构师 (CA) 合作，将 Amazon S3 存储桶策略声明添加到您的 CloudTrail 活动交付目的地。为了让您的用户能够从您的 Accelerate 账户中查询 CloudTrail 事件交付目标 Amazon S3 存储桶中的更改，您可以在组织中由 Accelerate 管理的每个账户中部署一个统一命名的 IAM 角色，并将其添加到所有 Amazon S3 存储桶策略声明的`aws:PrincipalArn`列表中。使用此配置，您的用户可以使用 Athena 在 Accelerate 中查询和分析您账户的 CloudTrail 组织跟踪事件。有关如何更新 Amazon S3 存储桶策略的更多信息，请参阅亚马逊简单存储服务用户指南中的使用 Amazon S3 控制台添加存储桶策略。

Important

只有在 Accelerate 与将事件传送到集中式 S3 存储桶的 CloudTrail 跟踪集成时，才需要更新您的 Amazon S3 存储桶策略。Accelerate 不支持与传送到集中存储桶但 AWS 组织下没有账户的 CloudTrail 跟踪集成。

Note

在更新您的 Amazon S3 存储桶策略之前，请将*red*字段替换为适用的值：

- *amzn-s3-demo-bucket*使用包含您账户中的跟踪事件的 Amazon S3 存储桶的名称。
- *your-organization-id*使用您的账户所属 AWS 组织的 ID。
- *your-optional-s3-log-delievery-prefix*使用您的 CloudTrail 跟踪的 Amazon S3 存储桶传送前缀。例如`my-bucket-prefix`，您在创建 CloudTrail 跟踪时可能已设置的内容。

  如果您尚未为跟踪配置 Amazon S3 存储桶传送前缀，请从以下 Amazon S3 存储桶策略声明中删除 *your-optional-s3-log-delievery-prefix* “” 和继续的正斜杠 (/)。

以下三个 Amazon S3 存储桶策略声明授予 Accelerate 访问权限，可以从您的 AWS Accelerate 账户中检索配置并运行 Athena 查询，以分析 CloudTrail 您的事件交付目标 Amazon S3 存储桶中的事件。

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWBUCKETCONFIGAUDIT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
```

```
    },
    "Action": [
        "s3:GetBucketLogging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
{
    "Sid": "DONOTDELETE-AMS-ALLOWLISTBUCKET",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:ListBucket",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringLike": {
            "s3:prefix": "your-optional-s3-log-delievery-prefix/AWSLogs/*"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
},
```

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWGETOBJECT",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": "s3:GetObject",
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/your-optional-s3-log-delievery-
prefix/AWSLogs/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "your-organization-id"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
    }
}
```

查看并更新 CloudTrail 活动投递目的地的 AWS KMS 关键政策

在入职期间，您需要与您的云架构师 (CA) 合作更新用于加密传送到您的 Amazon S3 存储桶的 CloudTrail 跟踪事件的 AWS KMS 密钥策略。确保将引用 AWS KMS 密钥策略声明附加到现有 AWS KMS 密钥中。这会将 Accelerate 配置为与您现有的 CloudTrail 跟踪事件传输目标 Amazon S3 存储桶集成并解密事件。为了让您的用户能够从您的 Accelerate 账户中查询 CloudTrail 事件交付目标 Amazon S3 存储桶中的更改，您可以在组织中由 Accelerate 管理的每个账户中部署一个统一命名的 IAM 角色，并将其添加到 “aws:PrincipalArn” 列表中。使用此配置，您的用户可以查询事件。

有不同的 AWS KMS 关键政策更新方案需要考虑。您可能只为 CloudTrail 跟踪配置了用于加密所有事件的 AWS KMS 密钥，而没有加密您的 Amazon S3 存储桶中对象的 AWS KMS 密钥。或者，您可能有一个 AWS KMS 密钥用于加密传递的事件 CloudTrail，另一个 AWS KMS 密钥用于加密存储在您的 Amazon S3 存储桶中的所有对象。当您有两个 AWS KMS 密钥时，您可以更新每个密钥的密 AWS KMS 钥策略，以授予 Accelerate 访问您的 CloudTrail 事件的权限。在更新策略之前，请务必将参考 AWS KMS 密 AWS KMS 钥政策声明修改为现有密钥策略。有关如何更新 AWS KMS 密钥策略的更多信息，请参阅AWS Key Management Service 用户指南中的更改密钥策略。

> **Important**
>
> 只有在 Accelerate 与启用了日志文件 SSE-KMS 加密的 CloudTrail 跟踪集成时，您才需要更新密 AWS KMS 钥策略。

> **Note**
>
> 在将此 AWS KMS 密钥策略声明应用于用于加密发送到 Amazon S3 存储桶 AWS CloudTrail 的事件的 AWS KMS 密钥之前，请将以下*red*字段替换为适用的值：
>
> - *YOUR-ORGANIZATION-ID*使用您的账户所属 AWS 组织的 ID。

本 AWS KMS 关键政策声明授予 Accelerate 访问从组织中每个账户发送到 Amazon S3 存储桶的解密和查询跟踪事件的权限，访问权限仅限于 Athena，Accelerate 使用它来查询和分析事件。 CloudTrail 。

```
{
    "Sid": "DONOTDELETE-AMS-ALLOWTRAILOBJECTDECRYPTION",
    "Effect": "Allow",
    "Principal": {
        "AWS": "*"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": "athena.amazonaws.com"
        },
        "StringEquals": {
            "aws:PrincipalOrgID": "YOUR-ORGANIZATION-ID"
        },
        "ArnLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/ams-access-*"
            ]
        }
```

```
    }
}
```

创建 AMS 角色的模板

以下 AMS 角色向您的 AMS 云架构师 (CA) 授予权限。以下 zip 文件包含 Terraform 代码和 CloudFormation 模板，可简化 IAM 角色、权限策略和信任策略的创建。有关更多信息，请咨询您的 CA。

角色名称	必填者	示例模板
`aws_managedservices_onboarding_role`	AMS 人员仅在入职期间使用	onboarding_role_minimal.zip

> **Note**
>
> 选择并下载示例模板（每个角色一个）后，您将把这些模板作为 CloudFormation 堆栈的定义上传到中为加速`aws_managedservices_onboarding_role`CloudFormation 而创作。

为加速**`aws_managedservices_onboarding_role`**CloudFormation 而创作

您可以 CloudFormation 从中创建 AWS Identity and Access Management 角色 AWS 管理控制台。`aws_managedservices_onboarding_role`或者，您可以使用中的命令 AWS CloudShell 来部署角色。

使用 AWS 管理控制台

> **Note**
>
> 开始之前，请准备好每个角色的 JSON 或 YAML 文件以供上传。有关更多信息，请参阅 创建 AMS 角色的模板。

要从中创建角色 AWS 管理控制台，请完成以下步骤：

1. 登录 AWS 管理控制台 并在 https://console.aws.amazon.com/cloudformat ion 上打开 CloudFormation 控制台。

2. 选择创建堆栈 > 使用新资源（标准）。您将看到以下页面。

3. 选择上传模板文件，上传 IAM 角色的 JSON 或 YAML 文件，然后选择下一步。您将看到以下页面。

4. 在堆栈名称字段中输入堆栈名称 **`ams-onboarding-role`** “”。DateOfExpiry使用 “YYYY-MM-DDT 00:00:00 Z” 格式输入 a（建议自当前日期起 30 天）。继续向下滚动并选择 “下一步”，直到到达此页面：

5. 确保选中该复选框，然后选择创建堆栈。
6. 确保堆栈已成功创建。

使用来自的命令 AWS CloudShell

要部署 `aws_managedservices_onboarding_role` IAM 角色，请在中运行以下命令 AWS CloudShell：

AWS CLI

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/
samples/onboarding_role_minimal.zip" -o "onboarding_role_minimal.zip"
unzip -q -o onboarding_role_minimal.zip
aws cloudformation create-stack \
    --stack-name "aws-managedservices-onboarding-role" \
    --capabilities CAPABILITY_NAMED_IAM \
    --template-body file://onboarding_role_minimal.json \
    --parameters ParameterKey=DateOfExpiry,ParameterValue="`date -d '+30 days' -u '+
%Y-%m-%dT%H:%M:%SZ'`"
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/
latest/accelerate-guide/samples/onboarding_role_minimal.zip' -OutFile
 'onboarding_role_minimal.zip'
Expand-Archive -Path 'onboarding_role_minimal.zip' -DestinationPath . -Force
```

```
New-CFNStack `
    -StackName 'aws-managedservices-onboarding-role' `
    -Capability CAPABILITY_NAMED_IAM `
    -TemplateBody (Get-Content 'onboarding_role_minimal.json' -Raw) `
    -Parameter @{ParameterKey = "DateOfExpiry"; ParameterValue = (Get-
Date).AddDays(30).ToString('yyyy-MM-ddTHH:mm:ssZ')}
```

创建角色后，请与您的云架构师 (CA) 合作完成该第 2 步：Accelerate 中的入职管理资源过程。在 AMS 通知您您的账户处于活动状态后，您就可以启动实例了。

第 3 步：使用默认策略加载 AMS 功能

在此阶段，您将使用默认策略加载 AMS 功能。其中包括添加 Amazon EC2 实例，以及根据您的偏好配置监控、备份、 AWS Config 修复和补丁（如果适用，AMS Patch Orchestrator 是您必须特别申请的附加组件）。你可以自己动手，也可以根据你的输入请求 AMS 上线功能。要向 AMS 请求帮助，请创建服务请求并提供所有必需的输入以完成任务。请记住，服务请求不会立即得到解决。

> **Note**
>
> 虽然账户可能使用默认策略进行备份、补丁或监控，但需要对资源进行标记才能使相应的策略生效。

主题

- （可选）加速中的快速入门模板
- 入职加速监控
- 加载 EC2 实例以加速
- 在“加速” AWS Backup 中入职
- Accelerate 中的入门补丁
- 在“加速”中查看不合格报告

（可选）加速中的快速入门模板

快速入门模板可在启用加速 AWS 功能的账户中自动部署和配置 AMS 资源标记器。与手动设置相比，此模板可以节省时间和精力。按原样使用此模板在一个账户中定义监控、修补和备份基础知识。或者，将其用作在 Organi StackSet zations Units 中应用设置，以标准化多个账户的设置。

您也可以将其作为起点来构建自己的自定义 AMS 资源标记器配置文件，并使用文档中的片段来创建更复杂的标签定义。

快速入门模板功能

快速入门模板可完成以下任务：

- 为 AMS 资源标记器创建和部署配置版本。
- 将标签应用于启用 AMS 管理和创建监控资源的 Amazon EC2 实例。
- （可选）将标签应用于托管 EC2 实例，使它们能够按所需的计划进行修补，并创建修补维护窗口以方便修补。

> **Warning**
>
> 默认情况下，实例会重启并自动启动已停止的实例以安装补丁。

- （可选）将标签应用于托管 EC2 实例，使它们能够按照默认 AMS 备份计划中的定义进行备份。
- （可选）将标签应用于托管的 Amazon Relational Database Service (Amazon RDS) 资源，以便根据增强型备份计划对其进行备份。备份计划还支持 Amazon RDS 的时间点恢复 (PITR)。如果未启用 Amazon RDS 自动备份，则数据库将在接近下一个备份窗口的时间点重新启动。

快速入门模板覆盖和排除项

使用此模板创建快速入门堆栈后，请使用以下步骤将特定实例排除在管理/监控、修补或备份之外：

- 管理和监控：要将 EC2 实例排除在 AMS 管理和监控之外，请将此标签添加到该实例：`ExcludeFromAMSQuickStartMonitoring=true`。
- 修补：此快速入门模板将属于 Auto Scaling 组、亚马逊弹性容器服务或亚马逊弹性 Kubernetes Service 集群成员的 EC2 实例排除在修补范围之外。

  要禁用创建修补窗口和对 EC2 实例进行与补丁相关的标记，请将堆栈参数设置为。 CloudFormation `EnablePatching=false`

  要将某个 EC2 实例排除在快速启动修补窗口的目标之外`EnablePatching=true`，请将此标签添加到该实例:`ExcludeFromAMSQuickStartPatching=true`.
- 备份：此快速入门模板将作为 Auto Scaling 组、ECS 或 EKS 集群成员的 EC2 实例排除在备份之外。

要将某个 EC2 实例排除在默认 AMS Backup 计划的目标之外`EnableBackup=true`，请在该实例中添加以下标签：`ExcludeFromAMSQuickStartBackup=true`。

> **Tip**
>
> 您可以批量标记 EC2 实例。使用标签编辑器在一个步骤中批量选择和标记资源。 AWS 管理控制台

快速入门模板参数

此快速入门模板将 Resource Tagger 配置为将标签`ams:rt:ams-managed=true`添加到账户中的所有 EC2 实例，不包括您向其添加`ExcludeFromAMSQuickStartMonitoring=true`标签的实例。根据您的要求使用以下参数来控制此堆栈的可选部分：

CFN 参数	值	效果
EnableBackup	'true'（默认）	根据默认 AMS 备份计划，所有 AMS 管理的 EC2 实例 (`ams:rt:ams-managed=true`) 都标记`ams:rt:backup-orchestrator=true` 为每天凌晨 4 点（世界标准时间）进行备份。 对于所有 RDS 实例和集群，根据增强型备份计划，该模板将应用具有最大保留期（31 天）的 `ams:rt:backup-orchestrator-enhanced=true` “持续备份”。 如果这更改了您的 PITR 保留期，则在某些情况下可能会重新启动数据库，例如，如果还有其他待处理的配置更新。

CFN 参数	值	效果
	'false'	此快速入门模板未将任何实例作为备份目标。
EnablePatching	'false'（默认）	此快速入门模板未针对任何实例进行修补。
	'是的'	所有 AMS 管理的实例 (`ams:rt:ams-managed=true`) 都标有，`ams:rt:Patch Group=AMS QuickStartPatchWindow` 并且会创建基本的 SSM 维护窗口资源，以便根据中定义的时间表进行修补。`CronExpression` 要将`ams:rt:Patch Group` 标签应用于 EC2 实例，您必须关闭对该实例的实例元数据中标签的访问权限。
CronExpression	-	的默认值根据`Timezone`参数将每月的第二个星期六`cron(0 30 19 ? * SAT#2 *)`设置为晚上 7:30。使用 cron 语法。
时区	-	目标实例的修补程序是根据`CronExpression` 的。使用 IANA 格式。

下载快速入门模板

下载 AMSQuickStart.zip 文件。

或者，在中运行以下命令AWS CloudShell来部署`AMSQuickStart.yaml`：

AWS Command Line Interface

```
curl -s "https://docs.aws.amazon.com/en_us/managedservices/latest/accelerate-guide/samples/AMSQuickStart.zip" -o "AMSQuickStart.zip"
```

```
unzip -q -o AMSQuickStart.zip
for region in region1 region2 ;
do
aws cloudformation create-stack \
    --region $region \
    --stack-name "AMSQuickStart" \
    --template-body file://AMSQuickStart.yaml \
    --parameters \
        ParameterKey=EnableBackup,ParameterValue="true" \
        ParameterKey=EnablePatching,ParameterValue="false" \
        ParameterKey=Timezone,ParameterValue="US/Eastern" \
        ParameterKey=CronExpression,ParameterValue="cron(0 30 19 ? * SAT#2 *)" \
;
done
```

AWS Tools for PowerShell

```
Invoke-WebRequest -Uri 'https://docs.aws.amazon.com/en_us/managedservices/latest/
accelerate-guide/samples/AMSQuickStart.zip' -OutFile 'AMSQuickStart.zip'
Expand-Archive -Path 'AMSQuickStart.zip' -DestinationPath . -Force
@('region1', 'region2') | `
ForEach-Object { `
New-CFNStack `
    -Region $_ `
    -StackName 'AMSQuickStart' `
    -TemplateBody (Get-Content 'AMSQuickStart.yaml' -Raw) `
    -Parameter @(
        @{ParameterKey = "EnableBackup"; ParameterValue = "true"},
        @{ParameterKey = "EnablePatching"; ParameterValue = "false"},
        @{ParameterKey = "Timezone"; ParameterValue = "US/Eastern"},
        @{ParameterKey = "CronExpression"; ParameterValue = "cron(0 30 19 ? * SAT#2
 *)"}
    )
}
```

有关每个参数的描述，请参阅前一节快速入门模板参数。

入职加速监控

默认情况下，除了 Amazon EC2 实例外，所有新资源都启用了监控。您可以通过标记您的 EC2 实例来开始监控您的 Amazon 实例。

要进行入门监控，首先要确保您的配置监控您希望 AMS 监控的资源，并忽略您希望它忽略的资源。

您可以使用以下 CloudWatch 仪表板来探索有多少资源是 AMS 监控和标记的目标，以及有多少不是目标资源。在您的账户中，导航到控制 CloudWatch 面板控制台，然后选择以下选项之一：

- AMS 警报管理器报告控制面板
- AMS 资源标记器报告控制面板

有关控制面板指标的完整说明，请参阅：

- 查看警报管理器监控的加速资源数量
- 查看资源标记器管理的资源数量

要在 Accelerate 中监控入职资源

例如，要覆盖默认行为，禁用对非EC2 资源的默认监控，您需要使用自定义配置文件取消对这些资源的标记。有关为监控添加标签的更多信息，请参阅加速中的监控。

在您注册 EC2 实例之前，实例的监控将处于禁用状态，包括使用自定义配置文件标记您的实例。下一节将介绍 EC2 实例加载。

在 Accelerate 中创建监控配置文件

- 有关使用默认配置的信息，请参见加速警报管理器。
- 有关使用自定义配置的信息，请参阅修改加速警报默认配置。

加载 EC2 实例以加速

EC2 实例通过名为 “自动实例配置” 的过程加入 AMS Accelerate，该过程可确保每个实例写入正确的日志并发出正确的指标，让 AMS 正确管理实例。除非你特别希望 AMS 忽略一些 EC2 实例，否则你应该加入所有实例。自动实例配置要求满足允许 AMS 配置实例的特定条件（有关详细信息，请参阅加速中自动配置实例的先决条件）。最重要的条件是，需要在您希望 AMS 为您管理的每个 Amazon EC2 实例上安装代 AWS Systems Manager 理（SSM 代理）。有关 SSM 代理的更多信息，请参阅使用 SSM 代理。

标准版中预装了 SSM，用于加速 AMIs

已在为以下操作系统 AWS提供的 AMIs 上安装了 SSM 代理。

- Amazon Linux 和 Amazon Linux 2
- SUSE Linux 企业服务器 (SLES) 12 和 15
- 微软 Windows Server 2019、2016、2012 R2、2012
- Ubuntu Linux 18.04 和 20.04

如果您使用的是 AWS提供的其中一个 AMIs，请参阅在加速中标记实例。

在 Accelerate 中手动 SSM 安装 SSM

对于以下操作系统或使用自定义 AMI 时，您可以手动安装 SSM 代理。或者，您可以使用 AMS SSM Agent 自动安装功能。要了解有关 SSM auto 安装的更多信息，请参阅SSM 代理自动安装。有关手动安装的说明，请选择与您的操作系统对应的链接：

- CentOS SSM 安装
- 安装甲骨文 SSM
- 安装红帽 SSM
- SUSE Linux 企业服务器 SSM 安装
- 安装 Windows SSM

在加速中标记实例

安装 SSM 代理后，您必须标记您的实例。请参阅在 AMS 中添加标签加速。

在 “加速” 中自动配置实例

您的实例被标记后，AMS 会执行自动实例配置，其中包括：

- 记录操作系统日志和指标
- 为 AMS 工程师启用远程访问
- 在实例上执行远程命令

这些任务对于 AMS 监控、补丁和日志服务以及 AMS 响应事件至关重要。有关设置自动实例配置的详细信息，请参阅AMS Accelerate 中的自动实例配置。

自动实例配置完成后，您能够：

- 使用 Support Center 控制台为 Amazon EC2 实例和操作系统创建事件和服务请求。有关更多信息，请参阅 AMS Accelerate 中的事件报告、服务请求和账单问题。
- 访问和审计 Amazon EC2 日志
- 获取补丁报告

在 “加速” AWS Backup 中入职

要配置备份，您需要创建名为备份计划的备份策略。备份计划指定要备份哪些 AWS 资源、需要备份的频率以及备份保留期。我们建议评估贵组织的连续性、安全性和合规性要求，以确定您需要哪些备份计划。

选择加入

- 请按照以下步骤确保 AWS Backup 为每个账户、区域和资源类型启用该功能：

  入门 1：服务选择加入。

  （可选）入门 2：在按需备份上创建。

选择备份计划

- 要选择备份计划，请参阅选择 AMS 备份计划。

添加资源

默认情况下，资源不与备份计划关联。它们需要添加到备份计划中。

- 要向备份计划添加资源，请参阅标记您的资源以应用 AMS 备份计划。
- 要使用标签对所有资源启用备份，请参阅在 “加速” 中管理备份标签。

Accelerate 中的入门补丁

您需要配置补丁以确保您的软件符合 up-to-date并符合您的合规性策略。

AWS Backup 先决条件：要允许在修补维护时段内创建根卷快照，请按照以下步骤确保 AWS Backup 为 Amazon EBS 资源类型的每个账户和区域启用该快照：入门 1：服务选择加入。（您无需继续 “入门 2：创建按需备份”。）

何时修补：在维护时段内进行修补。您可以安排维护时段，以便仅在预设时间内应用补丁。

要修补的内容：您必须将要修补的 Amazon EC2 实例与维护时段相关联。要将实例与维护时段关联，必须对 Amazon EC2 实例进行标记，并且维护时段应将这些标签作为目标。

要安装哪些补丁：使用补丁基准，您可以设置规则以自动批准某些类型的补丁，例如操作系统或高严重性补丁。您还可以指定规则的例外情况，例如，列出始终被批准或拒绝的补丁列表。

有关亚马逊 EC2 补丁政策的指导，请参阅修补建议。

- 要开始配置补丁管理，请参见 了解 AMS Accerate 中的补丁管理
- 要创建自定义补丁配置，请参阅使用 AMS Accelerate 自定义补丁。

在 “加速” 中查看不合格报告

AMS 部署的 AWS Config 规则可帮助您识别违反互联网安全中心 (CIS)、美国国家标准与技术研究院 (NIST) 云安全框架 (CSF) 制定的标准的行为。我们建议您与交付团队一起查看不合格报告，确定补救措施的优先顺序，以便将您的账户设定为合规状态。

第 4 步：在 “加速” 中自定义功能

在此阶段，您已经开始使用默认策略进行监控、修补和备份。现在，您有机会自定义策略以满足您的需求。

您可以选择使用默认策略进行修补、备份或监控，也可以根据需要选择自定义策略。AMS 使用标签将资源与运营策略相关联。AMS 提供了资源标记器，允许您根据应用程序分组或其他分组逻辑指定如何将标签应用于 AWS 资源的规则。有关更多信息，请参阅加速资源标记器。

客户提供的标签功能允许您向 AMS 资源添加和删除自定义标签。有关更多信息，请参阅 Accelerate 中客户提供的标签。

主题

- 在 “加速” 中自定义监控
- 在 “加速” 中自定义备份
- 在 “加速” 中自定义补丁

在 “加速” 中自定义监控

要根据应用程序需求自定义对云资源的监控，请执行以下操作：

1. 创建自定义监控策略。请参阅修改加速警报默认配置。

2. 使用标签对资源应用自定义策略。请参阅 加速中的监控。
3. 将警报发送给资源所有者。请参阅基于标签的警报通知。

您可以使用以下 CloudWatch 仪表板来探索有多少资源是 AMS 监控和标记的目标，以及有多少不是目标资源。在您的账户中，导航到控制 CloudWatch 面板控制台，然后选择以下选项之一：

- AMS 警报管理器报告控制面板
- AMS 资源标记器报告控制面板

有关控制面板指标的完整说明，请参阅：

- 查看警报管理器监控的加速资源数量
- 查看资源标记器管理的资源数量

在 “加速” 中自定义备份

您无法自定义 AMS 默认备份计划。取而代之的是，根据您的应用程序需求创建新的备份计划，然后使用标签将资源附加到您的自定义计划中。AMS 应备份哪些资源、备份频率以及保留期限由您自己决定。我们建议评估贵组织的连续性、安全性和合规性要求，以确定您需要哪些备份计划。

- 要创建备份计划，请参阅创建备份计划。
- 要为备份计划分配资源，请参阅为备份计划分配资源。

在 “加速” 中自定义补丁

修补可确保您的软件符合 up-to-date并符合您的合规性政策。

何时修补：在维护时段内进行修补。您可以安排维护时段，以便仅在预设时间内应用补丁。

要修补的内容：您必须将要修补的 Amazon EC2 实例与维护时段相关联。要将实例与维护时段关联，必须对 Amazon EC2 实例进行标记，并且维护时段应将这些标签作为目标。

要安装哪些补丁：使用补丁基准，您可以设置规则以自动批准某些类型的补丁，例如操作系统或高严重性补丁。您还可以指定规则的例外情况，例如，列出始终被批准或拒绝的补丁列表。

- 有关一般的修补建议，请参见修补建议。
- 要创建自定义维护时段，请参阅在 AMS 中创建补丁维护窗口。

- 要创建自定义补丁基准，请参阅使用 AMS Accelerate 自定义补丁。
- 要将补丁警报发送给资源所有者，请参阅了解 AMS Accelerate 中的补丁通知和补丁故障。

使用 AMS 控制台

AWS 管理控制台中的 AMS 控制台可供您与 AMS 交互并操作您的 AMS Advanced 管理资源和 AMS Accelerate 资源。AMS 控制台的行为通常与任何 AWS 主机类似；但是，由于 AMS 是私人组织，因此只有启用 AMS 的账户才能访问控制台。在您的账户中启用 AMS 后，您可以通过在统一搜索栏中搜索 “Managed Services” 来访问控制台。

> **Note**
>
> 根据您的账户角色，您可以访问 AMS 高级控制台或 AMS Accelerate 控制台。

使用 AMS 主机时，请注意以下注意事项：

- AMS 控制台是特定于账户的。因此，如果您使用的是组织的 “测试” 帐户，则无法在该组织的 “Prod” 帐户中查看资源。同样，您必须拥有 AMS 高级角色才能访问 AMS 高级控制台。
- 在您进行身份验证时，AMS 控制台会应用 IAM 策略，该策略决定了您可以访问哪个控制台以及可以在那里做什么。您的管理员可以对默认 AMS 策略应用其他策略，以限制您在控制台中可以看到和执行的操作。

AMS 加速控制台具有以下功能：

- 打开页面：开头页面包含信息框和链接，便于您访问事件、服务请求和报告。
- 专题页面，左侧导航窗格中的链接：
  - 控制面板：概述您的账户当前状态，包括：
    - 您的资源上的事件：用于在 AWS Support Center 中打开事件案例的按钮，以及有多少事件案例正在等待批准并需要您关注，以及有多少已处理的事件案例
    - 合规性状态：指向不合规或合规的规则和资源的链接
    - 服务请求：用于在 AWS Support Center 中打开服务请求案例的按钮，以及有多少请求正在等待批准并需要您注意以及有多少已处理中
    - 账户级安全：实时威胁检测 GuardDuty 结果以及数据安全和隐私 Macie 调查结果的详细信息链接

    - 快速操作：打开 Backup 保管库或 Patch 实例配置页面
  - 报告：打开 “报告” 页面和默认报告、“每日备份”、“每日补丁” 和 “每月账单”
  - 配置：确保按照您的规格成功管理您的资源。
    - 安装 SSM 代理：需要 SSM 代理
    - 配置标记规则：打开 AMS 资源标记器
    - 配置警报：打开 AMS CloudWatch 警报配置
    - 配置补丁计划：打开 AWS Systems Manager 控制台
    - 配置补丁基准：打开 AWS 补丁管理器控制台
    - 配置备份计划：打开 AWS Backup 控制台
- 功能聚焦：有关主机最新更新的信息
- 文档：AWS Managed Services 文档登录页面

AMS 模式

AWS Managed Services (AMS) 模式是一种通用解决方案，可解决 AMS 托管环境中的一系列用例。

当您在 AMS 平台上运营时，AMS 云架构师 (CAs) 会与您合作以满足您的业务和运营需求。虽然 AMS 客户以独特的方式运营，但我们注意到客户也有类似的用例。在这种情况下，只需最少的配置和部署工作即可 CAs 创建用于多个客户环境的通用解决方案模板或 “模式”。

AMS 模式旨在帮助向 AMS 客户提供功能，通常由提出请求的客户的账户 CA 构建。

AMS 模式的工作原理

要请求有关每种模式的更多详细信息，包括部署模式所需的 cloudformation 模板，请提交 AMS 服务请求，主题为 “请求提供有关模式的更多详细信息*Pattern_Name*”（替换所需的模式），然后将您的 AMS 云架构师 (CA) 添加到 “其他联系人” 选项中。

AMS 模式可分为两 (2) 类：

- 一般用途：模式被认为是稳定的，因为它们已被多个 AMS 客户部署和使用
- 预览模式：AMS 建议在非生产环境中部署预览模式以进行验证，并在部署前与您的云架构师讨论用例。

> **Important**
>
> AMS 模式不符合您的默认 AMS 服务级别协议服务级别协议 (SLAs) 和服务级别目标 (SLOs)。该模式的 Support 和更新是在尽力而为的基础上完成的。
> 本 AWS 内容的提供受AWS 客户协议的条款或客户与亚马逊网络服务公司或亚马逊网络服务 EMEA Sarl（“AWS 欧洲”）或两者之间的其他书面协议的约束。
> 本软件中包含的材料按“原样”提供给您，不提供任何明示、暗示或其他形式的担保，包括但不限于对特定目的的适用性的任何担保。

AMS 模式

AMS 模式。

AMS 模式

名称	概览	优势	类别
自定义 CloudWatch 警报通知	自定义 CloudWatch 警报通知以包含来自实例标签的信息，例如实例名称、应用程序 ID 等。	在警报通知中添加上下文信息将使警报更有意义，并提供可操作的信息。	监控
磁盘使用情况报告	磁盘使用情况报告模式收集多个应用程序账户的卷消耗空间，并通过 Athena 表查询功能在 Amazon S3 中以集中报告形式呈现结果。	深入了解账户量的实际使用情况，以确定节省成本的机会。	成本优化
Prowler Stack	对无法使用亚马逊 EC2 的账户进行 Prowler 检查。CloudShell	如果由于权限或超时问题而 CloudShell 无法使用，而不会对他们当前的安全状况产生任何影响，请	安全性

名称	概览	优势	类别
		帮助解除对加速入门 (Prowler) 的封锁。	
使用自定义对象密钥进行 AMS Amazon S3 复制	复制 Amazon S3 数据元并保留所有元数据和对象密钥（文件夹）。 删除部分源对象密钥，或者在复制过程中创建自定义目标对象密钥。	在 Amazon S3 复制期间自定义对象密钥（文件夹），无需其他脚本即可将对象移动到所需的文件夹。	可靠性
亚马逊 EBS 快照删除	基于 Lambda 和 CloudWatch 事件的自动化，可根据保留期 AWS Backup自动删除在外部拍摄的 Amazon EBS 快照。	帮助清除在 AWS Backup Orchestrator 之外拍摄的单个快照，随着时间的推移节省额外成本。	成本优化
AMS 亚马逊 RDS 密钥轮换	使用 CloudFormation 模板，自动部署支持的 Amazon RDS 数据库、Redshift 和 DocumentDB 轮换密钥所需的所有必需资源（Lambda 函数、安全组、弹性网络接口或 ENIs）。	自动轮换数据库密钥，并在轮换失败时提供通知机制。	安全性
自动密钥轮换	根据 CloudWatch 事件和 Lambda 自动轮换 IAM 用户的访问权限和密钥。	更轻松地轮换 IAM 用户的访问权限和密钥。	安全性

名称	概览	优势	类别
Amazon EBS 卷快照标记器	使用亚马逊 EC2 实例中的标签标记所有 Amazon EBS 卷和快照。	利用有意义的相关业务信息，帮助对成本进行分类和跟踪，从而更轻松地验证资金花在了哪里，并允许对带标签的卷和快照使用自动化。 AWS 成本优化支柱强烈推荐的最佳实践。	标记（成本优化、安全、事件管理和自动化）

AMS Accelerate 中的自动实例配置

AMS Accelerate 提供自动实例配置服务。该服务可确保实例发出正确的日志和指标，以便 AMS 正确管理该实例。自动实例配置有自己的先决条件和入门步骤，本节后面将对此进行介绍。

主题

自动实例配置在 Accelerate 中的工作原理

自动实例配置使 AMS Accelerate 能够每天对您通过添加特定代理和标签指定的实例执行某些配置。

加速中自动配置实例的先决条件

必须满足这些条件才能让 AMS Accelerate 对托管实例执行前面描述的自动操作。

SSM 代理已安装

AMS Accelerate 自动实例配置需要安装 AWS Systems Manager SSM 代理。

有关使用 AMS SSM Agent 自动安装功能的信息，请参阅SSM 代理自动安装。

有关手动安装 SSM 代理的信息，请参阅以下内容：

- Linux：在适用于 Linux 的亚马逊 EC2 实例上手动安装 SSM 代理- AWS Systems Manager
- Windows：在适用于 Windows 服务器的亚马逊 EC2 实例上手动安装 SSM 代理- AWS Systems Manager

SSM 代理处于托管状态

AMS 加速自动实例配置需要可运行的 SSM 代理。必须安装 SSM 代理，并且 Amazon EC2 实例必须处于托管状态。有关更多信息，请参阅 AWS 文档 “使用 SSM 代理”。

自动设置实例配置

假设已满足先决条件，则添加特定的 Amazon EC2 实例标签会自动启动 AMS Accelerate 自动实例配置。使用以下方法之一来添加此标签：

1. （强烈推荐）使用 AMS 加速资源标记器

   要为您的账户配置标签逻辑，请参阅标记的工作原理。标记完成后，将自动处理标签和自动实例配置。

2. 手动添加标签

   手动将以下标签添加到 Amazon EC2 实例：

   密钥：ams: rt: ams-managed，值：tr ue。

> **Note**
>
> 将 ams: rt: ams-managed 标签应用于实例后，实例配置服务会尝试应用所需的 AMS 配置。每当实例启动以及进行 AMS 每日配置检查时，该服务都会断言 AMS 所需的配置。

SSM 代理自动安装

要让 AMS 管理您的亚马逊弹性计算云 (Amazon EC2) 实例，您必须在每个实例上安装 AWS Systems Manager SSM 代理。如果您的实例未安装 SSM 代理，则可以使用 AMS SSM 代理自动安装功能。

> **Note**
>
> - 如果您的账户在 2024 年 3 月 6 日之后加入 AMS Accelerate，则此功能默认处于启用状态。要关闭此功能，请联系您的 CA 或 CSDM。
> - 要在 2024 年 3 月 6 日之前注册的账户中启用此功能，请联系您的 CA 或 CSDM。
> - 此功能仅适用于不在 Auto Scaling 组中且运行 AMS 支持的 Linux 操作系统的 EC2 实例。

使用 SSM 代理的先决条件

- 确保与目标实例关联的实例配置文件具有以下策略之一（或许可名单中的等效权限）：
  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- 确保没有明确拒绝上述策略中 AWS Organizations 列出的权限的服务控制策略。

  有关更多信息，请参阅配置 Systems Manager 所需的实例权限。
- 要阻止出站流量，请确保在目标实例所在的 VPC 上启用以下接口终端节点（相应地替换 URL 中的“区域”）：
  - ssm.<region>.amazonaws.com
  - ssmmessages.<region>.amazonaws.com
  - ec2messages。 <region>.amazonaws.co

  有关更多信息，请参阅使用适用于 Systems Manager 的 VPC 终端节点来提高 EC2 实例的安全性。

有关启用托管节点可用性或对其进行故障排除的一般提示，请参阅解决方案 2：验证是否已为实例指定了 IAM 实例配置文件（仅限EC2 实例）。

> **Note**
>
> 作为自动安装过程的一部分，AMS 会停止和启动每个实例。当实例停止时，存储在实例存储卷中的数据和存储在 RAM 上的数据都将丢失。有关更多信息，请参阅停止实例时会发生什么。

请求在您的实例上自动安装 SSM 代理

如果您的账户已加入 AMS Accelerate 补丁插件，请为实例配置补丁维护窗口 (MW)。需要一个能正常运行的 SSM 代理才能完成修补过程。如果实例上缺少 SSM 代理，AMS 会尝试在补丁维护时段内自动安装该代理。

> **Note**
>
> 作为自动安装过程的一部分，AMS 会停止和启动每个实例。当实例停止时，存储在实例存储卷中的数据和存储在 RAM 上的数据都将丢失。有关更多信息，请参阅停止实例时会发生什么。

SSM 代理自动安装的工作原理

AMS 使用 EC2 用户数据在您的实例上运行安装脚本。要添加用户数据脚本并在您的实例上运行该脚本，AMS 必须停止并启动每个实例。

如果您的实例已有用户数据脚本，则 AMS 将在自动安装过程中完成以下步骤：

1. 创建现有用户数据脚本的备份。
2. 用 SSM 代理安装脚本替换现有的用户数据脚本。
3. 重启实例以安装 SSM 代理。
4. 停止实例并恢复原始脚本。
5. 使用原始脚本重启实例。

自动更改实例配置

AMS Accelerate 实例配置自动化会在您的账户中进行以下更改：

1. IAM 权限

   添加授予实例使用由 AMS Accelerate 安装的代理的权限所需的 IAM 托管策略。
2. 座席
   a. Amazon CloudWatch 代理负责发布操作系统日志和指标。实例配置自动化可确保 CloudWatch 代理已安装并运行 AMS Accelerate 最低版本。
   b. AWS Systems Manager SSM 代理负责在实例上运行远程命令。实例配置自动化可确保 SSM 代理运行 AMS Accelerate 最低版本。

3. CloudWatch 配置

   a. 为了确保发出所需的指标和日志，AMS Accelerate 对配置进行了自定义。 CloudWatch 有关更多信息，请参阅CloudWatch 配置变更详情一节。

自动实例配置会更改或添加您的 IAM 实例配置文件和 CloudWatch 配置。

IAM 权限变更详情

每个托管实例必须有一个包含以下托管策略的 AWS Identity and Access Management 角色：

- arn: aws: iam:: aws: Policy/Amazon SSMManaged InstanceCore
- arn: aws: iam:: aws: policy/ CloudWatchAgentServerPolicy
- arn: aws: iam:: aws: policy/ AMSInstance ProfileBasePolicy

前两个是 AWS托管策略。AMS 管理的策略是：

AMSInstanceProfileBasePolicy

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:CreateSecret",
                "secretsmanager:UpdateSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:*:*:secret:/ams/byoa/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "*"
            ],
```

```
            "Effect": "Allow"
        }
    ]
}
```

如果您的实例已经附加了 IAM 角色，但缺少这些策略中的任何一个，那么 AMS 会将缺少的策略添加到您的 IAM 角色中。如果您的实例没有 IAM 角色，则 AMS 会附加该 AMSOSConfigurationCustomerInstanceProfileIAM 角色。AMSOSConfigurationCustomerInstanceProfileIAM 角色具有 AMS Accelerate 所需的所有策略。

> **Note**
>
> 如果达到 10 的默认实例配置文件限制，则 AMS 会将限制增加到 20，以便可以附加所需的实例配置文件。

CloudWatch 配置变更详情

有关 CloudWatch 配置的更多详细信息。

- CloudWatch 实例上的配置文件位置：
  - Windows：%ProgramData%\ Amazon\AmazonCloudWatchAgent\ amazon-cloudwatch-agent .json
  - Linux：/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/ams-加速配置.json
- CloudWatch 配置文件在 Amazon S3 中的位置：
  - Windows：https://ams-configuration-artifacts-*REGION_NAME* .s3。 *REGION_NAME*.amazonaws。com/configurations/cloudwatch/latest/windows-cloudwatch-config.j
  - Linux：https://ams-configuration-artifacts-*REGION_NAME* .s3。 *REGION_NAME*.amazonaws。com/configurations/cloudwatch/latest/linux-cloudwatch-config.j
- 收集的指标：
  - Windows:
    - AWS Systems Manager SSM 代理 (CPU_Usage)
    - CloudWatch 代理（CPU_Usage）
    - 所有磁盘的磁盘空间利用率（可用空间百分比）
    - 内存（已使用已提交字节的百分比）

- Linux：
  - AWS Systems Manager SSM 代理 (CPU_Usage)
  - CloudWatch 代理（CPU_Usage）
  - CPU（cpu_usage_idle、cpu_usage_iowait、cpu_usage_usage_user、cpu_usage_system）
  - 磁盘（已用百分比、inodes_used、inodes_total）
  - Diskio（io_time、write_bytes、read_bytes、写入、读取）
  - 内存（mem_used_percent）
  - 交换（交换使用百分比）
- 收集的日志：
  - Windows:
    - Amazon SSMAgent 日志
    - AmazonCloudWatchAgentLog
    - Amazon SSMError 日志
    - AmazonCloudFormationLog
    - ApplicationEventLog
    - EC2ConfigServiceEventLog
    - MicrosoftWindowsAppLockerEXEAndDLLEvent日志
    - MicrosoftWindowsAppLockerMSIAndScriptEventLog
    - MicrosoftWindowsGroupPolicyOperationalEventLog
    - SecurityEventLog
    - SystemEventLog
  - Linux：
    - /var/log/amazon/ssm/amazon-ssm-agent.log
    - /var/log/amazon/ssm/errors.log
    - /var/log/audit/audit.log
    - /var/log/cloud-init-output.log
    - /var/log/cloud-init.log
    - /var/log/cron
    - /var/log/dpkg.log
    - /var/log/maillog

- /var/log/messages
- /var/log/secure
- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

退出 AMS Accelerate

AMS Accelerate 提供了一种操作企业级操作环境的简便方法。而且，AMS Accelerate 为 AWS 迁移和使用提供了支持性基础设施运营模式。但是，在使用 AMS Accelerate 之后，您可能会决定将 AWS 基础设施运营职责内包或重新分配给其他团队。为此，您必须将您的账户从 AMS 服务中移除。

当您从 AMS Accelerate 注册账户时，AMS 会将我们的服务说明中定义的所有责任转还给您。例如，您将无法减少向 AMS 发送的事件或服务请求。同样，我们的运营工程师和自动化部门将无法再访问您的 Accelerate 账户，这使我们无法修复运行状况、可用性、安全性和合规性调查结果。您的 AWS 工作负载可以继续在 AMS 运营的相同账户中运行。

必须包括未来将执行基础设施运营服务的团队，以定义在Accelerate离职后将使用哪些人员、工具和流程。AMS 保留了一些 AMS 工具，例如护栏和日志，以便开发 “未来的” 操作环境和模型。请仔细阅读以下文档，了解您可以继续使用的工具以及如何申请退出账户。

AMS 加速下机效果

在准备退出 Accelerate 时，请记住以下注意事项。

- 访问权限：定义`ams-access-management` AWS Identity and Access Management 角色的`ams-access-management` CloudFormation 堆栈不会被删除。下线后，这些资源仍然存在，但留下的其他组件却无法使用。您可以随时删除堆栈和角色。
- AMS 资源保留：离职后，一些 AMS 资源仍保留在您的账户中。要查看保留了哪些资源以及您可以用它们做什么，请参阅`resource_inventory.zip`电子表格（压缩）。
- 自动化：下线后，AMS 策划的 AWS SSM 自动化运行手册和 AWS Lambda 函数将不再可用。
- 备份管理：AMS 使用备份管理来拍摄您的资源快照。离职后，您可以继续使用上定义的备份计划、频率和保留期，AMS 备份计划 AWS Backup 除外；请参阅选择 AMS 备份计划。AMS Backup Orchestrator 创建的 AWS Identity and Access Management 资源将被移除，但不会移除 AMS 创作

的备份保管库和相应的密钥。 AWS KMS Accelerate 不再监控备份任务或在事件发生期间执行恢复操作。

- 成本优化：下线后，AMS 资源调度器将被删除。AMS Resource Scheduler 可停止未使用的资源，并在需要容量时重新启动这些资源，从而帮助您降低运营成本。AMS 不再继续提供成本优化建议。有关资源调度器的详细信息，请参阅使用 AMS 资源调度器进行成本优化。
- 指定专家：离职后，您指定的云服务交付经理 (CSDM) 和云架构师 (CA) 将不再为您的离线 Accelerate 账户提供指导、报告或推动卓越运营和安全性。
- 事件管理：事件管理是 AMS 服务用来响应您报告的事件的流程。离职后，Accelerate 将不再检测和响应事件，也不会再协助您的团队解决问题。您将无法与 Accelerate 交换事件和服务请求通信，您的 Accelerate 账户的 Accelerate 控制台访问权限已停用。
- 日志和报告：退出后，您可以保留因 CloudWatch CloudTrail、和 VPC 流日志而存储的日志。您可以将这些服务的配置保持原样，以便继续生成日志；但是，AMS 不再监控此类配置。Accelerate 不再提供汇总 AMS 关键性能指标的月度服务报告。您可以保留通过自助服务报告 (SSR) 生成的数据（请参阅自助报告），但是 Accelerate 不会生成新的数据。
- 监控：监控是 AMS 服务用来跟踪您的资源的过程。在离职期间，AMS 会移除 AMS 特定的工具，例如警报管理器和资源标记器，以及 AMS 作为 AMS 监控基准的一部分部署的任何 EventBridge 事件规则和 CloudWatch 警报。下线后，Accelerate 将不再响应警报或配置新的警报。有关警报管理器和资源标记器的详细信息，请参阅基于标签的警报管理器和资源标记器。
- 操作工具：AMS Accelerate 可以为您在 AWS 中的工作负载基础设施提供持续运营。退出 Accelerate 账户后，您将无法再使用诸如资源标记器之类的工具来帮助您根据规则标记资源，也无法使用自动实例配置来在您的 EC2 实例中安装所需的代理。 CloudWatch 而且，实例上的 SSM 代理保留在现有配置中。`AMSOSConfigurationCustomer`IAM 配置文件和已从您的实例中分离并从您的 Accelerate 账户中删除。`InstanceRole``AMSInstanceProfileBasePolicy`
- 补丁管理：补丁管理是 AMS 服务用来更新 EC2 实例的流程。卸载后，AMS 不再在修补之前创建实例的快照，不再安装和监视补丁安装，也不会再将结果通知您。您可以保留过去创建的补丁基准和快照。此外，补丁维护窗口的配置仍然保留，但Accelerate不再安装补丁。
- 问题管理：离职后，Accelerate 不再执行分析以识别和调查问题以及确定根本原因。
- 安全：安全管理是 AMS 服务用来保护您的资源的流程。下线后，您可以保留您的 Amazon GuardDuty 探测器和发现结果以及您创建的所有 AWS Config 规则。 AWS Config Accelerate 部署的规则已删除。Accelerate 不再监控、补救或报告这些工具的调查结果。
- 服务终止日期：服务终止日期是必需的 30 天终止通知期结束后的日历月的最后一天。如果必要的终止通知期限在日历月的第20天之后，则服务终止日期为下一个日历月的最后一天。以下是终止日期的示例方案。

- 如果终止通知是在4月12日提供的，则为期30天的通知将于5月12日结束。服务终止日期为5月31日。
- 如果在4月29日发出终止通知，则为期30天的通知将于5月29日结束。服务终止日期为 6 月 30 日。

依赖警报管理器和资源标记器，从 AMS Accelerate 中脱颖而出

当您退出 AWS Managed Services 时，部署与警报管理器或资源标记器相关的配置的自定义 CloudFormation 堆栈以及 AMS 提供的警报管理器和资源标记器配置堆栈将保留在您的账户中。

要在离职过程中删除 AMS 配置堆栈，您必须先从自定义 CloudFormation 模板中移除 Alarm Manager 或 Resource Tagger 上的任何依赖关系和引用，然后再启动离线流程。删除引用有助于确保在您退出 AMS 时正确地从您的账户中删除堆栈。

> **Important**
>
> 在开始离职流程之前，请仔细检查您的 CloudFormation 模板并删除对警报管理器和资源标记器的所有引用。不这样做可能会导致这些堆栈保留在您的账户中，即使在您退出 AMS 之后也是如此。请注意，虽然这些堆栈包含 Alarm Manager 和 Resource Tagger 特有的配置信息，但它们的存在不会产生持续的费用或费用。

为 Accelerate 账户获取离职帮助

AMS 在收到至少 30 天的 AMS 账户服务终止请求通知后，将您的账户注销。服务终止日期是30天必要的终止通知期结束后的日历月的最后一天；前提是，如果必要的终止通知期的结束在日历月的第20天之后，则服务终止日期将是下一个日历月的最后一天。

要申请注销账户，您必须：

1. 使用服务请求提交正式申请，要求退出账户。一份服务请求 (SR)，记录您要退出的所有账户，或者每个账户一个 SR。

   在请求中，提供 IDs 要退出的账户列表、离职原因以及任何其他注意事项。
2. 告知您的 CSDM 您要退出的账户，并请求他们帮助执行离职流程。

加速中的通知设置

您和 AMS 之间的沟通有多种原因：

- 通过监控警报创建的事件
- 修补服务通知（如果您已选择加入修补程序）
- 服务请求和事件报告
- 不定期 AWS 发布重要公告（如果需要您采取任何行动，您的 CSDM 会与您联系）

所有通知均使用您在入职时为补丁通知提供的电子邮件发送。否则，通知将发送到您在入职时向 AMS 提供的默认电子邮件地址。由于很难保持单个电子邮件的更新，因此我们建议您使用可以随时更新的群组电子邮件。AMS 运营部门还会收到发送给您的所有通知，并在做出回复之前对其进行分析。

您可以使用已命名的联系人列表来发送非基于资源的通知，例如基于 GuardDuty 或 AWS Config 的警报。例如，您可能有一个名为`SecurityContacts`、另一个名为的列表`OperationsContacts`。AMS 向这些列表发送警报和通知。

有关更多信息，请参阅AWS Config 控制合规性报告。

在 AMS 中添加标签加速

大多数 Accelerate 功能（修补、备份、监控）都使用标签和配置文件来决定要管理哪些资源、应用哪些操作以及何时应用它们。标签是您应用于资源的标签。配置文件包含基于这些标签的规则。

每项加速功能都有自己的标记要求。有些功能要求您使用特定的标签，而另一些功能则允许您使用自己的任何标签。

有关所需标签的信息，请参阅Accelerate 中的客户管理标签。

有关可以定义为客户的标签的信息，请参阅 Accelerate 中客户提供的标签

目录

AMS 中的标签加速

目录

标签是什么？

标签是您分配给 AWS 资源的标签。每个标签都包含您定义的一个键和一个可选值。

您可以使用标签以不同的方式对 AWS 资源进行分类，例如按用途、所有者或环境进行分类。例如，您可以为账户的 Amazon EC2 实例定义一组标签，以帮助您跟踪每个实例的所有者和堆栈级别。

标签对 Amazon 没有任何语义意义 EC2 ，严格解释为字符串。

要了解更多信息，请参阅为AWS 资源添加标签。

标记的工作原理

有多种方法可以对您的资源应用标签。创建资源时，您可以直接在每项 AWS 服务的控制台中为资源添加 AWS 标签；使用标签编辑器为多个资源添加、移除或编辑标签；或者使用 CloudFormation 资源标签等配置工具。AMS Accelerate 还提供 AMS 加速资源标记器，您可以使用它来定义自动标签生命周期管理器的规则。有关在 AMS Accelerate 中使用资源标记器的信息，请参阅加速资源标记器。AMS Accelerate 还提供客户提供的标签，用于向您的 AMS 资源添加和删除自定义标签。有关客户提供的标签的更多信息，请参阅Accelerate 中客户提供的标签。

Accelerate 中的客户管理标签

需要某些标签才能触发各种 AMS 加速操作。

目录

加速中的监控

AMS Accelerate 监控支持的资源的运行状况、可用性和可靠性。有关此服务的更多信息，请参阅AMS Accelerate 中的监控和事件管理。

除了基线监控外，AMS 还会定期在机 AWS 服务 上加速。如果您使用 Resource Tagger 的默认配置，则这些更新会自动部署到您的账户，并且所做的更改会反映到支持的资源上。

要选择让 AMS Accelerate 管理您的 Amazon EC2 实例，您必须通过中的自定义配置文件应用以下标签 AppConfig；有关更多信息，请参阅步骤 3：创建配置和配置文件。

将以下标签应用于您的资源：

键	值
ams:rt:ams-managed	true

例如，您可以创建像这样的自定义配置文档，将标签应用于所有 AMS 支持的资源 EC2 ：

```
{
    "AWS::EC2::Instance": {
        "AllEC2": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Important

请记得在更改配置后再进行部署。在 SSM 中 AppConfig，您必须在创建配置后部署新版本的配置。

Amazon 以外的服务 EC2 将采用默认基准监控。要选择退出 AMS Accelerate 监控您的资源，您可以使用自定义配置文件来排除特定资源或 AWS 服务。这使您可以控制哪些资源应具有监控标签以部署基准警报定义。请参阅AMS Accelerate 中的资源标记器用例。

使用资源标记器

如果您应用这个标签（ams: rt: ams-managed），您的账户中的 AM S 加速资源标记器配置有助于确保自动部署以下标签。

您将看到以下标签已应用于您支持的基线监控资源。

键	值	规则
ams: rt: ams-monitoring-policy	ams 监控	适用于 AMS 支持的所有 EC2 资源

键	值	规则
ams: rt: ams-monitoring-policy-platform	ams-monitored-linux	适用于所有运行 Linux 操作系统的亚马逊 EC2 实例
ams: rt: ams-monitoring-policy-platform	ams-monitored-windows	适用于所有运行 Windows 操作系统的亚马逊 EC2 实例

对于其他支持的服务

根据给定的规则，将以下标签应用于您的资源：

键	值	规则
ams: rt: ams-monitoring-policy	ams 监控	适用于 AMS 加速监控支持的所有资源。
ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms	OpenSearch 使用 KMS 的域名
ams: rt: ams-monitoring-with-master	ams-monitored-with-master	OpenSearch 带有专用主节点的域

如果你没有使用资源标记器

在不使用资源标记器的情况下加速标签有关使用 AMS 资源标记器以外的方法应用正确监控标签的帮助，请参阅。

在 Accelerate 中为 EC2 实例配置标签

AMS Accelerate 管理您的 Amazon EC2 实例上的代理，例如 SSM 代理和 CloudWatch 代理。有关此服务的更多信息，请参阅 AMS Accelerate 中的自动实例配置

要选择让 AMS Accelerate 管理您的亚马逊 EC2 实例，您必须将以下标签应用于您的亚马逊 EC2 实例：

键	值
ams:rt:ams-managed	true

在 “加速” 中管理备份标签

AMS Accelerate 管理受支持资源的备份。有关此服务的更多信息，请参阅AMS 中的连续性管理加速。

AMS Accelerate 备份管理使用标签来识别应自动备份哪些资源（还提供手动备份功能）。您可以使用任何标签 key: value 组合将您的资源与备份计划相关联。要选择使用该ams-default-backup-plan AWS Backup 计划进行自动备份，您必须将以下标签应用于支持的资源：

键	值
ams:rt:backup-orchestrator	true

> **Note**
>
> 在入职期间，AMS Accelerate 使用 ams: rt: backup-orchestrator-onboarding 标记所有资源，其值为 true，用于短时间间隔、短保留期快照。这由ams-onboarding-backup-plan备份计划管理。有关 AMS Accelerate 托管 AWS Backup 计划的更多信息，请参阅。选择 AMS 备份计划

加速管理的标签

在加入 AMS Accelerate 期间，您的账户会部署多个 AWS 资源。因此，您可以识别它们，这些资源标有以下内容：

键	值
AMS: 资源所有者	AMS
ams: resourceOwnerService	提供此资源的哪个 AMS Accelerate 服务的描述来自于 AMS 部署、Backup、Controls、Monitors、Patch 等。

键	值
AppId	AMSInfrastructure
AppName	
Environment	

> **Note**
>
> 这些标签是使用 CloudFormation 堆栈级别的标签应用的，并且依赖于将标签 CloudFormation 传播到创建的资源。有关更多信息，请参阅资源标签。

Accelerate 中客户提供的标签

什么是客户提供的标签？

客户提供的标签是 AMS Accelerate 的一项服务功能，用于指定管理账户中如何标记 AMS 资源的规则。使用客户提供的标签，您可以向部署到您的账户的 AMS 资源添加用户定义的自定义标签。当您使用自动化服务向云服务交付管理器 (CSDM) 请求时，客户提供的标签功能会自动添加到请求的账户中。请注意，您无法覆盖 AMS 标签。AMS 标签以 “ams:” 开头。

您可以为所有 AMS Accelerate 资源定义自己的标签（标签）并指定这些标签的功能。您可以在加入 AMS 之前提供这些标签，以便在登机过程中应用 AMS 标签和您的自定义标签。或者，你可以在入职后提供标签。

如何添加客户提供的标签？

要请求在您的资源中添加这些标签，请联系您的 CSDM。这些标签将应用于您账户中的 AMS 资源。

标签的范围是什么？

此功能目前仅适用于加速客户和 AWS 商业区域。您可以为自己拥有的所有账户或特定的账户列表添加标签。

> **Note**
>
> 这些标签仅适用于 AMS 资源，不会影响您自己的资源。

用于加速的标签管理工具

内容

加速资源标记器

借助 Resource Tagger，您可以指定规则来管理账户中 AWS 资源的标记方式。在注册账户时，AMS Accelerate 会部署您的标签政策，以确保您的托管账户中的资源被标记。

目录

什么是资源标记器？

Resource Tagger 是一项 AMS Accelerate 服务，您可以使用它来指定规则来管理账户中 AWS 资源的标记方式。它旨在让你完全了解标签是如何应用于 AWS 资源的。

Resource Tagger 会根据您在配置文件中指定的标记规则，自动在支持的 AWS 资源上创建、更新和删除标签。例如，您可以指定一条规则，将标签应用于一组 Amazon EC2 实例，指示它们应由 AMS Accelerate 管理，从而监控或备份这些实例。您可以使用这样的标签根据 AWS AppConfig 配置文件中定义的策略来识别 AWS 资源的合规性状态。有关更多信息，请参阅 AWS AppConfig。

AMS Accelerate 提供默认的托管标签配置，因此您可以让 AMS Accelerate 监控您的资源。您可以定义哪些资源应由 AMS Accelerate 管理，托管标签规则可确保具有相应标签的资源受到 AMS Accelerate 的监控。

如果您愿意，您可以使用 Resource Tagger 覆盖或停用默认的 AMS Accelerate 托管标签，提供自己的标记规则以满足您的政策，并使用其他机制（例如 Terraform）来避免偏差。您可以根据自己的操作定义缩放的例外情况。例如，您可以定义策略，将标签应用于所有支持平台的亚马逊 EC2实例（例如 Windows 和 Linux），并排除对特定实例 IDs的标记。

> **Important**
>
> 资源标记器控制您账户中所有带有 ams: rt: 前缀的标签。所有以此前缀开头的标签都将被删除，除非它们存在于资源标记器的配置规则中。总而言之，任何以 ams: rt: 开头的受支持资源标签都被视为资源标记器所有。例如，如果您使用 ams: rt: 手动标记某些内容，则如果未在其中一个资源标记器配置配置文件中指定该标签，则该标签将被自动删除。

资源标记器的工作原理

当您的账户加入 AMS Accelerate 时，会将两个 JSON 配置文档部署到您的账户。 AWS AppConfig这两个文档称为配置配置文件，分别是 “AMSManaged标签”（称为默认配置文件）和 CustomerManagedTags“自定义配置文件”。您可以使用自定义配置文件为自己的账户定义自己的策略和规则，这些策略和规则不会被 AMS Accelerate 覆盖。

两个配置文件都驻留在 AMSResourceTagger 应用程序和AMSInfrastructure环境中。资源标记器应用的所有标签的密钥前缀均为 ams: rt:。

自定义配置文件：

账户注册时，自定义配置文件最初为空；但是，除了默认配置文件中的规则外，还会强制执行配置文件中放置的所有规则。自定义配置文件中的任何配置完全由您管理，除非您的请求，否则不会被 AMS Accelerate 覆盖。

您可以在支持的 AWS 资源的自定义配置文件中指定所需的任何自定义标记规则，也可以在此处指定对 AMS Accelerate 管理的默认配置的修改，请参阅。AMS Accelerate 中的资源标记器用例

> **Important**
>
> 如果您更新此配置文件，资源标记器会自动在您的所有相关资源中强制执行更改。 AWS 账户更改会自动生效，但最多可能需要 60 分钟才能生效。

您可以使用或通过 AWS CLI/SDK 工具更新此配置文件。 AWS 管理控制台有关更新自定义配置文件的信息，请参阅 AWS AppConfig 用户指南：什么是 AWS AppConfig？

默认配置文件：

默认配置文件文档位于 AMS Accelerate 内部，其中包含 AMS Accelerate 提供的默认规则，您无法永久修改或删除这些规则。AMS Accelerate 可以随时更新此个人资料并提供给您查看；您对其所做的任何更改都会自动删除。如果要修改或禁用任何默认配置规则，请使用自定义配置文件，请参阅AMS Accelerate 中的资源标记器用例。

AMS 中的资源标记器配置文件加速

配置文件有助于确保在资源的整个生命周期内将标签统一应用于资源。

语法和结构

配置文件是具有以下结构的 JSON 对象：

```
{
   "Options": {
      "ReadOnly": false
   },
   "ResourceType": {
      "ConfigurationID": {
      "Enabled": true,
      "Filter": { ... },
      "Tags": [  ...  ]
      },
```

```
      "ConfigurationID": {
      ...
      }
   },
   "ResourceType": {
     ...
   }
}
```

选项：（可选）指定您希望的行为方式 ResourceTagger 的选项。省略方块等同于将所有选项设置为其默认值。有关可用的选项设置，请参见下文：

- ReadOnly:（可选，默认为 false）：指定资源标记器的 ReadOnly 模式。设置 ReadOnly 为 true 可禁用资源标记器在 AWS 资源上创建或删除标签。有关更多信息，请参阅 阻止资源标记器修改资源。

ResourceType: 此密钥必须是以下支持的字符串之一，并且代表与所示资源类型相关的所有配置：

- AWS::AutoScaling::AutoScaling群组
- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::NatGateway
- AWS:EC2::: VPNConnection
- AWS::EFS::FileSystem
- AWS::EKS::Cluster
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::Elasticsearch::Domain
- AWS::FSx::FileSystem
- AWS::OpenSearch::Domain
- AWS:: RDS:: DBCluster
- AWS:: RDS:: DBInstance
- AWS::Redshift::Cluster
- AWS::S3::Bucket

- AWS::Synthetics::Canary

ConfigurationID：此密钥在配置文件文档中必须是唯一的，并且对以下配置块进行唯一命名。如果同一块中的两个配置ResourceType块具有相同的 C onfigurationId，则配置文件中最后出现的配置块生效。如果您在自定义配置文件中指定的 ConfigurationID 与默认文档中指定的配置文件相同，则自定义配置文件中定义的配置块将生效。

> **Important**
>
> ConfigurationID 应与 AMS Acceleration 配置文件***not***重叠；例如，它不应该是 AMSMonitoringLinux 或 AMSMonitoringWindows，否则它会禁用AMSManaged标签配置文件的相应配置。

启用（可选，默认为 true）：指定配置块是否生效。将其设置为 false 可禁用配置块。禁用的配置块不起作用。

筛选器：指定配置适用的资源。每个过滤器对象可以有以下任意一个（但只能有一个）字段：

- AWS::AutoScaling::AutoScaling群组:
  - AutoScalingGroupName: 自动扩缩组名称。此字段支持通配符匹配。
- AWS::DynamoDB::Table:
  - TableName: DynamoDB 表的名称。此字段支持通配符匹配。
- AWS::EC2::Instance:
  - AvailabilityZone：筛选条件匹配指定可用区中的 EC2 实例。此字段支持通配符匹配，因此 *a 匹配 us-east-1a、ap-northeast-1a 等。
  - InstanceId：筛选条件匹配具有指定 EC2 实例 ID 的实例。此字段支持通配符匹配，因此 i-00000* 将匹配实例 ID 以 i-00000 开头的任何实例。
  - 平台：筛选条件将 EC2 实例与指定平台进行匹配。有效值为 Windows、linux 或通配符 *（以匹配任何平台）。
- AWS::EC2::NatGateway:
  - NatGatewayId: NAT 网关的 ID。此字段支持通配符匹配。
  - 状态：NAT 网关的状态（待处理 | 失败 | 可用 | 正在删除 | 已删除或通配符 “*”）
  - VpcId：NAT 网关所在的 VPC 的 ID。此字段支持通配符匹配。
  - SubnetId：NAT 网关所在的子网的 ID。此字段支持通配符匹配

- AWS:EC2::: VPNConnection:
  - VpnConnectionId: 连接的 ID。此字段支持通配符匹配。
- AWS::EFS::FileSystem:
  - FileSystemId：EFS 文件系统的 ID。此字段支持通配符匹配。
- AWS::EKS::Cluster:
  - ClusterName：集群的名称。此字段支持通配符匹配。
- AWS::ElasticLoadBalancing::LoadBalancer（Classic Load Balancer）：
  - LoadBalancerName: 名 LoadBalancer 字。此字段支持通配符匹配。
  - 方案：可以是 “面向互联网”、“内部” 或通配符 “*”。
  - VPCId：部署负载均衡器的，可以是通配符 “*”。 VPCId
- AWS::ElasticLoadBalancingV2::LoadBalancer（Application Load Balancer (ALB)）：
  - LoadBalancerArn： LoadBalancer 亚马逊资源名称 (ARN)。
  - DNSName: DNSName 的 LoadBalancer. 此字段支持通配符匹配。
  - LoadBalancerName: 名 LoadBalancer 字。此字段支持通配符匹配。
- AWS::Elasticsearch::Domain:
  - DomainId: DomainId ElasticSearch 资源的。此字段支持通配符匹配。
  - DomainName: DomainName ElasticSearch 资源的。此字段支持通配符匹配。
  - HasMasterNode：布尔值为真或假。如果域有专用的主节点，则匹配。
  - HasKmsKey布尔值为真或假。如果该域具有用于静态加密的 KMS 密钥，则匹配。
- AWS::FSx::FileSystem:
  - FileSystemId: FSx 文件系统的 ID。此字段支持通配符匹配。
- AWS::OpenSearch::Domain:
  - DomainId: DomainId OpenSearch 资源的。此字段支持通配符匹配。
  - DomainName: DomainName OpenSearch 资源的。此字段支持通配符匹配。
  - HasMasterNode: 布尔值；如果域有专用的主节点，则可以将其设置为 true。
  - HasKmsKey：如果域有静态加密的 KMS 密钥，则可以将其设置为 true。
- AWS:: RDS::: DBCluster
  - DBCluster标识符：筛选器将 RDS 集群标识符与指定标识符进行匹配。此字段不支持通配符匹配，因此必须指定集群标识符。
  - 引擎：RDS 实例正在使用的引擎。此字段支持通配符匹配。
  - EngineVersion: 引擎版本。此字段支持通配符匹配。

- AWS:: RDS::: DBInstance
  - DBInstance标识符：筛选条件匹配具有指定实例 ID 的 RDS 实例。此字段不支持通配符匹配，因此必须指定实例标识符。
  - 引擎：RDS 实例正在使用的引擎。此字段支持通配符匹配。
  - EngineVersion: 引擎版本。此字段支持通配符匹配。
- AWS::Redshift::Cluster:
  - ClusterIdentifier: 集群标识符。此字段支持通配符匹配。
- AWS::S3::Bucket:
  - BucketName: S3 存储桶的名称。此字段支持通配符匹配。
- AWS::Synthetics::Canary:
  - CanaryName: Synthetics 金丝雀的名字。

其他过滤器属性：

- 标签：过滤器适用于已应用给定标签的任何资源。此属性的值必须是包含以下字段的 JSON 对象：
  - 密钥：必须是一个精确的字符串，并指定资源必须具有带有该密钥的标签。
  - 值：指定标签的匹配值。支持通配符，因此 Samp le 的值与任何以字符串 Samp le 结尾的值匹配。
- Fn:: AND: 一个由 JSON 对象组成的 JSON 数组。每个对象都遵循与过滤器配置块相同的规则。这指定过滤器匹配与所有子过滤器匹配的任何资源。
- Fn:: OR：JSON 对象的 JSON 数组。每个对象都遵循与过滤器配置块相同的规则。这指定过滤器与任何子过滤器匹配的任何资源相匹配。
- Fn:: NOT：遵循与筛选器配置块相同规则的 JSON 对象。这指定过滤器明确不匹配任何与子筛选器匹配的资源。使用它来指定标记规则的排除项。

标签：要应用于匹配资源的标签。（请参阅标签命名和使用惯例。）此字段是一个由键值对组成的数组：

- 密钥：要应用的标签的密钥。
- 值：要应用的标签的值。

> **Note**
>
> Resource Tagger 应用的标签的密钥始终以 ams: rt: 开头。如果您未在配置文件中指定此前缀，则资源标记器会为您插入该前缀。这就是 Resource Tagger 将其拥有和管理的标签与其他工具用于其他目的的标签区分开来的方式。

AMS Accelerate 中的资源标记器用例

本节列出了使用资源标记器执行的常用操作。

查看资源标记器应用的标签

Resource Tagger 应用的所有标签的密钥前缀都是 ams: rt:。例如，以下标签定义生成的标签密钥为 ams: rt: sampleKey，值为 sampleValue。所有带有此前缀的标签都被视为资源标记器的一部分。

```
{
 "Key": "sampleKey",
 "Value": "sampleValue"
}
```

> **Important**
>
> 如果您手动创建自己的带有 ams: rt: 前缀的标签，则该标签将被视为由资源标记器管理。这意味着，如果资源由 Resource Tagger 管理，但配置文件未指示应应用标记，则资源标记器会移除您手动添加的标签。如果您要手动标记由资源标记器管理的资源，请不要在标签键中使用 ams: rt: 前缀。

使用资源标记器创建标签

AMS 加速资源标记器是在 AMS Accelerate 入门期间部署在您的账户中的组件。Resource Tagger 有一组可配置的规则，用于定义如何标记您的资源，然后它会强制执行这些规则，自动在资源上添加和删除标签，以确保它们符合您的规则。

如果您想使用资源标记器来标记您的资源，请参阅加速资源标记器。

以下是资源标记器配置片段示例，它为所有亚马逊实例添加了值为 true 的 ams: rt: ams-managed 标签。 EC2 ams: rt: ams-managed 标签允许你选择让 AM S Accelerate 监控你的资源。

```
{
    "AWS::EC2::Instance": {
        "SampleConfigurationBlock": {
            "Enabled": true,
            "Filter": {
                "Platform": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

Warning

为新配置指定名称时要小心（SampleConfigurationBlock在提供的示例中），因为您可能会无意中使用相同的名称覆盖由 AMS 管理的配置。

阻止资源标记器修改资源

可以将资源标记器设置为只读模式，以防止其在资源上添加或删除任何标签。如果您想提供自己的标记机制，这很有用。

在只读模式下，Resource Tagger 仍会检查托管配置文件和客户配置文件中指定的标记规则，并扫描不符合这些标记规则的资源。任何不合规的资源都会显示出来。 AWS Config你可以查找的有前AMSResourceTagger-缀。 AWS Config 规则 例如，该AMSResourceTagger-EC2Instance AWS Config 规则根据配置文件评估是否为AWS::EC2::Instance资源创建了适当的标签。

Resource Tagger 此时停止，不会对您的资源进行任何更改（不添加或移除标签）。

您可以通过修改客户配置文件以将ReadOnly密钥包含在 “选项” 块中来启用只读模式。例如，以下配置文件片段显示了它的外观：

```
{
    "Options": {
        "ReadOnly": true
```

```
    },
    "AWS::EC2::Instance": {
        [... the rest of your configuration ...]
    }
}
```

Resource Tagger 将在部署完成后立即对此新配置做出反应，并停止在资源上添加和删除标签。

> **Note**
>
> 要重新启用标签修改，请将该ReadOnly值更改为 false，或者完全删除密钥，因为默认值为 false。

有关 “选项” 设置的更多信息语法和结构，请参阅 “下一步”。

配置文件示例

以下示例配置文件指定属于 CloudFormation 堆栈*堆栈的所有 Windows EC2 实例均由 AMS Accelerate 管理；但是，明确排除了 ID 为 i-00000000000000000001 的特定 EC2 实例。

```
{
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "Windows"
                    },
                    {
                        "Tag": {
                            "Key": "aws:cloudformation:stack-name",
                            "Value": "stack-*"
                        }
                    },
                    {
                        "Fn::NOT": {
                            "InstanceId": "i-00000000000000001"
                        }
                    }
                ]
            },
```

```
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

> **Warning**
>
> 为新配置指定名称时要小心（SampleConfigurationBlock在提供的示例中），因为您可能会无意中使用相同的名称覆盖由 AMS 管理的配置。

合并默认配置

默认配置文件由 AMS Accelerate 在账户注册时提供。此配置文件提供部署在您的账户中的默认规则。

虽然您无法修改默认配置文件，但您可以通过在自定义配置配置文件中指定与默认配置块相同的 ConfigurationID 的配置块来覆盖默认配置文件。如果这样做，您的配置块将覆盖默认配置块。

例如，考虑以下默认配置文档：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
}
```

要将此处应用的标签值从SampleValueA更改为SampleValueB，并将标签应用于所有实例，而不仅仅是 Windows 实例，您需要提供以下自定义配置文件：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "*"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueB"
   }]
  }
 }
}
```

> **Important**
>
> 请记得在更改配置后再进行部署。有关更多信息，请参阅 部署配置更改。在 SSM 中 AppConfig，您必须在创建配置后部署新版本的配置。

禁用默认配置

您可以禁用默认配置规则，方法是将具有相同 ConfigurationI d 的配置块添加到您的自定义配置文件中，并将 “启用” 字段的值设为 false。

例如，如果默认配置文件中存在以下配置：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": true,
   "Filter": {
    "Platform": "Windows"
   },
   "Tags": [{
    "Key": "my-tag",
    "Value": "SampleValueA"
   }]
  }
 }
```

```
}
```

您可以通过在自定义配置文件中包含以下内容来禁用此标记规则：

```
{
 "AWS::EC2::Instance": {
  "AMSManagedBlock1": {
   "Enabled": false
  }
 }
}
```

> **Important**
>
> 请记得在配置更改后进行部署；有关信息，请参阅部署配置更改。在 SSM 中 AppConfig，您必须在创建配置后部署新版本的配置。

移除资源标记器应用的标签

如果配置配置文件中不存在任何以 ams: rt 为前缀的标签，或者，如果这些标签确实存在，则筛选条件不匹配，则资源标记器会将其删除。这意味着您可以通过执行以下任一操作来移除资源标记器应用的标签：

- 修改定义标签的自定义配置部分。
- 为特定资源添加例外，使其不再与筛选条件匹配。

例如：如果 L inux 实例具有以下标签：

```
"Tags": [{
    "Key": "ams:rt:MyOwnTag",
    "Value": true
},{
    "Key": "myTag",
    "Value": true
}]
```

然后部署以下资源标记器配置文件：

```
{
```

```
    "AWS::EC2::Instance": {
        "AMSMonitoringWindows": {
            "Enabled": true,
            "Filter": {
                "Platform": "Windows"
            },
            "Tags": [{
                "Key": "ams:rt:ams-managed",
                "Value": "true"
            }]
        }
    }
}
```

Resource Tagger 会对新的配置更改做出反应，实例上的唯一标签变为：

```
"Tags": [{
    "Key": "myTag",
    "Value": true
}]
```

> **Warning**
>
> 为新配置指定名称时要小心（SampleConfigurationBlock在提供的示例中），因为您可能会无意中使用相同的名称覆盖由 AMS 管理的配置。

> **Important**
>
> 请记得在配置更改后进行部署；有关信息，请参阅部署配置更改。在 SSM 中 AppConfig，您必须在创建配置后部署新版本的配置。

查看或更改资源标记器配置

可以通过的 API 查看两个 JSON 配置文件 CustomerManagedTags，即AMSManaged标签和，它们AppConfig在入门时部署到您在 AWS 中的账户，并驻留在 AMSResource Tagger 应用程序中，以及AMSInfrastructure环境中。 AppConfig GetConfiguration

以下是此次 GetConfiguration 调用的示例：

```
aws appconfig get-configuration
 --application AMSResourceTagger
 --environment AMSInfrastructure
 --configuration AMSManagedTags
 --client-id ANY_STRING
 outfile.json
```

应用程序：提供功能的 AppConfig 逻辑单元，对于资源标记器来说，这是 AMSResource标签器。

- 环境： AMSInfrastructure。
- 配置：要查看 AMS Accelerate 默认标签定义，值为 AMSManaged标签，而要查看客户标签定义，值为 CustomerManagedTags。
- 客户端 ID：应用程序实例的唯一标识符，可以是任何字符串。
- 然后可以在指定的输出文件（在本例中为 outfile.json）中查看标签定义。

然后可以在指定的输出文件（在本例中为 outfile.json）中查看警报定义。

您可以通过查看AMSInfrastructure环境中过去的部署来查看您的账户中部署了哪个版本的配置。

要覆盖标签规则，请执行以下操作：

通过使用或更新自定义配置文件，使用 for Accelerat CloudFormation e 部署配置文件或者直接使用使用 AppConfig的 API，可以覆盖任何现有的标签规则。 CloudFormation CreateHostedConfigurationVersion使用相同的 ConfigurationID 作为默认配置标签规则会覆盖默认规则，并取而代之的是自定义规则。

要部署对CustomerManagedTags文档所做的更改，请执行以下操作：

对自定义配置文件进行更改后，必须为其部署更改。要部署新更改， AppConfig必须使用 AWS AppConfig 控制台或 CLI 运行的 StartDeploymentAPI。

部署配置更改

自定义完成后，必须通过 AWS AppConfig StartDeploymentAPI 部署这些更改。以下说明说明如何使用进行部署 AWS CLI。此外，您还可以使用 AWS 管理控制台 进行这些更改。有关信息，请参阅步骤 5：部署配置。

```
aws appconfig start-deployment
--application-id <application_id>
--environment-id <environment_id>
```

```
--deployment-strategy-id <deployment_strategy_id>
--configuration-profile-id <configuration_profile_id>
--configuration-version 1
```

- 应用程序 ID：应用程序 AMSResource Tagger 的应用程序 ID。 ListApplications通过 API 调用获取这个。
- 环境 ID：环境 ID； ListEnvironments通过 API 调用获取。
- 部署策略 ID：部署策略 ID； ListDeploymentStrategies通过 API 调用获取。
- 配置配置文件 ID：的配置文件 ID CustomerManagedTags； ListConfigurationProfiles通过 API 调用获取。
- 配置版本：您要部署的配置文件的版本。

> **Important**
>
> Resource Tagger 应用配置文件中指定的标签。您对资源标签所 AWS 管理控制台做的任何手动修改（使用或 CloudWatch CLI/SDK）都会自动恢复，因此请确保您的更改是通过资源标记器定义的。要知道哪些标签是由资源标记器创建的，请查找前缀为的标签键。`ams:rt:`

使用StartDeployment和 StopDeploymentAPI 操作将部署的访问权限限制为了解向目标部署新配置的责任和后果的可信用户。

要详细了解如何使用 AWS AppConfig 功能来创建和部署配置，请参阅使用 AWS 中的文档 AppConfig。

将 Terraform 配置为忽略资源标记器标签

如果您使用 Terraform 来配置资源，并且想使用资源标记器来标记资源，则资源标记器标签可能会被 Terraform 标识为漂移。

您可以使用生命周期配置块或 ignore_tags 全局配置块将 Terraform 配置为忽略所有资源标记器标签。有关更多信息，请参阅 Terraform 关于资源标记的文档资源标记。

以下示例说明如何创建全局配置以忽略所有以 Resource Tagger 标签前缀`ams:rt:`开头的标签：

```
provider "aws" {
  # ... potentially other configuration ...

  ignore_tags {
```

```
    key_prefixes = ["ams:rt:"]
  }
}
```

查看资源标记器管理的资源数量

Resource Tagger 每小时向AMS/ResourceTagger命名空间中的 Amazon CloudWatch 发送指标。仅针对资源标记器支持的资源类型发布指标。

指标名称	Dimensions	说明
ResourceCount	组件， ResourceType	在该区域部署的（指定资源类型的）资源数量。 单位：计数
ResourcesMissingManagedTags	组件， ResourceType	根据配置配置文件，需要托管标签但尚未由资源标记器标记的资源（指定资源类型）的数量。 单位：计数
UnmanagedResources	组件， ResourceType	Resource Tagger 未应用托管标签的资源（指定资源类型）的数量。通常，这些资源与任何 Resource Tagger 配置块都不匹配，或者被明确排除在配置块之外。 单位：计数
MatchingResourceCount	组件、 ResourceType、ConfigClauseName	与 Resource Tagger 配置块相匹配的资源（指定资源类型）的数量。要使资源与配置块匹配，则必须启用该块，并且资源必须与区块的过滤器匹配。 单位：计数

这些指标也可以在 AM S-Resource-Tagger-Reporting-Dashboard 中以图表形式查看。要查看控制面板，请在亚马逊 CloudWatch 管理控制台中选择 AMS-Resource-Tagger-Reporting-D ashboard。默认情况下，此控制面板中的图表显示前 12 小时的数据。

AMS Accel CloudWatch erate 会向您的账户部署警报，以检测非托管资源数量的显著增加，例如，AMS 资源标记器排除在管理之外的资源。AMS Operations 将调查非托管资源的增加情况，这些

资源超过三个相同类型的资源，或者在相同类型的所有资源基础上增加 50%。如果变更似乎不是故意的，AMS Operations 可能会与您联系以审查变更。

用于 CloudFormation 为 AMS Accelerate 创建标签

您可以使用 CloudFormation 在堆栈级别（参见 CloudFormation 文档，资源标签）或单个资源级别（例如，参见标记您的 Amazon EC2 资源）应用标签。

> **Important**
>
> 某些 AMS 加速服务组件需要带有 ams: rt: 前缀的标签。Resource Tagger 认为自己拥有这些标签，如果资源标记器配置规则不允许，则会将其删除。即使您使用的是 CloudFormation 或 Terraform，您也始终需要为这些标签部署资源标记器配置文件。

CloudFormation AMS 加速的用例

本节列出了常用执行的操作 CloudFormation。

主题

- 使用 for Accel EC2 erate CloudFormation 标记实例
- 使用标记 AutoScaling 群组 (ASG) 以获得加速 CloudFormation
- 使用 for Accelerat CloudFormation e 部署配置文件

使用 for Accel EC2 erate CloudFormation 标记实例

以下示例说明如何将值为 true 的 ams: rt: ams-managed 标签应用于由管理的亚马逊实例。 EC2 CloudFormationams: rt: ams-managed 标签允许你选择让 AM S Accelerate 监控你的资源。

```
 Type: AWS::EC2::Instance

Properties:
  InstanceType: "t3.micro"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
```

```
      Value: "true"
```

使用标记 AutoScaling 群组 (ASG) 以获得加速 CloudFormation

以下示例说明了如何将值为 true 的 ams: rt: ams-managed 标签应用于由管理的 Auto S caling 组。CloudFormation请注意，Auto Scaling 组会将其标签传播到由其创建的亚马逊 EC2 实例。ams: rt: ams-managed 标签允许你选择让 AM S Accelerate 监控你的资源。

```
  Type: AWS::AutoScaling::AutoScalingGroup
Properties:
  AutoScalingGroupName: "SampleASG"

  # ...other properties...

  Tags:
    - Key: "ams:rt:ams-managed"
      Value: "true"
```

使用 for Accelerat CloudFormation e 部署配置文件

如果您希望使用部署`CustomerManagedTags`配置文件 CloudFormation，则可以使用以下 CloudFormation 模板。在`AMSResourceTaggerConfigurationVersion.Content`字段中输入所需的 JSON 配置。

在 CloudFormation 堆栈或堆栈集中部署模板时，如果您未遵循配置所需的 JSON 格式，则`AMSResourceTaggerDeployment` 资源部署将失败。有关预期格式语法和结构的详细信息，请参阅。

有关将这些模板部署为 CloudFormation 堆栈或堆栈集的帮助，请参阅以下相关 AWS CloudFormation 文档：

- 在 AWS CloudFormation 控制台上创建堆栈
- 使用创建堆栈 AWS CLI
- 创建堆栈集

> **Note**
>
> 如果您使用其中一个模板部署配置版本，然后删除 CloudFormation 堆栈/堆栈集，则该模板配置版本将保持当前部署的版本，并且不会进行其他部署。如果您希望恢复到默认配置，则需要手动部署空配置（也就是说，只是{}），或者将堆栈更新为空配置，而不是删除堆栈。

JSON

```
{
  "Description": "Custom configuration for the AMS Resource Tagger.",
  "Resources": {
    "AMSResourceTaggerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "Content": "{\"Options\": {\"ReadOnly\": false}}",
        "ContentType": "application/json"
      }
    },
    "AMSResourceTaggerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-CustomerManagedTags-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSResourceTaggerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-Deployment-StrategyID"
        },
```

```
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-ResourceTagger-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Resource Tagger.
Resources:
  AMSResourceTaggerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      Content: |
        {
          "Options": {
            "ReadOnly": false
          }
        }
      ContentType: application/json
  AMSResourceTaggerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-ResourceTagger-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID
      ConfigurationVersion:
        !Ref AMSResourceTaggerConfigurationVersion
      DeploymentStrategyId:
        !ImportValue AMS-ResourceTagger-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-ResourceTagger-Configuration-EnvironmentId
```

使用 Terraform 为 AMS Accelerate 创建标签

如果你不想使用 AMS Accelerate Resource Tagger，你可以使用 Terraform 应用自己的标签。但是，如果你不想使用资源标记器，因为它与你的 Terraform 定义有偏差，那么有一种方法可以让你使用资源标记器并忽略它造成的漂移；请参阅。[将 Terraform 配置为忽略资源标记器标签]

> **Important**
>
> 某些 AMS 加速服务组件需要带有 ams: rt: 前缀的标签。Resource Tagger 认为自己拥有这些标签，如果资源标记器配置规则不允许，则将其删除。即使您使用的是 CloudFormation 或 Terraform，也必须为这些标签部署资源标记器配置文件。

以下示例说明了如何将值为 true 的 ams: rt: ams-managed 标签应用于 Terraform 管理的亚马逊实例。EC2 ams: rt: ams-managed 标签允许你选择让 AM S Accelerate 监控你的资源。

```
  resource "aws_instance" "sample_linux_instance" {
    # ...ami and other properties...

    instance_type = "t3.micro"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
}
```

以下示例说明了如何将值为 true 的 ams: rt: ams-managed 标签应用于 Terraform 管理的 Auto S caling 组。请注意，Auto Scaling 组会将其标签传播到由其创建的 Amazon EC2 实例。ams: rt: ams-managed 标签允许你选择让 AM S Accelerate 监控你的资源。

```
  resource "aws_autoscaling_group" "sample_asg" {
    # ...other properties...

    name = "terraform-sample"

    tags = {
        "ams:rt:ams-managed" = "true"
    }
```

```
}
```

有关如何管理 Terraform 创建的资源标签的说明，请参阅。[将 Terraform 配置为忽略资源标记器标签]

AMS Accelerate 中的事件报告、服务请求和账单问题

使用 AMS Accelerate，您可以随时通过中的 AWS 支持中心请求有关操作问题和请求的帮助 AWS 管理控制台。AMS Accelerate 运营工程师可以响应您的事件和服务请求 round-the-clock，并提供服务的响应时间服务级别协议 (SLAs)。AMS Accelerate 运营工程师使用相同的机制主动通知您重要的警报和问题。

AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。要快速了解 AMS 如何利用我们的一些关键运营功能（包括 round-the-clock服务台、主动监控、安全、补丁、日志记录和备份）来帮助您的团队实现整体卓越运营，请参阅 AMS 参考架构图。 AWS 云

主题

AMS Accerate 中的事件管理

在 AMS Accelerate 中 AWS Support Center Console，您可以使用来提交事件报告。事件是影响您的托管环境的 AWS 服务 性能问题，由 AMS Accelerate 或您决定。AMS Accelerate 团队识别的事件首先作为事件（监控捕获的系统状态变化）接收。如果突破了配置的阈值，则该事件会触发警报，也称为警报。AMS Accelerate 运营团队负责确定事件是无影响、事件（服务中断或降级）还是问题（一个或多个事件的根本原因）。

> **Note**
>
> AMS Accelerate 团队还会接收您使用带有服务代码`service-ams-operations-report-incident`的 AWS Support API 以编程方式创建的事件。

有关使用的信息 支持，请参阅入门 支持。

什么是事件管理？

事件管理是 AMS 用来记录、采取行动、沟通活动事件进展和提供通知的流程。

事件管理流程的目标是确保尽快恢复托管服务的正常运行，最大限度地减少业务影响，并随时向所有相关方通报情况。

事件的示例包括（但不限于）网络连接中断或降级、进程或 API 无响应或计划任务未执行（例如，备份失败）。

下图描述了您向 AMS 报告的事件的工作流程。

此图描绘了 AMS 向您报告的事件的工作流程。

事件优先级

在 AWS Support 中心、控制台或支持 API (SAPI) 中创建的事件与在 AMS 控制台中创建的事件具有不同的分类。

- 低：您的业务服务或应用程序中与 AWS 或 AMS 资源相关的非关键功能受到影响。
- 中：与 AWS and/or AMS 资源相关的业务服务或应用程序受到中度影响，且运行处于降级状态。
- 高：您的业务受到严重影响。与 AWS and/or AMS 资源相关的应用程序的关键功能不可用。专为影响生产系统的最严重的停机而设计。

> **Note**
>
> AWS Support 控制台提供五个事件优先级别，我们将其转换为三个 AMS 级别。

事件响应和解决方案的工作原理

AMS Accelerate 使用 IT 服务管理 (ITSM) 事件管理最佳实践，在需要时尽快恢复服务。

我们通过世界各地的运营中心提供全天候 follow-the-sun支持，专门的操作员会积极关注监控仪表板和事件队列。

我们的运营工程师使用内部事件跟踪工具来识别、记录、分类、确定事件优先级、诊断、解决和关闭事件；我们通过 Support Center 和 Su AWS pport API 为您提供所有这些活动的最新信息。 AWS 我们的运营商利用各种内部 AWS 支持工具来帮助完成所有这些活动。这些运营商对 AMS Accelerate 支持的基础设施非常熟悉，并且拥有解决已确定的支持问题的专家级技术技能。如果我们的操作员需要帮助，Premium Support 和 AWS 服务团队随时待命。

AMS Accelerate 运营团队收到您的事件后，如果需要任何澄清，我们会与您一起验证优先级和分类。例如，如果最好将事件报告归类为服务请求，则会将其重新分类，AMS Accelerate 服务请求团队接管并通知您。如果接收操作员能够解决事件，则会采取措施快速解决事件。AMS Accelerate 操作员请查阅内部文档以获得解决方案，并在需要时将事件上报给其他支持资源，直到事件得到解决。问题解决后，AMS Accelerate 运营团队会记录事件和解决方案，以备将来使用。

如果严重事件影响您的关键工作负载，AMS Accelerate 可能会建议恢复基础架构。在排除问题故障和简单地从已知功能备份中恢复之间通常需要权衡取舍，而服务停机带来的风险和影响是决定性因素。如果您有时间解决问题，AMS Accelerate 将为您提供帮助，您的云服务交付经理 (CSDM) 可能会参与其中，但是如果恢复的紧迫性很高，AMS Accelerate 可以立即启动恢复。

在 AMS Accelerate 中处理事件

在 S AWS upport Center 中，您可以执行以下任务：

- 报告并更新事件。要报告 AMS Accelerate 事件，请从 “服务” 菜单中选择 AMS 运营——报告事件。
- 获取您提交的所有事件的列表和详细信息。
- 按状态和其他过滤器缩小对事件的搜索范围。
- 在事件中添加通信和文件附件，并为案例通信添加电子邮件收件人。
- 发起实时聊天或请求回电您的事件。

> **Note**
>
> 实时聊天功能不适用于安全事件；对于安全问题，请创建高优先级（P1 或 P2）支持案例。

- 解决事件。
- 对事件通信进行评分。

以下示例介绍如何使用 Support Center 提交事件。提交后，AMS Accelerate 团队将与您合作，根据标准 AMS Accelerate SLA 解决事件。

为 Accelerate 提交事件

要使用 Support Center 报告事件，请参阅支持文档：创建支持案例

要使用 支持 中心举报事件，请执行以下操作：

1. 单击 “创建案例”。创建事件案例页面打开。

2. 打开技术支持问题类型菜单，然后选择 AMS 运营--报告事件。提供有关您的事件的信息，然后选择“创建”。
3. 要在事件解决过程的每个步骤中通过电子邮件随时了解情况，请务必填写 “抄送电子邮件” 选项；如果您通过联合身份连接，请在点击 AMS Accelerate 发送给您的电子邮件中的有关事件的链接之前登录。

> **Note**
>
> 使您的描述尽可能的详细。包含相关的资源信息，以及可能有助于我们了解您问题的任何其他信息。例如，要排查性能问题，可提供时间戳和日志。对于功能请求或一般指导问题，请提供对您的环境和目的的描述。在所有案例中，都请遵从案例提交表单中的 Description Guidance (描述指导)。
> 您提供尽可能多的详细信息意味着提升了快速解决案例的可能性。

您还可以使用带有服务代码的 AWS Support API `service-ams-operations-report-incident` 来报告事件。

监控和更新 Accelerate 事件

您可以使用 Support Center 或以编程方式使用 支持 API `DescribeCases`操作来更新、监控和查看事件报告和服务请求（均为已调用的案例）。

要使用 Cent 支持 er 监控案例、事件或服务请求，请按照以下步骤操作。

1. 在 AWS 管理控制台中，浏览到 Supp ort。
2. 从左侧导航栏中选择 “您的支持案例”，浏览至案例，然后选择 “主题” 链接以打开包含当前状态和通信内容的详细信息页面。

   如果您此时想使用电话或聊天，请单击 “在 Su pport Center 中打开案例”，在 支持 中心打开问题创建页面，该页面会自动填充 AMS 服务类型。

   当 Accelerate 运营团队更新已报告的事件或服务请求案例时，您会在 Support Center 中收到一封电子邮件和事件链接，以便您做出回应。

   > **Note**
   >
   > 您无法通过回复电子邮件来回复案例信件。

如果仪表板中有许多案例，则可以使用 “筛选” 选项：

- 主题：使用此过滤器搜索案例主题中的关键字。
- 严重性：使用此选项可通过从列表中选择严重性来按严重性筛选案例。
- 案例类型：使用它来查看特定案例类型的所有案例。加速事件和服务请求与任何特定于服务的案例一起显示在 “技术支持案例类型” 下。
- 状态：使用此选项可通过从列表中选择特定状态来按状态筛选案例。

3. 要查看最新状态，请刷新页面。
4. 如果有太多信件以至于没有全部显示在页面上，请选择 “加载更多”。
5. 要更新案例状态，请选择 “回复”，输入新的信件，然后选择 “提交”。
6. 要在问题得到令您满意的解决后将其结案，请选择 “关闭案例”。

请务必通过1-5星对服务进行评级，让AMS知道我们的表现如何。

使用支持 API 管理加速事件

在调查问题期间，您可以使用 支持 API 创建事件并添加与 支持 工作人员的通信。 支持 API 模拟了 Support Cent er 的大部分行为。AWS

有关您可以使用此 AWS 支持服务的信息，请参阅 Support C ase AWS 的生命周期编程。

> **Note**
>
> AMS Accelerate 团队使用服务代码`service-ams-operations-report-incident`以编程方式接收您创建的事件。

响应 AMS 加速引发的事件

AMS Accelerate 会主动监控您的资源。有关更多信息，请参阅 AMS Accelerate 中的监控和事件管理。有时，AMS Accelerate 会识别并创建事件，通常是为了将事件通知您。如果需要您采取行动来解决事件，AMS Accelerate 团队会将通知发送到您为该账户提供的联系信息。您回复此通知的方式与任何其他事件的回复方式相同，通常是通过 Support Center 回复，但在某些情况下需要通过电子邮件或电话进行联系。

> **Important**
>
> 要接收事件案例或服务请求的状态变更通知，请在地址字段中输入电子邮件地址。

观看 Akshay 的视频以了解更多信息 (4:15)

Accelerate 中的服务请求管理

主题

AMS Accelerate 使用服务请求管理来记录、采取行动、沟通当前服务请求的进度并提供通知。

服务请求管理流程的目标是确保您的托管服务能够满足您的需求。

对于与账单相关的查询，请创建服务请求。

> **Note**
>
> AMS Accelerate 团队使用带有服务代码`service-ams-operations-service-request`的 AWS Support API 以编程方式接收您创建的服务请求。

使用 AWS Support 中心，您可以执行以下任务：

- 报告和更新服务请求。对于 AMS Accelerate 服务请求，请从 “服务” 菜单中选择 AMS 操作--服务请求。
- 获取您提交的所有服务请求的列表和详细信息。
- 按状态和其他筛选条件缩小对服务请求的搜索范围。
- 在请求中添加通信和文件附件，并添加案例通信的电子邮件收件人。

- 解决服务请求。
- 对服务请求通信进行评分。

何时使用服务请求进行加速

以下示例描述了服务请求。在您提交服务请求后，AMS Accelerate 团队将与您合作，根据您的 AMS SLA 解决请求。

- AMS 或 AWS 一般指导
- 补丁 MW 相关问题
- Backup 计划相关问题
- 有关 AWS 服务功能的问题

以下是不应在服务请求中提出的内容的示例：

- 访问问题
- 补丁失败
- Backup 失败

在 Accelerate 中管理服务请求的工作原理

服务请求由待命的 AMS Accelerate 运营团队处理。

AMS Accelerate 运营团队收到您的服务请求后，会对其进行审核，以确保将其正确归类为服务请求或事件。如果将其重新归类为事件，AMS Accelerate 事件管理流程将开始，并向您发送通知。

如果 AMS Accelerate 操作员能够解决服务请求，则会立即采取相应措施。例如，如果服务请求是为了提供架构建议或其他信息，则操作员会将您推荐给相应的资源或直接回答问题。

如果对您的服务请求的分析发现了错误或功能请求，则 AMS 会通过服务请求向您发送通知。由于功能请求或错误修复没有预计到达时间，因此原始服务请求已关闭。有关原始服务请求的后续问题，请联系您的 CSDM。

如果服务请求超出了 AMS Accelerate 运营的范围，运营商要么将请求发送给您的云服务交付经理，以便他们可以与您沟通，或者发送给相应的 AWS 支持团队，同时向您发送一封关于正在采取的措施的电子邮件。

在您表示对结果感到满意之前，服务请求才会得到解决。

> **Note**
>
> 我们建议您在任何情况下都提供联系人电子邮件、姓名和电话号码，以便于沟通。

在 Accelerate 中创建服务请求

要创建服务请求，请执行以下步骤：

1. 从 AMS Accelerate 控制台中，浏览至控制面板。
2. 选择 “打开服务请求”，“AMS — 服务请求” 已预先选择。
3. 选择一个类别。
4. 选择 “严重性”（仅限高级或高级级别）。
5. 输入以下信息：
   - 主题：服务请求的描述性标题。
   - 描述：对服务请求、受影响的系统以及解决方案的预期结果的全面描述。
6. 要添加附件，请选择 “附加文件”，浏览到所需的附件，然后选择 “打开”。要删除附件，请选择删除图标
7. 联系我们：默认通过网络联系 AMS。要选择其他选项，请执行以下操作：
   - 首选联系语言：英语是 AMS Accelerate 服务请求支持的语言。
   - 网页：您的服务请求通过网络提交，并由 AMS 运营团队处理。
   - 聊天：与 AMS Accelerate 运营代表在线聊天。此选项会将您添加到聊天队列中。
   - 电话：AMS 运营代表给您回电。输入您的 AWS 区域、电话号码和分机号（如果适用）。
   - 其他联系人：输入您要在服务请求中复制的任何其他电子邮件地址。
8. 选择提交。

   将打开一个案例详情页面，其中包含有关服务请求的信息，例如类型、主题、已创建、ID 和状态。另外，还有一个 “信件” 区域，其中包含对您创建的请求的描述。

   要打开信件区域并提供更多详细信息或状态更新，请选择 “回复”。

   解决服务请求后，选择 “解决案例”。

如果信件太多以至于没有全部显示在页面上，请选择 “加载更多”。

请务必通过1-5星对服务进行评级，让AMS知道我们的表现如何。

> **Note**
>
> 如果您要测试服务请求功能，我们建议您在服务请求的主题中添加一个不采取行动标志，例如`AMSTestNoOpsActionRequired`。然后，您无需启动服务请求解决过程即可进行测试。AMS Accelerate 团队使用带有服务代码`service-ams-operations-service-request`的 AWS Support API 以编程方式接收您创建的服务请求。

监控和更新 Accelerate 的服务请求

要使用 Cent 支持 er 监控案例、事件或服务请求，请按照以下步骤操作。

1. 在 AWS 管理控制台中，浏览到 Supp ort。
2. 从左侧导航栏中选择 “您的支持案例”，浏览至案例，然后选择 “主题” 链接以打开包含当前状态和通信内容的详细信息页面。

   如果您此时想使用电话或聊天，请单击 “在 Su pport Center 中打开案例”，在 支持 中心打开问题创建页面，该页面会自动填充 AMS 服务类型。

   当 Accelerate 运营团队更新已报告的事件或服务请求案例时，您会在 Support Center 中收到一封电子邮件和事件链接，以便您做出回应。

   > **Note**
   >
   > 您无法通过回复电子邮件来回复案例信件。

   如果仪表板中有许多案例，则可以使用 “筛选” 选项：

   - 主题：使用此过滤器搜索案例主题中的关键字。
   - 严重性：使用此选项可通过从列表中选择严重性来按严重性筛选案例。
   - 案例类型：使用它来查看特定案例类型的所有案例。加速事件和服务请求与任何特定于服务的案例一起显示在 “技术支持案例类型” 下。

- 状态：使用此选项可通过从列表中选择特定状态来按状态筛选案例。

3. 要查看最新状态，请刷新页面。
4. 如果有太多信件以至于没有全部显示在页面上，请选择 “加载更多”。
5. 要更新案例状态，请选择 “回复”，输入新的信件，然后选择 “提交”。
6. 要在问题得到令您满意的解决后结案，请选择 “关闭案例”。

   请务必通过1-5星对服务进行评级，让AMS知道我们的表现如何。

使用加速支持 API 管理服务请求

您可以使用 Supp AWS ort API 创建服务请求，并在调查您的问题和与 AWS 支持人员互动的过程中向这些请求添加信件。 AWS 支持 API 模拟了AWS 支持中心的大部分行为。

AMS 团队还会接收您使用 AWS Support API 和服务代码service-ams-operations-service请求以编程方式创建的服务请求。

有关如何使用此 AWS 支持服务的更多信息，请参阅编程 AWS 支持案例的生命周期。

回应 AMS Accelerate 生成的服务请求

AMS Accelerate 会主动监控您的资源；有关更多信息，请参阅AMS Accelerate 中的监控和事件管理。有时，AMS Accelerate 会为您创建服务请求或服务通知，通常是在需要您采取行动来解决服务请求的情况下。在这种情况下，AMS Accelerate 团队会向您为该账户提供的联系人发送通知。您以与任何其他案例相同的方式回复此服务请求，通常是通过 Support Center 回复，但在某些情况下，需要电子邮件或电话通信。

> **Important**
>
> 要接收服务请求或事件案例的状态变更通知，您必须在地址字段中输入电子邮件地址。通知仅发送到创建案例时添加到案例中的电子邮件地址。

只有当您在 AMS Accelerate 联合网络上使用电子邮件服务器时，通知电子邮件中的链接才有效。否则，您可以前往 AMS Accelerate 控制台并使用案例详情页面来回复信件。

> **Note**
>
> AMS Accelerate 会将通信发送到您 AWS 账户的主电子邮件地址；我们建议您添加备用操作联系人电子邮件别名，以简 request/notification 化服务管理流程。AMS Accelerate 入职流程和相关的入职文档中对此进行了介绍。

Accelerate 中的事件报告和服务请求测试

在测试事件报告或服务请求时，我们要求您在主题文本AMSTestNoOpsActionRequired中注明。这让 AMS 知道事件或请求仅用于测试。当 AMS 运营工程师看到它时，他们不会以任何方式做出回应。

AMS 加速的账单问题

要提交与账单相关的问题，请完成以下步骤：

1. 在家中打开AWS 支持 中心 https://console.aws.amazon.com/support/ #/。
2. 选择 “账户和账单”。
3. 选择创建案例。
4. 选择 “账户和账单”，然后按照提示提交您的案例。

AWS Managed Services 中的计划活动管理

AWS Managed Services (AMS) 计划活动管理 (PEM) 是一项 AMS 服务。PEM 使用 AMS 服务在客户活动和项目期间参与、协调和协助。PEM 协助协调一系列与 PEM 活动或项目的商定范围和时间表一致的相关活动。

AMS PEM 标准

计划中的活动是一个有范围限制和有时限的项目。AMS 使用您提供的详细信息（包括计划和范围、预期结果以及 AMS 运营部门预计要执行的变更）来在 PEM 活动期间为您提供有效支持。然后，您的云架构师 (CAs) 审查和评估 PEM 活动的完整性、技术实施和 AMS 运营参与度。CA 审查后，AMS 运营部门会审查计划，并与您的云服务交付经理 (CSDM) 协调运营团队的参与。

PEM 的类型

以下是可用的 PEM 类型：

- 比赛日
  - O@@ perational Gameday：一种基于场景的游戏操作响应方法，旨在验证流程、人员和系统的集成。
  - Sec@@ urity Gameday：一种安全事件响应策略，它采用基于场景的游戏方法来评估系统、流程和人员的集成。
- 客户安全事件：计划中的安全事件。例如，渗透测试。
- 迁移支持：为计划的入职和迁移活动提供支持。

此工作流程促进了与 AMS 的合作，以协调与 AMS 支持相关的计划活动和迁移活动。如需有关您的特定要求的帮助，请联系您的 CSDM。

AMS PEM 流程

PEM 流程包括以下阶段：

- PEM 启动：您与 CSDM 合作，为计划中的活动定义目标，并确定 AMS 运营部门需要什么。AMS CAs 审查 PEM 计划的技术方面。他们 CAs 与 AMS Security and Operations 合作进行合规、执行优化和自动化，并定义 PEM 前的执行任务和可交付成果。然后，您的 CSDM 会创建 PEM 工单，并

向 AMS 提供项目信息和技术细节。AMS 需要 14 个日历日的准备时间，让 AMS 运营团队有时间进行规划、提供技术审查和分配资源。

- PEM 审查：AMS 运营团队审查 PEM 申请，并与您的 CSDM 合作，验证 PEM 计划中的信息是否正确和完整。
- PEM 接受：AMS 会审查所提供的信息，并向 CSDM 通报 PEM 活动期间的支持级别。如果 PEM 包含完整的信息，并且您的 CSDM 同意工作范围，则 PEM 就会获得批准。
- 准备和执行：AMS 确保在 PEM 开始之前完成所需的任务，并促进内部和客户沟通。AMS 确保 PEM 计划正确运行，并提供状态和进度报告。

PEM FAQs

如何在 PEM 活动期间通过案例：服务请求 (SRs) /事件与 AMS 接触？

- 在格式的 RFC/SR 主题行中使用您的 CSDM 共享的 PEM ID。*PEM-ID*

  在适用的情况下，您可以使用实时联系选项。
- 您也可以创建服务请求 (SR) 来讨论您的用例或询问有关您计划中的活动的问题。如果你使用 SR，那么 PEM 不一定是有效的。

提交 PEM 相关案例时会进行哪些验证？

- 验证账户 ID 是否已在 PEM 上列出。
- 验证 PEM 状态是否在提供的开始日期和结束日期之间获得批准且处于活动状态。
- 内部向 AMS 工程师提供了指向 PEM 详细信息的链接。

是否有 SLAs 或 SLOs 适用于 PEM 请求？

- PEMs 与 SLAs 或无关 SLOs。
- SLAs SLOs 而与 PEM 相关的工作项目（服务请求、事件）由 AMS 定义。 SLOs

  有关更多信息，请参阅 AMS Accelerate 中的事件报告、服务请求和账单问题。

我们可以通过服务请求 (SR) 创建 PEM 吗？

- 不，PEM 的创建必须由云服务交付管理器 (CSDM) 管理。

按需运营

按需运营 (OOD) 是 AWS Managed Services (AMS) 的一项功能，它通过提供 AMS 运营计划当前未提供的运营服务来扩展您的 AMS 运营计划的标准范围，或 AWS者。 选定后，目录产品将由自动化和高技能的 AMS 资源组合提供。没有长期承诺或额外合同，允许您根据需要扩展现有的 AMS 以及 AWS 运营和能力。您同意按月购买时段（OOD 区块），每个区块 20 小时。

您可以从标准化产品目录中进行选择，并通过服务请求启动新的 OOD 项目。OOD 产品的示例包括协助维护 Amazon EKS、SAP 集群的 AWS Control Tower运营和管理。我们会根据需求和我们最常看到的运营用例定期添加新的目录产品。

OOD 可用于 AMS Advanced 和 AMS Accelerate 运营计划，并且适用于所有可用 AMS AWS 区域的地方。

AMS 在实施您请求的更改时执行客户安全风险管理 (CSRM)。要了解有关 CSRM 流程的更多信息，请参阅更改请求安全审查。

按需运营产品目录

按需操作 (OOD) 为您提供下表中所述的服务。

> **Note**
>
> 有关关键术语的定义，请参阅 AWS Managed Services 文档关键术语。

运营计划	标题	说明	预期成果
AMS Accelerate	亚马逊 EKS 集群维护	AMS 通过处理您的亚马逊 Elastic Kubernetes Service（亚马逊 EKS）部署的持续维护，让您的容器开发人员腾出时间。AMS 执行更新集群所需的 end-to-end程序，包括控制平面、插件和节点的组件。AMS 对托管节点类型以及一组精选的 Amazon EKS 和 Kubernetes 插件进行更新。	客户团队协助完成了更新 Amazon EKS 集群的底层运营工作。

AMS Accelerate	AMI 大楼和自动售货机	AMS 为客户提供 AMI 大楼和自动售货机的持续管理。 我们的工程师每月发布订阅版 AMIs，AMIs 针对紧急修补活动按需发布，使用运行手册管理变更，并使用监控监控 AMI 构建。CloudWatch 我们还为指定账户中的所有 AMIs 用户提供故障排除帮助和详细报告。此产品要求通过 EC2 映像生成器部署 AMI 构建管道。AMS 不支持任何其他与 EC2 图像生成器交互的自动化或服务。	客户安全状况得到改善，AMIs 减少了客户在建筑和自动售货上花费的时间。
AMS Accelerate	精心策划的变更执行	与我们熟练的运营工程师合作，将您的业务需求转化为可在您的 AWS 环境中安全执行的经过验证的变更请求。无论是简单的规模变更还是具有下游影响的复杂行动，都可以利用我们独特的自动化方法和最佳运营实践（例如，影响评估、回滚、两人规则）。	帮助客户定义、创建和执行自定义变更请求。更改可以是手动的，也可以是自动的（CloudFormation，SSM）。必要时包括咨询以 支持获取配置指导。不适用于更改应用程序代码、应用程序安装/部署、数据迁移或操作系统配置更改。

AMS Accelerate	AWS Network Firewall 操作	AMS 与您合作，为您的防火墙加入并实施和管理持续防火墙操作的策略和规则。为此，我们的工程师利用我们的最佳运营实践和自动化来配置标准化的策略和规则，并启用监控功能以检测自动化流程之外所做的更改。AMS 会迅速通知您不需要的更改，并提供选项，以便在需要时将其包括在内，或者将账户恢复到之前的配置，以确保系统的整体稳定性。	客户团队通过快速检测网络防火墙的意外更改来帮助减少管理开销，从而改善了事件解决方案，缩短了预期和意外问题的根本原因分析时间。
AMS Accelerate	AWS Control Tower 操作	持续运营和管理您的 AWS Control Tower 着陆区，包括T AWS ransit Gateway和 AWS Organizations——提供全面的着陆区解决方案。我们使用我们的自定义控件和护栏库处理账户自动售卖、SCP 和 OU 管理、漂移补救、SSO 用户管理以及 AWS Control Tower 升级。	客户团队协助完成了管理 AWS Control Tower、T AWS ransit Gateway 和 AWS Organizations.
AMS Accelerate	AWS landing zone 加快行动	AMS 提供通过 AWS 着陆区加速器 (LZA) 部署的 AWS 着陆区的持续运营。 我们的工程师负责配置文件更改、AWS Control Tower (CT) 环境管理（账户售卖、OU 创建、CT 护栏）、服务控制策略 (SCP) 管理、CT 漂移检测和修复、网络配置管理以及 CT 和 LZA 框架的更新。AWS LZA 提供了一种使用最佳运营实践和服务（例如）来设置和管理安全的多账户 AWS 环境的方法。AWS Control Tower	客户团队为 AWS 着陆区加速器解决方案的持续运营和管理提供了协助。

AMS Accelerate	SAP 集群协助	为您的 SAP 集群提供专门的警报、监控、集群修补、备份和事件修复。此目录项允许您从 SAP 运营团队中卸下一些正在进行的运营工作，以便他们可以专注于容量管理和性能调整。	客户或合作伙伴 SAP 团队协助完成了一些底层运营工作。仍然需要客户提供其他 SAP 功能，例如容量管理、性能调整、数据库管理员和 SAP 基础管理。
AMS Accelerate	EC2 操作中的 SQL Server	AMS 与您协作，对部署在 EC2 实例上的 SQL Server 数据库进行登记、实施和管理其持续操作。 我们的工程师利用我们的最佳运营实践和自动化，通过执行备份和修补等任务、将 AMS 运营支持扩展到 SQL Server 补丁以包括集群感知滚动更新、符合我们的勒索软件防御策略的备份和还原服务，以及监控客户提供的备份和补丁控制的遵守情况，从而腾出您的数据库团队。	SQL Server 客户协助卸载修补和备份数据库操作，以提高其工作负载的弹性和安全状况，此外还通过自带许可证 (BYOL) 来优化许可成本。 EC2
AMS 高级版	亚马逊 EKS 集群维护	AMS 通过处理您的亚马逊 Elastic Kubernetes Service（亚马逊 EKS）部署的持续维护和运行状况来解放您的容器开发人员。AMS 执行更新集群所需的 end-to-end 程序，包括控制平面、插件和节点的组件。AMS 对托管节点类型以及一组精选的 Amazon EKS 和 Kubernetes 插件进行更新。	客户团队协助完成了更新 Amazon EKS 集群的底层运营工作。

AMS 高级版	优先执行 RFC	指定 AMS 运营工程师能力，可优先执行您的变更请求 (RFC)。通过Amazon Chime会议室直接与工程师互动，可以对所有提交的内容进行更高级别的回应，并且可以调整优先顺序。	买家会收到 8 小时的回复 SLO。 RFCs
AMS 高级版和 AMS 加速版	旧版操作系统升级	通过将实例升级到支持的操作系统版本来避免实例迁移。我们可以利用软件供应商的自动化和升级功能（例如，从微软 Windows 2008 R2 到微软 Windows 2012 R2）对您选定的实例进行就地升级。这种方法非常适合无法轻易在新实例上重新安装的旧版应用程序，并且在较旧的操作系统版本上提供了额外的保护，使其免受已知和未缓解的安全威胁。 支持以下操作系统进行就地升级： • 微软 Windows 2012 R2 到微软 Windows 2016 及更高版本 • 微软 Windows 2016 到微软 Windows 2022 及更高版本 • 红帽企业 Linux 7 到红帽企业 Linux 8 • 红帽企业 Linux 8 到红帽企业 Linux 9 • 甲骨文 Linux 7 到甲骨文 Linu	此解决方案适用于无法再在新实例上重新安装的应用程序（例如，源代码丢失、ISV 停业等）。您可以将失败的升级恢复到其原始状态。从操作角度来看，回滚是首选，因为它使用最新的安全补丁可以使实例处于更可支持的状态。

主题

- 按需请求 AMS 操作
- 对按需运营产品进行更改

按需请求 AMS 操作

AWS Managed Services (AMS) 按需运营 (OOD) 适用于所有 AWS 账户 已加入 AMS 的用户。要利用按需运营，请向您的云服务交付经理 (CSDM)、解决方案架构师 (SA)、客户经理或云架构师 (CA) 索取更多信息。前面的按需运营产品目录中列出了可用的 OOD 产品。项目范围界定完成后，向 AMS 运营部门提交服务请求以启动 OOD 项目。

每个 OOD 服务请求都必须包含与项目相关的以下详细信息：

- 所要求的具体 OOD 产品以及每种特定的 OOD 产品：
  - 分配给特定 OOD 产品的区块数量（一个区块等于给定日历月内的 20 小时运营资源时间，按当时 AWS的标准费率为适用的按需运营产品收费）。
  - 申请特定 OOD 产品的每个 AWS Managed Services 账户的账户 ID。

OOD 服务请求必须由您通过以下任一方式提交：

- 接收适用的按需运营产品的 AWS Managed Services 账户，或
- AWS Man AWS Organizations aged Services 账户，代表其任何成员账户（即 AWS Managed Services 账户）处于所有功能模式的管理账户。

收到 OOD 服务请求后，AMS Operations 会审核并更新账户的批准、部分批准或拒绝。

OOD 提供的服务请求获得批准后，AMS 和您就会协调开始合作。在服务请求获得批准并商定项目开始日期之前，不会启动 OOD 产品。

AMS 使用按月订阅的 OOD 区块分配。我们每月分配批准的区块数量，从参与开始日期开始，直到您通过新的服务请求申请退出。OOD 区块在一个日历月内有效。未使用的区块或区块部分不会结转或结转到未来的月份。

无论实际使用的小时数如何，您每月至少需要支付一个 OOD 区块的费用。任何未使用工时的额外分配的 OOD 区块均不计费。

对按需运营产品进行更改

要申请更改按需运营 (OOD) 产品的持续参与，请提交包含以下信息的服务申请：

- 请求的修改，以及
- 所请求的修改生效日期。

收到 OOD 服务请求后，AMS Operations 会审查该请求并更新其批准情况，或者要求分配的 CSDM 与您合作确定修改的范围和影响。如果确定修改需要与 CSDM 进行范围界定，则您需要在范围界定工作完成后提交第二份 OOD 服务请求以启动修改后的项目。

获得批准后，最近修改的区块分配将变为并继续保持活跃状态，取代之前的任何区块分配，除非您 AWS 和您另行同意。

报告和选项

AWS Managed Services (AMS) 整理来自各种原生 AWS 服务的数据，以提供有关主要 AMS 产品的增值报告。

AMS 提供两种类型的详细报告：

- 根据请求报告：您可以通过云服务交付管理器 (CSDM) 临时请求某些报告。这些报告没有限制，因为在入职或关键事件期间，您可能需要多次请求这些报告。但是，请注意，这些报告并不是为了像每周报告那样按计划提供的。要更好地了解您的需求或了解有关使用自助报告的更多信息，请联系您的 CSDM。
- 自助报告：AMS 自助服务报告允许您根据需要随时直接查询和分析数据。使用自助服务报告从 AMS 控制台访问报告，并通过 S3 存储桶（每个账户一个存储桶）报告数据集。这使您可以将数据集成到您最喜欢的商业智能 (BI) 工具中，以便您可以根据自己的要求自定义报告。

主题

应要求报告

主题

AMS 整理来自各种原生 AWS 服务的数据，以提供有关主要 AMS 产品的增值报告。要获取这些报告的副本，请向您的云服务交付经理 (CSDM) 提出申请。

AMS 主机管理报告

可用报告

- SSM 代理覆盖率报告

SSM 代理覆盖率报告

AMS SSM 代理覆盖率报告会告知您账户中的 EC2 实例是否安装了 SSM 代理。

字段名	定义
客户姓名	有多个子客户时的客户名称
资源区域	AWS 资源所在的区域
帐户名称	账户的名称
AWS 账户编号	AWS 账户的 ID
资源 ID	EC2 实例的 ID
资源名称	EC2 实例名称
合规标志	表示资源是否安装了 SSM 代理（“合规”）（“不兼容”）

AMS Backup 报告

可用报告

- Backup Job 成功/失败报告
- Backup 摘要报告
- Backup Summary/Coverage 报告

Backup Job 成功/失败报告

Backup Job Success/Failure 报告提供了有关过去几周内运行的备份的信息。要自定义报告，请指定要检索数据的周数。默认周数为 12。下表列出了报告中包含的数据：

字段名	定义
AWS 账户 ID	资源所属的 AWS 账户 ID
账户名	AWS 账户名称
Backup Job ID	Backup 任务的 ID
资源 ID	备份资源的 ID
资源类型	正在备份的资源类型
资源区域	已备份资源的 AWS 区域
Backup 状态	备份的状态。有关更多信息，请参阅 Backup 作业状态
恢复点 ID	恢复点的唯一标识符
状态消息	备份作业期间发生的错误或警告的描述
Backup 大小	备份的大小（以 GB 为单位）
恢复点 ARN	创建的备份的 ARN
恢复点年限（以天为单位）	自恢复点创建以来已过去的天数
未满 30 天	少于 30 天的备份指示器

Backup 摘要报告

字段名	定义
客户姓名	多个子客户所在情况的客户名称
Backup 月	备份月份
Backup 年份	备份年份
资源类型	正在备份的资源类型

字段名	定义
资源数量	已备份的资源数量
恢复点数	不同快照的数量
备份时间不足 30 天	少于 30 天的备份数量
最大恢复点使用年限	以天为单位的最早恢复点年龄
最小恢复点使用年限	最近的恢复点年限（以天为单位）

Backup Summary/Coverage 报告

Backup Summary/Coverage 报告列出了当前有多少资源未受任何 AWS Backup 计划保护。与您的CDSM讨论适当的计划，以尽可能增加覆盖范围并降低数据丢失的风险。

字段名	定义
客户姓名	多个子客户所在情况的客户名称
区域	AWS 资源所在的区域
帐户名称	账户的名称
AWS 账户编号	AWS 账户的 ID
资源类型	资源类型。资源由 AWS Backup （Aurora、DocumentDB、DynamoDB、EBS、、EFS、RDS EC2 S 和 S3）提供支持 FSx
资源 ARN	资源的 ARN
资源 ID	资源的 ID
覆盖范围	表示资源是否被覆盖（“已覆盖” 或 “未覆盖”）
资源数量	账户中支持的资源数量

字段名	定义
perc_coverage	过去 30 天内执行过备份的受支持资源的百分比。

AWS Config 控制合规性报告

AWS Config 控制合规性报告深入了解 AMS 账户的资源和 AWS Config 规则合规性，您可以按 Config 规则严重性筛选报告，以确定最关键的发现的优先级。下表列出了此报告提供的数据：

字段	说明
日期	举报日期
客户名称	客户名称
AWS 账号	买家的关联 AWS 账户 ID
来源标识符	AWS Config 规则唯一来源标识符
规则描述	AWS Config 规则描述
规则类型	AWS Config 规则类型
合规标志	AWS Config 规则合规性状态
资源类型	AWS 资源类型
资源名称	AWS 资源名称
严重性	AMS 为该 AWS Config 规则定义的默认推荐严重性
补救类别	AWS Config 规则的关联修正响应类别
补救说明	解释补救措施以使 AWS Config 规则合规
客户操作	客户需要采取行动才能使 AWS Config 规则合规
增量指标报告	在给定 2 个日期之间为遵守规则而进行的更改

AMS Config 规则响应配置报告

AMS Config 规则响应配置报告深入了解了您当前如何将 Accelerate 配置为响应不合规的 AMS 配置规则。有关如何更改 AMS 配置规则响应的更多信息，请参阅 AMS 加速自定义结果响应。

此报告仅显示您更改的配置，不包括 AMS Config 规则库中列出的 AMS 默认配置。该报告提供有关 AMS 账户的资源和 AMS 配置规则响应配置的数据，包括以下内容：

- 您更改了 AMS 配置规则默认响应的 AWS 账户列表。
- 您已关联了 AMS 配置规则响应的标签列表。
- 每个规则、账户和标签的响应配置列表。
- 您已更改 AMS 配置规则的默认响应的资源列表。

最新响应配置报告

字段	说明
日期	报告的生成日期
客户名称	客户名称
AWS 账号	与配置关联的 AWS 账户 ID
账户名	AWS 账户级别资源组的账户名
查找类型	已确定的发现类型。在这种情况下， AWS Config
来源标识符	AWS Config 规则唯一来源标识符
资源组 ID	与响应配置关联的资源组 ID
已配置响应操作	由 AMS 触发的操作类型
SSM 运行手册相关联	将要运行的修复运行手册（如果有）
资源组类型	这可以是账号或标签

带有自定义默认响应的 Config 规则的资源

字段名	定义
客户姓名	客户名称
日期	报告的生成日期
AWS 账户名	AWS 账户名
账户 ID	关联 AWS 账户 ID
AMS Config 规则	针对资源并应用配置的 AMS 配置规则
资源 ID	AMS 配置规则所针对的客户账户中的资源 ID
资源区域	应用配置的 AWS 区域
资源类型	AWS 资源类型
资源组 ID	与响应配置关联的资源组 ID
资源 AMS 标志	如果 AWS 资源由 AMS 部署，则此字段将设置为 `True`
触发器类型	为资源配置的响应类型
合规标志	AMS 配置规则合规性状态

“已防止的事件和监控热门话题者” 报告

可用报告

- 已阻止的事件报告
- 监控 Top Talkers 报告

已阻止的事件报告

“已阻止的事件” 报告列出了自动补救的 Amazon CloudWatch 警报，以防止可能发生的事件。要了解更多信息，请参阅自动修复。下表列出了此报告中包含的信息：

字段名	定义
execution_start_time_time_	执行自动化的日期
customer_name	账户客户姓名
account_name	账户的名称
AwsAccountId	AWS 账户的 ID
文档_名称	已执行的 SSM 文档或自动化的名称
持续时间（以分钟为单位）	自动化的时长（以分钟为单位）
区域	AWS 资源所在的区域
自动化_执行_id	执行的 ID
自动化执行状态	执行的状态

监控 Top Talkers 报告

监控 Top Talkers 报告显示了在特定时间段内生成的 Amazon CloudWatch 警报数量，并提供了生成最多警报数量的资源的可视化效果。此报告可帮助您识别生成警报数量最多的资源。这些资源可能是执行根本原因分析以修复问题或修改警报阈值以防止在没有实际问题时出现不必要的触发的候选资源。下表列出了此报告中包含的信息：

字段名	定义
客户名称	客户姓名
AccountId	AWS 账户的 ID
警报类别	触发的警报类型
说明	警报的描述
资源 ID	触发警报的资源的 ID
资源名称	触发警报的资源的名称

字段名	定义
区域	AWS资源所在的区域
事件状态	警报生成的事件的最新状态
第一次出现	警报第一次被触发
最近发生的事件	最近一次触发警报的时间
警报计数	在第一次和最近一次发生之间生成的警报数量

账单费用明细报告

AWS Managed Services (AMS) 账单费用详情报告提供了有关关联账户和相应的 AWS 服务的 AMS 账单费用的详细信息，包括：

- AMS 服务级别费用、提升百分比、账户级 AMS 服务等级和 AMS 费用。
- 关联账户和 AWS 使用费

字段名	定义
账单月份	服务计费的月份和年份
付款人账户 ID	用于识别将负责支付 AMS 费用的账户的 12 位数身份证
关联账户 ID	用于标识使用产生费用的服务的 AMS 账户的 12 位数字 ID
AWS 服务名称	使用的 AWS 服务
AWS 收费	服务名称中列出的 AWS 服务名称的 AWS AWS 费用
定价计划	与关联账户关联的定价计划的名称

字段名	定义
上升比例	基于 pricing_plan、SLA 和 AWS 服务的提升百分比（以十进制 V.WXYZ 表示）
调整后的 AWS 费用	AWS 已针对 AMS 调整使用量
AWS 费用上调	对 AMS 收取的 AWS 费用百分比；adjusted_aws_charges * uplift_percent
实例 EC2 RDS 支出	在 RDS 实例上 EC2 花钱
AMS 费用	该商品的 AMS 费用总额；uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
按比例分配的最低费用	我们为满足合同最低要求而收取的金额
最低费用	AMS 最低费用（如果适用）
关联账户 AMS 费用总额	关联账户的所有费用总和
付款人账户 AMS 费用总额	付款人账户所有费用的总和

可信修正者报告

可用报告

- 可信修正者修正摘要报告
- 可信修正者配置摘要报告
- Trusted Advisor 查看摘要报告

可信修正者修正摘要报告

“可信修正者修正状态” 报告提供有关在先前修正周期中发生的修正的信息。默认周数为 1。要自定义报告，请根据您的补救计划指定周数。

字段名	定义
日期	收集数据的日期。
账户 ID	资源所属的 AWS 账户 ID
账户名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	已修正 Trusted Advisor 的检查的名称
检查 ID	已修正的检查的 Trusted Advisor ID
执行模式	为特定 Trusted Advisor 检查配置的执行模式
OpsItem 身份证	为修复而 OpsItem 创建 Trusted Advisor 的 ID
OpsItem 状态	报告时 OpsItem 创建者的 Trusted Advisor 状态
资源 ID	为修复而创建的资源的 ARN

可信修正者配置摘要报告

“可信修正者配置摘要” 报告提供有关每 Trusted Advisor 项检查的当前可信修正者修正配置的信息。

字段名	定义
日期	收集数据的日期。
账户 ID	配置适用的 AWS 账户 ID
账户名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	配置适用的已修正 Trusted Advisor 检查的名称
检查 ID	配置适用的已修正 Trusted Advisor 检查的 ID

字段名	定义
执行模式	为特定 Trusted Advisor 检查配置的执行模式
改写为 “自动”	标签模式（如果已配置）将执行模式改为 “自动”
改为手动	标签模式（如果已配置）将执行模式改为手动

Trusted Advisor 查看摘要报告

支 Trusted Advisor 票摘要报告提供有关当前 Trusted Advisor 支票的信息。该报告在每个每周补救计划之后收集数据。默认周数为 1。要自定义报告，请根据您的修复周期指定周数。

字段名	定义
日期	收集数据的日期。
账户 ID	配置适用的 AWS 账户 ID
客户姓名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	配置适用的已修正 Trusted Advisor 检查的名称
检查 ID	配置适用的已修正 Trusted Advisor 检查的 ID
状态	支票的警报状态。可能的状态为正常（绿色）、警告（黄色）、错误（红色）或 not_available
已标记的资源	Trusted Advisor 支票标记（列出）的 AWS 资源数量。
资源已忽略	Trusted Advisor 由于您将 AWS 资源标记为已禁止而被忽略的资源数量。
处于危急状态的资源	处于临界状态的资源数量
资源处于警告状态	处于警告状态的资源数量

自助报告

AWS Managed Services (AMS) 自助服务报告 (SSR) 是一项功能，可从各种原生 AWS 服务收集数据，并提供对主要 AMS 产品报告的访问权限。SSR 提供的信息可用于支持运营、配置管理、资产管理、安全管理和合规性。

使用 SSR 从 AMS 控制台访问报告，并通过 Amazon S3 存储桶（每个账户一个存储桶）报告数据集。您可以将数据插入您最喜欢的商业智能 (BI) 工具，以根据您的独特需求自定义报告。AMS <Account_ID>在您的主 AWS 区域创建此 S3 存储桶（S3 存储桶名称:(ams-reporting-data-a)，数据将从 us-east-1 区域托管的 AMS 控制平面共享。

要允许您的用户在 AMS 控制台中查看 AMS Accelerate 报告，您必须在 AWS Identity and Access Management (IAM) 中授予执行这些操作的明确权限。有关 IAM 策略的示例，请参阅使用 AMS 功能的权限。

> **Important**
>
> 将自定义密钥与 AWS Glue
> 要使用客户管理的 KMS 密钥加密您的 AWS Glue 元数据，您必须执行以下额外步骤以允许 AMS 聚合账户中的数据：
>
> 1. 在 https://console.aws.amazon.com/km s 处打开 AWS Key Management Service 控制台，然后选择客户托管密钥。
> 2. 选择您计划用于加密 AWS Glue 元数据的密钥 ID。
> 3. 选择 “别名” 选项卡，然后选择 “创建别名”。
> 4. 在文本框中输入 AmsReportingFlywheelCustomKey，然后选择创建别名。

主题

- 数据保留策略
- 从 SSR 中脱颖而出

内部 API 操作

如果您监控 API 操作，则可能会看到对以下仅限内部操作的调用：

- `GetDashboardUrl`
- `ListReportsV2`

内部 API 操作： GetDashboardUrl

当 AMS 控制台调用此操作时，此操作会显示在系统日志中。它没有其他用例。它不能直接供您使用。

返回相应报告的嵌入式仪表板 URL。此操作接受`dashboardName`返回的`ListReports`。

请求语法

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

请求元素

`dashboardName`：请求网址的 QuickSight仪表板的名称。在 ListReports V2 中返回仪表板名称。

类型：字符串

响应语法

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。服务以 JSON 格式返回以下数据。

`url`: 返回所请求的 QuickSight 网址`dashboardName`。

类型：字符串

错误

有关所有操作中常见的错误的信息，请参阅常见错误。

`BadRequestException`:

提交的请求无效。例如，如果输入不完整或不正确。有关详细信息，请参阅随附的错误消息。

HTTP 状态代码：400

`NotFoundException`:

未找到请求的资源。请确保请求的 URI 正确无误。

HTTP 状态代码：404

`TooManyRequestsException`:

该请求已达到其限制限制。在指定的时间段后重试。

HTTP 状态代码：429

`UnauthorizedException`:

请求被拒绝，因为来电者的权限不足。

HTTP 状态代码：401

内部 API 操作： ListReportsV2

当 AMS 控制台调用时，此 API 会出现在系统日志中。它没有其他用例。它不能直接供您使用。

返回指定账户可用的操作报告列表。

请求语法

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json
{
```

```
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。服务以 JSON 格式返回以下数据。

reportsList: 现有行动报告清单。

类型：仪表板对象数组

reportsType：表示报告是否跨多个账户汇总。

类型：字符串

错误

有关所有操作中常见的错误的信息，请参阅常见错误。

BadRequestException:

提交的请求无效。例如，输入不完整或不正确。有关详细信息，请参阅随附的错误消息。

HTTP 状态代码：400

NotFoundException:

未找到请求的资源。请确保请求的 URI 正确无误。

HTTP 状态代码：404

TooManyRequestsException:

该请求已达到其限制限制。在指定的时间段后重试。

HTTP 状态代码：429

UnauthorizedException:

请求被拒绝，因为来电者的权限不足。

HTTP 状态代码：401

补丁报告（每日）

可用报告

- AMS 修补的实例详细信息摘要
- 补丁详情
- 错过补丁的实例

AMS 修补的实例详细信息摘要

这是一份信息性报告，可帮助识别已加入 AMS Patching 的所有实例、账户状态、实例详细信息、维护时段覆盖范围、维护时段执行时间、堆栈详细信息和平台类型。

该数据集提供：

- 账户的生产和非生产实例的数据。生产和非生产阶段源自账户名，而不是实例标签。
- 按平台类型划分的实例分布数据。当 Sy AWS stems Manager (SSM) 无法获取平台信息时，就会出现 “N/A” 平台类型。
- 有关实例状态分布、正在运行、停止或终止的实例数量的数据。

控制台字段名称	数据集字段名称	定义
访问限制	访问限制	访问受限的地区
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名
账户状态	账户状态	AMS 账户状态
	account_sla	AMS 账户服务承诺
Account Type (账户类型)	malz_role	MALZ 角色

控制台字段名称	数据集字段名称	定义
自动扩缩组名	instance_asg_name	包含实例的 Auto Scaling 组 (ASG) 的名称
实例 ID	instance_id	EC2 实例的 ID
实例名称	实例名	EC2 实例的名称
实例补丁组	实例_补丁_组	修补组名称用于将实例分组在一起并应用相同的维护时段
实例补丁组类型	实例_补丁_组_类型	补丁组类型
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例平台名称	实例_平台_名称	操作系统 (OS) 名称
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签
着陆区	malz_flag	举报与 MALZ 相关的账户
维护时段覆盖范围	mw_covered_flag	如果实例至少有一个已启用的维护时段，且执行日期为 future，则该实例被视为已覆盖，否则不包括在内
维护时段执行日期/时间	最早的 window_execution_time	下次预计会执行维护时段
维护时段执行日期/时间	最早的 window_execution_time	下次预计会执行维护时段
生产账户	产品账号	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值 “PROD”、“NONPROD”。

控制台字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间。
堆栈名称	实例堆栈名称	包含实例的堆栈名称
堆栈类型	实例堆栈类型	AMS 堆栈（客户账户中的 AMS 基础架构）或客户堆栈（支持客户应用程序的 AMS 托管基础架构）

补丁详情

该报告提供了各种实例的补丁详细信息和维护时段覆盖范围。

该报告提供：

- 有关补丁组及其类型的数据。
- 有关维护时段、持续时间、截止时间、维护时段执行的未来日期（计划）以及每个窗口中受影响的实例的数据。
- 该账户下所有操作系统的数据以及安装该操作系统的实例数量。

字段名	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
账户名	account_name	AWS 账户名
账户状态	账户状态	AMS 账户状态
合规-关键	合规性_关键	严重性为 “严重” 的兼容补丁数量
合规-高	合规性高	严重性为 “高” 的兼容补丁数量

字段名	数据集字段名称	定义
合规-中等	合规_中等	严重性为 “中等” 的兼容补丁数量
合规-低	合规性低	严重性为 “低” 的兼容补丁数量
合规-信息性	合规_信息	严重性为 “信息性” 的兼容补丁数量
合规-未指定	合规_未指定	严重性为 “未指定” 的兼容补丁数量
合规-总计	合规总计	合规补丁数量（所有严重性）
实例 ID	instance_id	EC2 实例的 ID
实例名称	实例名	EC2 实例的名称
	account_sla	AMS 账户服务等级
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例平台名称	实例_平台_名称	操作系统 (OS) 名称
实例补丁组类型	实例_补丁_组_类型	默认：默认补丁组和默认维护时段，由实例上的:True AMSDefault PatchGroup 标签确定 客户：客户创建的补丁组 未分配：未分配补丁组
实例补丁组	实例_补丁_组	修补组名称用于将实例分组在一起并应用相同的维护时段
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签

字段名	数据集字段名称	定义
上次执行维护窗口	上次执行窗口	最近一次执行维护时段的时间
维护时段 ID	window_id	维护时段 ID
维护窗口状态	window_state	维护窗口状态
维护时段类型	窗口类型	维护时段类型
维护时段下次执行日期时间	window_next execution_time	下次预计会执行维护时段
维护时段持续时间 (小时)	窗口持续时间	维护时段的持续时间（以小时为单位）
维护时段覆盖范围	mw_covered_flag	如果实例至少有一个已启用的维护时段，且执行日期为 future，则该实例被视为已覆盖，否则不包括在内
不合规-严重	不合规_严重	严重性为 “严重” 的不合规补丁数量
不合规-高	不合规_高	严重性为 “高” 的不合规补丁数量
不合规-中等	不合规_中等	严重性为 “中等” 的不合规补丁数量
不合规-低	不合规_低	严重性为 “低” 的不合规补丁数量
不合规-信息性	不合规 _信息	严重性为 “信息性” 的不合规补丁数量
不合规-未指定	不合规 _未指定	严重性为 “未指定” 的不合规补丁数量

字段名	数据集字段名称	定义
不合规-合计	不合规总数	不合规补丁数量（所有严重性）
补丁基准 ID	patch_baseline_id	当前附加到实例的补丁基准
补丁状态	补丁状态	总体补丁合规性状态。如果至少缺少一个补丁，则认为实例不合规，否则视为合规。
生产账户	产品账号	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值 “PROD”、“NONPROD”。
堆栈类型	实例堆栈类型	AMS 堆栈（客户账户中的 AMS 基础架构）或客户堆栈（支持客户应用程序的 AMS 托管基础架构）
	window_next_exec_yyyy	window_next_execution_time 的年份部分
	window_next_exec_mm	window_next_execution_time 的月份部分
	window_next_exec_D	window_next_execution_time 的当天部分
	window_next _exec_HHMI	小时:window_next_execution_time 的分钟部分

错过补丁的实例

此报告提供了在上次执行维护时段期间错过补丁的实例的详细信息。

该报告提供：

- 补丁 ID 级别的缺失补丁数据。
- 有关至少缺少一个补丁的所有实例以及补丁严重性、未修补天数、补丁范围和补丁发布日期等属性的数据。

字段名	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
账户名	account_name	AWS 账户名
客户姓名父公司	客户_姓名_父级	
客户姓名	customer_name	
生产账户	产品账号	AMS 生产账户或非生产账户的标识符，具体取决于账户名称包含值 “PROD” 还是 “NONPROD”。
账户状态	账户状态	AMS 账户状态
Account Type (账户类型)	账户类型	
	account_sla	AMS 账户服务等级
实例 ID	instance_id	您的 EC2 实例的 ID
实例名称	实例名	您的 EC2 实例的名称
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签
补丁编号	补丁_id	已发布补丁的 ID

字段名	数据集字段名称	定义
补丁严重性	patch_sev	每个发行商的补丁严重程度
补丁分类	补丁类	补丁发布者对补丁的分类
补丁发布日期时间 (UTC)	release_dt_utc	每个发行商的补丁发布日期
补丁安装状态	安装状态	每个 SSM 在实例上安装补丁状态
未修补的天数	days_unpatched	自上次 SSM 扫描以来实例未修补的天数
未修补天数范围	days_unpatched_bucke	一大堆未修补的天数

Backup 报告（每日）

备份报告涵盖主要和次要区域（如果适用）。它涵盖了备份的状态（成功/失败）以及拍摄的快照的数据。

该报告提供：

- Backup 状态
- 拍摄的快照数量
- 恢复点
- Backup 计划和保管库信息

字段名	数据集字段名称	定义
报告日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	实例 ID 所属的 AWS 账户 ID
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名称

字段名	数据集字段名称	定义
账户 SLA	account_sla	AMS 账户服务承诺
	malz_flag	举报与 MALZ 相关的账户
	malz_role	MALZ 角色
	访问限制	访问受限的地区
Backup 快照计划开始日期/时间	start_by_dt_utc	计划开始快照的时间戳
Backup 快照实际开始日期/时间	creation_dt_utc	快照实际开始的时间戳
Backup 快照完成日期/时间	completion_dt_utc	快照完成的时间戳
Backup 快照到期日期/时间	expiration_dt_utc	快照过期的时间戳
Backup Job 状态	备份任务状态	快照的状态
Backup 类型	backup_type	备份类型
Backup Job ID	备份作业 ID	备份任务的唯一标识符
Backup 大小（字节）	backup_size_in_bytes	以字节为单位的备份大小
Backup Plan ARN	backup_plan_arn	备份计划 ARN
Backup Plan ID	备份计划_ID	Backup 计划唯一标识符
备份计划名称	备份计划名称	Backup 计划名称
Backup 计划版本	备份计划版本	备份计划版本
Backup 规则 ID	backup_rule_id	备份规则 ID
Backup Vault ARN	backup_vault_arn	Backup 保管库 ARN
备份文件库名称	备份保管库名称	备份库名称

字段名	数据集字段名称	定义
IAM 角色 ARN	iam_role_arn	IAM 角色 ARN
实例 ID	instance_id	唯一的实例 ID
实例状态	实例状态	实例状态
实例标签	ec2_tags	与 EC2 实例 ID 关联的标签
资源 ARN	resource_arn	Amazon 资源名称
资源 ID	资源_id	唯一的资源标识符
资源区域	资源_区域	资源的主要（以及次要区域，如果适用）。
资源类型	resource_type	资源的类型
恢复点 ARN	recovery_point_arn	恢复点的 ARN
恢复点 ID	恢复点_id	恢复点的唯一标识符
恢复点状态	恢复点状态	恢复点状态
恢复点数天后删除	恢复点_delete_delete_delete_days	恢复点将在几天后删除
几天后，恢复点会移至冷库	recovery_point_move_to_to_to_cold_storage_days	完成日期之后将备份快照移至冷存储的天数
恢复点加密状态	recovery_point_已加密	恢复点加密状态
恢复点加密密钥 ARN	recovery_point_cryption_key_arn	恢复点加密密钥 ARN
堆栈编号	stack_id	云形成堆栈唯一标识符
堆栈名称	stack_name	堆栈名称
标签：AMS 默认补丁组	tag_ams_default_patch_group	标签值：AMS 默认补丁组

字段名	数据集字段名称	定义
标签：应用程序 ID	tag_app_id	标签值：应用程序 ID
标签：应用程序名称	tag_app_name	标签值：应用程序名称
标签：Backup	标签_备份	标签值：Backup
标签：合规框架	标签合规框架	标签价值：合规框架
标签：成本中心	tag_cost_center	标签价值：成本中心
标签：客户	标签_客户	标签值：客户
标签：数据分类	标签_数据_分类	标签值：数据分类
标签：环境类型	标签_环境_类型	标签值：环境类型
标签：营业时间	标签操作时间	标签值：营业时间
标签：车主团队	tag_owner_team	标签值：所有者团队
标签：车主团队电子邮件	tag_owner_team_email	标签值：所有者团队电子邮件
标签：补丁组	tag_patch_group	标签值：补丁组
标签：Support 优先级	标签_支持_优先级	标签值：Support Priority
音量状态	音量状态	音量状态

事件报告（每周）

该报告提供了事件的汇总列表及其优先级、严重程度和最新状态，包括：

- 被归类为托管账户事件的支持案例数据
- 可视化托管账户的事件指标所需的事件信息
- 有关每起事件的事件类别和补救状态的数据

每周事件报告均提供可视化和数据。

- 可视化可以通过账户中的 AMS 控制台通过 “报告” 页面进行访问。
- 具有以下架构的数据集可通过托管账户中的 S3 存储桶进行访问。
- 使用提供的日期字段，根据事件创建或解决的月、季度、周、 and/or 日筛选事件。

字段名	数据集字段名称	定义
报告日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	AWS 事件所属的账户 ID。
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名。
案例编号	case_id	事件的 ID。
创建月份	创建月份	事件发生的月份。
优先级	priority	事件的优先级。
严重性	severity	事件的严重程度。
状态	状态	事件的状态。
类别	yuma_类别	事件的类别。
创建日	created_day	以 YYYY-MM-DD格式创建事件的那一天。
创建周	created_wk	事件以 YYYY-WW 格式创建的那一周。星期日至星期六算作一周的开始和结束。每周从 01 到 52。第 01 周始终是包含一年中第一天的那一周。例如，2023-12-31和2024-01-01在2024-01周。

字段名	数据集字段名称	定义
创建季度	created_qtr	以 YYYYY-Q 格式创建事件的季度。01/01 到 03/31 被定义为第一季度，依此类推。
已解决的日子	resolved_day	以 YYYY-MM-DD格式解决事件的那一天。
已解决周	resolved_wk	以 YYYYY-WW 格式解决事件的那一周。星期日至星期六算作一周的开始和结束。每周从 01 到 52。第 01 周始终是包含一年中第一天的那一周。例如，2023-12-31和2024-01-01在2024-01周。
已解决月份	已解决_month	事件得到解决的月份，格式为 YYYY-MM。
已解决的季度	resolved_qtr	以 YYYYY-Q 格式解决事件的季度。01/01 到 03/31 被定义为第一季度，依此类推。
已创建分组规则	分组规则	适用于事件的分组规则。“no_grouping” 或 “实例分组”。
实例 IDs	实例_id	与事件关联的实例。
警报数量	警报数量	与该事件相关的警报数量。如果您启用了分组，则此数字可以大于 1。如果您未启用分组，则它将始终为 1。
创建于	created_at	事件发生的时间戳。
警报 ARNs	alarm_arns	与您的事件相关的警报的 Amazon 资源名称 (“arn”)。

字段名	数据集字段名称	定义
相关警报	相关警报	与事件相关的所有警报的易读名称。

账单报告（每月）

账单费用详情

该报告详细介绍了关联账户和相应的 AWS 服务的 AMS 账单费用。

该报告提供：

- 有关 AMS 服务级别费用、提升百分比、账户级 AMS 服务等级和 AMS 费用的数据。
- 关联账户和 AWS 使用费用的数据。

> **Important**
>
> 月度账单报告仅在您的管理付款人账户 (MPA) 或您定义的借记账户中可用。这些账户是发送您的 AMS 月度账单的账户。如果您无法找到这些帐户，请联系您的云服务交付经理 (CSDM) 寻求帮助。

字段名	数据集字段名称	定义
账单日期	date	服务计费的月份和年份
付款人账户 ID	payer_account_id	用于识别负责支付 AMS 费用的账户的 12 位数身份证
关联账户 ID	linked_account_id	用于标识 AMS 账户的 12 位数字 ID，该账户使用可生成扩展的服务
AWS 服务名称	product_name	使用的 AWS 服务

字段名	数据集字段名称	定义
AWS 收费	aws_charg	AWS 服务名称中 AWS 服务名称的 AWS 费用
定价计划	定价计划	与关联账户关联的定价计划
AMS 服务组	tier_uplifting_groups	用于确定提升百分比的 AMS 服务组代码
上升比例	上升百分比	基于 pricing_plan、SLA 和服务的提升百分比（以十进制 V.WXYZ 表示） AWS
调整后的 AWS 费用	调整后的 aws_usage	AWS 已针对 AMS 调整使用量
提高冲锋量 AWS	uplifted_aws_charges	AMS 要 AWS 收取的费用百分比；adjusted_aws_charges * uplift_percent
实例 EC2 RDS 支出	instances_ec2_rds_spend	在 RDS 实例上 EC2 花钱
预留实例费用	ris_charges	预留实例费用
上调的预留实例费用	uplifted_ris	向 AMS 收取的预留实例费用的百分比；ris_charges * uplift_percent
Savings Plan 费用	sp_charges	SavingsPlan 使用费
Uplifted Savings Plan 费用	uplifted_sp	向 AMS 收取的储蓄计划费用百分比；sp_charges * uplift_percent
AMS 费用	ams_charges	ams 对该产品的总费用；uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp

字段名	数据集字段名称	定义
按比例分配的最低费用	按比例分配的最小值	我们为满足合同最低要求而收取的金额
关联账户 AMS 费用总额	关联账户总计 ams_charges	关联账户的所有费用总和
付款人账户 AMS 费用总额	付款人账户总计 ams_charges	付款人账户所有费用的总和
最低费用	最低费用	AMS 最低费用（如果适用）
预留实例和 Savings Plan 折扣	adj_ri_sp_charges	RI/SP discount to be applied against RI/SP费用（在某些情况下适用）

汇总报告

聚合自助服务报告 (SSR) 为您提供在组织层面、跨账户汇总的现有自助服务报告的视图。这使您可以了解您内部所有账户中由 AMS 管理的所有账户的关键运营指标，例如补丁合规性、备份覆盖范围和事件 AWS Organizations。

所有提供 AWS Managed Services AWS 区域 的商业版均提供聚合 SSR。有关可用区域的完整列表，请参阅区域表。

启用汇总报告

您必须通过管理账户 AWS Organizations 管理聚合的 SSR。管理 AWS 账户是您用来创建组织的账户。

要为已登录 AMS 的 AWS Organizations 管理账户启用聚合 SSR，请访问您的 AMS 控制台并导航到报告。选择 top-right-hand角落的组织访问权限以打开 AWS Managed Services 控制台：组织视图窗格。在此窗格中，您可以管理聚合 SSR 功能。

AWS Organizations 未加入 AMS 的管理账户无权访问 AMS 控制台。要为未加入 AMS 的 AWS Organizations 管理账户启用聚合 SSR，请先向您的账户进行身份验证 AWS 账户，然后导航到AWS

控制台并搜索 Managed Services。这将打开 AMS 营销页面。在此页面上，选择导航栏中的组织访问权限链接，打开 AWS Managed Services 控制台：组织视图，您可以在其中管理聚合 SSR 功能。

首次访问 AWS Managed Services 控制台：组织视图时，请完成以下步骤：

1. 如果您尚未设置 AWS Organizations，请 AWS Organizations从您的主机中选择 “启用”。有关设置的更多信息 AWS Organizations，请参阅《AWS Organizations 用户指南》。如果您已经在使用，则可以跳过此步骤 AWS Organizations。
2. 要启用聚合自助服务报告服务，请在控制台上选择启用可信访问。
3. （可选）注册授权管理员以获得组织视图的读取权限。

以授权管理员身份查看汇总报告

委托管理员是您选择拥有汇总报告的读取权限的账户。委派的管理员必须是 AMS 已注册的账户，并且是唯一拥有汇总报告读取权限的账户。

要选择委托管理员，请在 AWS Managed Services 控制台：组织视图的步骤 3 中输入账户 ID。您一次只能注册一个委托管理员账户。请注意，委派的管理员账户必须是 AMS 管理的账户。

要更新委托管理员账户，请导航至 AWS Managed Services 控制台：组织视图，然后选择移除授权管理员。控制台会提示您插入新的账户 ID 以注册为委派管理员。

阅读汇总报告

如果您未注册授权管理员，并且您的 AWS Organizations 管理账户已加入 AMS，则默认情况下，该 AWS Organizations 管理账户将获得对汇总报告的读取权限。如果 AWS Organizations 管理账户不由 AMS 管理，则必须选择授权管理员账户才能读取汇总报告。

在任何时候，只有一个注册到 AMS 的账户拥有对汇总报告的读取权限，无论是 AWS Organizations 管理账户还是注册的委托管理员。您组织内的所有其他成员账户（并已加入 AMS）仍然只能访问每个个人账户的单一账户报告。

启用聚合 SSR 后，导航到您的报告。此部分列出了您现有的所有自助服务报告，蓝色标签表示这些报告已汇总。请注意，您必须使用您选择的账户访问 AMS 控制台，才能读取汇总报告。这要么是 AWS Organizations 管理账号，要么是委派管理员账号。

启用聚合 SSR 后，可以从下一个报告周期开始使用聚合报告。

禁用聚合报告

要禁用聚合 SSR，请打开 AWS Managed Services 控制台：组织视图。选择 “禁用可信访问”。禁用聚合 SSR 的可信访问权限后，将停止在组织级别跨账户汇总您的 AMS 自助服务报告。另请注意，停用从下一个报告周期开始生效。

禁用 “聚合 SSR” 后，您需要等待 AMS 控制台中的报告才会显示为单一账户报告。之所以出现这种延迟，是因为该功能的停用从下一个报告周期开始生效。

AMS 自助服务报告仪表板

AMS 自助服务报告提供两个仪表板：资源标记器控制面板和安全配置 Rules 控制面板。

资源标记器控制面板

AMS 资源标记器控制面板提供有关资源标记器支持的资源的详细信息，以及资源标记器配置为应用于这些资源的标签的当前状态。

按资源类型划分的资源标记器覆盖率

该数据集由具有资源标记器管理的标签的资源列表组成。

按资源类型划分的资源覆盖率可视化为四个折线图，这些折线图描述了以下指标：

- 资源数量：按资源类型划分的区域中的资源总数。
- 缺少托管标签的资源：按资源类型划分的区域中需要托管标签但未由资源标记器标记的资源总数。
- 非托管资源：按资源类型划分的区域中未使用资源标记器应用托管标签的资源总数。这通常意味着这些资源与任何资源标记器配置都不匹配，或者被明确排除在配置之外。
- 托管资源：对应于非托管资源指标（资源计数-非托管资源）。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间（UTC 时间）
AWS 账户 身份证	aws_account_id	AWS 账户 身份证

字段名称	数据集字段名称	定义
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
资源计数	资源计数	在该区域部署的（指定资源类型的）资源数量。
ResourcesMissingManagedTags	资源缺失托管标签计数	根据配置配置文件，需要托管标签但尚未由资源标记器标记的资源（指定资源类型）的数量。
UnmanagedResources	unmanaged_resource_count	Resource Tagger 未应用托管标签的资源（指定资源类型）的数量。通常，这些资源与任何 Resource Tagger 配置块都不匹配，或者被明确排除在配置块之外。

资源标记器配置规则合规性

该数据集由按资源类型划分的资源列表组成，这些资源应用了特定的配置文件。 AWS 区域它被可视化为折线图。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间（UTC 时间）

字段名称	数据集字段名称	定义
AWS 账户 身份证	aws_account_id	AWS 账户 身份证
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
配置配置文件 ID	配置_配置文件_ID	资源标记器配置文件的 ID。配置文件用于定义用于标记资源的策略和规则。
MatchingResourceCount	资源计数	与 Resource Tagger 配置配置文件 ID 相匹配的资源（指定资源类型）的数量。要使资源与配置文件匹配，必须启用配置文件并且资源必须与配置文件的规则相匹配。

资源标记器不合规的资源

此数据集由不符合单个资源标记器配置的资源列表组成。这些数据是资源合规性的每日快照，显示了将这些报告交付给客户账户时客户资源的状态（没有历史视图）。它可视化为一个数据透视表，由不适用于给定配置的资源组成。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间（UTC 时间）
AWS 账户 身份证	aws_account_id	AWS 账户 身份证

字段名称	数据集字段名称	定义
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
资源 ID	资源_id	资源标记器支持的资源的唯一标识符。
覆盖状态	coverage_state	此字段表示资源是否按资源标记器配置 ID 的配置进行标记。
配置配置文件 ID	配置_配置文件_ID	资源标记器配置文件的 ID。配置文件用于定义用于标记资源的策略和规则。

安全配置 Rules 控制面板

Security Config 规则控制面板可深入了解 AMS 账户的资源和 AWS Config 规则合规性。您可以按规则严重性筛选报告，以确定最关键的发现的优先级。下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
AWS 账户 身份证	AWS 账户 身份证	与相关资源关联的账户 ID。
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
报告日期时间	举报日期	报告的生成日期和时间。
customer_name	客户姓名	客户名称。
account_name	账户名	与账户 ID 关联的名称

字段名称	数据集字段名称	定义
资源_id	资源 ID	资源的标识符。
资源_区域	资源区域	资源 AWS 区域 所在的位置。
resource_type	资源类型	AWS 服务 或资源类型。
资源名称	资源名称	资源的名称。
资源_ams_flag	资源 AMS 标志	如果资源由 AMS 拥有，则此标志设置为 TRUE。如果资源归客户所有，则此标志设置为 FALSE。如果所有权未知，则此标志将设置为 UNKNOWN。
配置规则	Config 规则	配置规则的不可自定义名称。
配置规则_描述	Config 规则描述	配置规则的描述。
源标识符	来源标识符	托管配置规则的唯一标识符，没有自定义配置规则的标识符。
合规标志	合规标志	显示资源是符合还是不符合配置规则。
规则_类型	规则类型	表示规则是预定义的还是定制的。
异常标志	异常标志	资源异常标志显示针对不合规资源的风险接受程度。如果资源的资源异常标志为 TRUE，则该资源将被豁免。如果异常标志为 NULL，则该资源不会被豁免。
cal_dt	日期	规则的评估日期。

字段名称	数据集字段名称	定义
补救说明	补救说明	关于如何修复规则合规性的描述。
severity	严重性	Config 规则严重性表示不合规的影响。
客户行动	客户行动	您需要采取措施来纠正此规则。
建议	建议	对配置规则检查内容的描述。
补救类别	补救类别	当此规则变得不合规时，AMS 采取的默认操作。

数据保留策略

AMS SSR 对每份报告都有数据保留政策，报告期过后，数据将被清除且不再可用。

报告名称	数据保留 SSR 控制台	数据保留 SSR S3 存储桶
AMS 修补的实例详细信息摘要	2 个月	2 年
补丁详情	2 个月	2 年
在维护时段执行期间错过补丁的实例	2 个月	2 年
AMS 账单费用详情	2 年	2 年
每日备份报告	1 个月	2 年
每周事件报告	2 个月	2 年
安全配置 Config 规则控制面板	3 个月	2 年
资源标记器控制面板	1 年	2 年

从 SSR 中脱颖而出

要退出 SSR 服务，请通过 AMS 控制台创建服务请求 (SR)。提交 SR 后，AMS 运营工程师会帮助您退出 SSR。在 SR 中，提供你想下车的原因。

要退出账户并执行资源清理，请通过 AMS 控制台创建 SR。提交 SR 后，AMS 操作工程师会帮助您删除 SSR 的 Amazon S3 存储桶。

如果您已退出 AMS，则会自动退出 AMS SSR 控制台。AMS 会自动停止向您的账户发送数据。作为离职流程的一部分，AMS 会删除您的 SSR S3 存储桶。

AMS 中的访问管理加速

访问管理是通过仅允许授权和经过身份验证的访问来保护您的资源的方式。使用 AMS Accelerate，您负责管理对您 AWS 账户 及其底层资源的访问权限，例如访问管理解决方案、访问策略和相关流程。为了帮助您管理访问解决方案，AMS Accelerate 部署了检测常见的 IAM 错误配置的 AWS Config 规则，然后发送补救通知。一个常见的 IAM 配置错误是根用户拥有访问密钥。`iam-root-access-key-check`配置规则检查根用户访问密钥是否可用且合规，或者访问密钥是否不存在。有关 AMS 部署的配置规则列表，请参阅 AMS AWS Config 规则库。

主题

访问加速控制台

当你加入 Accelerate 时，你可以自动访问加速控制台。您可以通过在 AWS 管理控制台中搜索 Managed Services 来访问控制台。Accelerate 控制台可让你概括了解你的 Accelerate 所拥有的功能。此视图包括仪表板和配置页面上显示的各个组件。

使用 AMS 功能的权限

要允许您的用户读取和配置 AMS Accelerate 功能，例如访问 AMS 控制台或配置备份，您必须向他们的 IAM 角色授予执行这些操作的明确权限。以下 CloudFormation 模板包含读取和配置与 AMS 关联的服务所需的策略，以便您可以将其分配给您的 IAM 角色。它们旨在与 IT 行业中需要管理员或只读权限的常见工作职责保持一致；但是，如果您需要向用户授予不同的权限，则可以编辑策略以包含或排除特定权限。您还可以创建自己的自定义策略。

该模板提供了两个策略。该`AMSAccelerateAdminAccess`政策旨在用于设置和操作 AMS Accelerate 组件。此策略通常由 IT 管理员执行，并授予配置 AMS 功能（例如修补和备份）的权限。`AMSAccelerateReadOnly`授予查看 AMS Accelerate 相关资源所需的最低权限。

```
AWSTemplateFormatVersion: 2010-09-09
Description: AMSAccelerateCustomerAccessPolicies
```

```
Resources:
  AMSAccelerateAdminAccess:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateAdminAccess
      Path: /
      PolicyDocument:
        Fn::Sub:
        - |
          {
            "Version": "2012-10-17",
            "Statement": [
              {
                 "Sid": "AmsSelfServiceReport",
                 "Effect": "Allow",
                 "Action": "amsssrv:*",
                 "Resource": "*"
              },
              {
                "Sid": "AmsBackupPolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/ams-backup-iam-role"
              },
              {
                "Sid": "AmsChangeRecordKMSPolicy",
                "Effect": "Allow",
                "Action": [
                  "kms:Encrypt",
                  "kms:Decrypt",
                  "kms:GenerateDataKey"
                ],
                "Resource": [
                  "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
                ],
                "Condition": {
                  "ForAnyValue:StringLike": {
                    "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                  }
                }
              },
              {
                "Sid": "AmsChangeRecordAthenaReadPolicy",
```

```
                "Effect": "Allow",
                "Action": [
                  "athena:BatchGetNamedQuery",
                  "athena:Get*",
                  "athena:List*",
                  "athena:StartQueryExecution",
                  "athena:UpdateWorkGroup",
                  "glue:GetDatabase*",
                  "glue:GetTable*",
                  "s3:GetAccountPublicAccessBlock",
                  "s3:ListAccessPoints",
                  "s3:ListAllMyBuckets"
                ],
                "Resource": "*"
              },
              {
                "Sid": "AmsChangeRecordS3ReadPolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:Get*",
                  "s3:List*"
                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/
*",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                  "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
                ]
              },
              {
                "Sid": "AmsChangeRecordS3WritePolicy",
                "Effect": "Allow",
                "Action": [
                  "s3:PutObject",
                  "s3:PutObjectLegalHold",
                  "s3:PutObjectRetention"

                ],
                "Resource": [
                  "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
                ]
              },
              {
```

```
      "Sid": "MaciePolicy",
      "Effect": "Allow",
      "Action": [
        "macie2:GetFindingStatistics"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPolicy",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetFindingsStatistics",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SupportPolicy",
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
    },
    {
      "Sid": "ConfigPolicy",
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:StartConfigRulesEvaluation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppConfigReadPolicy",
      "Effect": "Allow",
      "Action": [
        "appconfig:List*",
        "appconfig:Get*"
      ],
      "Resource": "*"
    },
    {
```

```
                "Sid": "AppConfigPolicy",
                "Effect": "Allow",
                "Action": [
                  "appconfig:StartDeployment",
                  "appconfig:StopDeployment",
                  "appconfig:CreateHostedConfigurationVersion",
                  "appconfig:ValidateConfiguration"
                ],
                "Resource": [
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/configurationprofile/
${AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSAlarmManagerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/configurationprofile/
${AMSResourceTaggerConfigurationCustomerManagedTagsProfileID}",
                  "arn:aws:appconfig:*:${AWS::AccountId}:application/
${AMSResourceTaggerConfigurationApplicationId}/environment/*",
                  "arn:aws:appconfig:*:${AWS::AccountId}:deploymentstrategy/*"
                ]
              },
              {
                "Sid": "CloudFormationStacksPolicy",
                "Effect": "Allow",
                "Action": [
                  "cloudformation:DescribeStacks"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EC2Policy",
                "Action": [
                  "ec2:DescribeInstances"
                ],
                "Effect": "Allow",
                "Resource": "*"
              },
              {
                "Sid": "SSMPolicy",
```

```
            "Effect": "Allow",
            "Action": [
              "ssm:AddTagsToResource",
              "ssm:CancelCommand",
              "ssm:CancelMaintenanceWindowExecution",
              "ssm:CreateAssociation",
              "ssm:CreateAssociationBatch",
              "ssm:CreateMaintenanceWindow",
              "ssm:CreateOpsItem",
              "ssm:CreatePatchBaseline",
              "ssm:DeleteAssociation",
              "ssm:DeleteMaintenanceWindow",
              "ssm:DeletePatchBaseline",
              "ssm:DeregisterPatchBaselineForPatchGroup",
              "ssm:DeregisterTargetFromMaintenanceWindow",
              "ssm:DeregisterTaskFromMaintenanceWindow",
              "ssm:Describe*",
              "ssm:Get*",
              "ssm:List*",
              "ssm:PutConfigurePackageResult",
              "ssm:RegisterDefaultPatchBaseline",
              "ssm:RegisterPatchBaselineForPatchGroup",
              "ssm:RegisterTargetWithMaintenanceWindow",
              "ssm:RegisterTaskWithMaintenanceWindow",
              "ssm:RemoveTagsFromResource",
              "ssm:SendCommand",
              "ssm:StartAssociationsOnce",
              "ssm:StartAutomationExecution",
              "ssm:StartSession",
              "ssm:StopAutomationExecution",
              "ssm:TerminateSession",
              "ssm:UpdateAssociation",
              "ssm:UpdateAssociationStatus",
              "ssm:UpdateMaintenanceWindow",
              "ssm:UpdateMaintenanceWindowTarget",
              "ssm:UpdateMaintenanceWindowTask",
              "ssm:UpdateOpsItem",
              "ssm:UpdatePatchBaseline"
            ],
            "Resource": "*"
          },
          {
            "Sid": "AmsPatchRestrictAMSResources",
            "Effect": "Deny",
```

```
      "Action": [
        "ssm:DeletePatchBaseline",
        "ssm:UpdatePatchBaseline"
      ],
      "Resource": [
        "arn:aws:ssm:${AWS::Region}:${AWS::AccountId}:patchbaseline/*"
      ],
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/ams:resourceOwner": "*"
        }
      }
    },
    {
      "Sid": "AmsPatchRestrictAmsTags",
      "Effect": "Deny",
      "Action": [
        "ssm:AddTagsToResource",
        "ssm:RemoveTagsFromResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringLike": {
          "aws:TagKeys": [
            "AMS*",
            "Ams*",
            "ams*"
          ]
        }
      }
    },
    {
      "Sid": "TagReadPolicy",
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:GetTagKeys"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudtrailReadPolicy",
      "Effect": "Allow",
      "Action": [
```

```
                  "cloudtrail:DescribeTrails",
                  "cloudtrail:GetTrailStatus",
                  "cloudtrail:LookupEvents"
                ],
                "Resource": "*"
              },
              {
                "Sid": "EventBridgePolicy",
                "Effect": "Allow",
                "Action": [
                  "events:Describe*",
                  "events:List*",
                  "events:TestEventPattern"
                ],
                "Resource": "*"
              },
              {
                "Sid": "IAMReadOnlyPolicy",
                "Action": [
                    "iam:ListRoles",
                    "iam:GetRole"
                ],
                "Effect": "Allow",
                "Resource": "*"
              },
              {
                "Sid": "AmsResourceSchedulerPassRolePolicy",
                "Effect": "Allow",
                "Action": "iam:PassRole",
                "Resource": "arn:aws:iam::${AWS::AccountId}:role/
ams_resource_scheduler_ssm_automation_role",
                "Condition": {
                    "StringEquals": {
                        "iam:PassedToService": "ssm.amazonaws.com"
                    }
                }
              }
            ]
          }
        - AMSAlarmManagerConfigurationApplicationId: !ImportValue "AMS-Alarm-Manager-
Configuration-ApplicationId"
          AMSAlarmManagerConfigurationCustomerManagedAlarmsProfileID: !ImportValue
 "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID"
```

```
          AMSResourceTaggerConfigurationApplicationId: !ImportValue "AMS-
ResourceTagger-Configuration-ApplicationId"
          AMSResourceTaggerConfigurationCustomerManagedTagsProfileID: !ImportValue
 "AMS-ResourceTagger-Configuration-CustomerManagedTags-ProfileID"

  AMSAccelerateReadOnly:
    Type: 'AWS::IAM::ManagedPolicy'
    Properties:
      ManagedPolicyName: AMSAccelerateReadOnly
      Path: /
      PolicyDocument: !Sub |
        {
          "Version": "2012-10-17",
          "Statement": [
          {
                "Sid": "AmsSelfServiceReport",
                "Effect": "Allow",
                "Action": "amsssrv:*",
                "Resource": "*"
             },
           {
              "Sid": "AmsBackupPolicy",
              "Effect": "Allow",
              "Action": [
                "backup:Describe*",
                "backup:Get*",
                "backup:List*"
              ],
              "Resource": "*"
           },
           {
               "Action": [
                   "rds:DescribeDBSnapshots",
                   "rds:ListTagsForResource",
                   "rds:DescribeDBInstances",
                   "rds:describeDBSnapshots",
                   "rds:describeDBEngineVersions",
                   "rds:describeOptionGroups",
                   "rds:describeOrderableDBInstanceOptions",
                   "rds:describeDBSubnetGroups",
                   "rds:DescribeDBClusterSnapshots",
                   "rds:DescribeDBClusters",
                   "rds:DescribeDBParameterGroups",
                   "rds:DescribeDBClusterParameterGroups",
```

```
                "rds:DescribeDBInstanceAutomatedBackups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "dynamodb:ListBackups",
                "dynamodb:ListTables"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "elasticfilesystem:DescribeFilesystems"
            ],
            "Resource": "arn:aws:elasticfilesystem:*:*:file-system/*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:describeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeSubnets",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:GetResources"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeCachediSCSIVolumes",
                "storagegateway:DescribeStorediSCSIVolumes"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*/volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListGateways"
            ],
            "Resource": "arn:aws:storagegateway:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:DescribeGatewayInformation",
                "storagegateway:ListVolumes",
                "storagegateway:ListLocalDisks"
            ],
            "Resource": "arn:aws:storagegateway:*:*:gateway/*"
        },
        {
            "Action": [
                "iam:ListRoles",
                "iam:GetRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "organizations:DescribeOrganization",
            "Resource": "*"
        },
        {
            "Action": "fsx:DescribeBackups",
            "Effect": "Allow",
            "Resource": "arn:aws:fsx:*:*:backup/*"
        },
```

```
            {
                "Action": "fsx:DescribeFileSystems",
                "Effect": "Allow",
                "Resource": "arn:aws:fsx:*:*:file-system/*"
            },
            {
                "Action": "ds:DescribeDirectories",
                "Effect": "Allow",
                "Resource": "*"
            },
            {
              "Sid": "AmsChangeRecordKMSPolicy",
              "Effect": "Allow",
              "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey"
              ],
              "Resource": [
                "arn:aws:kms:${AWS::Region}:${AWS::AccountId}:key/*"
              ],
              "Condition": {
                "ForAnyValue:StringLike": {
                  "kms:ResourceAliases": "alias/AMSCloudTrailLogManagement"
                }
              }
            },
            {
              "Sid": "AmsChangeRecordAthenaReadPolicy",
              "Effect": "Allow",
              "Action": [
                "athena:BatchGetNamedQuery",
                "athena:Get*",
                "athena:List*",
                "athena:StartQueryExecution",
                "athena:UpdateWorkGroup",
                "glue:GetDatabase*",
                "glue:GetTable*",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets"
              ],
              "Resource": "*"
            },
```

```
            {
              "Sid": "AmsChangeRecordS3ReadPolicy",
              "Effect": "Allow",
              "Action": [
                "s3:Get*",
                "s3:List*"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}",
                "arn:aws:s3:::ams-a${AWS::AccountId}-cloudtrail-${AWS::Region}/*"
              ]
            },
            {
              "Sid": "AmsChangeRecordS3WritePolicy",
              "Effect": "Allow",
              "Action": [
                "s3:PutObject",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention"
              ],
              "Resource": [
                "arn:aws:s3:::ams-a${AWS::AccountId}-athena-results-${AWS::Region}/*"
              ]
            },
            {
              "Sid": "MaciePolicy",
              "Effect": "Allow",
              "Action": [
                "macie2:GetFindingStatistics"
              ],
              "Resource": "*"
            },
            {
              "Sid": "GuardDutyReadPolicy",
              "Effect": "Allow",
              "Action": [
                "guardduty:GetFindingsStatistics",
                "guardduty:ListDetectors"
              ],
              "Resource": "*"
            },
            {
```

```
      "Sid": "SupportReadPolicy",
      "Effect": "Allow",
      "Action": "support:Describe*",
      "Resource": "*"
    },
    {
      "Sid": "ConfigReadPolicy",
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:List*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AppConfigReadPolicy",
      "Effect": "Allow",
      "Action": [
        "appconfig:List*",
        "appconfig:Get*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFormationReadPolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "EC2ReadPolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMReadPolicy",
      "Effect": "Allow",
      "Action": [
```

```
                "ssm:Describe*",
                "ssm:Get*",
                "ssm:List*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "TagReadPolicy",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudtrailReadPolicy",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Sid": "EventBridgePolicy",
            "Effect": "Allow",
            "Action": [
                "events:Describe*",
                "events:List*",
                "events:TestEventPattern"
            ],
            "Resource": "*"
        }
    ]
}
```

AMS 访问您的账户的原因和时间

在某些情况下，AMS Accelerate（加速）操作员可以访问您的账户控制台和实例，以管理您的资源。这些访问事件记录在您的 AWS CloudTrail (CloudTrail) 日志中。有关如何查看 AMS Accelerate 运营

团队和 AMS Accelerate 自动化的账户活动的详细信息，请参阅跟踪您的 AMS Accelerate 账户中的更改。

以下主题解释了 AMS 访问您的账户的原因、时间和方式。

AMS 客户账户访问触发器

AMS 客户账户访问活动由触发器驱动。今天的触发器是在我们的问题管理系统中为响应 Amazon CloudWatch (CloudWatch) 警报和事件以及您提交的事件报告或服务请求而创建的 AWS 票证。每次访问可能会执行多个服务呼叫和主机级别的活动。

下表列出了访问理由、触发器和触发器的启动者。

访问触发器

访问	发起者	触发器
修补	AMS	补丁问题
内部问题调查	AMS	问题问题（已确定为系统性问题）
警报调查和补救	AMS	AWS Systems Manager 运营工作项目 (SSM OpsItems)
事故调查和补救	您	入站支持案例（您提交的事件或服务请求）
入库服务请求配送	您	

AMS 客户账户访问权限 IAM 角色

AMS 运营商需要以下角色才能为您的账户提供服务。

> **Note**
>
> AMS 访问角色允许 AMS 操作员访问您的资源以提供 AMS 功能（请参阅服务描述）。改变这些角色可能会抑制我们提供这些能力的能力。如果您需要更改 AMS 访问角色，请咨询您的云架构师。

用于 AMS 访问客户账户的 IAM 角色

角色名称	说明
ams-access-admin	此角色对您的账户拥有完全的管理权限，不受任何限制。AMS 服务将此角色与限制性会话策略一起使用，这些策略限制了部署 AMS 基础设施和操作您的账户的访问权限。
ams-access-admin-operations	此角色授予 AMS 操作员操作您账户的管理权限。此角色不授予对通常用作数据存储的服务（例如亚马逊简单存储服务、亚马逊关系数据库 AWS 服务、亚马逊 DynamoDB、Amazon Redshift 和亚马逊）中的客户内容的读取、写入或删除权限。 ElastiCache只有在访问管理方面具有深刻理解和背景的合格 AMS 操作员才能担任此角色。这些操作员充当访问管理问题的上报点，并访问您的帐户以解决 AMS 操作员的访问问题。
ams-access-management	在入职期间手动部署。AMS Access 系统需要此角色来`ams-access-roles` 管理和`ams-access-managed-policies` 堆叠。
ams-access-operations	此角色有权在您的账户中执行管理任务。此角色对通常用作数据存储的服务（例如亚马逊简单存储服务、亚马逊关系数据库 AWS 服务、亚马逊 DynamoDB、Amazon Redshift 和亚马逊）中的客户内容没有读取、写入或删除权限。 ElastiCache此角色还不包括执行 AWS Identity and Access Management 写入操作的权限。AMS Accelerate 运营人员和云架构师 (CAs) 可以担任此角色。
ams-access-read-only	此角色对您的账户具有只读访问权限。AMS Accelerate 运营人员和云架构师 (CAs) 可以担任此角色。未授予对通常用作数据存储的 AWS 服务（例如 Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift ElastiCache 和）中客户内容的读取权限。

角色名称	说明
ams-access-security-analyst	此 AMS 安全角色有权在您的 AMS 账户中执行专门的安全警报监控和安全事件处理。只有极少数精选的 AMS Security 人员可以担任此角色。
ams-access-security-analyst-只读	此 AMS 安全角色仅限于您 AMS 账户中的只读权限，用于执行专门的安全警报监控和安全事件处理。

> **Note**
>
> 这是 ams-access-management角色的模板。这是云架构师 (CAs) 在入职时在你的账户中手动部署的堆栈：management-role.yaml 。
> 这是不同访问级别的不同访问角色的模板： ams-access-read-only、、 ams-access-operations、:accelerate-roles ams-access-admin-operations. ams-access-admin y aml。

AMS 如何访问您的账户

在某些情况下，AMS Accelerate 操作员可以访问您的账户控制台和实例。

AMS 运营商使用内部 AMS Accelerate 访问服务，以安全且经过审计的方式访问您的账户。要访问您的实例，AMS 运营商使用与代理相同的内部 AMS 访问服务，在授予访问权限后，AMS Accelerate 操作员使用 SSM 会话管理器通过会话凭证获得访问权限。Windows 实例的 RDP 访问权限是通过建立到实例的端口转发并使用 SSM 创建本地用户来提供的。本地用户凭证用于 RDP 访问并在会话结束时删除。

如何以及何时在 AMS 中使用 root 用户账户

r oot 用户是您 AWS 账户中的超级用户。AMS 监控根用户使用情况。我们建议您仅将 root 用于少数需要它的任务，例如：更改账户设置、激活 AWS Identity and Access Management (IAM) 账单和成本管理权限、更改根密码以及启用多因素身份验证 (MFA)。请参阅《用户指南》中的 “需要根用户凭据的 AWS Identity and Access Management 任务”。

使用 AMS 加速 Root：

AMS 不禁止您使用根用户账户。但是，AMS Operations and Security 确实将其使用视为需要调查的问题，每次使用我们都会联系您的安全团队。

我们建议您提前 24 小时联系您的 CSDM 和 CA，告知他们您打算执行的根访问工作。

AMS 操作和对 root 用户使用情况的安全响应：

使用 root 用户帐户时，AMS 会收到警报。如果未计划使用根证书，他们会联系 AMS Security 团队和您的账户团队，以验证这是否是预期的活动。如果不是预期的活动，AMS 会与您的安全团队合作调查问题。

AMS 中的安全管理加速

AWS Managed Services 使用多种控制措施来保护您的信息资产并帮助您保护 AWS 基础设施的安全。AMS Acceler AWS Config 规则 ate 维护着一个补救措施库，以确保您的所有账户都符合安全性和运营完整性的行业标准。 AWS Config 规则 持续跟踪您录制的资源之间的配置更改。如果更改违反了任何规则条件，AMS 会报告其调查结果，并允许您根据违规的严重程度自动或根据请求进行补救。 AWS Config 规则 促进遵守互联网安全中心 (CIS)、美国国家标准与技术研究院 (NIST) 云安全框架 (CSF)、《健康保险便携性和责任法案》(HIPAA) 以及支付卡行业 (PCI) 数据安全标准 (DSS) 制定的标准。

此外，AMS 还利用 Amazon GuardDuty 来识别您 AWS 环境中可能存在的未经授权或恶意的活动。AMS 全天候监测 GuardDuty 调查结果。AMS 与您合作，了解调查结果的影响，并根据最佳实践建议确定补救措施。AMS 还使用 Amazon Macie 来保护您的敏感数据，例如个人健康信息 (PHI)、个人身份信息 (PII) 和财务数据。

> **Note**
>
> Amazon Macie 是一项可选服务，默认情况下未启用。

AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。要详细了解 AMS 如何通过 AMS 关键运营功能（包括全天候服务台、主动监控、安全、修补、日志记录和备份）来帮助您的团队实现整体卓越运营，请参阅 AMS 参考架构图。 AWS 云

主题

- 《加速》中的安全最佳实践
- 更改请求安全审查
- 安全常见问题解答

使用 Log4j SSM 文档来发现 Accelerate 中出现的情况

Log4j AWS Systems Manager 文档（SSM 文档）可帮助您在摄取的工作负载中搜索 Apache Log4j2 库。自动化文档提供了 Log4j2 库处于活动状态的 Java 应用程序的进程 ID 的报告。

该报告包含有关在包含该 JndiLookup 类的指定环境中找到的 Java 档案（JAR 文件）的信息。最佳做法是将发现的库升级到最新的可用版本。此升级可缓解通过 CVE-2021-44228 识别的远程代码执行 (RCE)。从 Apache 下载最新版本的 Log4j 库。有关更多信息，请参阅下载 Apache Log4j 2。

该文档已共享给所有已加入加速的区域。要访问该文档，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 在导航窗格中，选择文档。
3. 选择 “与我共享”。
4. 在搜索框中，输入 AWSManagedServices-GatherLog4j Information。
5. 使用速率控制大规模运行文档。

AWSManagedServices-GatherLog4jInformation 文档收集了以下参数：

- InstanceId:（必填）您的 EC2 实例的 ID。
- S3Bucket：（可选）要将结果上传到的 S3 预签名 URL 或 S3 URI (s3://BUCKET_NAME)。
- AutomationAssumeRole:（必填）允许自动机代表您执行操作的角色的 ARN。

最好使用速率控制来运行此文档。您可以将速率控制参数设置为 InstanceId，然后为其分配实例列表，或者应用标签键组合来定位具有特定标签的所有 EC2 实例。AWS Managed Services 还建议您提供一个亚马逊简单存储服务 (Amazon S3) 存储桶来上传结果，以便您可以根据存储在 S3 中的数据生成报告。有关如何在 S3 中聚合结果的示例，请参阅EC2 实例堆栈 | 收集 Log4j 信息。

如果您无法升级软件包，请遵循使用 AWS 安全服务防御、检测和响应 Log4j 漏洞 AWS 的安全性中概述的指导方针。要通过删除 JndiLookup 类功能来缓解漏洞，请与 Java 应用程序内联运行 Log4j 热补丁。有关热补丁的更多信息，请参阅适用于 Apache Log4j 的热补丁。

有关自动化的输出或如何继续采取其他缓解措施的问题，请提交服务请求。

AMS 中的基础设施安全监控

当您加入 AMS Accelerate， AWS 部署以下 AWS Config 基准基础设施和一组规则时，AMS Accelerate 会使用这些规则来监控您的账户。

- AWS Config 服务相关角色：AMS Accelerate 部署名为的服务相关角色 AWSServiceRoleForConfig，该角色 AWS Config 用于查询其他服务的状态。 AWS AWSServiceRoleForConfig服务相关角色信任 AWS Config 服务来代替该角色。该AWSServiceRoleForConfig角色的权限策略包含对 AWS Config 资源的只读和只写权限，以及其他支持的服务中资源的只读权限。 AWS Config 如果您已经为角色配置了 AWS Config Recorder，AMS Accelerate 会验证现有角色是否附加了 AWS Config 托管策略。否则，AMS Accelerate 会将该角色替换为服务相关角色AWSServiceRoleForConfig。
- AWS Config 记录器和交付渠道： AWS Config 使用配置记录器检测资源配置中的更改，并将这些更改捕获为配置项目。AMS Accelerate 在所有服务中部署配置记录器 AWS 区域，并持续记录所有资源。AMS Accelerate 还创建了配置传输渠道，即 Amazon S3 存储桶，用于记录 AWS 资源中发生的更改。配置记录器通过交付渠道更新配置状态。需要配置记录器和传送渠道 AWS Config 才能正常工作。AMS Accelerate 总共创建了录音机 AWS 区域，将交付渠道合而为一 AWS 区域。如果您在中已经有录音机和交付渠道 AWS 区域，那么 AMS Accelerate 不会删除现有 AWS Config 资源，而是在验证现有录像机和交付渠道配置正确后，AMS Accelerate 会使用您现有的录像机和交付渠道。有关如何降低 AWS Config 成本的更多信息，请参阅在 “加速” 中降低 AWS Config 成本。
- AWS Config 规则：AMS Accelerat AWS Config 规则 e 维护着一个补救措施库，以帮助您遵守安全性和运营完整性的行业标准。 AWS Config 规则 持续跟踪您录制的资源之间的配置更改。如果更改违反了任何规则条件，AMS 会报告其调查结果，并允许您根据违规的严重程度自动或根据请求进行补救。 AWS Config 规则 促进遵守互联网安全中心 (CIS)、美国国家标准与技术研究院 (NIST) 云安全框架 (CSF)、《健康保险便携性和责任法案》(HIPAA) 以及支付卡行业 (PCI) 数据安全标准 (DSS) 制定的标准。
- AWS Config 聚合器授权：聚合器是一种从多个账户和多个 AWS Config 区域收集配置和合规性数据的 AWS Config 资源类型。AMS Accelerate 将您的账户登录到配置聚合器，AMS Accelerate 会从该聚合器中汇总您账户的资源配置信息和配置合规性数据，并生成合规性报告。如果在 AMS 拥有的账户中配置了现有聚合器，则 AMS Accelerate 将部署额外的聚合器，并且不会修改现有的聚合器。

> **Note**
>
> Config 聚合器不是在您的账户中设置的；而是在 AMS 拥有的账户中设置的，您的账户已加入该聚合器。

要了解更多信息 AWS Config，请参阅：

- AWS Config: 什么是 Config？
- AWS Config 规则: 使用规则评估资源
- AWS Config 规则: 动态合规性检查: AWS Config 规则 — 云资源的动态合规性检查
- AWS Config 聚合器：多账户多区域数据聚合

有关报告的信息，请参阅AWS Config 控制合规性报告。

在 AMS Accelerate 中使用服务相关角色

AMS 加速使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色 (SLR) 是一种独特的 IAM 角色类型，直接关联到 AMS Accelerate。服务相关角色由 AMS Accelerate 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可以更轻松地设置 AMS Accelerate，因为您无需手动添加必要的权限。AMS Accelerate 定义了其服务相关角色的权限，除非另有定义，否则只有 AMS Accelerate 可以担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。

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，并在服务相关角色列中查找标有 “是” 的服务。选择是和链接，查看该服务的服务相关角色文档。

AMS Accelerate 的部署工具包服务相关角色

AMS Accelerate 使用名为AWSServiceRoleForAWSManagedServicesDeploymentToolkit的服务关联角色 (SLR)，该角色将 AMS Accelerate 基础设施部署到客户账户。

> **Note**
>
> 该政策最近已更新；有关详细信息，请参阅加快服务相关角色的更新。

AMS 加速部署工具包 SLR

AWSServiceRoleForAWSManagedServicesDeploymentToolkit 服务相关角色信任以下服务来代入该角色：

- `deploymenttoolkit.managedservices.amazonaws.com`

名为的策略AWSManagedServicesDeploymentToolkitPolicy允许 AMS Accelerate 对以下资源执行操作：

- `arn:aws*:s3:::ams-cdktoolkit*`
- `arn:aws*:cloudformation:*:*:stack/ams-cdk-toolkit*`
- `arn:aws:ecr:*:*:repository/ams-cdktoolkit*`

此 SLR 授予 Amazon S3 创建和管理部署存储桶的权限，AMS 用于将资源（例如 CloudFormation 模板或 Lambda 资产捆绑包）上传到用于组件部署的账户。此 SLR 授予部署定义部署存储 CloudFormation 桶的堆栈的 CloudFormation 权限。有关详细信息或下载政策，请参阅AWSManagedServices_DeploymentToolkitPolicy。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AMS Accelerate 创建部署工具包 SLR

您无需手动创建服务相关角色。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时 AWS CLI，AMS Accelerate 会为您创建与服务相关的角色。

> **Important**
>
> 如果您在 2022 年 6 月 9 日之前使用 AMS Accelerate 服务，该服务相关角色开始支持服务相关角色，然后 AMS Accelerate 在您的账户中创建了该角色，则该 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 服务相关角色可能会出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中出现新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入 AMS 时，AMS Accelerate 会再次为您创建与服务相关的角色。

编辑 AMS Accelerate 的部署工具包 SLR

AMS Accelerate 不允许您编辑 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AMS Accelerate 的部署工具包 SLR

您无需手动删除该 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 角色。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时 AWS CLI，AMS Accelerate 会清理资源并为您删除服务相关角色。

您也可以使用 IAM 控制台、 AWS CLI 或 AWS API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

> **Note**
>
> 如果您尝试删除资源时 AMS Accelerate 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForAWSManagedServicesDeploymentToolkit 服务相关角色使用的 AMS Accelerate 资源

在 AMS 中从您的账户加入的所有区域中删除`ams-cdk-toolkit`堆栈（您可能需要先手动清空 S3 存储桶）。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAWSManagedServicesDeploymentToolkit服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

Detective 控制 AMS Accerate 的服务相关角色

AMS Accelerate 使用名为的服务相关角色 (SLR) AWSServiceRoleForManagedServices_DetectiveControlsConfig— AWS Managed Services 使用此服务相关角色来部署配置记录器、配置规则和 S3 存储桶侦测控件。

附加到AWSServiceRoleForManagedServices_DetectiveControlsConfig服务相关角色的是以下托管策略：AWSManagedServices_DetectiveControlsConfig_ ServiceRolePolicy。有关此策略的更新，请参阅加快 AWS 托管策略的更新。

侦探权限控制 AMS Accelerate 的单反相机

AWSServiceRoleForManagedServices_DetectiveControlsConfig 服务相关角色信任以下服务来代入该角色：

- `detectivecontrols.managedservices.amazonaws.com`

该角色附带的是`AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy` AWS 托管策略（请参阅该服务使用AWS 托管策略: AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy该角色在您的账户中创建配置 AMS Detective Controls，这需要部署 s3 存储桶、配置规则和聚合器等资源。 您必须配置权限以允许 IAM 实体（例如用户、群组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《Identity and A ccess Managem AWS ent 用户指南》中的服务相关角色权限。

创建侦探控制 AMS Accelerate 的单反相机

您无需手动创建服务相关角色。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时 AWS CLI，AMS Accelerate 会为您创建与服务相关的角色。

> **Important**
>
> 如果您在 2022 年 6 月 9 日之前使用 AMS Accelerate 服务，则该服务相关角色可能会出现在您的账户中，该服务相关角色开始支持服务相关角色，然后 AMS Accelerate 在您的账户中创建了该 AWSServiceRoleForManagedServices_DetectiveControlsConfig 角色。要了解更多信息，请参阅我的 IAM 账户中出现新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入 AMS 时，AMS Accelerate 会再次为您创建与服务相关的角色。

编辑侦探可以控制 AMS Accelerate 的单反相机

AMS Accelerate 不允许您编辑 AWSServiceRoleForManagedServices_DetectiveControlsConfig 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除侦探会控制 AMS Accelerate 的单反效果

您无需手动删除该 AWSServiceRoleForManagedServices_DetectiveControlsConfig 角色。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时 AWS CLI，AMS Accelerate 会清理资源并为您删除服务相关角色。

您也可以使用 IAM 控制台、 AWS CLI 或 AWS API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

> **Note**
>
> 如果您尝试删除资源时 AMS Accelerate 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForManagedServices_DetectiveControlsConfig 服务相关角色使用的 AMS Accelerate 资源

在 AMS 中`ams-detective-controls-config-recorder`，从您的账户加入的所有区域中删除`ams-detective-controls-config-rules-cdk`和`ams-detective-controls-infrastructure-cdk`堆栈（您可能需要先手动清空 S3 存储桶）。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForManagedServices_DetectiveControlsConfig服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

Amazon EventBridge 规则 AMS Accelerate 的服务相关角色

AMS Accelerate 使用名为的服务相关角色 (SLR)。AWSServiceRoleForManagedServices_Events该角色信任 AWS Managed Services 服务委托人（events.managedservices.amazonaws.com）代您担任该角色。该服务使用该角色来创建 Amazon EventBridge 托管规则。此规则是您的 AWS 账户中所需的基础设施，用于将警报状态变更信息从您的账户传送到 AWS Managed Services。

AMS Acc EventBridge elerate 的 SLR 权限

AWSServiceRoleForManagedServices_Events 服务相关角色信任以下服务来代入该角色：

- `events.managedservices.amazonaws.com`

附属于此角色的是AWSManagedServices_EventsServiceRolePolicy AWS 托管策略（请参阅AWS 托管策略： AWSManagedServices_EventsServiceRolePolicy）。该服务使用该角色将警报状态更改信息从您的账户传送到 AMS。您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的服务相关角色权限。

你可以下载这个压缩文件 AWSManagedServices_EventsServiceRolePolicy 中的 JSON：EventsServiceRolePolicy.zip。

为 AMS Acc EventBridge elerate 创建单反相机

您无需手动创建服务相关角色。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时 AWS CLI，AMS Accelerate 会为您创建与服务相关的角色。

> **Important**
>
> 如果您在 2023 年 2 月 7 日之前使用 AMS Accelerate 服务，则该服务相关角色可以显示在您的账户中，该 AWSServiceRoleForManagedServices_Events 服务相关角色将出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中出现新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入 AMS 时，AMS Accelerate 会再次为您创建与服务相关的角色。

为 AMS Acc EventBridge elerate 编辑单反相机

AMS Accelerate 不允许您编辑 AWSServiceRoleForManagedServices_Events 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AMS Acc EventBridge elerate 的单反相机

您无需手动删除该 AWSServiceRoleForManagedServices_Events 角色。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时 AWS CLI，AMS Accelerate 会清理资源并为您删除服务相关角色。

您也可以使用 IAM 控制台、 AWS CLI 或 AWS API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

> **Note**
>
> 如果您尝试删除资源时 AMS Accelerate 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForManagedServices_Events 服务相关角色使用的 AMS Accelerate 资源

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForManagedServices_Events 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

联系人 AMS Accelerate 的服务相关角色

AMS Accelerate 使用名为的服务相关角色 (SLR) AWSServiceRoleForManagedServices_Contacts—该角色允许服务读取受影响资源的现有标签并检索相应联系人的已配置电子邮件，从而便于在事件发生时自动发出通知。

这是唯一使用此服务相关角色的服务。

附加到AWSServiceRoleForManagedServices_Contacts服务相关角色的是以下托管策略:AWSManagedServices_ContactsServiceRolePolicy. 有关此策略的更新，请参阅加快 AWS 托管策略的更新。

AMS Accelerate 的联系人权限 SLR

AWSServiceRoleForManagedServices_Contacts 服务相关角色信任以下服务来代入该角色：

- `contacts-service.managedservices.amazonaws.com`

此角色附带的是 `AWSManagedServices_ContactsServiceRolePolicy` AWS 托管策略（参见AWS 托管策略： AWSManagedServices_ContactsServiceRolePolicy）。该服务使用该角色来读取任何 AWS 资源上的标签，并找到标签中包含的电子邮件，即事件发生时的相应联系人。此角色允许 AMS 读取受影响资源上的标签并检索电子邮件，从而便于在事件发生时自动发出通知。有关更多信息，请参阅《Identity and A ccess Managem AWS ent 用户指南》中的服务相关角色权限。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AMS 使用标签为您提供管理服务。标签不适合用于私有或敏感数据。

名为的角色权限策略 AWSManagedServices_ContactsServiceRolePolicy 允许 AMS Accelerate 对指定资源完成以下操作：

- 操作：允许联系人服务读取专门设置为包含 AMS 在任何 AWS 资源上发送事件通知的电子邮件的标签。

你可以下载这个压缩文件 AWSManagedServices_ContactsServiceRolePolicy 中的 JSON：ContactsServicePolicy.zip。

为 AMS Accelerate 创建联系人单反相机

您无需手动创建服务相关角色。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时 AWS CLI，AMS Accelerate 会为您创建与服务相关的角色。

> **Important**
>
> 如果您在 2023 年 2 月 16 日之前使用 AMS Accelerate 服务，则该服务相关角色可以出现在您的账户中，该服务相关角色开始支持服务相关角色，然后 AMS Accelerate 在您的账户中创建了该 AWSServiceRoleForManagedServices_Contacts 角色。要了解更多信息，请参阅我的 IAM 账户中出现新角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入 AMS 时，AMS Accelerate 会再次为您创建与服务相关的角色。

为 AMS Accelerate 编辑联系人单反相机

AMS Accelerate 不允许您编辑 AWSServiceRoleForManagedServices_Contacts 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AMS Accelerate 的联系人单反相机

您无需手动删除该 AWSServiceRoleForManagedServices_Contacts 角色。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时 AWS CLI，AMS Accelerate 会清理资源并为您删除服务相关角色。

您也可以使用 IAM 控制台、 AWS CLI 或 AWS API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

> **Note**
>
> 如果您尝试删除资源时 AMS Accelerate 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForManagedServices_Contacts 服务相关角色使用的 AMS Accelerate 资源

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForManagedServices_Contacts 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AMS 支持的区域加速服务相关角色

AMS Accelerate 支持在提供服务的所有地区使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

加快服务相关角色的更新

查看有关自该服务开始跟踪服务相关角色变更以来这些更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “加速” AMS Accelerate 用户指南的文档历史记录 页面上的 RSS 提要。

更改	描述	日期

更新的政策-部署工具包	• 为资源添加了以下新权限`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` ：
	`ecr:BatchGetRepositoryScanningConfiguration`
	`ecr:PutImageScanningConfiguration`
		2024 年 4 月 4 日

更改	描述	日期

更新的政策-部署工具包	• 为资源添加了以下新权限`arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit*` ：
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• 为资源添加了以下新权限`arn:aws:ecr:*:*:repository/ams-cdktoolkit*` ：
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	• 此外，一些带有通配符的现有操作的范围缩小到单个操作：
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
	`+ s3:GetObjectAttributes`
	`+ s3:GetObjectLegalHold`
	`+ s3:GetObjectRetention`
		2023年5月9日

更改	描述	日期

	<pre>+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProtection</pre>	

更新后的政策 — Detective Cont	• 在与安全和访问团队确认后，已进一步缩小了 CloudFormation 行动的范围 • Lambda 操作已从政策中删除，因为它们不会影响登机 onboarding/off	2023 年 4 月 10 日
更新后的政策 — Detective Cont	更新了策略并添加了权限边界策略。	2023 年 3 月 21 日
新的服务相关角色-联系人 SLR	Accelerate 为通讯录服务添加了一个新的服务相关角色。 该角色允许服务读取受影响资源的现有标签并检索相应联系人的已配置电子邮件，从而便于在事件发生时自动发出通知。	2023 年 2 月 16 日
新的服务相关角色 — EventBridge	Accelerate 为 Amazon EventBridge 规则添加了一个新的服务相关角色。 该角色信任 AWS Managed Services 服务委托人（events.managedservices.amazonaws.com）代您担任该角色。该服务使用该角色来创建 Amazon EventBridge 托管规则。此规则是您的 AWS 账户中所需的基础设施，用于将警报状态变更信息从您的账户传送到 AWS Managed Services。	2023 年 2 月 7 日

更改	描述	日期

更新了服务相关角色-部署工具包	AWSServiceRoleForAWSManagedServicesDeployment Toolkit 使用新的 S3 权限加快更新速度。
	
	添加了以下新权限：
	
	`"s3:GetLifecycleConfiguration",`
	`"s3:GetBucketLogging",`
	`"s3:ListBucket",`
	`"s3:GetBucketVersioning",`
	`"s3:PutLifecycleConfiguration",`
	`"s3:GetBucketLocation",`
	`"s3:GetObject*"`
		2023 年 1 月 30 日

加速开始跟踪更改	Accelerate 开始跟踪其服务相关角色的变化。	2022 年 11 月 30 日
新的服务相关角色 — Detective Contro ls	Accelerate 添加了一个新的服务相关角色来部署加速侦探控制。 AWS Managed Services 使用此服务相关角色来部署配置记录器、配置规则和 S3 存储桶侦测控件。	2022 年 10 月 13 日
新的服务相关角色-部署工具包	Accelerate 添加了一个新的服务相关角色来部署加速基础架构。 此角色将 AMS Accelerate 基础设施部署到客户账户。	2022 年 6 月 9 日

AWS AMS 加速的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

有关变更表，请参见加快 AWS 托管策略的更新。

AWS 托管策略： AWSManagedServices_AlarmManagerPermissionsBoundary

AWS Managed Services (AMS) 使用AWSManagedServices_AlarmManagerPermissionsBoundary AWS 托管策略。AWSManagedServices_AlarmManager_ 中使用此 AWS托管策略ServiceRolePolicy 来限制由AWSServiceRoleForManagedServices_AlarmManager创建的 IAM 角色的权限。

此策略授予作为其中一部分创建的 IAM 角色执行 AWS 配置评估警报管理器的工作原理、 AWS 读取 Config 以获取 Alarm Manager 配置以及创建必要的 Amazon CloudWatch 警报等操作的权限。

该AWSManagedServices_AlarmManagerPermissionsBoundary策略附加到AWSServiceRoleForManagedServices_DetectiveControlsConfig服务相关角色。有关此角色的更新，请参阅加快服务相关角色的更新。

您可以将 策略附加得到 IAM 身份。

权限详细信息

该策略包含以下权限。

- AWS Config— 允许评估配置规则和选择资源配置的权限。
- AWS AppConfig— 允许获取 AlarmManager 配置的权限。
- Amazon S3— 允许操作 AlarmManager 存储桶和对象的权限。
- Amazon CloudWatch— 允许读取和发布 AlarmManager 托管警报和指标的权限。
- AWS Resource Groups and Tags— 允许读取资源标签的权限。
- Amazon EC2— 允许读取 Amazon EC2 资源。
- Amazon Redshift— 允许读取 Redshift 实例和集群的权限。
- Amazon FSx— 允许描述文件系统、卷和资源标签的权限。
- Amazon CloudWatch Synthetics— 允许读取 Synthetics 资源的权限。
- Amazon Elastic Kubernetes Service— 允许描述 Amazon EKS 集群的权限。
- Amazon ElastiCache— 允许描述资源的权限。

您可以下载此压缩包中的策略文件：RecommendedPermissionBoundary.zip。

AWS 托管策略: AWSManagedServices_DetectiveControlsConfig_ ServiceRolePolicy

AWS Managed Services (AMS) 使用AWSManagedServices_DetectiveControlsConfig_ServiceRolePolicy AWS 托管策略。此 AWS托管策略附加到AWSServiceRoleForManagedServices_DetectiveControlsConfig服务相关角色（请参阅Detective 控制 AMS Accerate 的服务相关角色）。有关AWSServiceRoleForManagedServices_DetectiveControlsConfig服务相关角色的更新，请参阅加快服务相关角色的更新。

该策略允许服务相关角色为您完成操作。

您可以将 AWSManagedServices_DetectiveControlsConfig _ ServiceRolePolicy 策略附加到您的 IAM 实体。

有关更多信息，请参阅 在 AMS Accelerate 中使用服务相关角色。

权限详细信息

此策略具有以下权限，允许 Det AWS Managed Services ective Controls 部署和配置所有必要的资源。

- CloudFormation— 允许 AMS Detective Controls 部署包含 s3 存储桶、配置规则和配置记录器等资源的 CloudFormation 堆栈。
- AWS Config— 允许 AMS Detective Controls 创建 AMS 配置规则、配置聚合器和标记资源。
- Amazon S3— 允许 AMS Detective Controls 管理其 s3 存储桶。

你可以下载此 ZIP 文件中的 JSON 策略文件：DetectiveControlsConfig_ ServiceRolePolicy .zip。

AWS 托管策略： AWSManagedServicesDeploymentToolkitPolicy

AWS Managed Services (AMS) 使用AWSManagedServicesDeploymentToolkitPolicy AWS 托管策略。此 AWS托管策略附加到AWSServiceRoleForAWSManagedServicesDeploymentToolkit服务相关角色（请参阅AMS Accelerate 的部署工具包服务相关角色）。该策略允许服务相关角色为您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅 在 AMS Accelerate 中使用服务相关角色。

有关AWSServiceRoleForManagedServicesDeploymentToolkitPolicy服务相关角色的更新，请参阅加快服务相关角色的更新。

权限详细信息

此策略具有以下权限，允许 Det AWS Managed Services ective Controls 部署和配置所有必要的资源。

- CloudFormation— 允许 AMS 部署工具包使用 CDK 所需的 S3 资源部署 CFN 堆栈。
- Amazon S3— 允许 AMS 部署工具包管理其 S3 存储桶。
- Elastic Container Registry— 允许 AMS 部署工具包管理其 ECR 存储库，该存储库用于部署 AMS CDK 应用程序所需的资产。

你可以下载这个压缩文件中的 JSON 策略文件：AWSManagedServicesDeploymentToolkitPolicy.zip。

AWS 托管策略： AWSManagedServices_EventsServiceRolePolicy

AWS Managed Services (AMS) 使用 AWSManagedServices_EventsServiceRolePolicy AWS 托管策略。此 AWS托管策略附加到AWSServiceRoleForManagedServices_Events服务相关角色。该策略允许服务相关角色为您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅 在 AMS Accelerate 中使用服务相关角色。

有关AWSServiceRoleForManagedServices_Events服务相关角色的更新，请参阅加快服务相关角色的更新。

权限详细信息

此策略具有以下权限，允许亚马逊将警报状态变更信息从您的账户传送 EventBridge 到 AWS Managed Services。

- events— 允许 Accelerate 创建亚马逊 EventBridge 托管规则。此规则是将警报状态变更信息从您的账户传送 AWS 账户 到您的账户所需的基础架构 AWS Managed Services。

你可以下载这个压缩文件中的 JSON 策略文件：EventsServiceRolePolicy.zip。

AWS 托管策略： AWSManagedServices_ContactsServiceRolePolicy

AWS Managed Services (AMS) 使用 AWSManagedServices_ContactsServiceRolePolicy AWS 托管策略。此 AWS托管策略附加到AWSServiceRoleForManagedServices_Contacts服务

相关角色（请参阅为 AMS Accelerate 创建联系人单反相机）。该策略允许 AMS 联系人 SLR 查看您在 AWS 资源上的资源标签及其值。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅 在 AMS Accelerate 中使用服务相关角色。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AMS 使用标签为您提供管理服务。标签不适合用于私有或敏感数据。

有关AWSServiceRoleForManagedServices_Contacts服务相关角色的更新，请参阅加快服务相关角色的更新。

权限详细信息

此策略具有以下权限，允许联系人 SLR 读取您的资源标签，以检索您提前设置的资源联系人信息。

- IAM— 允许联系人服务查看 IAM 角色和 IAM 用户的标签。
- Amazon EC2— 允许联系人服务查看 Amazon EC2 资源上的标签。
- Amazon S3— 允许联系人服务查看 Amazon S3 存储桶上的标签。此操作使用条件来确保 AMS 使用 HTTP 授权标头、Sigv4 签名协议以及使用 TLS 1.2 或更高版本的 HTTPS 访问您的存储桶标签。有关更多信息，请参阅身份验证方法和 Amazon S3 签名版本 4 身份验证特定策略密钥。
- Tag— 允许联系人服务查看其他 AWS 资源上的标签。

- “iam：ListRoleTags”、“iam：ListUserTags”、“tag：”、GetResources “tag：”、GetTagKeys “tag：”、GetTagValues “tag：”、DescribeTags “ec2：”、“s3：GetBucketTagging”

你可以下载这个压缩文件中的 JSON 策略文件：ContactsServicePolicy.zip。

加快 AWS 托管策略的更新

查看有关自该服务开始跟踪这些更改以来对 Accelerate AWS 托管策略更新的详细信息。

更改	描述	日期
更新的政策-部署工具包	• 为资源添加了以下新权限arn:aws:ecr:*:*:repository/ams-cdktoolkit* :	2024 年 4 月 4 日

更改	描述	日期
	`ecr:BatchGetRepositoryScanningConfiguration` `ecr:PutImageScanningConfiguration`	

更改	描述	日期

更新的政策-部署工具包	• 为资源添加了以下新权限arn:aws:cloudformation:*:*:stack/ams-cdk-toolkit* ：
	`cloudformation:DeleteChangeSet`
	`cloudformation:DescribeStackEvents`
	`cloudformation:GetTemplate`
	`cloudformation:TagResource`
	`cloudformation:UntagResource`
	• 为资源添加了以下新权限arn:aws:ecr:*:*:repository/ams-cdktoolkit* ：
	`ecr:CreateRepository`
	`ecr:DeleteLifecyclePolicy`
	`ecr:DeleteRepository`
	`ecr:DeleteRepositoryPolicy`
	`ecr:DescribeRepositories`
	`ecr:GetLifecyclePolicy`
	`ecr:ListTagsForResource`
	`ecr:PutImageTagMutability`
	`ecr:PutLifecyclePolicy`
	`ecr:SetRepositoryPolicy`
	`ecr:TagResource`
	`ecr:UntagResource`
	• 此外，一些带有通配符的现有操作的范围缩小到单个操作：
	`- s3:DeleteObject*`
	`+ s3:DeleteObject`
	`+ s3:DeleteObjectTagging`
	`+ s3:DeleteObjectVersion`
	`+ s3:DeleteObjectVersionTagging`
	`- s3:GetObject*`
	`+ s3:GetObject`
	`+ s3:GetObjectAcl`
		2023 年 5 月 9 日

更改	描述	日期

	<pre>+ s3:GetObjectAttributes
	+ s3:GetObjectLegalHold
	+ s3:GetObjectRetention
	+ s3:GetObjectTagging
	+ s3:GetObjectVersion
	+ s3:GetObjectVersionAcl
	+ s3:GetObjectVersionAttributes
	+ s3:GetObjectVersionForReplication
	+ s3:GetObjectVersionTagging
	+ s3:GetObjectVersionTorrent
	
	- cloudformation:UpdateTermination*
	+ cloudformation:UpdateTerminationProt
	ection</pre>	

更新的政策 — Det ective Con t	• 在与安全和访问团队确认后，已进一步缩小了 CloudFormation 行动范围 • Lambda 操作已从政策中删除，因为它们不会影响登机 onboarding/off	2023 年 4 月 10 日
更新的政策 — Det ective Con t	该`ListAttachedRolePolicies` 操作已从策略中删除。该操作使用资源作为通配符 (*)。由于 “列表” 是一个非变异操作，因此它可以访问所有资源，并且不允许使用通配符。	2023 年 3 月 28 日
更新的政策 — Det ective Con t	更新了策略并添加了权限边界策略。	2023 年 3 月 21 日
新政策-通讯录服务	Accelerate 添加了一项新政策，用于查看资源标签中的账户联系信息。 Accelerate 添加了一项新的策略来读取您的资源标签，以便它可以检索您提前设置的资源联系信息。	2023 年 2 月 16 日

更改	描述	日期
新政策-活动服务	Accelerate 添加了一项新政策，用于将警报状态变更信息从您的账户发送到 AWS Managed Services。 向作为警报管理器的工作原理权限一部分创建的 IAM 角色授予创建必需的 Amazon EventBridge 托管规则的权限。	2023年2月7日
更新的政策-部署工具包	添加了 S3 权限以支持客户从 Accelerate 中离线。	2023 年 1 月 30 日
新政策 — 侦探控制	允许服务相关角色完成操作Detective 控制 AMS Accerate 的服务相关角色，以便您部署 Accelerate 侦探控件。	2022 年 12 月 19 日
新政策-警报管理器	Accelerate 添加了一项新政策，允许权限执行警报管理器任务。 授予作为警报管理器的工作原理权限一部分创建的 IAM 角色执行诸如 AWS 配置评估、读取 Con AWS fig 以获取警报管理器配置、创建必要的 Amazon CloudWatch 警报等操作。	2022 年 11 月 30 日
加速开始跟踪变更	Accelerate 开始跟踪其 AWS 托管策略的变更。	2022 年 11 月 30 日
新政策-部署工具包	加速为部署任务添加了此策略。 向服务相关角色授予访问和更新与部署相关的 Amazon S3 存储桶和堆栈的AWSServiceRoleForAWSManagedServicesDeploymentToolkit权限。 CloudFormation	2022 年 6 月 9 日

“加速” 中的数据保护

AMS Accelerate 利用亚马逊 GuardDuty、Amazon Macie（可选）和其他内部专有工具和流程 AWS 服务 等原生工具和流程来持续监控您的托管账户。警报触发后，AMS Accelerate 将负责警报的初始分类和响应。AMS 响应流程基于 NIST 标准。AMS Accelerate 与您一起使用安全事件响应模拟定期测试响应流程，使您的工作流程与现有客户安全响应计划保持一致。

当 AMS Accelerate 检测到您的安全策略存在违规行为 AWS 或即将发生的违规威胁时，Accelerate 会收集信息，包括受影响的资源和任何与配置相关的更改。AMS Accelerate 提供全天候 follow-the-sun支持，由专门的操作员主动审查和调查所有托管账户的监控仪表板、事件队列和服务请求。Accelerate 会与内部安全专家一起调查调查结果，以分析活动并通过您账户中列出的安全升级联系人通知您。

根据调查结果，Accelerate 会主动与您互动。如果您发现活动未经授权或可疑，AMS 会与您合作，调查和补救或遏制问题。由 GuardDuty 此生成的某些发现类型要求您在Accelerate采取任何措施之前确认影响。例如， GuardDuty 查找结果类型 UnauthorizedAccess：IAMUser/ConsoleLogin表示您的一个用户从不寻常的位置登录；AMS 会通知您并要求您查看调查结果以确认这种行为是否合法。

使用亚马逊 Macie 进行监控

AMS Accelerate 支持 Amazon Macie 检测大量而全面的敏感数据，例如个人健康信息 (PHI)、个人身份信息 (PII) 和财务数据，这是一种最佳实践。

您可以将 Macie 配置为在任何 Amazon S3 存储桶上定期运行。随着时间的推移，这可以自动评估存储桶中新的或修改过的对象。生成安全调查结果后，AMS 会通知您并根据需要与您合作对发现进行补救。

有关更多信息，请参阅分析 Amazon Macie 调查结果。

使用监视器 GuardDuty

GuardDuty 是一项持续的安全监控服务，它使用威胁情报源（例如恶意 IP 地址和域名列表）以及机器学习来识别 AWS 环境中意外且可能未经授权的恶意活动。这可能包括诸如权限升级、使用暴露的凭据或与恶意 IP 地址或域进行通信之类的问题。 GuardDuty 监控 AWS 账户 访问行为是否存在入侵迹象，例如未经授权的基础设施部署、在您从未使用过的 AWS 区域中部署的实例。 GuardDuty 还可以检测异常的 API 调用，例如更改密码策略以降低密码强度。有关更多信息，请参阅 GuardDuty 《用户指南》 。

要查看和分析您的 GuardDuty 发现，请完成以下步骤：

1. 打开 GuardDuty 控制台，网址为https://console.aws.amazon.com/guardduty/。
2. 选择 “调查结果”，然后选择特定的调查结果以查看详细信息。每个发现的详细信息因发现类型、所涉及的资源和活动性质而异。

有关可用查找字段的更多信息，请参阅GuardDuty 查找结果详细信息。

使用 GuardDuty 抑制规则筛选结果

抑制规则是一组标准，由过滤器属性和值配对组成。您可以使用抑制规则来筛选您不打算采取行动的低价值发现，例如误报调查结果或已知活动。筛选您的发现有助于更轻松地识别可能对您的环境影响最大的安全威胁。

要筛选搜索结果，抑制规则会自动存档符合您指定条件的新搜索结果。存档的发现不会发送到 S AWS ecurity Hub、Amazon S3 或 CloudTrail 活动。因此，如果您通过 Security Hub 或第三方 SIEM 警报和票务应用程序使用 GuardDuty 发现，则抑制过滤器会减少不可操作的数据。

AMS 有一套明确的标准来确定您的托管账户的封禁规则。当托管账户符合此条件时，AMS 会应用筛选条件并向您创建服务请求 (SR)，详细说明已部署的抑制过滤器。

您可以通过 SR 与 AMS 通信，以修改或恢复抑制过滤器。

查看存档的调查结果

GuardDuty 即使这些发现符合您的抑制规则，也会继续生成搜索结果。隐藏的搜索结果将标记为已存档。 GuardDuty 商店将查找结果存档了 90 天。通过从调查结果表中选择已存档，可以在 GuardDuty 控制台中查看这 90 天的存档调查结果。或者，使用 GuardDuty API 通过 API 查看存档的调查结果，findingCriteria 为 s ervic e. archived 等于 true。ListFindings

禁止规则的常见用例

以下调查发现类型具有使用抑制规则的常见应用场景。

- Recon: EC2 /Portscan：使用授权漏洞扫描程序时，使用抑制规则自动存档发现的结果。
- UnauthorizedAccess:EC2/SSHBruteForc e：使用抑制规则在针对堡垒实例时自动存档调查结果。
- Recon:EC2/PortProbeUnprotectedPort：使用抑制规则在有意暴露的实例上自动存档调查结果。

使用亚马逊 Route 53 解析器 DNS 防火墙进行监控

Amazon Route 53 Resolver 以递归方式响应来自公共记录 AWS 资源、亚马逊 VPC 特定的 DNS 名称和 Amazon Route 53 私有托管区域的 DNS 查询，默认情况下全部可用。 VPCs使用 Route 53 Resolver DNS Firewall，您可以筛选和管理 Virtual Private Cloud (VPC) 的出站 DNS 流量。为此，您需要在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，将规则组关联到您的 VPC，然后监控 DNS Firewall 日志和指标中的活动。根据活动，您可以相应地调整 DNS Firewall 的行为。有关更多信息，请参阅使用 DNS 防火墙过滤出站 DNS 流量。

要查看和管理 Route 53 解析器 DNS 防火墙配置，请按以下步骤操作：

1. 登录 AWS 管理控制台 并打开 Amazon VPC 控制台，网址为https://console.aws.amazon.com/vpc/。
2. 在 DNS 防火墙下，选择规则组。
3. 查看、编辑或删除现有配置，或创建新的规则组。有关更多信息，请参阅 Route 53 解析器 DNS 防火墙的工作原理。

Amazon Route 53 解析器 DNS 防火墙监控和安全

Amazon Route 53 DNS 防火墙使用规则关联、规则操作和规则评估优先级等概念。域列表是您在规则组内的 DNS Firewall 规则中使用的一组可重复使用的域规范。当您关联规则组与 VPC 时，DNS Firewall 会将您的 DNS 查询与规则中使用的域列表进行比较。如果 DNS 防火墙找到匹配项，则它会根据匹配规则的操作处理 DNS 查询。有关规则组和规则的更多信息，请参阅 DNS 防火墙规则组和规则。

域列表分为两大类：

- 托管域名列表， AWS 可为您创建和维护。
- 您自己的域名列表，由您创建和维护。

根据规则组的关联优先级指数对其进行评估。

默认情况下，AMS 部署的基准配置由以下规则和规则组组成：

- 一个名为的规则组DefaultSecurityMonitoringRule。对于每个已启用的现有 VPC，规则组在创建时具有最高的关联优先级 AWS 区域。
- 规则组中一个优先级为 DefaultSecurityMonitoringRule 1 的DefaultSecurityMonitoringRule规则，使用带有操作 A LE RT 的AWSManagedDomainsAggregateThreatList托管域列表。

如果您已有配置，则部署基准配置的优先级将低于现有配置。您的现有配置是默认配置。如果您的现有配置没有提供有关如何处理查询解析的更高优先级的指令，则可以使用 AMS 基准配置作为包罗万象的配置。要更改或移除基准配置，请执行以下操作之一：

- 请联系您的云服务交付经理 (CSDM) 或云架构师 (CA)。
- 创建服务请求。

AMS 中的数据加密加速

AMS Accelerate 使用多种方法 AWS 服务 进行数据加密。

Amazon Simple Storage Service 提供了多种对象加密选项，可保护传输中的数据和静态数据。服务器端加密在将对象保存到数据中心的磁盘上之前加密对象，然后在下载对象时对数据进行解密。只要您验证了您的请求并且拥有访问权限，您访问加密和未加密对象的方式就没有区别。有关更多信息，请参阅 Amazon S3 中的数据保护。

AWS Identity and Access Management 在 AMS 中加速

AWS Identity and Access Management 是一项 Web 服务，可帮助您安全地控制对 AWS 资源的访问。可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（具有相应权限）来使用资源。在 AMS Accelerate 入职期间，您负责在每个托管账户中创建跨账户 IAM 管理员角色。

在 AMS Accelerate 中，您负责管理对您 AWS 账户 及其底层资源的访问权限，例如访问管理解决方案、访问策略和相关流程。这意味着您可以管理用户生命周期、目录服务权限和联合身份验证系统，以访问 AWS 控制台或 AWS APIs。为了帮助您管理访问解决方案，AMS Accelerate 部署了检测常见的 IAM 错误配置的 AWS Config 规则，并提供补救通知。有关更多信息，请参阅 AWS Config Managed Rules。

在 AMS 加速中使用身份进行身份验证

AMS 使用 IAM 角色，这是一种 IAM 身份。IAM 角色与用户类似，因为它是一个具有权限策略的身份，该策略决定了该身份可以做什么和不能做什么 AWS。但是，一个角色没有与之关联的凭证，与其与一个人有唯一的关联，而是可以由任何需要它的人担任。IAM 用户可担任角色来暂时获得针对特定任务的不同权限。

访问角色由内部组成员资格控制，内部组成员资格由运营管理部门管理和定期审查。AMS 使用以下 IAM 角色。

> **Note**
>
> AMS 访问角色允许 AMS 操作员访问您的资源以提供 AMS 功能（请参阅服务描述）。改变这些角色可能会抑制我们提供这些能力的能力。如果您需要更改 AMS 访问角色，请咨询您的云架构师。

角色名称	说明
使用者（实体）：仅限 AMS 访问服务	
ams-access-management	由您在入职期间手动部署。仅由 AMS 拥有部署或更新访问角色的访问权限。入职后仍保留在您的账户中，以备将来对访问角色进行任何更新。
使用者（实体）：AMS 运营部门	
ams-access-admin-operations	此角色具有账户操作的管理权限，但无权读取、写入或删除常用作数据存储的服务（例如亚马逊简单存储 AWS 服务、亚马逊关系数据库服务、Amazon DynamoDB、Amazon Redshift 和亚马逊）中的客户内容。 ElastiCache只有极少数精选的 AMS 人员可以担任此角色。
ams-access-operations	此 AMS 运营角色有权在您的账户中执行管理任务。此角色对通常用作数据存储的服务（例如亚马逊简单存储服务、亚马逊关系数据库 AWS 服务、亚马逊 DynamoDB、Amazon Redshift 和亚马逊）中的客户内容没有读取、写入或删除权限。 ElastiCache此角色还不包括执行 AWS Identity and Access Management 写入操作的权限。
ams-access-read-only	此 AMS 只读角色仅限于您的 AMS 账户中的只读权限。该角色不授予对通常用作数据存储的 AWS 服务（例如 Amazon S3、Amazon RDS、DynamoDB、Amazon Redshift ElastiCache 和）中客户内容的读取权限。
使用方（实体）：AMS 运营和 AMS 服务	
ams_ssm_automation_role	假设 AWS Systems Manager 在您的账户中执行 SSM 自动化文档。
ams_ssm_automation_role	
使用者（实体）：AMS Secur ity	

角色名称	说明
ams-access-security-analyst	此 AMS 安全角色有权在您的 AMS 账户中执行专门的安全警报监控和安全事件处理。只有极少数精选的 AMS Security 人员可以担任此角色。该角色不授予对通常用作数据存储的 AWS 服务（例如 Amazon S3;、Amazon RDS;、Amazon DynamoDB、Amazon Redshift ElastiCache 和）中客户内容的读取权限。
ams-access-security-analyst-只读	此 AMS 安全角色仅限于您 AMS 账户中的只读权限，用于执行专门的安全警报监控和安全事件处理。该角色不授予对通常用作数据存储的 AWS 服务（例如 Amazon S3;、Amazon RDS;、Amazon DynamoDB、Amazon Redshift ElastiCache 和）中客户内容的读取权限。
使用方（实体）：AWS 服务	
ams-access-admin	此 AMS 管理员角色拥有不受限制地在账户中操作的完全权限。只有 AMS 内部服务（使用范围缩小的会话策略）可以担任管理员角色。
ams-opscenter-eventbridge-role	Amazon EventBridge 假定在 AMS 特定的 AWS Config 规则 补救工作流程中创建 AWS Systems Manager OpsItems 。
AMSOSConfigurationCustomerInstanceRole	当 AMS 操作系统配置服务发现缺少所需的 IAM 策略时，此 IAM 角色将应用于您的 Amazon EC2 实例。它允许您的亚马逊 EC2实例与亚马逊和亚马逊 CloudWatch EventBridge 服务进行交互。 AWS Systems Manager它还附加了 AMS 自定义托管策略，以启用 RDP 访问您的 Windows 实例。
mc-patch-glue-service-角色	AWS Glue ETL 工作流程假设执行数据转换并为 AMS 补丁报告生成器做好准备。

角色名称	说明
使用方（实体）：AMS 服务	
ams-alarm-manager-AWSManaged ServicesAlarmManagerDe-<8-digit hash>	由您的 AMS 账户中的 AMS 警报管理器基础设施承担，用于对新 AWS AppConfig 部署进行 AWS Config 规则 评估。
ams-alarm-manager-AWSManaged ServicesAlarmManagerRe-<8-digit hash>	由您的 AMS 账户中的 AMS 警报管理器补救基础设施承担，允许创建或删除警报以进行补救。
ams-alarm-manager-AWSManaged ServicesAlarmManager SS-<8-digit hash>	假设在您的 AWS Systems Manager AMS 账户中调用 AMS 警报管理器补救服务。
ams-alarm-manager-AWSManaged ServicesAlarmManagerTr-<8-digit hash>	由您 AWS 账户中的 AMS 警报管理器基础设施承担，用于定期进行 AMS AWS Config 规则 评估。
ams-alarm-manager-AWSManaged ServicesAlarmManagerVa-<8-digit hash>	由您的 AMS 账户中的 AMS 警报管理器基础设施承担，以确保 AWS 账户中存在所需的警报。
ams-backup-iam-role	此角色用于在您的账户 AWS Backup 中运行。
ams-monitoring--AWSManaged ServicesLogGroupLimitLamb <8-digit hash>	由您的 AMS 账户中的 AMS 日志和监控基础设施假设，用于评估 Amazon CloudWatch 日志组限制并与服务配额进行比较。
ams-monitoring-AWSManaged 服务 RDSERDSMonitoring-<8-digit hash>	由您的 AMS 账户中的 AMS 日志和监控基础设施承担，用于将 Amazon RDS 事件转发给 Amaz CloudWatch on Events。
ams-monitoring--AWSManaged ServicesRedshiftMonitorin <8-digit hash>	由您的 AMS 账户中的 AMS 日志和监控基础设施承担，用于将 Amazon Redshift 事件（CreateCluster 和 DeleteCuster）转发到亚马逊 CloudWatch 活动。
ams-monitoring-infrastruc-AWSManaged ServicesMonito-<8-digit hash>	由您的 AMS 账户中的 AMS 日志和监控基础设施假设向 Amazon 简单通知服务发布消息，以验证该账户是否在报告所有必要数据。

角色名称	说明
ams-opscenter-role	由您的 AMS 账户中的 AMS 通知管理系统承担，用于管理您账户中 AWS Systems Manager OpsItems 与提醒相关的信息。
ams-opsitem-autoexecution-role	由 AMS 通知管理系统假设，使用 SSM 文档处理自动补救，以监控与您账户中的资源相关的警报。
ams-patch-infrastructure-amspatchconfigruleroleC1-<8-digit hash>	假设 AWS Config 为评估 AMS 补丁资源并检测其 CloudFormation 堆栈中的偏差。
ams-patch-infrastructure-amspatchcwruleopsitemams-<8-digit hash>	由 Amazon EventBridge 假定 AWS Systems Manager OpsItems 为补丁失败而创建。
ams-patch-infrastructure-amspatchservicebusamspat-<8-digit hash>	Amazon 假设将事件发送 EventBridge 到 AMS Patch 协调器事件总线，用于 AWS Systems Manager 维护 Windows 状态更改通知。
ams-patch-reporting-infra-amspatchreportingconfigr-<8-digit hash>	假设 AWS Config 为评估 AMS 补丁报告资源并检测其 CloudFormation 堆栈中的偏差。
ams-resource-tagger-AWSManaged ServicesResourceTagg-<8-digit hash>	由您的 AMS 账户中的 AMS 资源标记器基础设施承担，用于在新 AWS AppConfig 部署时执行 AWS Config 规则 评估。
ams-resource-tagger-AWSManaged ServicesResourceTagg-<8-digit hash>	由您的 AMS 账户中的 AMS 资源标签基础架构使用，以验证托管资源是否存在所需的 AWS 标签。
ams-resource-tagger-AWSManaged ServicesResourceTagg-<8-digit hash>	假设 AWS Systems Manager 在您的 AMS 账户中调用 AMS 资源标记器补救工作流程。
ams-resource-tagger-AWSManaged ServicesResourceTagg-<8-digit hash>	由您的 AMS 账户中的 AMS 资源标签修复基础设施负责为托管资源创建或删除 AWS 标签。
ams-resource-tagger-AWSManaged ServicesResourceTagg-<8-digit hash>	由您 AWS 账户中的 AMS 资源标记器基础设施负责定期评估 AMS Config 规则。

角色名称	说明
ams_os_configuration_event_rule_role-<AWS Region>	Amazon 假设将事件从您的账户转发 EventBridge 到正确区域的 AMS 操作系统配置服务 EventBus 。
mc-patch-reporting-service	由 AMS 补丁数据聚合器和报告生成器假设。

> **Note**
>
> 这是 ams-access-management角色的模板。这是云架构师 (CAs) 在入职时在你的账户中手动部署的堆栈：man ag ement-role.yaml。
> 这是不同访问角色和访问级别的模板： ams-access-read-only、、 ams-access-operations、:accelerate-roles ams-access-admin-operations. ams-access-admin y aml。

要了解有关 AWS Cloud Development Kit (AWS CDK) (AWS CDK) 标识符（包括哈希）的更多信息，请参阅 Uni q IDs ue。

AMS Accelerate 功能服务负责以编程方式访问账户，但会话策略的范围仅限于相应的功能服务（例如，补丁、备份、监控等）。ams-access-admin

AMS Accelerate 遵循行业最佳实践，以满足并保持合规资格。AMS Accelerate 对您账户的访问已记录在 CloudTrail 案，您也可以通过变更跟踪进行审查。有关可用于获取此信息的查询的信息，请参阅跟踪您的 AMS Accelerate 账户中的更改。

使用策略管理访问

各个 AMS Accelerate 支持团队，例如运营工程师、云架构师和云服务交付经理 (CSDMs)，有时需要访问您的账户才能响应服务请求和事件。他们的访问受内部AMS访问服务的约束，该服务强制实施控制措施，例如业务理由、服务请求、运营项目和支持案例。默认访问权限为只读，并且会跟踪和记录所有访问权限；另请参阅跟踪您的 AMS Accelerate 账户中的更改。

验证 IAM 资源

AMS Accelerate 访问系统会定期在您的账户中扮演角色（至少每 24 小时一次），并验证我们的所有 IAM 资源是否符合预期。

为了保护您的账户，AMS Accelerate 有一个 “金丝雀”，用于监控上述 IAM 角色的存在和状态及其附加策略，并发出警报。金丝雀会定期担任该ams-access-read-only角色并对您的账户发起 CloudFormation 和 IAM API 调用。金丝雀会评估 AMS Accelerate 访问角色的状态，以确保它们始终未被修改，并且. up-to-date 此活动会在账户中创建 CloudTrail 日志。

如中所示，金丝雀的 AWS Security Token Service (AWS STS) 会话名称为 ams-access-roles-auditor-{ uuid4 ()}，并且会进行以下 API 调用： CloudTrail

- 云形成 API 调用：`describe_stacks()`
- IAM API 调用：
  - `get_role()`
  - `list_attached_role_policies()`
  - `list_role_policies()`
  - `get_policy()`
  - `get_policy_version()`
  - `get_role_policy()`

AMS 中的安全事件响应

安全是 AWS Managed Services (AMS) 的重中之重。AMS 在您的账户中部署资源和控制来对其进行管理。 AWS 有一个责任共担模式： AWS 管理云的安全，你负责云中的安全。AMS 通过使用安全控制和主动监控安全问题，保护您的数据和资产，并帮助确保您的 AWS 基础设施安全。这些功能可帮助您为在 AWS 云中运行的应用程序建立安全基准。AMS 通过安全事件响应与您合作，评估其影响，然后根据最佳实践建议进行遏制和补救。

当出现偏离基线的情况（例如配置错误或外部因素的变化）时，您需要做出回应并进行调查。要成功做到这一点，您需要了解 AMS 环境中安全事件响应的基本概念。您还必须了解在安全问题发生之前做好准备、教育和培训云团队的要求。重要的是要了解您可以使用的控制和功能，针对常见的安全问题（例如用户帐户受损或滥用特权帐户）制定应对计划，并确定使用自动化来提高响应速度和一致性的补救方法。此外，您需要了解您的合规和监管要求，因为它们与制定安全事件响应计划以满足这些要求有关。

安全事件响应可能很复杂，但是通过实施迭代方法，您可以简化流程，并允许事件响应团队通过提供早期和持续的检测和响应来让资产利益相关者满意。在本指南中，我们向您提供 AMS 用于事件响应的方法、AMS 责任矩阵 (RACI)、如何为安全事件做好准备、如何在安全事件期间与 AMS 接触，以及 AMS 使用的一些事件响应操作手册。

AMS 安全事件响应的工作原理

AWS Managed Services 与 NIST 800-61 安全事件响应计算机安全事件处理指南保持一致。通过与该行业标准保持一致，我们提供了一种一致的安全事件管理方法，并遵守保护和响应云端安全事件的最佳实践。

事件响应生命周期

当检测发现并生成安全警报，或者您请求安全帮助时，AWS Managed Services Operations 团队会确保及时进行调查，自动执行数据收集、分类和分析，通知您分析情况，执行调查和任何遏制活动，然后发布事件分析。

事件响应期间执行的数据收集、分类、分析和遏制活动因所调查的安全事件的类型而异。本文档末尾列出了特定场景的安全事件响应工作流程示例。

在事故发生期间，AMS 会动态确定正确的行动方案，这可能会导致对记录在案的步骤进行重新排序或酌情绕过，以确保产生正确的结果。

准备

随着威胁形势的演变，AMS 继续扩大检测和响应能力。随着新检测的增加，AMS 会将这些新检测产生的警报整合到检测和响应平台中。AMS 安全响应人员经过培训，可以在整个安全事件响应生命周期中进行调查并与您合作。

由于这种合作方式，您的安全和应用团队必须做好与 AMS 合作的准备，以便在这些事件发生时处理这些事件，这一点非常重要。本文档解释了安全事件期间的预期，并帮助您为安全事件发生时的快速响应做好准备。

本文档使用 NIST 800-61 的定义，将事件定义为系统或网络中任何可观察到的事件，将事件定义为违反政策、可接受使用策略或标准安全实践的违规行为或迫在眉睫的威胁。

准备清单

与您的 AMS 云解决方案交付经理 (CSDM) 和 AMS 云架构师 (CA) 一起完成以下清单：

- 了解哪些工作负载在哪些账户中运行。
- 了解哪些内部团队负责各种工作负载，并在工作负载中对其进行适当标记。
- 在内部保留在安全事件调查和控制决策期间可能需要的其他团队的联系方式。

- 确认安全联系人是最新的，并已添加到所有托管 AWS 账户。联系人按账户进行管理。
- 知道如何向 AMS 举报安全事件，并熟悉严重程度和预期的响应时间。
- 确保在收到安全通知时，将它们发送给相应的人员和系统，例如寻呼机或您的安全运营中心。
- 了解哪些日志源可供您使用，这些日志源存储在您的账户中的位置以及谁有权访问它们。
- 了解如何在调查期间使用 CloudWatch Insights 查询日志。
- 了解按资源（EC2、IAM、S3 等）可供您使用的控制选项，以及处于控制状态时对工作负载可用性的影响。

Detect

在管理您的 AWS 账户期间，AMS 会使用从检测来源和控件（包括但不限于亚马逊、亚马逊、GuardDuty VPC 流日志、Amazon Macie 和 CloudWatch亚马逊内部威胁情报源）收集的数据来监控用户行为、账户活动 AWS Config 和潜在安全事件中的异常情况。

AMS 使用原生 AWS 服务和其他检测技术来响应由以下原因创建的安全事件：

- Config 一致性查找类型
- GuardDuty 查找类型
- Macie 查找类型
- 亚马逊 Route 53 解析器 DNS 防火墙事件
- AMS 安全事件（云监视警报）

随着服务、产品和威胁生态系统的发展，还增加了其他发现。

向 AMS 报告安全事件

通过 AMS Support 门户或 支持 中心举报事件，向 AMS 通报安全事件或请求调查。

分析

识别并报告安全事件后，下一步是分析报告的事件是误报事件还是真实事件。AMS 使用自动化和手动调查技术来处理安全事件。分析包括调查来自不同检测源的日志，例如网络流量日志、主机日志、CloudTrail 事件、 AWS 服务日志等。该分析还通过相关性寻找显示异常行为的模式。

您的合作伙伴关系需要了解特定于账户环境的背景，并确定您的账户和工作负载的正常情况。这有助于 AMS 更快地识别异常并加快事件响应。

处理来自 AMS 的有关安全事件的通信

在调查期间，AMS 会通过事件单与您的安全联系人联系，随时向您通报情况。在主动安全调查期间，您的 AMS 云服务交付经理 (CSDM) 和 AMS 云架构师 (CA) 是联系人，可以联系他们进行任何沟通。

通信包括在生成安全警报时自动通知、事件分析后进行通信、建立呼叫桥接以及持续交付项目（例如日志文件、受感染资源的快照），以及在安全事件期间向您提供调查结果。

AMS 安全警报通知中包含的标准字段如下所示。这些字段为您提供信息，以便您可以将事件发送给组织内的相应团队进行补救。

- 查找类型
- 查找标识符（如果相关）
- 查找严重性
- 查找描述
- 查找创建日期和时间
- AWS 账户编号
- 区域（如果相关）
- AWS 资源（IAM user/role/policy、 EC2、S3、EKS）

根据查找结果类型，还会提供其他字段，例如，EKS Finding 包括 Pod、容器和集群详细信息。

遏制

AMS 的遏制方法是与您合作。您了解您的业务以及遏制活动可能对工作负载产生的影响，例如网络隔离、IAM 用户或角色取消预配、实例重建等。

遏制的一个重要部分是决策。例如，关闭系统、将资源与网络隔离开来，或者关闭访问或结束会话。如果有预先确定的策略和程序来遏制事件，则更容易做出这些决定。AMS 提供遏制策略，然后在您考虑实施遏制措施所涉及的风险后实施解决方案。

根据所分析的资源，有不同的控制选项。AMS预计，在事故调查期间，将同时部署多种类型的遏制措施。其中一些例子包括：

- 应用保护规则来阻止未经授权的流量（安全组、NACL、WAF 规则、SCP 规则、拒绝列出、将签名操作设置为隔离或阻止）
- 资源隔离

- 网络隔离
- 禁用 IAM 用户、角色和策略
- 修改/减少 IAM 用户、角色权限
- 终止/暂停/删除计算资源
- 限制公众访问受影响资源
- 轮换访问密钥、API 密钥和密码
- 清理披露的凭据和敏感信息

AMS鼓励您考虑风险偏好范围内的每种重大事件类型的遏制策略类型，并明确记录标准，以帮助在发生事件时做出决策。确定适当策略的标准包括：

- 资源潜在损害程度
- 保存证据
- 服务不可用性（如网络连接、向外部提供的服务）
- 实施策略所需的时间与资源
- 策略的有效性（例如，部分遏制、完全遏制）
- 解决方案的永久性（例如，单向门与双向门的决策）
- 解决方案的持续时间（例如，紧急变通方案将在四小时内删除，临时变通方案将在两周内删除，永久解决方案）。
- 应用您可以开启的安全控制措施来降低风险，并留出时间来定义和实施更有效的遏制措施。

遏制速度至关重要，AMS建议采取分阶段的方法，通过制定短期和长期方法来实现高效和有效的遏制。

使用本指南来考虑您的遏制策略，该策略涉及基于资源类型的不同技术。

- 遏制策略
  - AMS 能否确定安全事件的范围？
    - 是：标记所有相关资源（用户、系统、资源）。
    - 否：对已识别资源执行下一步，同时继续调查。
  - 资源是否能被隔离？
    - 是：立即隔离受影响资源。
    - 否：协同系统负责人确定替代遏制方案。

- 所有受影响的资源是否都已与未受影响的资源隔离开来？
  - 是：进入下一阶段。
  - 如果不是，则继续隔离受影响的资源，直到完成短期遏制，以防止事件进一步升级。
- 系统备份
  - 是否已创建受影响系统备份用于分析？
  - 取证副本是否已加密并安全存储？
    - 是：进入下一阶段。
    - 否：立即加密取证映像并安全存储，防止意外使用、损坏或篡改。

根除

事件得到控制后，在进入下一个恢复阶段之前，可能需要根除威胁以完全消除威胁源，从而保护系统。根除步骤可能包括删除恶意软件和移除受感染的用户帐户，以及识别和缓解所有被利用的漏洞。在根除期间，重要的是要识别环境中所有受影响的账户、资源和实例，以便对其进行补救。

最佳做法是分阶段进行根除和恢复，以便确定补救措施的优先顺序。对于大规模事件，恢复可能需要几个月的时间。早期阶段的目的必须是通过相对较快（几天到几周）的高价值更改来提高整体安全性，以防止将来发生事件。后期阶段必须侧重于长期变革（例如基础架构变更）和持续的工作，以尽可能确保企业的安全。

对于某些事件，要么没有必要，要么在恢复期间进行消除。

请考虑以下事项：

- 能否对系统进行重新映像，然后通过补丁或其他对策进行强化以防止或降低攻击风险？
- 攻击者留下的所有恶意软件和其他工件是否都被清除，受影响的系统是否已得到加强，可以抵御进一步的攻击？

恢复

AMS 与您合作，将系统恢复到正常运行，确认系统运行正常，并（如适用）修复漏洞以防止发生类似事件。

请考虑以下事项：

- 受影响的系统是否经过修补和强化，可以抵御最近的攻击和未来可能的攻击？

- 哪一天和什么时间可以将受影响的系统恢复到生产状态？
- 您将使用哪些工具来测试、监控和验证恢复到生产环境的系统是否不容易受到初始攻击技术的攻击？

事故后报告

事件发生后，AMS 会对所有安全事件进行调查审查。而且，AMS 启动了错误更正 (COE) 流程，以解决由系统或程序失误引起的安全事件，这些事件可能还有改进余地。AMS 与您合作，不断改善安全调查体验。COE 流程可帮助 AMS 识别影响客户的事件的促成因素，并将这些原因与下一步的行动项目联系起来，这些项目可以防止类似事件再次发生，或者有助于缓解影响的持续时间或程度。

安全事件调查审查流程涉及以下事项，以确定改进机会：

- 从事件开始到事件发现，到最初的影响评估，再到事件处理过程的每个阶段（例如遏制、恢复），经过了多长时间？
- 事件响应小组花了多长时间才对事件的初步报告做出回应？
- 进行初步影响分析花了多长时间？
- 这是可以预防的吗？如何预防？ 有没有可以阻止这种情况的工具或流程？
- 我们能早点发现吗？如何发现？
- 什么能让调查更快地进行？
- 是否遵循了记录在案的事故响应程序？ 它们足够吗？
- 与其他利益相关者的信息共享是否及时？如何加以改进？
- 与其他团队（AWS 安全、客户团队、 AWS 开发团队和客户安全团队）的合作是否有效？ 如果不是，还有什么可以改进的地方？
- 缺少了哪些可能有所帮助的准备步骤，升级矩阵、RACI、分担责任模型等等？ 是否需要更新任何 Runbook？
- 初步影响评估和最终影响评估有什么区别？ 在事件响应的早期阶段，我们可以做些什么来提高评估的准确性？
- 经验教训中的行动项目有哪些？

AMS 中的安全事件响应操作手册

本节包含两个运行手册：

- 对 root 用户活动的响应

- 对恶意软件事件的响应

对 root 用户活动的响应

r oot 用户是您 AWS 账户中的超级用户。请注意，AMS 会监控根用户使用情况。最佳做法是仅将根用户用于少数需要它的任务，例如更改账户设置、激活 AWS Identity and Access Management (IAM) 账单和成本管理权限、更改根密码以及开启多重身份验证 (MFA)。有关更多信息，请参阅需要 root 用户凭据的任务。

有关如何通知 AMS 计划的 root 用户使用情况的更多信息，请参阅何时以及如何在 AMS 中使用根账户。

当检测到 root 用户活动时，无论是登录尝试失败（可能表示暴力攻击）或成功登录后账户中的活动，都会生成一个事件并将事件发送给您定义的安全联系人。

AWS Managed Services Operations 调查计划外的根用户活动，执行数据收集、分类和分析，并按照您的指示执行遏制活动，然后进行事件后分析。

如果您使用的是 AMS Advanced 操作模式，则会收到来自 AMS CSDM 和 AMS Ops 工程师的额外通信，这些通信确认了由于 AMS 有责任保护根用户凭证而导致的计划外根用户活动。AMS 会调查 root 用户活动，直到您确认前进方向。

准备

通过提交 AMS 服务请求，告知 AMS 计划使用 root 用户的情况，包括计划中的事件的数据和时间，以防止不必要的事件响应活动。

定期 GameDays 与 AMS 合作，验证 AMS 的客户事件响应流程、人员和系统是否处于最新状态，并与负责任的个人建立肌肉记忆，以实现更快的事件响应。

阶段 A：检测

AMS 通过检测源（包括 GuardDuty AMS 监控）来监控账户中的根用户活动。

如果您有 AMS Accelerate，则操作模型会对请求对意外根用户活动进行调查的事件做出响应。发生这种情况时，AMS 运营部门会启动被盗账户操作手册。

如果您有 AMS Advanced，则运营模式会对事件做出响应，或者将 root 用户的任何计划活动通知给 CSDM，以终止正在进行的账户泄露调查。

B 阶段：分析

当确定根用户事件未获得授权时，AMS 会对该活动进行彻底调查。使用自动化和 AMS 安全响应团队，对日志和事件进行分析，以确定根用户的异常和意外行为。向您提供日志是为了帮助您确定活动是否未知、是否是授权的 root 用户事件，或者是否需要进一步调查。

调查期间为支持内部检查而提供的信息的一些示例包括：

- 账户信息：root 账户用于哪个账户？
- root 用户的电子邮件地址：每个 root 用户都与贵组织中的一个电子邮件地址相关联
- 身份验证详情：root 用户从何时何地访问您的环境？
- 活动记录：用户以 root 身份登录后做了什么？ 这些记录以 CloudWatch 事件的形式出现。了解如何阅读这些日志有助于调查。

最佳做法是准备好接收分析信息，并计划如何联系组织内客户的授权联系人。由于 root 用户不是以个人身份命名的，因此确定谁有权访问组织内用于该帐户的根电子邮件地址有助于在内部快速传递问题。

C阶段：遏制和消灭

AMS 与您的安全团队合作，在您授权的客户安全联系人的指导下进行遏制。密封选项包括：

- 轮换适当的凭证和密钥。
- 终止与账户和资源的活动会话。
- 清除已创建的资源。

在控制活动期间，AMS 会与您的安全团队密切合作，确保最大限度地减少对您的工作负载的任何干扰，并适当保护根凭证。

控制计划完成后，您可以根据需要与 AMS 运营团队合作采取任何恢复行动。

事故后报告

根据要求，AMS启动调查审查流程，以确定任何经验教训。作为完成 COE 的一部分，AMS 会将所有相关发现传达给受影响的客户，以帮助他们改善事件响应流程。

AMS 记录调查的所有最终细节，收集适当的指标，然后将事件报告给任何需要信息的 AMS 内部团队，包括您分配的 CSDM 和 CA。

对恶意软件事件的响应

Amazon EC2 实例用于托管各种工作负载，包括由组织内部应用程序团队部署的第三方软件和定制开发的软件。AMS 提供并鼓励您在由 AMS 持续修补和维护的映像上部署工作负载。

在实例运行期间，AMS 通过各种安全检测控件（包括 Amazon GuardDuty、网络流量和亚马逊内部威胁情报源）来监控行为或活动中的异常情况。

AMS 还会监控 GuardDuty 恶意软件发现。如果启用，它们在 AMS Advanced 和 AMS Accelerate 上都可用。有关更多信息，请参阅 Amazon GuardDuty 中的恶意软件防护。

> **Note**
>
> 如果您选择了 Brin g Your Own EPS，则事件响应的流程与本页上概述的流程不同。有关更多信息，请参阅参考文档。

当检测到恶意软件时，就会创建事件并向您通知该事件。在此通知之后，将显示已发生的任何补救活动。AMS Operations 负责调查、执行数据收集、分类和分析，然后按照您的指示执行遏制活动，然后进行事后分析。

阶段 A：检测

AMS 使用监控实例上的事件 GuardDuty。AMS 确定适当的浓缩和分类活动，以帮助您根据发现或警报类型做出遏制或风险接受决策。

数据收集是根据发现类型进行的。数据收集涉及查询受影响账户内部和外部的多个数据源，以了解观察到的活动或关注的配置。

AMS 将发现结果与来自任何受影响账户或 AMS 威胁情报平台的任何其他警报和警报或遥测数据进行关联。

B 阶段：分析

收集数据后，对其进行分析以确定任何活动或令人担忧的指标。在调查的这一阶段，AMS 将与您合作，整合实例和工作负载的业务和领域知识，以帮助了解预期情况和异常情况。

调查期间为支持内部检查而提供的信息的一些示例包括：

- 账户信息：在哪个账户上观察到恶意软件活动？
- 实例详情：哪些实例与恶意软件事件有关？
- 事件时间戳：警报是什么时候触发的？

- 工作负载信息：实例上正在运行什么？
- 恶意软件详细信息（如果相关）：恶意软件系列和有关恶意软件的开源信息。
- 用户或角色详情：哪些用户或角色受活动影响并参与其中？
- 活动记录：实例上记录了哪些活动？ 它们以 CloudWatch 事件和来自实例的系统事件的形式出现。了解如何阅读这些日志将有助于您进行调查
- 网络活动：哪些终端节点正在连接到实例，实例正在连接什么，以及流量分析是什么？

最佳做法是做好接收调查信息的准备，并就如何联系组织内的客户、实例和工作负载的相应联系人制定计划。了解您的网络拓扑和预期的连接有助于加快影响分析。了解环境中计划的渗透测试以及应用程序所有者最近执行的部署也可以加快调查速度。

如果您确定该活动已计划并已获得授权，则会更新事件并结束调查。如果确认妥协，则您和 AMS 将确定适当的控制计划。

C 阶段：遏制和消灭

AMS 与您合作，根据收集的数据和已知信息确定适当的遏制活动。封闭选项包括但不限于：

- 通过快照保留数据
- 修改网络规则以限制进出实例的流量
- 修改 SCP、IAM 用户和角色策略以限制访问权限
- 终止、暂停或关闭实例
- 终止所有持久连接
- 轮换适当的凭据/密钥

如果您选择对实例执行清除活动，那么 AMS 将支持您实现这一目标。选项包括但不限于：

- 正在删除所有不需要的软件
- 从干净的完全修补的映像重建实例，然后重新部署应用程序和配置
- 从之前的备份中恢复实例
- 将应用程序和服务部署到您账户中可能适合托管工作负载的另一个实例。

在恢复服务之前，必须确定恶意软件是如何传递和在实例上运行的，以确保应用任何其他控制措施来防止恶意软件在实例上再次出现。AMS 根据需要向您的取证合作伙伴或团队提供其他见解或信息，以支持取证。

此时，您将与 AMS 运营部门合作开展恢复活动。AMS 与您密切合作，以最大限度地减少对工作负载的干扰并保护实例。

事故后报告

根据要求，AMS启动调查审查流程，以总结经验教训。作为完成 COE 的一部分，AMS 会向您传达相关调查结果，以帮助您改进事件响应流程。

AMS 记录调查的最终细节，收集适当的指标，并将事件报告给 AMS 内部团队，这些团队需要信息，包括您分配的 CSDM 和 CA。

在 Accelerate 中记录和监控安全事件

在 AMS Accelerate 中注册的账户配置了 CloudWatch 事件和警报的基准部署，这些事件和警报已经过优化，可以减少噪音并识别真实事件的迹象。AMS Accelerate 还 GuardDuty 用于账户监控。有关更多信息，请参阅 使用监视器 GuardDuty。

加速中的配置合规性

AMS Accelerate 可帮助您按照安全性和运营完整性的高标准配置资源，并遵守以下行业标准：

- 互联网安全中心 (CIS)
- 美国国家标准与技术研究院 (NIST) 云安全框架 (CSF)
- 健康保险流通与责任法案 (HIPAA)
- 支付卡行业 (PCI) 数据安全标准 (DSS)

为此，我们将整个合规 AWS Config 规则集部署到您的账户，请参阅AMS Config 规则库。 AWS Config 规则代表资源的所需配置，并根据资源设置的配置更改进行评估。 AWS 任何配置更改都会触发大量规则来测试合规性。例如，假设您创建了一个 Amazon S3 存储桶，并将其配置为可公开读取，这违反了 NIST 标准。ams-nist-cis-s3-bucket-public-read-prohibited 规则会检测到违规行为，并在配置报告中将您的 S3 存储桶标记为 “不合规”。由于此规则属于自动事故补救类别，因此它会立即创建事件报告，提醒您注意问题。其他更严重的违反规则的行为可能会导致 AMS 自动修复问题。请参阅对 “加速” 中违规行为的回应。

> **Important**
>
> 如果您希望我们采取更多措施，例如，如果您希望 AMS 为您纠正违规行为，无论其补救类别如何，请提交服务请求，要求 AMS 为您补救违规资源。在服务请求中，添加诸

如 “作为 AMS 配置规则补救的一部分，请修复账户*CONFIG_RULE_NAME*中的非投诉资源*RESOURCE_ARNS_OR_IDs*、配置规则” 之类的评论，并添加必要的输入以纠正违规行为。如果您希望我们少做一些事情，例如，如果您不希望我们对设计上需要公开访问的特定 S3 存储桶采取行动，则可以创建例外，请参阅在 “加速” 中创建规则例外。

AMS Config 规则库

Accelerate 会部署 AMS 配置规则库来保护您的账户。这些配置规则以开头ams-。您可以通过 AWS Config 控制台、CLI 或 AWS Config AP AWS I 查看账户中的规则及其合规状态。有关使用的一般信息 AWS Config，请参阅 ViewingConfiguration 合规性。

> **Note**
>
> 对于选择加入 AWS 区域和 gov cloud 区域，由于区域限制，我们只部署配置规则的子集。通过在 AMS Accelerate 配置规则表中查看与 AMS Accelerate 配置规则表中的标识符关联的链接，检查规则在区域中的可用性。
> 您无法删除任何已部署的 AMS Config 规则。

规则表

作为 ams_config_rules.zip 下载。

AMS 配置规则

规则名称	服务	触发器	操作	框架
ams-nist-cis-guardduty-启用集中式	GuardDuty	定期	修复	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) 164.312 (e) (2) (ii)；PCI：2.2,3.4,8.2.1；
ams-nist-cis-vpc-flow-logs-enabled	VPC	定期	修复	C@@ IS：CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-5、PR.PT-1；HIPAA：164

规则名称	服务	触发器	操作	框架
				.308 (a) (3) (ii) (A) 164.312 (b)；PCI：2.2,10.1,1 0.3.2,10.3.2,10.3.3,10.3.4, 10.3.5,10 .3.6；
ams-eks-secrets-encrypted	EKS	定期	事件	CIS：不适用；NIS T-CSF：不适用； HIPAA：不适用；PCI：不适用；
ams-eks-endpoint-no-公共访问	EKS	定期	事件	CIS：不适用；NIS T-CSF：不适用； HIPAA：不适用；PCI：不适用；
ams-nist-cis-vpc-default-security-group-closed	VPC	Config 更改	事件	C@@ IS：CIS.11、CI S.12、CIS.9；NIST-CSF：DE.AE-1、P R.AC-3、PR.AC-5、PR. PT-4；HIPAA：164.312 (e) (1)；PCI：1.2,1.3,2. 1,2.1,2.2,1.2.1,1.3.2,2.2.2 ；
ams-nist-cis-iam-密码政策	IAM	定期	事件	CIS：NA；NIS T-CSF：PR.AC-1，P R.AC-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (a) (3) (ii) 164.308 (a) (ii) 164.308 (a) (i) 164.308 (a) (a) (4)) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (a) (1)；PCI：7.1.2,7.1. 3,7.2.3,7.2.1,7.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-iam-root-access-key-check	IAM	定期	事件	C@@ IS：CIS.16、CIS.4；NIST-CSF：PR.AC-1、PR.AC-4、PR.PT-3；HIPAA：164.308 (a) (3) (i) 164.308 (a) (ii) (A) 164.308 (ii) (A) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) (4) (a) (a) (a) (3) (a) (3) (ii) (4) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (a) (a) (1)；PCI：2.2,7.1.2,7.1.3,7.2.1,7.2.2；
ams-nist-cis-iam-user-mfa-enabled	IAM	定期	事件	C@@ IS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) (a) (3) (ii) 164.308 (a) (3) (ii) 164.308 (a) (3) (ii) 164.308 (a) (3) (ii) 164.308 (a) (3) (ii) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) ,164.312 (a) (a) (1)；PCI：2.2,7.1.2,7.1.3,7.2.3,7.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-restricted-ssh	安全组	Config 更改	事件	C@@ IS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (C) 164.308 (a) (4) (ii) (C) 164.308 (a) (4) (ii) (C) 164.308 (a) (4) (ii) (C) 164.308 (a) (4) (ii) (C) 164.312 (a) (1)；PCI：2.2,7.2.1,8.1.4；
ams-nist-cis-restricted-公共端口	安全组	Config 更改	事件	C@@ IS：CIS.11、CIS.12、CIS.9；NIST-CSF：DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) ,164.308 (a) (i) ,164.308 (a) (i) 164.308 (a) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.32.2,1.2.1,1.3.1,1.3.2,2.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-s3 account-level-public-access-方块	S3	Config 更改	事件	C@@ IS：CIS.9、CIS .12、CIS.14；NIST-CSF：PR.AC-3、P R.AC- 4、PR.AC-5 、PR.DS-5、PR.PT-3、P R.PT-4；HIPAA：164 .308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)； PCI：1.2,1.2.1,1.2.1,1. 3.1,1.3.1,1.3.2,1.3.2,1.3.2 ,1.3.4,1.3.4,1.3.6,2.2,2.2. 2；
ams-nist-cis-s3-bucket-public-read-prohibited	S3	Config 更改	事件	C@@ IS：CIS.12、CI S.14、CIS.9；NIST-CSF：PR.AC-3、P R.AC- 4、PR.AC-5 、PR.DS-5、PR.PT-3、P R.PT-4；HIPAA：164 .308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)； PCI：1.2,1.3,2.2,1.2.1, 1.3.1,1.3.1,1.3.1,1.3.1,1.3 .2,1.3.2,1.3.4,1.3.4,1.3.6, 2.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-s3-bucket-public-write-prohibited	S3	Config 更改	事件	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,2.2,1.2.1,1.3.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-s3-已启bucket-server-side-encryption用	S3	Config 更改	事件	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) 164.312 (c) (2) (2) ,164.312 (e) (2) (2) (ii)；PCI：2.2,3.4,10.5,8.2.1；
ams-nist-cis-securityhub-已启用	Security Hub	定期	事件	C@@ IS：CIS.3、CIS.4、CIS.6、CIS.12、CIS.16、CIS.19；NIST-CSF：PR.DS-5、PR.PT-1；HIPAA：164.312 (b)；PCI：N A；

规则名称	服务	触发器	操作	框架
ams-nist-cis-ec2-经instance-managed-by-systems理	EC2	Config 更改	报告	C@@ IS：CIS.2，CIS.5；NIST-CSF：ID.AM-2，PR.IP-1；HIPAA：164.308 (a) (5) (ii) (B)；PCI：2.4；
ams-nist-cis-cloudtrail-已启用	CloudTrail	定期	报告	C@@ IS：CIS.16、CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-5、PR.MA-2、PR.PT-1；HIPAA：164.308 (a) (3) (ii) (A) 164.308 (a) (5) (ii) (C) 164.312 (b)；PCI：10.1,10.2.1,10.2.2,10.2.3,10.2.4,10.2.5,10.2.5,10.2.6,10.2.7,10.3.1,10.3.2,10.3.3,10.3.4,10.3.4,10.3.4,10.3.5,10.3.6；
ams-nist-cis-access-按键旋转	IAM	定期	报告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308 (a) (4) (ii) (B)；PCI：2.2；
ams-nist-cis-acm-certificate-expiration-check	Certificate Manager	Config 更改	报告	CIS：CIS.13，CIS.14；NIST-CSF：PR.AC-5，PR.PT-4；HIPAA：NA；PCI：4.1；

规则名称	服务	触发器	操作	框架
ams-nist-cis-alb-http-to-https-redirection-检查	ALB	定期	报告	独联体：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312 (a) (2) (iv) 164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii) ,164.312 (e) (2) (ii)；PCI：2.34.1,8.2.1；
ams-nist-cis-api-已加gw-cache-enabled-and密	API Gateway	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4；
ams-nist-cis-api-gw-execution-logging-enabled	API Gateway	Config 更改	报告	CIS：CIS .6；NIST-CSF：DE.AE-1、DE.AE-3、PR.PT-1；HIPAA：164. 312 (b)；PCI：10.1,10.3.1,10.3.2,10.3.3,10.3.3,10.3.4,10.3.4,10.3.5,10.3.6,10.5.4；
ams-nist-autoscaling-group-elb-healthcheck-required	ELB	Config 更改	报告	CIS：NA；NIS T-CSF：PR.PT-1，PR.PT-5；HIPAA：164.312 (b)；PCI：2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-cloud-trail-encryption-enabled	CloudTrail	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：2.2,3.4,10.5；
ams-nist-cis-cloud-已启trail-log-file-validation用	CloudTrail	定期	报告	C@@ IS：CIS.6；NIST-CSF：PR.DS-6；HIPAA：164.312 (c) (1) 164.312 (c) (2)；PCI：2.2,10.5,11.5,11.5,10.5,10.5.2,10.5.5；
ams-nist-cis-cloudtrail-s3数据事件已启用	CloudTrail	定期	报告	C@@ IS：CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-5、PR.PT-1；HIPAA：164.308 (a) (3) (ii) (A) 164.312 (b)；PCI：2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.5,10.3.3,10.3.3,10.3.3,10.3.4,10.2.3,10.3.3,10.3.4,10.2.3,10.3.3,10.3.3,10.3.4,10.3,10.3.3,10.3.4,10.3.5,10.3.6；
ams-nist-cis-cloudwatch-alarm-action-check	CloudWatch	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：不适用；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4；

规则名称	服务	触发器	操作	框架
ams-nist-cis-cloudwatch-log-group-encrypted	CloudWatch	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：不适用；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4；
ams-nist-cis-codebuild-project-envvar-awscred-check	CodeBuild	Config 更改	报告	C@@ IS：CIS.18；NIST-CSF：PR.DS-5；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (C) 164.312 (a) (1)；PCI：8.2.1；
ams-nist-cis-codebuild-project-source-repo-url-检查	CodeBuild	Config 更改	报告	C@@ IS：CIS.18；NIST-CSF：PR.DS-5；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (C) 164.312 (a) (1)；PCI：8.2.1；
ams-nist-cis-db-instance-backup-enabled	RDS	Config 更改	报告	C@@ IS：CIS.10；NIST-CSF：ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) 164.308 (a) (7) (ii) (A) 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B)；PCI：不适用;

规则名称	服务	触发器	操作	框架
ams-nist-cis-dms-replication-not-public	DMS	定期	报告	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-dynamodb-autoscaling-已启用	DynamoDB	定期	报告	CIS：不适用；NIST-CSF：ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) ,164.308 (a) (7) (7) (ii) (C)；PCI：NA；
ams-nist-cis-dynamodb-启用 pitr	DynamoDB	定期	报告	C@@ IS：CIS.10；NIST-CSF：ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) 164.308 (a) (7) (ii) (A) 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B)；PCI：不适用;

规则名称	服务	触发器	操作	框架
ams-nist-dynamodb-throughput-限额检查	DynamoDB	定期	报告	CIS：不适用；NIS T-CSF：NA；HIPAA：164 .312 (b)；PCI：NA；
ams-nist-ebs-optimized-实例	EBS	Config 更改	报告	CIS：不适用；NIS T-CSF：NA；HIPAA：164.308 (a) (7) (i)；PCI：不适用；
ams-nist-cis-ebs-snapshot-public-restorable-check	EBS	定期	报告	C@@ IS：CIS.12、CI S.14、CIS.9；NIST-CSF：PR.AC-3、P R.AC- 4、PR.AC-5 、PR.DS-5、PR.PT-3、P R.PT-4；HIPAA：164 .308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)； PCI：1.2,1.3,1.2.1,1.3. 1,1.3.1,1.3.1,1.3.2,1.3.2,1 .3.2,1.3.4,1.3.4,1.3.6,2.2. 2；
ams-nist-ec2-instance-detailed-monitoring-enabled	EC2	Config 更改	报告	CIS：NA；NIS T-CSF：DE.AE-1，P R.PT-1；HIPAA：164.312 (b)；PCI：NA；

规则名称	服务	触发器	操作	框架
ams-nist-cis-ec2-instance-no-public-ip	EC2	Config 更改	报告	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC-4、PR.AC-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (i) 164.308 (a) (4) (ii) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) 164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-ec2-managedinstance-association-compliance-status-check	EC2	Config 更改	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC- 3、PR.AC-4、PR.AC-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C) 64.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.4,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-ec2-managedinstance-patch-compliance-status-check	EC2	Config 更改	报告	C@@ IS：CIS.2，CIS.5；NIST-CSF：ID.AM-2，PR.IP-1；HIPAA：164.308 (a) (5) (ii) (B)；PCI：6.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-ec2 个停止的实例	EC2	定期	报告	CIS：CIS.2；NIST-CSF：ID.AM-2，PR.IP-1；HIPAA：NA；PCI：NA；PCI：NA；
ams-nist-cis-ec2-volume-inuse-check	EC2	Config 更改	报告	CIS：CIS.2；NIST-CSF：PR.IP-1；HIPAA：NA；PCI：NA；PCI：NA；
ams-nist-cis-efs-加密支票	EFS	定期	报告	C@@IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-eip-已附上	EC2	Config 更改	报告	C@@IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-elasticache-redis-cluster-automatic-backup-检查	ElastiCache	定期	报告	C@@IS：CIS.10；NIST-CSF：ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) 164.308 (a) (7) (ii) (A) 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B)；PCI：不适用;

规则名称	服务	触发器	操作	框架
ams-nist-cis-opensearch-encrypted-at-rest	OpenSearch	定期	报告	C@@ IS：CIS.14，CIS.13；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-opensearch-in-vpc-only	OpenSearch	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-elb-acm-certificate-required	Certificate Manager	Config 更改	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (i) 164.308 (a) (4) (a) (4) ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-elb-deletion-已启用保护	ELB	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312 (a) (2) (iv) 164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii) ,164.312 (e) (2) (ii)；PCI：4.1,8.2.1；
ams-nist-cis-elb-启用日志功能	ELB	Config 更改	报告	CIS：CIS .6；NIST-CSF：DE.AE-1、DE.AE-3、PR.PT-1；HIPAA：164. 312 (b)；PCI：10.1,10.3.1,10.3.2,10.3.3,10.3.3,10.3.4,10.3.4,10.3.5,10.3.6,10.5.4；
ams-nist-cis-emr-已启用 kerberos	EMR	定期	报告	CIS：CIS .6；NIST-CSF：DE.AE-1、DE.AE-3、PR.PT-1；HIPAA：164. 312 (b)；PCI：10.1,10.3.1,10.3.2,10.3.3,10.3.3,10.3.4,10.3.4,10.3.5,10.3.6,10.5.4；

规则名称	服务	触发器	操作	框架
ams-nist-cis-emr-master-no-public-ip	EMR	定期	报告	C@@ IS：CIS.14、CIS.16；NIST-CSF：PR.AC- 1、PR.AC-4、PR.AC-6；HIPAA：164.308 (a) (3) (i) 164.308 (a) (ii) (A) 164.308 (ii) (A) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) (4) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) ,164.308 (a) (ii) (C) ,164.312 (a) (1)；PCI：7.2.1；
ams-nist-cis-encrypted-卷	EBS	Config 更改	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC- 3、PR.AC-4、PR.AC-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C) 64.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.4,1.3.4,1.3.4,1.3.6,2.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-guardduty-non-archived-findings	GuardDuty	定期	报告	C@@ IS：CIS.12、CIS.13、CIS.16、CIS.19、CIS.3、CIS.4、CIS.6、CIS.8；NIST-CSF：DE.AE-2、DE.AE-3、DE.CM-4、DE.DP-5、ID.RA-1、ID.RA-3、PR.DS-5、PR.PT-1；HIPAA：164.308 (a) (5) (ii) (C) 164.308 (a) (6) (ii) 164.312 (b)；PCI：6.1,11.4,5.1.2；
ams-nist-iam-group-has-users-check	IAM	Config 更改	报告	CIS：NA；NIS T-CSF：PR.AC-4，PR.AC-1；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) (A) ,164.308 (a) (3) (ii) (a) (3) (ii) 164.308 (a) (ii) 164.308 (a) (i) 164.308 (a) (a) (4)) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (a) (1)；PCI：7.1.2,7.1.3,7.2.3,7.2.1,7.2.2；
ams-nist-cis-iam-管理员访问policy-no-statements-with权限	IAM	Config 更改	报告	C@@ IS：CIS.16；NIST-CSF：PR.AC-6，PR.AC-7；HIPAA：164.308 (a) (4) (ii) (B) 164.308 (a) (5) (ii) (D) ,164.312 (d)；PCI：8.2.3,8.2.4,8.2.5；

规则名称	服务	触发器	操作	框架
ams-nist-cis-iam-user-group-membership-check	IAM	Config 更改	报告	C@@ IS：CIS.16、CIS.4；NIST-CSF：PR.AC-1、PR.AC-4、PR.PT-3；HIPAA：164.308 (a) (3) (i) ,164.308 (a) (ii) (A) 164.308 (ii) (A) 164.308 (a) (4) (a) (a) (4) (a) (4) (a) (4) (a) (4) (a) (4) (a) (4) ii) (C) ,164.312 (a) (1) ,164.312 (a) (2) (i)；PCI：2.2,7.1.2,7.2.1,7.2.1,8.1.1；
ams-nist-cis-iam-user-no-policies-check	IAM	Config 更改	报告	C@@ IS：CIS.16；NIST-CSF：PR.AC-1，PR.AC-7；HIPAA：164.308 (a) (4) (ii) (B) ,164.312 (d)；PCI：8.3；

规则名称	服务	触发器	操作	框架
ams-nist-cis-iam-user-unused-credentials-check	IAM	定期	报告	C@@ IS：CIS.16；NIST-CSF：PR.AC-1、PR.AC-4、PR.PT-3；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) (A) 164.308 (a) (3) (ii) 164.308 (a) (3) (ii) 164.308 (a) (3) (i) 164.308 (a) (3) (i) 164.308 (a) (3) (i) ,164.308 (a) (i) ,164.308 (a) (i) ,164.308 (a) (i) 164.308 (a) (i) ,164.308 (a) 4.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (a) (1)；PCI：2.2,7.1.2,7.1.3,7.2.3,7.2.1, 7.2.2；
ams-nist-cis-ec2-instances-in-vpc	EC2	Config 更改	报告	C@@ IS：CIS.11、CIS.12、CIS.9；NIST-CSF：DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (3) (ii) ,164.308 (a) (i) ,164.308 (a) (i) 164.308 (a) (i) 164.308 (a) (4) (ii) (A) 164.308 (a) (4) (ii) (B) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.32.2,1.2.1,1.3.1,1.3.2,2.2.2；

规则名称	服务	触发器	操作	框架
ams-nist-cis-internet-gateway-authorized-vpc-only	互联网网关	定期	报告	CIS：CIS.9、CIS.12；NIST-CSF：NA；HIP AA：NA；PCI：NA；PCI：NA；NA；
ams-nist-cis-kms-cmk-not-scheduled-for-删除	KMS	定期	报告	CIS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：NA；PCI：3.5,3.6；
ams-nist-lambda-concurrency-检查	Lambda	Config 更改	报告	CIS：不适用；NIS T-CSF：NA；HIPAA：164.312 (b)；PCI：NA；
ams-nist-lambda-dlq-检查	Lambda	Config 更改	报告	CIS：不适用；NIS T-CSF：NA；HIPAA：164.312 (b)；PCI：NA；
ams-nist-cis-lambda-function-public-access-prohibited	Lambda	Config 更改	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (i) 164.308 (a) (4) (a) (4) ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.

规则名称	服务	触发器	操作	框架
ams-nist-cis-lambda-inside-vpc	Lambda	Config 更改	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC-3、PR.AC-4、PR.AC-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (4) (ii) (A) ,164.308 (a) (4) (ii) (C) 64.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.2,1.3.2,1.3.4,2.2,1.3.2,1.3.4,2.2.2；
ams-nist-cis-mfa-enabled-for-iam-console-访问	IAM	定期	报告	CIS：CIS.16；NIST-CSF：PR.AC-7；HIPAA：164.312 (d)；PCI：2.2,8.3；
ams-nist-cis-multi-region-cloudtrail-enabled	CloudTrail	定期	报告	C@@ IS：CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-5、PR.MA-2、PR.PT-1；HIPAA：164.308 (a) (3) (ii) (A) ,164.312 (b)；PCI：2.2,10.2.1,10.2.1,10.2.2,10.2.3,10.2.4,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,10.2.6,2.7,10.3.1,10.3.2,10.3.3,10.3.3,10.3.4,10.3.5,10.3.6；

规则名称	服务	触发器	操作	框架
ams-nist-rds-enhanced-启用监控	RDS	Config 更改	报告	CIS：NA；NIS T-CSF：PR.PT-1；HIPAA：164.312 (b)；PCI：NA；
ams-nist-cis-rds-instance-public-access-check	RDS	Config 更改	报告	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-rds-multi-az-support	RDS	Config 更改	报告	CIS：不适用；NIS T-CSF：ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) ,164.308 (a) (7) (7) (ii) (C)；PCI：NA；

规则名称	服务	触发器	操作	框架
ams-nist-cis-rds-snapshots-public-prohibited	RDS	Config 更改	报告	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-rds-存储加密	RDS	Config 更改	报告	C@@ IS：CIS.13、CIS.5、CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-1、PR.PT-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (e) (2) (ii)；PCI：3.4,10.1,10.2.1,10.2.2.1 (ii)；PCI：3.4,10.1,10.2.1,10.2.2.12,10.2.3,10.2.4,10.2.5,10.3.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.5,10.3.6,8.2.1；

规则名称	服务	触发器	操作	框架
ams-nist-cis-redshift-cluster-configuration-check	RedShift	Config 更改	报告	C@@ IS：CIS.6、CIS.13、CIS.5；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-1、PR.PT-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (b) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1,10.1.10.2.2.1 1,10.2.2,10.2.3,10.2.4,10.2.5,10.3.1,10.3.1,10.3.2,10.3.3,10.3.4,10.3.5,10.3.5,10.3.6；
ams-nist-cis-redshift-cluster-public-access-check	RedShift	Config 更改	报告	C@@ IS：CIS.12、CIS.14、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (a) 164.308 (a) 164.308 (a) 164.308 (a) (4) (ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-redshift-require-tls-ssl	RedShift	定期	报告	独联体：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312 (a) (2) (iv) 164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii)；PCI：2.34.1；

规则名称	服务	触发器	操作	框架
ams-nist-cis-root-account-hardware-mfa-enabled	IAM	定期	报告	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-7；HIPAA：164.312 (d)；PCI：2.2,8.3；
ams-nist-cis-root-account-mfa-enabled	IAM	定期	报告	CIS：CIS.16，CIS.4；NIST-CSF：PR.AC-7；HIPAA：164.312 (d)；PCI：2.2,8.3；
ams-nist-cis-s3-bucket-default-lock-enabled	S3	Config 更改	报告	CIS：CIS.14、CIS.13；NIST-CSF：ID.BE-5、PR.PT-5、RC.RP-1；HIPAA：NA；PCI：NA；PCI：NA；
ams-nist-cis-s3-bucket-logging-enabled	S3	Config 更改	报告	C@@ IS：CIS.6；NIST-CSF：DE.AE-1、DE.AE-3、PR.DS-5、PR.PT-1；HIPAA：164.308 (a) (3) (ii) (A) ,164.312 (b)；PCI：2.2,10.1,10.2.1,10.2.2,10.2.3,10.2.3,10.2.4,10.2.7,10.3.1,10.3.2,10.2.5,10.2.7,10.3.1,10.3.2,10.2.5,10.2.7,10.3.1,10.3.2,10.2.2,10.2.7,10.3.1,10.3.2,10.2.2,10.2.10.3.3,10.3.4,10.3.4 ,10.3.6；

规则名称	服务	触发器	操作	框架
ams-nist-cis-s3-bucket-replication-enabled	S3	Config 更改	报告	C@@ IS：CIS.10；NIST-CSF：ID.BE-5、PR.DS-4、PR.IP-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) 164.308 (a) (7) (ii) (A) 164.308 (a) (7) (ii) (A) ,164.308 (a) (7) (ii) (B)；PCI：2.2,10.5.3；
ams-nist-cis-s3-bucket-ssl-requests-only	S3	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-2；HIPAA：164.312 (a) (2) (iv) 164.312 (c) (2) 164.312 (e) (1) ,164.312 (e) (2) (i) ,164.312 (e) (2) (ii)；PCI：2.2,4.312 (e) (2) (ii)；PCI：2.2,4.312 (e) (2) (ii) 1,8.2.1；
ams-nist-cis-s3-bucket-versioning-enabled	S3	定期	报告	C@@ IS：CIS.10；NIST-CSF：ID.BE- 5、PR.DS-4、PR.DS-6、PR.IP-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i) 164.308 (a) (7) (ii) (a) (7) (ii) (A) 164.308 (a) (7) (ii) (a) 164.308 (a) (7) (ii) (A) 164.308 (a) (7) (ii) B) 164.312 (c) (1) ,164.312 (c) (2)；PCI：10.5.3；

规则名称	服务	触发器	操作	框架
ams-nist-cis-sagemaker-已endpoint-configuration-kms-key配置	SageMaker	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-sagemaker-已notebook-instance-kms-key配置	SageMaker	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-nist-cis-sagemaker-notebook-no-direct-internet-访问	SageMaker	定期	报告	C@@ IS：CIS.12、CIS.9；NIST-CSF：PR.AC-3、PR.AC- 4、PR.AC-5、PR.DS-5、PR.PT-3、PR.PT-4；HIPAA：164.308 (a) (3) (i) 164.308 (a) (i) 164.308 (a) (4) (a) (4) ii) (C) 164.312 (a) (1) ,164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.3.1,1.3.1,1.3.2,1.3.2,1.3.2,1.3.2,1.3.4,1.3.4,1.3.6,2.2.2；
ams-nist-cis-secretsmanager-rotation-enabled-check	Secrets Manager	Config 更改	报告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308 (a) (4) (ii) (B)；PCI：NA；

规则名称	服务	触发器	操作	框架
ams-nist-cis-secretsmanager-scheduled-rotation-success-check	Secrets Manager	Config 更改	报告	CIS：CIS.16；NIST-CSF：PR.AC-1；HIPAA：164.308 (a) (4) (ii) (B)；PCI：NA；
ams-nist-cis-sns-加密的kms	SNS	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：8.2.1；
ams-nist-cis-vpc-sg-open-only-to-授权端口	VPC	Config 更改	报告	C@@ IS：CIS.11、CIS.12、CIS.9；NIST-CSF：DE.AE-1、PR.AC-3、PR.AC-5、PR.PT-4；HIPAA：164.312 (e) (1)；PCI：1.2,1.3,1.2.1,1.2.1,1.3.1,1.3.2,2.2.2；
ams-nist-vpc-vpn2 个隧道向上	VPC	Config 更改	报告	CIS：不适用；NIST-CSF：ID.BE-5、PR.DS-4、PR.PT-5、RC.RP-1；HIPAA：164.308 (a) (7) (i)；PCI：NA；
ams-cis-ec2-ebs-encryption-by-default	EC2	定期	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) 164.312 (e) (2) (ii)；PCI：2.2,3.4,8.2.1；

规则名称	服务	触发器	操作	框架
ams-cis-rds-snapshot-已加密	RDS	Config 更改	报告	C@@ IS：CIS.13，CIS.14；NIST-CSF：PR.DS-1；HIPAA：164.312 (a) (2) (iv) ,164.312 (e) (2) (ii)；PCI：3.4,8.2.1；
ams-cis-redshift-cluster-维护设置-检查	RedShift	Config 更改	报告	C@@ IS：CIS.5；NIST-CSF：PR.DS-4、PR.IP-1、PR.IP-4；HIPAA：164.308 (a) (5) (ii) (A) 164.308 (a) (7) (ii) (A)；PCI：6.2；

对 “加速” 中违规行为的回应

所有 Config 规则违规行为都会出现在您的配置报告中。这是一种普遍的回应。根据规则的补救类别（严重程度），AMS 可能会采取其他措施，如下表所示。有关如何为某些规则自定义操作代码的详细信息，请参阅自定义调查结果响应。

补救措施

操作码	AMS 行动
报告	1. 添加到 Config 报告
事件	1. 添加到 Config 报告 2. Accelerate 中的自动事件报告
修复	1. 添加到 Config 报告 2. Accelerate 中的自动事件报告 3. 在 “加速” 中自动修复

请求其他帮助

> **Note**
>
> AMS 可以为您纠正任何违规行为，无论其补救类别如何。要请求帮助，请提交服务请求，并注明您希望 AMS 修复哪些资源，并附上诸如 “作为 AMS 配置规则补救的一部分，请修复非投诉*RESOURCE_ARNS_OR_IDs*资源资源 ARNs/IDs>，账户*CONFIG_RULE_NAME*中的配置规则” 之类的评论，并添加必要的输入以纠正违规行为。

AMS Accelerate 有一个 AWS Systems Manager 自动化文档和运行手册库，可帮助修复不合规的资源。

添加到 Config 报告

AMS 会生成一份 Config 报告，用于跟踪您账户中所有规则和资源的合规状态。您可以向 CSDM 索取报告。您还可以通过 C AWS onfig 控制台、 AWS CLI 或 Confi AWS g API 查看合规性状态。您的 Config 报告包括：

- 您环境中最重要的不合规资源，用于发现潜在威胁和错误配置
- 随着时间的推移，资源和配置规则的合规性
- Config 规则描述、规则严重性以及修复不合规资源的建议补救步骤

当任何资源进入不合规状态时，资源状态（和规则状态）在您的 Config 报告中变为 “不合规”。如果该规则属于仅限 Config Rep ort 的补救类别，则默认情况下，AMS 不会采取任何进一步的措施。您可以随时创建服务请求，向 AMS 请求其他帮助或补救措施。

有关更多详细信息，请参阅 AWS Config 报告。

Accelerate 中的自动事件报告

对于中等严重的违规行为，AMS 会自动创建事件报告，通知您资源已进入不合规状态，并询问您希望执行哪些操作。在应对事件时，您可以选择以下选项：

- 请求 AMS 修复事件中列出的不合规资源。然后，我们会尝试修复不合规的资源，并在潜在事件得到解决后通知您。
- 您可以在控制台中或通过自动部署系统（例如，Pi CI/CD peline 模板更新）手动解决不合规项目；然后，您可以解决事件。将根据规则的时间表重新评估不合规的资源，如果资源被评估为不合规，则会创建新的事件报告。

- 您可以选择不解决不合规的资源，而直接解决事件。如果您稍后更新资源的 AWS 配置，Config 将触发重新评估，并再次提醒您评估该资源的不合规性。

在 “加速” 中自动修复

最重要的规则属于自动修复类别。不遵守这些规则可能会严重影响您的账户的安全性和可用性。当资源违反以下规则之一时：

1. AMS 会自动通过事件报告通知您。
2. AMS 使用我们的自动 SSM 文档开始自动修复。
3. AMS 会根据自动修复的成功或失败来更新事件报告。
4. 如果自动修复失败，AMS 工程师将调查问题。

在 “加速” 中创建规则例外

AWS Config 规则 资源异常功能允许您禁止针对特定规则报告特定、不合规的资源。

> **Note**
>
> 豁免的资源在您的 Confi AWS g Service 控制台中仍显示为 “不合规”。豁免的资源在 Config 报告中带有特殊标志（resource_Exception: True）。生成报告时， CSDMs 您可以根据该列筛选出这些资源。

如果您知道有不合规的资源，则可以在他们的 Config Reports 中删除特定配置规则的特定资源。要实现此目的，应按照以下步骤进行：

针对您的账户向 Accelerate 提交服务请求，并列出应免于报告的配置规则和资源。您必须提供明确的业务理由（例如，无需举报*resource_name_1*，*resource_name_2*也无需备份，因为我们不希望对其进行备份）。有关提交加速服务请求的帮助，请参阅在 Accelerate 中创建服务请求。

将以下输入粘贴到请求中（为每个资源添加一个包含所有必填字段的单独块，如图所示），然后提交：

```
[
    {
        "resource_name": "resource_name_1",
        "config_rule_name": "config_rule_name_1",
```

```
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    },
    {
        "resource_name": "resource_name_2",
        "config_rule_name": "config_rule_name_2",
        "business_justification": "REASON_TO_EXEMPT_RESOURCE",
        "resource_type": "resource_type"
    }
]
```

在 “加速” 中降低 AWS Config 成本

您可以通过使用定期记录AWS::EC2::Instance资源类型的选项来降低 AWS Config 成本。定期记录每 24 小时捕获一次资源的最新配置更改，从而减少交付的更改数量。启用后， AWS Config 仅记录 24 小时后资源的最新配置。这使您可以根据不需要持续监控的特定运营规划、合规性和审计用例定制配置数据。只有当您的应用程序依赖于临时架构（这意味着您要不断扩大或缩小实例的数量）时，才建议您进行此更改。

要选择定期记录AWS::EC2::Instance资源类型，请联系您的 AMS 交付团队。

自定义调查结果响应

您可以选择希望 AMS Accelerate 如何响应某些发现（不合规的 Config 规则）。您可以将 AMS 配置为对调查结果做出回应，方法是修正调查结果，请求您批准补救，或者只是在下次月度业务回顾 (MBR) 中向您报告。您可以更改 AMS Accelerate Config 规则的默认响应。要查看规则，请前往 “配置合规性” > “规则表”，或者将规则表下载为 ZIP 文件 ams_config_rules.zip。

更改默认响应允许对更多发现进行补救，从而帮助您提高账户的安全性和合规性状态。当你修复更多的调查结果时，需要等待人工审核和批准的案例就会减少。大量的 AMS 补救运行手册库会不断修复不合规的资源，只有在需要时才会与您联系。

自定义响应仅适用于新资源或包含新事件的现有资源。例如，变更后变为不合规的资源。这是因为较旧的资源往往需要在修复之前进行更深入的检查，而且在创建或更改资源时更容易强制执行资源修复。要随时请求对任何资源的发现进行补救，请提交服务请求。

请求更改默认回复

Cloud Architects (CAs) 会在入职期间与你合作，收集你的偏好。 CAs然后在内部 AMS 系统上设置初始配置。入职后，创建服务请求以请求更新您的配置。您可以根据需要多次请求配置更新。请注意，操

作仅更新创建服务请求的账户的配置。如果您需要同时更新多个帐户，请联系您的云架构师。出于审计目的，您的 CA 会要求您根据自己的偏好删除服务请求。

更改调查结果和账户的默认回复

您始终需要为每个账户和发现设置一个回复偏好。AMS 提供默认响应（请参阅配置合规性），因此此配置是可选的。您可以将每个查找结果的默认响应更改为以下选项：

- 修复：AMS 手动或自动修复发现。AMS 会审查补救措施并告知您是否失败。
- 申请批准：AMS 创建出站案例以通知您有关调查结果。如果您想在批准补救措施或豁免补救措施之前查看调查结果，请使用此选项。然后，AMS 会执行您喜欢的操作。
- 不采取任何行动（仅限报告）：AMS 不采取任何措施来补救或上报调查结果。调查结果可能仍会显示在控制台上，并在控制台期间显示报告 MBRs。

> **Note**
>
> 您无法更改必须由 AMS 补救的规则的配置。例如，启用 Amazon GuardDuty 和 VPC 流日志。

按资源更改默认响应

您可以使用标签进一步配置对特定资源的响应。您可以使用 Resource Tagger 使用已存在的标签或标记资源。有关详细信息，请参阅加速资源标记器）。带有标签的资源的配置优先于查找结果的默认操作。当资源有多个标签且关联配置不同时，AMS 无法运行自定义补救措施。相反，AMS 会向您发送出站服务请求，以告知您情况。例如，对于bucket-server-side-encryption启用 s3- 的查找结果，您可以：

- 将响应更改为 “修复” 未加密的 S3 存储桶，标签密钥值对为 “监管：True”
- 当未加密的 S3 存储桶的标签为 “监管：False” 时，将响应更改为 “无操作”，并且
- 将未加密的 S3 存储桶的默认响应更改为 “请求批准”。这适用于所有没有 “监管：真” 或 “监管：假” 标签的 S3 存储桶

您还可以添加运行自定义查找响应所需的输入。例如，对于需要加密密钥的补救措施，您可以向 AMS IDs 提供密钥。您可以更改修复运行手册的输入参数，但是 AMS 不支持与自定义 runbook 集成。有关 Config 报告中对 AMS 补救运行手册的描述，请参阅AWS Config 控制合规性报告。

加速中的事件响应

收到警报后，AMS 团队会使用自动和手动补救措施将资源恢复到正常状态。如果补救失败，AMS 将启动事件管理流程，与您的团队合作。您可以通过更新配置文件中的默认配置来更改基准。

AMS Accelerate 中的事件响应和入职培训

在入职期间，AMS Accelerate 禁止自动为现有的不合规资源创建事件；相反，您的云服务交付管理器 (CSDM) 会为您提供一份包含所有不合规规则和资源的报告，供您审查。确定希望 AMS 修复的规则后，在 Cent 支持 er 控制台中创建服务请求，说明这些规则和资源。以下服务请求模板是客户向 AMS 提出的手动修复不合规资源的请求示例。如果 AMS 还有其他问题，我们会在服务请求中与您合作，收集所需的信息。

```
Hello,
Please remediate the following resources for the Config Rule "ENCRYPTED_VOLUMES".
Resource List:
    "Vol-12345678"
    "Vol-87654312"
Thank you
```

入职流程完成后，AMS Accelerate 会自动为标记为 “自动事件” 的规则的每个不合规资源创建事件。

加速中的弹性

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。借助可用区，您可以设计和操作可在区域之间自动进行故障转移而不会中断的应用程序和数据库。与传统的单一或多数据中心基础架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础架构。

有关 AMS 加速连续性管理的信息，请参阅AMS 中的连续性管理加速。

end-of-support操作系统的安全控制

不在操作系统制造商的 “end-of-support” 或 EOS 的常规支持期内，并且未收到安全更新的操作系统的安全风险会增加。

AWS 提供一些服务来帮助处理操作系统 end-of-support。有关 Windows 的信息 end-of-support，请参阅适用于 Windows 服务器的 End-of-Support迁移程序。

> **Note**
>
> 有关此主题的更多信息，请访问 AWS Artifact 报告。有关更多信息，请参阅在 Amazon Artifact 中下载报告。要访问 AWS Artifact，您可以联系您的 CSDM 获取说明或前往 AWS Artifact 入门。此信息未包含在本用户指南中，因为它包含敏感的安全内容。

《加速》中的安全最佳实践

AMS Accelerate 使用一致性包，它提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则 以及 AWS Config 补救措施来创建安全、运营或成本优化治理检查。有关如何最好地配置这些一致性包的信息，请参阅 AWS ConfigNIST CSF 操作最佳实践和 CIS 前 20 名的运营最佳实践。

更改请求安全审查

AWS Managed Services 变更请求审查流程可确保 AMS 在您的账户中代表您实施变更时对请求的更改进行安全审查。

AMS 加速实现技术标准定义最低安全标准、配置和流程，以建立账户的基本安全性。当 AMS 实施所要求的变更时，我们会遵循这些标准。

AMS 根据 AMS 技术标准评估所有变更请求。任何可能因偏离技术标准而降低账户安全状况的变更都要经过安全审查流程。在此过程中，AMS会强调相关风险，并由您的授权风险审批人进行审查和批准，以平衡安全和业务需求。

客户安全风险管理流程

AMS 加速客户安全风险管理 (CSRM) 流程有助于清楚地识别风险并将其传达给合适的所有者。此过程可最大限度地降低您环境中的安全风险，并减少已识别风险的持续运营开销。

默认情况下，当贵组织中的某人请求 AMS 对您的托管环境进行更改时，AMS 会审查更改以确定该请求是否超出了技术标准，这可能会改变您账户的安全状况。如果存在高或非常高的安全风险，则您的授权安全人员会接受或拒绝变更审查。还会评估所要求的变更是否会对AMS的账户运营能力产生不利影响。如果审查发现可能的不利影响，则需要在AMS内部进行额外的审查和批准。

对于高风险或非常高的风险，您可以选择退出 CSRM 流程中基于审批的工作流程。要将特定账户的 CSRM 选项从标准 CSRM 更改为 “仅限通知”，请与您的云服务交付经理合作创建一次性风险承受单。如果您选择继续使用 “仅限通知” 选项，则无论风险类别如何，AMS 都会实施所请求的更改。而且，AMS 会向您的授权风险批准者发送风险通知，而不是在变更实施之前寻求批准。请咨询您的云架

构师或云服务交付经理，了解有关 AMS CSRM 流程、如何在注册新 AMS 账户时更改默认 CSRM 选项或如何更新现有账户的更多信息。

> **Note**
>
> AMS 强烈建议您在所有账户中使用默认的标准 CSRM 选项。

AMS 加速实现技术标准

以下是加速技术标准类别：

ID	类别
AMS-STD-X002	AWS Identity and Access Management
AMS-STD-X003	网络安全性
AMS-STD-X004	渗透测试
AMS-STD-X005	Amazon GuardDuty
AMS-STD-X007	日志系统

AMS 加速中的标准控件

以下是 AMS 中的标准控件：

AMS-STD-X002- AWS Identity and Access Management (IAM)

ID	技术标准
1.0	超时持续时间
1.1	联邦用户的默认超时会话为一小时，最多可以增加到四小时。
1.2	微软 Windows Server 的 RDP 会话超时设置为 15 分钟，可以根据用例进行延长。

ID	技术标准
2.0	AWS 主账号使用情况
2.1	如果出于任何原因使用了根账户，则 GuardDuty 必须将 Amazon 配置为生成相关调查结果。
2.2	不得创建根账户的访问密钥。
3.0	用户创建和修改
3.1	无需任何时间限制策略即可创建 users/roles 具有编程访问权限和只读权限的 IAM。但是，不允许允许读取账户中所有 Amazon Simple Storage Service 存储桶中的对象（例如 S3:GetObject）的权限。
3.1.1	可以使用时间限制策略（最长 180 天）创建用于控制台访问和只读权限的 IAM 人类用户，而时间限制策略将生成风险通知。removal/renewal/extension但是，不允许读取账户中所有 S3 存储桶中的对象（例如 S3:GetObject）的权限。
3.2	在不接受风险的情况下，不得在客户账户中创建具有任何基础架构变更权限（写入和权限管理）的 IAM 用户和用于控制台和编程访问的角色。S3 对象级写入权限存在例外情况，只要特定的存储桶在范围内，并且对非 AMS 相关标签进行标记操作，则无需接受风险。
3.3	在微软 Windows 服务器上，只需要创建微软群组托管服务帐户 (GMSA)。
4.0	政策、行动和 APIs
4.4	在不接受风险的情况下，策略不得向管理员提供等同于 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*” 的语句。

ID	技术标准
4.6	不得允许针对客户 IAM 策略中的 AMS 基础设施密钥的 KMS 密钥策略进行 API 调用。
4.8	不得允许更改 Amazon Route 53 中的 AMS 基础设施 DNS 记录的操作。
4.9	按照正当程序创建的具有控制台访问权限的 IAM 人类用户，除了信任策略、代入角色和限时策略外，不得直接附加任何策略。
4.10	可以在同一账户中创建对特定密钥或命名空间具有读取 AWS Secrets Manager 权限的 Amazon EC2 实例配置文件。
4.12	IAM 策略不得包含任何包含在任何 AMS Amazon 日志组上的 “允许日志:DeleteLogStream ” DeleteLogGroup 和 “日 CloudWatch 志:” 操作的操作。
4.13	不得允许创建多区域密钥。
4.14	通过使用特定于服务的 S3 条件密钥 s3: 指定账号，限制客户账户对存储桶的访问权限，即可访问尚未在客户账户中创建的 S3 存储桶 ARN。ResourceAccount
4.15.1	您可以查看、创建、列出和删除您的 S3 存储镜头自定义仪表板。
4.16	可以授予与 SQL Workbench 相关的完全权限，roles/users 允许其使用 Amazon Redshift 数据库。
4.17	可以将任何 AWS CloudShell 权限授予客户角色作为 CLI 的替代方案。

ID	技术标准
4.18	以 AWS 服务为可信委托人的 IAM 角色还需要符合 IAM 技术标准。
4.19	服务关联角色 (SLRs) 不受 AMS IAM 技术标准的约束，因为它们由 IAM 服务团队构建和维护。
4.20	IAM 策略不应允许读取账户中所有 S3 存储桶中的对象（例如 S3:GetObject）。
4.21	可以向客户授予资源类型 “savingsplan” 的所有 IAM 权限。
4.22	AMS 工程师不得在任何数据存储服务（如亚马逊 S3、Amazon Relational Database Service、Amazon DynamoDB 等）或操作系统文件系统中手动复制或移动客户数据（文件、S3 对象、数据库等）。
6.0	跨账户政策
6.1	根据客户记录，可以配置属于同一客户的 AMS 账户之间的 IAM 角色信任策略。
6.2	只有当非 AMS 账户由同一 AMS 客户拥有时，才必须配置 AMS 账户和非 AMS 账户之间的 IAM 角色信任策略（通过确认他们属于同一个 AWS Organizations 账户或将电子邮件域名与客户的公司名称进行匹配）。
6.3	如果不接受风险，则不得配置 AMS 账户和第三方账户之间的 IAM 角色信任策略。
6.4	可以配置跨账户策略，以便在同一客户的 AMS 账户 CMKs 之间访问任何客户管理的账户。

ID	技术标准
6.5	可以配置跨账户策略，通过 AMS 账户访问非 AMS 账户中的任何 KMS 密钥。
6.6	在不接受风险的情况下，不得允许第三方账户访问AMS账户内的任何 KMS 密钥的跨账户政策。
6.6.1	只有当非 AMS 账户由同一 AMS 客户拥有时，才能配置跨账户策略，允许非 AMS 账户访问 AMS 账户内的任何 KMS 密钥。
6.7	可以配置跨账户策略，用于访问可在同一客户的 AMS 账户之间存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.8	可以配置跨账户策略，从具有只读访问权限的 AMS 账户访问可在非 AMS 账户中存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.9	只有当非 AMS 账户归同一 AMS 客户所有（通过确认他们属于同一个账户或将电子邮件域名与客户匹配时），才必须配置跨账户策略，才能访问任何 S3 存储桶数据或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift），并具有从 AMS 到非 AMS 账户（或非 AMS 到 AMS 账户）的写入权限的公司名称）。 AWS Organizations
6.10	可以配置跨账户策略，允许从具有只读权限的 AMS 账户访问第三方账户中可以存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。

ID	技术标准
6.11	不得配置跨账户策略，用于从具有写入权限的 AMS 账户访问第三方账户中可以存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.12	未经风险接受，不得配置第三方账户用于访问 AMS 客户 S3 存储桶或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）的跨账户策略。
7.0	用户组
7.1	允许具有只读权限和非变异权限的 IAM 群组。
8.0	基于资源的策略
8.4	应通过附加基于资源的策略来保护 AMS 基础设施资源免受未经授权的身份的管理。
8.2	除非客户明确指定不同的策略，否则应使用基于最低权限资源的策略来配置客户资源。

AMS-STD-X003-网络安全

以下是 X003-网络安全的标准控件：

ID	技术标准
	联网
1.0	留待将来控制
2.0	允许在 EC2 实例上使用弹性 IP
3.0	必须使用 AMS 控制平面，进而在数据平面中使用 TLS 1.2+。

ID	技术标准
5.0	如果安全组未按照 9.0 连接到负载均衡器，则其入站规则中不得将源设置为 0.0.0.0/0
6.0	未经风险接受，不得将 S3 存储桶或对象公开。
7.0	服务器管理端口 SSH/22 或 SSH/2222（不是 SFTP/2222）、TELNET/23、RDP/3389、winRM/5985-5986、VNC/ 5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 以及 RPC/135、NETBIOS/137-139 上的访问权限。
8.0	不得允许公共端口（mySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433）或自定义端口进行数据库管理访问，不得允许未通过 DX、vpc-Peer 或通过安全组路由到 VPC 的公共端口。 IPs
8.1	任何可以存储客户数据的资源都不应直接暴露在公共互联网上。
9.0	仅允许负载均衡器通过端口 HTTP/80、HTTPS/8443 和 HTTPS/443 直接访问应用程序，不允许直接访问任何计算资源，例如实例、容器等。 EC2 ECS/EKS/Fargate
10.0	可以允许应用程序通过端口 HTTP/80 和 HTTPS/443 从客户私有 IP 范围进行访问。
11.0	未经风险接受，不得允许对控制 AMS 基础设施访问权限的安全组进行任何更改。
12.0	每次请求将安全组附加到实例时，AMS Security 都会参考这些标准。

ID	技术标准
14.0	只有当非 AMS 账户由同一 AMS 客户（通过确认他们属于同一 AWS 组织账户或通过将电子邮件域与客户的公司名称进行匹配）时，才必须使用内部工具配置私有托管区域与 VPCs 从 AMS 到非 AMS 账户（或非 AMS 到 AMS 账户）的跨账户关联。
15.0	可以允许属于同一客户的账户之间的 VPC 对等连接。
16.0	只要两个账户均归同一个客户所有（通过确认他们属于同一个账户，或者将电子邮件域名与客户的公司名称进行匹配），AMIs 即可使用内部工具与非 AMS AWS Organizations 账户共享 AMS 库。
17.0	未经风险认可，不得在任何安全组中配置 FTP 端口 21。
18.0	只要所有账户均归客户所有，则允许通过公交网关进行跨账户网络连接。
19.0	不允许将私有子网设为公有子网
20.0	不得允许与第三方账户（不归客户所有）的 VPC 对等连接。
21.0	不得允许使用第三方账户（不归客户所有）连接 Transit Gateway。
22.0	AMS 向客户提供服务所需的任何网络流量都不得在客户网络出口点被屏蔽。
23.0	EC2 从买家基础设施向 Amazon 发出的入库 ICMP 请求需要风险通知。

ID	技术标准
24.0	允许通过安全组通过 DX、vpc-Peer 或 VPN 从公共 IPs 路由到 Amazon VPC 的入站请求。
25.0	来自公众的入站请求 IPs 如果未通过 DX、vpc-Peer 或 VPN 通过安全组路由到 Amazon VPC，则需要接受风险。
26.0	允许从 Amazon EC2 向任何目的地发出出站 ICMP 请求。
27.0	安全组共享
27.1	如果安全组符合此安全标准，则可以在同一个账户和同一组织 VPCs 中的账户之间共享该安全组。
27.2	如果安全组不符合此标准，并且此安全组以前需要接受风险，则 VPCs 在不接受新的 VPC 或账户风险的情况下，不允许在同一账户之间或同一组织中的账户之间使用安全组共享功能。

AMS-STD-X004-渗透测试

以下是 X004-渗透测试的标准控件

1. AMS 不支持 pentest 基础架构。这是客户的责任。例如，Kali 不是 AMS 支持的 Linux 发行版。
2. 客户需要遵守渗透测试。
3. 如果客户想在账户内进行基础设施渗透测试，则应提前 24 小时预先通知 AMS。
4. AMS 将根据客户在变更请求或服务请求中明确说明的客户要求配置客户渗透测试基础设施。
5. 客户渗透测试基础设施的身份管理由客户负责。

AMS-STD-X005- GuardDuty

以下是 X005 的标准控件- GuardDuty

1. GuardDuty 必须始终在所有客户账户中启用。

2. GuardDuty 警报必须存储在同一账户或同一组织下的任何其他托管账户中。
3. GuardDuty 不得使用的 “可信 IP 列表” 功能。取而代之的是，自动存档可以用作替代方案，这对于审计目的很有用。

AMS-STD-X007-日志记录

以下是 X007-日志记录的标准控件

ID	技术标准
1.0	日志类型
1.1	操作系统日志：所有主机都必须记录最少的主机身份验证事件、所有使用提升权限的访问事件以及访问和权限配置的所有更改的访问事件，包括成功和失败。
1.2	AWS CloudTrail：必须启用并配置 CloudTrail 管理事件日志记录以将日志传送到 S3 存储桶。
1.3	VPC 流日志：必须通过 VPC 流日志记录所有网络流量日志。
1.4	Amazon S3 服务器访问日志：AMS 强制存储日志的 S3 存储桶必须启用服务器访问日志记录。
1.5	AWS Config 快照： AWS Config 必须记录所有区域中所有受支持资源的配置更改，并且每天至少将配置快照文件传送到 S3 存储桶一次。
1.7	应用程序日志：客户有权在其应用程序中启用日志记录并存储在 CloudWatch 日志日志组或 S3 存储桶中。
1.8	S3 对象级日志记录：客户有权在其 S3 存储桶中启用对象级日志记录。
1.9	服务日志：客户可以像任何核心服务一样启用和转发 SSP 服务的日志。

ID	技术标准
1.10	Elastic Loa Classic/Application Load Balancer/ Network d Balancing（Load Balancer）日志：访问和错误日志条目必须存储在 AMS 2.0 托管的 S3 存储桶中。
2.0	访问控制
2.3	作为存储桶策略中的原则，AMS 规定的存储日志的 S3 存储桶不得允许第三方账户用户使用。
2.4	未经客户授权的安全联系人明确批准，不得删除 CloudWatch 日志日志组中的日志。
3.0	日志保留
3.1	AMS 规定的 CloudWatch 日志日志组的日志保留期必须至少为 90 天。
3.2	AMS 规定的用于存储日志的 S3 存储桶的日志保留期必须至少为 18 个月。
3.3	AWS Backup 在支持的资源上，快照应至少保留 31 天。
4.0	加密
4.1	必须在 AMS Teams 要求的存储日志的所有 S3 存储桶中启用加密。
4.2	从客户账户向任何其他账户转发的任何日志都必须经过加密。
5.0	完整性
5.1	必须启用日志文件完整性机制。这意味着在 AMS 团队要求的 AWS CloudTrail 跟踪中配置“日志文件验证”。

ID	技术标准
6.0	日志转发
6.1	任何日志都可以从一个 AMS 账户转发到同一客户的另一个 AMS 账户。
6.2	只有当非 AMS 账户归同一 AMS 客户所有（通过确认他们属于同一个账户，或者将电子邮件域名与客户的公司名称和付款人关联 AWS Organizations 账户进行匹配）时，才能使用内部工具将任何日志从 AMS 转发到非 AMS 账户。

给您的环境带来高或非常高的安全风险的更改

以下更改会给您的环境带来高或非常高的安全风险：

AWS Identity and Access Management

- High_risk-iam-001：为根账户创建访问密钥
- High_risk-iam-002：修改 SCP 策略以允许其他访问权限
- High_risk-iam-003：SCP 政策修改可能会破坏 AMS 基础设施
- High_risk-iam-004：在客户账户中创建 role/user 基础架构变更权限（写入、权限管理或标记）
- High_risk-iam-005：AMS 账户和第三方账户（不归客户所有）之间的 IAM 角色信任策略
- High_risk-iam-006：跨账户政策，允许第三方账户从 AMS 账户访问任何 KMS 密钥）
- High_risk-iam-007：来自第三方账户的跨账户政策，用于访问 AMS 客户 S3 存储桶或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）
- High_risk-iam-008：为客户账户中的任何基础设施变更权限分配 IAM 权限
- High_risk-iam-009：允许列出和读取账户中的所有 S3 存储桶

网络安全

- High_risk-net-001：从互联网上打开操作系统管理端口 SSH/22 或 SSH/2222（不是 SFTP/2222）、TELNET/23、RDP/3389、winrm/5985-5986、VNC/ 5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 NETBIOS/137-139

- High_risk-net-002：打开数据库管理端口 mysql/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433 或互联网上的任何管理客户端口
- High_risk-net-003：直接在任何计算资源上打开应用程序端口 HTTP/80、HTTPS/8443 和 HTTPS/443。例如，来自互联网的 EC2 实例、ECS/EKS/Fargate容器等
- High_risk-net-004：对控制 AMS 基础设施访问权限的安全组进行的任何更改
- High_risk-net-006：与第三方账户（不归客户所有）的 VPC 对等
- High_risk-net-007：添加客户防火墙作为所有 AMS 流量的出口点
- High_risk-net-008：不允许与第三方账户连接 Transit Gateway
- High_Risk-S3-001：在 S3 存储桶中配置或启用公共访问权限

日志系统

- High_risk-log-001：禁用。 CloudTrail
- High_risk-log-002：禁用 VPC 流日志。
- High_risk-log-003：通过任何方法（S3 事件通知、SIEM 代理提取、SIEM 代理推送等）将日志从 AMS 托管账户转发到第三方账户（不归客户所有）
- high_risk-log-004：使用非 AMS 跟踪进行 CloudTrail

其他

- High_risk-enc-001：如果启用了任何资源的加密，则将其禁用

安全常见问题解答

AMS 通过全球运营中心提供全天候 follow-the-sun支持。专职的 AMS 运营工程师主动监控仪表板和事件队列。通常，AMS 会通过自动化来管理您的账户。在极少数情况下，需要特定的故障排除或部署专业知识，AMS 运营工程师可能会访问您的 AWS 账户。

以下是有关 AMS 运营工程师或自动化人员访问您的账户时 AMS Accelerate 使用的安全最佳实践、控制、访问模型和审计机制的常见问题。

AMS 运营工程师何时可以访问我的环境？

AMS 运营工程师无法永久访问您的账户或实例。AMS 运营商只能在合理的业务用例中访问客户账户，例如警报、事件、变更请求等。访问记录在 AWS CloudTrail 日志中。

有关访问理由、触发器和触发器启动器的信息，请参阅AMS 客户账户访问触发器。

AMS 运营工程师在访问我的账户时扮演什么角色？

在极少数情况下（约 5%）需要人为干预您的环境，AMS 运营工程师会使用默认的只读访问权限登录您的账户。默认角色无权访问通常存储在数据存储中的任何内容，例如亚马逊简单存储服务、亚马逊关系数据库服务、亚马逊 DynamoDB、Amazon Redshift 和亚马逊。 ElastiCache

有关 AMS 运营工程师和系统在您的账户中提供服务所需的角色列表，请参阅AMS 客户账户访问权限 IAM 角色。

AMS 运营工程师如何访问我的账户？

要访问客户账户，AMS 运营工程师使用 AWS 内部 AMS 访问服务。此内部服务仅通过安全的私人渠道提供，因此对您的账户的访问是安全的，并且经过审计。

1. AMS 运营工程师使用内部 AMS 接入服务身份验证和双因素身份验证。而且，运营工程师必须提供业务理由（事件单或服务请求编号），概述访问您的 AWS 账户的需求。
2. 根据运营工程师的授权，AMS 访问服务为工程师提供相应的角色（读取-only/Operator/Admin）和您的 AWS 控制台的登录 URL。对您的帐户的访问权限是短暂的，并且是有时限的。
3. 要访问 Amazon EC2 实例，AMS 运营工程师使用与代理相同的内部 AMS 访问服务。授予访问权限后，AMS 运营工程师使用 AWS Systems Manager Session Manager 短期会话凭证访问您的实例。

   为了为 Windows 实例提供 RDP 访问权限，操作工程师使用 Amazon S EC2 ystems Manager 在实例上创建本地用户并建立到该实例的端口转发。运营工程师使用本地用户凭证对实例进行 RDP 访问。本地用户凭证将在会话结束时删除。

下图概述了 AMS 运营工程师访问您的账户所使用的流程：

如何追踪 AMS 在我的 AMS 托管 AWS 账户中所做的更改？

账户访问权限

为了帮助您跟踪自动化或 AMS Accelerate 运营团队所做的更改，AMS 在 Amazon Athena 控制台中提供了更改记录 SQL 界面和 AMS Accelerate 日志。这些资源提供以下信息：

- 谁访问了你的账户。

- 账户何时被访问。
- 使用了哪些权限来访问您的账户。
- AMS Accelerate 对您的账户进行了哪些更改。
- 为什么要对您的账户进行更改。

资源配置

查看 CloudTrail 日志以跟踪过去 90 天内 AWS 资源中的配置。如果您的配置已超过 90 天，请访问 Amazon S3 中的日志。

实例日志

Amazon CloudWatch 代理收集操作系统日志。查看日 CloudWatch 志，查看您的操作系统支持的登录和其他操作日志。

有关更多信息，请参阅 跟踪您的 AMS Accelerate 账户中的更改。

AMS 运营工程师访问我的账户的流程控制有哪些？

在加入AMS之前，运营工程师要接受犯罪背景调查。由于 AMS 工程师负责管理客户基础架构，因此他们还必须进行年度背景调查。如果工程师未通过背景调查，则访问权限将被撤销。

所有 AMS 运营工程师都必须完成必修的安全培训，例如基础设施安全、数据安全和事件响应，然后才能获得资源访问权限。

如何管理特权访问权限？

一部分用户必须完成额外的培训并保持特权访问权限才能获得更高的访问权限。对访问和使用情况进行检查和审计。AMS 将特权访问限制在特殊情况下或最低权限访问无法满足您的请求时。特权访问也是有时间限制的。

AMS 运营工程师是否使用 MFA？

是。所有用户都必须使用 MFA 和存在证明才能向您提供服务。

当 AMS 员工离开组织或更改工作角色时，他们的访问权限会怎样？

通过内部群组成员资格配置对客户账户和资源的访问权限。成员资格基于严格的标准，包括具体的工作职位、报告经理和AMS的就业状况。如果运营工程师的工作类别发生变化或其用户 ID 被禁用，则访问权限将被撤销。

哪些访问控制控制 AMS 运营工程师对我的账户的访问权限？

有多层技术控制措施可以强制执行 “需要知道” 和 “最低权限” 的原则来访问您的环境。以下是访问控制的列表：

- 所有运营工程师都必须是特定内部 AWS 小组的成员，才能访问客户账户和资源。群组成员资格严格基于需要知道的基础，并根据预定义的标准进行自动化。
- AMS 对您的环境实行 “非持久性” 访问权限。这意味着 AMS 操作对您的 AWS 账户的访问权限是使用短期凭据的 just-in-time “”。只有在提交并审核了内部业务案例理由（服务请求、事件、变更管理请求等）之后，才能访问您的账户。
- AMS 遵循最低权限原则。因此，默认情况下，授权运营工程师假设只读访问权限。只有当由于事件或变更请求而需要对环境进行更改时，工程师才会使用写入权限。
- AMS 使用标准的、易于识别的 AWS Identity and Access Management 角色来监控和管理您的账户，这些角色使用 “ams” 前缀。所有访问权限均已登录 AWS CloudTrail 供您审计。
- 在变更执行的客户信息验证阶段，AMS 使用自动后端工具来检测对您账户的未经授权的更改。

AMS 如何监控根用户访问权限？

root 访问权限始终会触发事件响应流程。AMS 使用 Amazon GuardDuty 检测来监控根用户活动。如果 GuardDuty 生成警报，则 AMS 会创建一个事件以供进一步调查。如果检测到意外的 root 账户活动，AMS 会通知您，AMS 安全团队会启动调查。

AMS 如何应对安全事件？

AMS 会调查由诸如亚马逊 GuardDuty、Amazon Macie 之类的检测服务以及客户报告的安全问题所产生的安全事件。AMS 与您的安全响应团队合作运行安全事件响应 (SIR) 流程。AMS SIR 流程基于 NIST SP 800-61 Rev. 2《计算机安全事件处理指南》框架，提供全天候安全响应。 follow-the-sunAMS 与您合作，快速分析和遏制安全事件。

AMS 遵守哪些行业标准认证和框架？

与其他 AWS 服务一样，AWS Managed Services 也获得了
OSPAR、HIPAA、HITRUST、GDPR、SOC*、ISO*、FedRAMP（中/高）、IRAP 和 PCI 认证。有关 AWS 符合的客户合规认证、法规和框架的更多信息，请参阅 AWS 合规性。

安全护栏

AWS Managed Services 使用多种控制措施来保护您的信息资产并帮助您保护 AWS 基础设施的安全。AMS Accelerate 维护着一个 AWS Config 规则和补救措施库，以帮助您确保您的账户符合安全性和运营完整性的行业标准。 AWS Config 规则会持续跟踪您记录的资源的配置更改。如果变更违反了规则的条件，AMS 会向您报告其调查结果。根据违规的严重程度，您可以自动或根据请求进行补救。

AMS 使用 AWS Config 规则来帮助满足以下标准的要求：

- 互联网安全中心 (CIS)
- 美国国家标准与技术研究院 (NIST) 云安全框架 (CSF)
- 健康保险流通与责任法案 (HIPAA)
- 支付卡行业 (PCI) 数据安全标准 (DSS)

有关更多信息，请参阅 AMS 中的安全管理加速。

如何才能访问有关安全认证、框架和合规性的最新报告 AWS？

您可以使用以下方法查找 AWS 服务的当前安全与合规性报告：

- 您可以使用下载AWS Artifact有关 AWS 服务安全性、可用性和机密性的最新报告。
- 有关大多数符合全球合规框架的 AWS 服务（包括 AWS Managed Services）的列表，请参阅https://aws.amazon.com/compliance/services-in-scope/。例如，选择 PCI 并搜索 AWS Managed Services。

  您可以搜索 “AMS”，从 AMS 托管 AWS 账户中查找 AMS 特定的安全构件。AWS Managed Services 在 S OC 3 的范围内。
- S AWS OC 2（系统和组织控制）报告已发布到 AWS Artifact 存储库。本报告评估了符合美国注册会计师协会 (AICPA) TSP 第 100 节 “信托服务标准” 中安全性、可用性和机密性标准的 AWS 控制措施。

AMS 是否共享 AMS 功能不同方面的参考架构图？

要查看 AMS 参考架构，请下载用于主动监控的 AWS Managed Services PDF。

AMS 如何跟踪谁访问了我的账户以及访问我的账户的业务需求？

为了支持服务连续性和账户安全，AMS 仅在主动运行状况或维护、运行状况或安全事件、计划活动或客户请求时才访问您的账户或实例。您的账户访问权限是通过 AMS Accelerate 访问模式中所述

的 AMS 流程进行授权。这些授权流程包含防护栏，可防止无意中或不当访问。作为访问流程的一部分，AMS 根据业务需求为授权系统提供服务。此业务需求可能是与您的账户关联的工作项目，例如您向 AMS 提交的案例。或者，业务需求可能是授权的工作流程，例如修补解决方案。所有访问都需要提供理由，由内部 AMS 系统根据业务规则实时验证、验证和授权，以使访问请求与业务需求保持一致。

如果没有有效的业务需求，AMS 运营工程师将无法访问您的账户。所有账户访问权限和相关的业务需求都将发送到您 AWS 账户内的 AWS CloudTrail 条目中。这提供了完全的透明度，并使您有机会进行自己的审计和检查。除了您的检查外，AMS 还提供自动检查，并根据需要对访问请求进行手动检查，并对工具和人员访问进行审计，以审查异常访问权限。

AMS 工程师能否访问存储在 AWS 数据存储服务（例如亚马逊 S3、亚马逊 RDS、DynamoDB 和 Amazon Redshift）中的数据？

AMS 工程师无法访问存储在通常用于数据存储的 AWS 服务中的客户内容。 AWS APIs 用于读取、写入、修改或删除这些服务中数据的访问权限受到与用于 AMS 工程师访问的 IAM 角色关联的明确的 IAM 拒绝策略的限制。此外，内部 AMS 护栏和自动化功能可阻止 AMS 运营工程师删除或修改拒绝条件。

AMS 工程师能否访问存储在亚马逊 EBS、Amazon EFS 和亚马逊 FSx中的客户数据？

AMS 工程师可以以管理员身份登录 Amazon EC2 实例。在某些情况下（包括但不限于操作系统 (OS) 问题和补丁故障），需要管理员访问权限才能进行修复。AMS 工程师通常会访问系统卷来修复检测到的问题。但是，AMS 工程师的访问权限不受系统音量的限制或限制。

如何限制或控制对我的环境具有高权限的自动化角色的访问权限？

该`ams-access-admin`角色仅由 AMS 自动化使用。这些自动化可以部署、管理和维护 AMS 部署到您的环境中所需的资源，用于收集遥测、运行状况和安全数据，以执行操作功能。AMS 工程师无法担任自动化角色，并且受到内部系统中角色映射的限制。在运行时，AMS 会动态地将范围缩小的最低权限会话策略应用于每个自动化。此会话策略限制了自动化的功能和权限。

AMS 如何实现 Well-Architected Framework 中为 AWS 自动化角色所倡导的最低权限原则？

在运行时，AMS 会对每个自动化应用范围缩小、权限最低的会话策略。这种缩小范围的会话策略限制了自动化的功能和权限。有权创建 IAM 资源的会话策略还需要附加权限边界。此权限边界降低了权限升级的风险。每个团队都制定了仅供该团队使用的会话策略。

使用哪些日志和监控系统来检测未经授权的访问尝试或涉及自动化角色的可疑活动？

AWS 维护集中式存储库，提供核心日志存档功能供 AWS 服务团队内部使用。这些日志存储在 Amazon S3 中，具有很高的可扩展性、耐久性和可用性。 AWS 然后，服务团队可以在中央日志服务中收集、存档和查看服务日志。

上的生产主机 AWS 是使用主基准映像部署的。基准映像配备了一组标准的配置和功能，包括出于安全目的的记录和监控。这些日志存储起来， AWS 安全团队可以访问这些日志，以便在发生疑似安全事件时进行根本原因分析。

给定主机的日志可供拥有该主机的团队使用。团队可以在日志中搜索操作和安全分析。

如何处理与自动化基础设施有关的安全事件或漏洞，哪些协议有助于快速响应和缓解？

AWS 应急计划和事件响应手册定义并测试了用于检测、缓解、调查和评估安全事件的工具和流程。这些计划和行动手册包括根据合同和监管要求应对潜在数据泄露的指导方针。

是否定期对自动化基础设施进行安全评估、漏洞扫描和渗透测试？

AWS 安全部门使用各种工具定期对 AWS 环境中的主机操作系统、Web 应用程序和数据库进行漏洞扫描。 AWS 安全团队还会订阅适用的供应商缺陷的新闻提要，并主动监控供应商的网站和其他相关渠道是否有新的补丁。

如何仅限授权人员才能访问自动化基础架构？

AWS 系统访问权限根据最低权限进行分配，并由授权人员批准。职责和责任领域（例如，访问请求和批准、变更管理请求和批准、变更开发、测试和部署等）在不同人员之间分开，以减少对系统的未经授权或无意的 AWS 修改或滥用。不允许在系统边界内使用群组或共享帐户。

采取了哪些措施来维护安全标准并防止自动化管道中未经授权的访问或数据泄露？

对资源（包括服务、主机、网络设备以及 Windows 和 UNIX 组）的访问由相应的所有者或管理员在 AWS 专有权限管理系统中批准。权限管理工具日志捕获访问权限更改请求。Job 职能的更改会自动撤消员工对资源的访问权限。必须申请并批准该员工的继续访问权限。

AWS 需要通过经批准的加密通道进行双因素身份验证，才能从远程位置对内部 AWS 网络进行身份验证。防火墙设备限制对计算环境的访问，强制计算集群的边界，并限制对生产网络的访问。

实施的流程是为了保护审计信息和审计工具免遭未经授权的访问、修改和删除。审计记录包含一组数据元素，以支持必要的分析要求。此外，审计记录可供授权用户根据需要进行检查或分析，以应对与安全相关或影响业务的事件。

用户对 AWS 系统（例如网络、应用程序、工具等）的访问权限将在终止或停用后的 24 小时内被撤销。至少每 90 天禁 and/or 用一次不活跃的用户帐户。

是否开启了异常检测或监控以进行访问或审计日志以检测权限升级或访问滥用以主动提醒 AMS 团队？

出于安全考虑 AWS ，的生产主机配备了日志功能。该服务记录主机上的人为操作，包括登录、登录尝试失败和注销。这些日志存储起来， AWS 安全团队可以访问这些日志，以便在发生疑似安全事件时进行根本原因分析。给定主机的日志也可供拥有该主机的团队使用。前端日志分析工具可供服务团队搜索其日志以进行操作和安全分析。实施流程是为了帮助保护日志和审计工具免遭未经授权的访问、修改和删除。 AWS 安全团队执行日志分析，根据定义的风险管理参数识别事件。

从 AMS 托管账户中提取了哪些类型的客户数据，以及如何使用和存储这些数据？

AMS 不会出于任何目的访问或使用您的内容。AMS 将客户内容定义为客户或任何最终用户传输 AWS 用于处理、存储或托管的软件（包括机器图像）、数据、文本、音频、视频或图像，以及客户或其最终用户通过使用上述内容得出的任何计算结果。 AWS 服务 AWS 服务

AMS Accelerate 中的监控和事件管理

AMS Accelerate 监控系统会监控您的 AWS 资源是否存在故障、性能下降和安全问题。

作为托管账户，AMS Accelerate 可为适用 AWS 资源配置和部署警报，监控这些资源，并在需要时执行补救。

AMS Accelerate 监控系统依赖内部工具，例如资源标记器和警报管理器，以及亚马逊 () AWS 服务、AWS AppConfig亚马逊 CloudWatch EventBridge （以前称为 CloudWatch CloudWatch）、亚马逊、亚马逊 GuardDuty、Amazon Macie 和。 AWS Health

AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。要快速了解 AMS 如何利用我们的一些关键运营功能（包括全天候服务台、主动监控、安全、补丁、日志记录和备份）来帮助您的团队实现整体卓越运营，请参阅 AMS 参考架构图。 AWS 云

主题

有关监控 Amazon EKS 的信息，请参阅 AMS Accelerate 中对 Amazon EKS 进行监控和事件管理

什么是监控？

AMS 加速监控具有以下好处：

- 一种默认配置，用于在您的托管账户中为您选择的所有资源或支持的 AWS 资源创建、管理和部署策略。
- 监控基准，即使您没有为托管账户配置任何其他监控，也可以使用默认的保护级别。有关更多信息，请参阅 来自 AMS 基线监测的警报。

- 能够自定义基准资源警报以满足您的要求。
- 如有可能，AMS Operations 会自动修复警报，以防止或减少对应用程序的影响。例如，如果您使用的是独立的 Amazon EC2 实例，但该实例未通过系统运行状况检查，AMS 会尝试通过停止并重启该实例来恢复该实例。有关更多信息，请参阅 AMS 自动修复警报。
- 使用查看活动警报和之前已解决的警报 OpsCenter。例如，如果您在某个 Amazon EC2 实例上的 CPU 使用率异常高，则可以请求访问 AWS Systems Manager 控制台（包括访问 OpsCenter 控制台），然后 OpsItem直接在 OpsCenter 控制台中查看。
- 调查警报以确定适当的操作。有关更多信息，请参阅 AMS Accerate 中的事件管理。
- 根据您的账户和支持的 AWS 服务中的配置生成的警报。账户的监控配置是指账户中创建警报的所有资源参数。账户的监控配置包括 CloudWatch 警报定义和生成警报 EventBridge （警报或 CloudWatch 事件）（以前称为事件）。有关资源参数的更多信息，请参阅来自 AMS 基线监测的警报。
- 关于账户中配置的基准监控所产生的即将发生的、持续的、消退的或潜在的故障、性能下降或安全问题的通知（称为警报）。警报的示例包括 CloudWatch 警报、事件或来自 AWS 服务的调查结果，例如 GuardDuty 或 AWS Health。

监控的工作原理

参见以下有关 AWS Managed Services (AMS) 监控架构的图片。

下图描述了 AMS 加速监控架构。

根据使用资源标记器定义的策略对您的资源进行标记并部署警报定义后，以下列表描述了 AMS 监控流程。

- 生成：在账户注册时，AMS 会为您在托管账户中创建的所有资源配置基准监控 CloudWatch （（CW）警报和 CW 事件规则的组合）。当触发 CW 警报或生成 CW 事件时，基准监控配置会生成警报。
- 聚合：您的资源生成的所有警报都将通过将它们定向到账户中的 SNS 主题来发送到 AMS 监控系统。您还可以配置 AMS 如何将 Amazon EC2 提醒组合在一起。AMS 要么将与同一 EC2 实例相关的所有警报分组为单个事件，要么根据您的偏好为每个警报创建一个事件。您可以随时与云服务交付经理或云架构师合作更改此配置。
- 处理：AMS 分析警报并根据其潜在影响进行处理。警报按下文所述进行处理。
  - 具有已知客户影响的警报：这些警报会导致创建新的事件报告，AMS 遵循事件管理流程。

警报示例：Amazon EC2 实例未通过系统运行状况检查，AMS 尝试通过停止并重启实例来恢复该实例。

- 对客户影响不确定的警报：对于这些类型的警报，AMS 会发送事件报告，在许多情况下，要求您在 AMS 采取行动之前验证影响。但是，如果与基础设施相关的检查通过，则 AMS 不会向您发送事件报告。

  例如：Amazon EC2 实例上 CPU 使用率超过 85% 且持续时间超过 10 分钟的警报不能立即归类为事件，因为根据使用情况，可能会出现这种行为。在此示例中，AMS Automation 对资源执行与基础设施相关的检查。如果这些检查通过，即使 CPU 使用率超过 99%，AMS 也不会发送警报通知。如果 Automation 检测到资源上与基础设施相关的检查失败，则 AMS 会发送警报通知并检查是否需要缓解措施。本节将详细讨论警报通知。AMS 在通知中提供了缓解选项。当您回复确认警报为事件的通知时，AMS 会创建新的事件报告，AMS 事件管理流程随即开始。如果服务通知收到“对客户没有影响” 的响应，或者在三天内完全没有回复，则会标记为已解决，相应的警报被标记为已解决。

- 不影响客户的警报：如果 AMS 在评估后确定该警报对客户没有影响，则该警报将关闭。

  例如， AWS Health 通知需要替换的 EC2 实例，但该实例此后已终止。

EC2 实例分组通知

您可以将 AMS 监控配置为将来自同一 EC2 实例的警报组合成单个事件。您的云服务交付经理或云架构师可以为您进行配置。您可以为每个 AMS 管理的账户配置四个参数。

1. 范围：选择账户范围或基于标签的范围。
   - 要指定适用于该账户中每个 EC2 实例的配置，请选择范围 = 账户范围。
   - 要指定仅适用于该账户中带有特定标签的 EC2 实例的配置，请选择 scope = based tag。
2. 分组规则：选择经典或实例。
   - 要为账户中的每个资源配置实例级分组，请选择范围 = 账户范围和分组规则 = 实例。
   - 要将账户中的特定资源配置为使用实例级别分组，请标记这些实例，然后选择范围 = 基于标签和分组规则 = 实例级别。
   - 要不对账户中的警报使用实例分组，请选择分组规则 = c lassic。
3. 参与选项：选择 “无”、“仅限报告” 或 “默认”。
   - 要使 AMS 在配置处于活动状态时不创建事件或自动处理来自这些资源的警报，请选择 “无”。

- 要让 AMS 在配置处于活动状态时不创建事件或自动处理来自这些资源的警报，也不要运行自动修复 Systems Manager 文档，但要在报告中包含这些事件的记录，请选择仅报告。如果您想减少与之互动的事件支持案例数量，并且某些资源中的某些事件（例如非生产账户中的事件）不需要立即关注，这可能会很有用。
- 要让 AMS 处理您的警报、运行自动化程序并在需要时创建事件案例，请选择默认。

4. 之后解决：选择 24 小时、48 小时或 72 小时。最后，配置何时自动关闭事件案例。如果从上次案例对应的时间达到配置的 “解决后解决” 值，则事件将关闭。

警报通知

作为警报处理的一部分，AWS Managed Services (AMS) 会根据影响分析创建事件，并在确定影响后启动事件管理流程进行补救。如果无法确定影响，AMS 会通过服务通知向与您的账户关联的电子邮件地址发送提醒通知。在某些情况下，不会发送此警报通知。例如，如果与基础设施相关的检查通过 CPU 使用率高警报，则不会向您发送警报通知。有关更多信息，请参阅中有关警报处理过程的 AMS 监控架构图监控的工作原理。

基于标签的警报通知

使用标签将资源的警报通知发送到不同的电子邮件地址。最佳做法是使用基于标签的提醒通知，因为当多个开发者团队使用同一个账号时，发送到单个电子邮件地址的通知可能会造成混乱。基于标签的警报通知不受您选择的EC2 实例分组通知设置的影响。

使用基于标签的警报通知，您可以：

- 向特定的电子邮件地址发送警报：使用标记具有必须发送到特定电子邮件地址的警报的`key = OwnerTeamEmail`资源`value = EMAIL_ADDRESS`。
- 向多个电子邮件地址发送警报：要使用多个电子邮件地址，请指定以逗号分隔的值列表。例如 `key = OwnerTeamEmail`、`value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`。值字段的字符总数不能超过 260。
- 使用自定义标签密钥：要使用自定义标签密钥，请在电子邮件中向您的 CSDM 提供自定义标签密钥名称，明确表示同意为基于标签的通信激活自动通知。最佳做法是对所有实例和资源的联系人标签使用相同的标记策略。

> **Note**
>
> 键值`OwnerTeamEmail`不必是驼峰大小写。但是，标签区分大小写，最佳做法是使用推荐的格式。

必须完整指定电子邮件地址，并用 “at 符号” (@) 将本地部分与域名分开。无效电子邮件地址示例：*Team.AppATabc.xyz*或*john.doe*。有关标记策略的一般指导，请参阅标记资源。AWS不要在标签中添加个人身份信息 (PII)。尽可能使用通讯组列表或别名。
以下亚马逊服务的资源支持基于标签的警报通知： EC2、弹性块存储 (EBS)、弹性负载平衡 (ELB)、应用程序负载均衡器 (ALB)、网络负载均衡器、关系数据库服务 (RDS) OpenSearch、弹性文件系统 (EFS) 和 VPN。 FSx Site-to-Site

来自 AMS 基线监测的警报

了解有关 AMS 加速监控默认设置的信息。有关更多信息，请参阅 AMS Accelerate 中的监控和事件管理。

下表显示了监控的内容和默认警报阈值。您可以使用自定义配置文档更改警报阈值，也可以提交服务请求。有关更改自定义警报配置的说明，请参阅更改加速警报配置。要在警报超过阈值时接收通知，除了 AMS 的标准警报流程外，您还可以覆盖警报配置。有关说明，请参阅加速警报管理器。

Amazon CloudWatch 提供了更长的指标保留期。有关更多信息，请参阅CloudWatch 限制。

> **Note**
>
> AMS Accelerate 会定期校准其基线监测。新账户始终使用最新的基准监控，该表描述了新加入账户的基准监控。AMS Accelerate 会定期更新现有账户的基准监控，在更新到位之前，您可能会遇到延迟。

来自基线监控的警报

服务/资源类型	警报来源和触发条件	警报名称和备注
对于已加星标的 (*) 警报，AMS 会主动评估影响并在可能的情况下进行补救；如果无法进行补救，AMS 就会造成事故。如果自动化无法纠正问题，AMS 会通知您事故案例，并让 AMS 工程师参与。此外，如果您选择加入 Direct-Customer-Alerts SNS 主题，则这些提醒将直接发送到您的电子邮件中。		
Application Load Balanc	ApplicationLoadBalancerErrorCount	应用程序 LoadBalancer HTTP 5XX 错误计数

服务/资源类型	警报来源和触发条件	警报名称和备注
	(HTTPCode_elb_5xx_count/RequestCount) *100 总和 > 15%，持续 1 分钟，连续 5 次。	CloudWatch 在负载均衡器生成的 HTTP 5XX 响应代码数量过多时发出警报。
Application Load Balanc	RejectedConnectionCount 总和 > 0%，持续 1 分钟，连续 5 次。	应用程序 LoadBalancer 被拒绝的连接计数 CloudWatch 如果因为负载均衡器达到最大值而被拒绝的连接数发出警报
应用程序 Load Balancer 目标	TargetConnectionErrorCount (HTTPCode_target_5xx_count/RequestCount) *100 总和 > 15%，持续 1 分钟，连续 5 次。	$ {ElasticLoadBalancingV2:::TargetGroup:FullName}-应用程序 LoadBalancer 目标连接错误计数-$ {ElasticLoadBalancingV2:::TargetGroup: UUID} CloudWatch 当目标生成的 HTTP 5XX 响应代码数量过多时发出警报。
应用程序 Load Balancer 目标	ApplicationLoadBalancerTargetGroupErrorCount 总和 > 0%，持续 1 分钟，连续 5 次。	$ {ElasticLoadBalancingV2:::TargetGroup:FullName}-应用程序 LoadBalancer 目标 HTTP 5XX 错误计数-$ {ElasticLoadBalancingV2:::: TargetGroup UUID} CloudWatch 如果负载均衡器和注册实例之间未成功建立连接数，则发出警报。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon EC2 实例-全部 OSs	CPUUtilization* 大于 95%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}: CPU 太高 CloudWatch 警报。CPU 利用率高表明应用程序状态发生了变化，例如死锁、无限循环、恶意攻击和其他异常。 这些是 Direct-Customer-Alerts 警报。
Amazon EC2 实例-全部 OSs	StatusCheckFailed 大于 0%，持续 5 分钟，连续 3 次。	$ {EC2::InstanceId}: 状态检查失败 CloudWatch 警报。状态检查失败表示具有指定 ID 的 Amazon EC2 实例未通过一项或多项自动状态检查。这意味着该实例遇到了问题，导致其无法正常运行或无法访问。
亚马逊 EC2 实例-Linux	最小内存使用百分比 大于 95%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}：内存不足 CloudWatch 警报。内存可用表示指定 Amazon EC2 实例上的可用内存 (RAM) 已降至定义的阈值以下。这可能会导致内存问题和系统崩溃，并表明实例可能需要更多 RAM。 这些是 Direct-Customer-Alerts 警报。

服务/资源类型	警报来源和触发条件	警报名称和备注
亚马逊 EC2 实例-Linux	平均掉期使用百分比 大于 95%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}：免掉期 CloudWatch 警报。A EC2 mazon 实例上的平均 swap_used_percent 表示当前使用的已分配交换空间的平均百分比已超过预定义的阈值。这可能会导致性能降低、瓶颈和内存问题。 这些是 Direct-Customer-Alerts 警报。
亚马逊 EC2 实例-Linux	最大已用磁盘百分比 大于 95%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}：磁盘使用率太高-$ {EC2:: Disk:: UUID} CloudWatch 警报。磁盘使用率过高表示特定 Amazon EC2 或已识别磁盘上的磁盘利用率已接近其容量。这可能导致性能降低、应用程序错误和系统不稳定。 这些是 Direct-Customer-Alerts 警报。
亚马逊 EC2 实例-Windows	已使用的最小内存已提交字节数百分比 大于 95%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}：内存不足 CloudWatch 警报。内存可用表示指定 Amazon EC2 实例上的可用内存 (RAM) 已降至定义的阈值以下。这可能会导致内存问题和系统崩溃，并表明实例可能需要更多 RAM。 这些是 Direct-Customer-Alerts 警报。

服务/资源类型	警报来源和触发条件	警报名称和备注
亚马逊 EC2 实例-Windows	最大可用空间 LogicalDisk 百分比 <= 5%，持续 5 分钟，连续 6 次。	$ {EC2::InstanceId}：磁盘使用率太高-$ {EC2:: Disk:: UUID} CloudWatch 警报。表示 Amazon EC2 Windows 实例中逻辑磁盘（文件系统分区）的可用空间百分比已超过预定义的阈值。磁盘空间不足可能导致磁盘空间不足 这些是 Direct-Customer-Alerts 警报。
Amazon EFS	AMSEFSBurstCreditBalanceExhausted. BurstCreditBalance 十五分钟内少于 1000。	$ {EFS::FileSystemId}: EFS：突发信用余额 CloudWatch Amazon EFS 文件系统的警报。 BurstCreditBalance
Amazon EFS	AMSEFSClientConnectionsLimit. ClientConnections > 24,000 持续十五分钟。	$ {EFS::FileSystemId}: EFS：客户端连接限制 CloudWatch Amazon EFS 文件系统的警报。 ClientConnections
Amazon EFS	AMSEFSThroughputUtilizationLimit. 一小时内 EFS 吞吐量利用率> 80%。	$ {EFS::FileSystemId}: EFS：吞吐量利用率限制 CloudWatch 有关 Amazon EFS 文件系统的吞吐量利用率的警报。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon EFS	AMSEFSPercentIOLimit. 百分比 IOLimit > 95，持续七十五分钟。	$ {EFS::FileSystemId}: EFS：百分比 IOLimit CloudWatch 在 Amazon EFS 文件系统的百分比IOLimit 上发出警报。
Amazon EKS	参见 Amazon EKS AMS Accelerate 中的 Amazon EKS 监控和事件管理中的基准警报。	
Elastic Load Balancin	SpilloverCountBackendConnectionErrors > 1，持续 1 分钟，连续 15 次。	经典 LoadBalancer 溢出计数警报 CloudWatch 如果由于激增队列已满而被拒绝的请求数量过多，则发出警报。
Elastic Load Balancin	HTTPCode_elb_5xx_count 总和 > 0，持续 5 分钟，连续 3 次。	CloudWatch 如果来自负载均衡器的 HTTP 5XX 响应代码数量过多，则发出警报。
Elastic Load Balancin	SurgeQueueLength 大于 100，持续 1 分钟，连续 15 次。	经典 LoadBalancer 浪涌队列长度警报。 CloudWatch 如果有多余的请求等待路由，则发出警报。
FSx 适用于 ONTAP	AMSFSXONTAPIOPSUtilization. FSX：ONTAP IOPS 利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: FSX: ONTAP IOPS 利用率 CloudWatch 针对 ONTAP 实例的 IOPS 利用率限制发出警报。 FSx

服务/资源类型	警报来源和触发条件	警报名称和备注
FSx 适用于 ONTAP	AMSFSXONTAPThroughput利用率。 FSX：ONTAP 吞吐量利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: FSX: ONTAP 吞吐量利用率 CloudWatch 针对 ONTAP 卷的 FSx 吞吐量限制发出警报。
FSx 适用于 ONTAP	AMSFSXONTAPVolumeI nodeUtilization. FSX: ONTAP 信息节点利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: $ {:: ONTAPFSx::} FSX: ONTAP Inod VolumeId e 利用率 CloudWatch 针对 ONTAP 卷的文件容量利用率限制发出警报。 FSx
FSx 适用于 ONTAP	AMSFSXONTAPVolumeC apacityUtilization. FSX：ONTAP 卷容量利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: $ {:FSx: ONTAP::} VolumeId CloudWatch 针对 ONTAP 卷的卷容量利用率限制发出警报。 FSx
FSx 适用于 Windows 文件服务器	AMSFSXWindowsThrou ghputUtilization. fsx：Windows 吞吐量利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: fsx: Windows 吞吐量利用率 CloudWatch 针对 Windows 文件服务器实例 FSx 的吞吐量限制发出警报。
FSx 适用于 Windows 文件服务器	AMSFSXWindowsIOPSU tilization. fsx：Windows IOPS 利用率 > 80%，持续两个小时。	$ {FSx::FileSystemId}: fsx: Windows IOPS 利用率 CloudWatch 针对 Windows 文件服务器实例的 IOPS 利用率限制发出警报。 FSx

服务/资源类型	警报来源和触发条件	警报名称和备注
GuardDuty 服务	不适用；所有发现（威胁目的）都受到监控。每个发现都对应一个警报。 GuardDuty 调查结果的变化。这些变化包括新生成的发现或后续出现的现有发现。	有关支持的 GuardDuty 查找类型列表，请参阅GuardDuty 活动查找类型。
Health	AWS Health Dashboard	当与 AMS 监控的服务相关的 AWS Health Dashboard (AWS Health) 事件状态发生变化时，系统会发送通知。有关更多信息，请参阅支持的服务。
IAM	亚马逊 EC2 IAM 实例配置文件不存在。 IAM 实例配置文件丢失。	有关替换 EC2 Amazon IAM 实例配置文件的说明，请参阅替换 IAM 角色中的 IAM 文档。

服务/资源类型	警报来源和触发条件	警报名称和备注
IAM	EC2 Amazon IAM 实例配置文件有太多的策略。 IAM 实例配置文件有 10 个策略，无法添加其他策略。	• 修改 IAM 的 AWS 服务配额，将每个角色的托管策略数量增加到 20。有关服务配额的信息，请参阅查看服务配额。 • 通过删除与这些实例关联的 IAM 角色的不必要托管策略，将托管策略数量降低到当前 IAM 配额以下。请务必保留 AMS 必需的政策。 • 通过整合与这些实例关联的 IAM 角色的策略，将托管策略数量降低到当前 IAM 配额以下。请务必保留 AMS 必需的政策。 有关 AMS 必需的策略，请参阅 AMS 加速用户指南：IAM 权限变更详情。
Macie	新生成的警报和对现有警报的更新。 Macie 发现调查结果有任何变化。这些变化包括新生成的发现或后续出现的现有发现。	亚马逊 Macie 提醒。有关支持的亚马逊 Macie 警报类型列表，请参阅分析亚马逊 Macie 调查结果。请注意，并非所有账户都启用 Macie。
NATGateways	PacketsDropCount：如果 packetsdropcount 在 15 分钟内超过 0，则发出警报	NatGateway PacketsDr opCount 大于零的值可能指示 NAT 网关持续存在暂时性问题。

服务/资源类型	警报来源和触发条件	警报名称和备注
NATGateways	ErrorPortAllocation：如果 NAT 网关在超过 15 分钟的评估期内无法分配端口，则发出警报	NatGateway ErrorPortAllocation NAT 网关无法分配源端口的次数。大于零的值表示打开的并发连接太多。
OpenSearch 集群	ClusterStatus 红色最大值为 >= 1，持续 1 分钟，连续 1 次。	ClusterStatus 红色 CloudWatch 警报。用于 AWS KMS 加密域中静态数据的加密密钥已禁用。重新启用它可恢复正常操作。要了解更多信息，请参阅 Red Cluster 状态。
OpenSearch 域	KMSKey错误 >= 1 持续 1 分钟，连续 1 次。	KMS 密钥错误 CloudWatch 警报。至少有一个主分片其及副本未分配给节点。要了解更多信息，请参阅 Amazon OpenSearch 服务的静态数据加密。
OpenSearch 域	KMSKey无法访问 >= 1 持续 1 分钟，连续 1 次。	KMS 密钥无法访问错误 CloudWatch 警报。至少有一个主分片其及副本未分配给节点。要了解更多信息，请参阅 Amazon OpenSearch 服务的静态数据加密。
OpenSearch 域	ClusterStatus 黄色最大值为 >= 1，持续 1 分钟，连续 1 次。	ClusterStatus 黄色 至少有一个副本分片未分配给节点。要了解更多信息，请参阅黄色群集状态。

服务/资源类型	警报来源和触发条件	警报名称和备注
OpenSearch 域	FreeStorageSpace 最小值为 <= 20480，持续 1 分钟，连续 1 次。	可用存储空间不足 您的集群中的节点已降至 20GiB 的可用存储空间。要了解更多信息，请参阅可用存储空间不足。
OpenSearch 域	ClusterIndexWritesBlocked >= 1 持续 5 分钟，连续 1 次。	集群索引写入已阻止 集群正在阻止写入请求。要了解更多信息，请参阅ClusterBlockException。
OpenSearch 域	节点 最小值 < x，持续 1 天。	节点已关闭 x 是您的集群中的节点数。此警报表示您的群集中至少有一个节点无法访问的时间已达到一天。要了解更多信息，请参阅集群节点故障。
OpenSearch 域	CPUUtilization 连续 3 次，15 分钟内平均值大于 80%。	数据节点的 CPU 使用率过高 100% CPU 利用率不常见，但是持续的 高平均值是有问题的。考虑调整现有实例类型的大小或添加实例。

服务/资源类型	警报来源和触发条件	警报名称和备注
OpenSearch 域	JVMMemory压力 最大 >= 80%，持续 5 分钟，连续 3 次。	数据节点的内存使用率很高 如果使用量增加，群集可能会遇到内存不足错误。考虑垂直缩放。 OpenSearch 将实例的 RAM 的一半用于 Java 堆，最大堆大小为 32GiB。您最多可以将实例的 RAM 垂直扩展至 64GiB，此时可以通过添加实例水平扩展。
OpenSearch 域	大师 CPUUtilization 15 分钟内平均值大于 50%，连续 3 次。	主节点 CPU 使用率高 考虑为您的专用主节点使用更大的实例类型。由于其在集群稳定性和蓝/绿部署中的作用，专用主节点的平均 CPU 使用率应比数据节点低。
OpenSearch 域	主JVMMemory压力 最大 >= 80%，持续 15 分钟，连续 1 次。	主节点高 JVM 内存压力 考虑为您的专用主节点使用更大的实例类型。由于其在集群稳定性和蓝/绿部署中的作用，专用主节点的平均 CPU 使用率应比数据节点低。
OpenSearch 实例	AutomatedSnapshotFailure 最大值为 >= 1，持续 1 分钟，连续 1 次。	自动快照失败 CloudWatch 警报。自动快照失败。此故障通常由红色群集运行状况导致。要了解更多信息，请参阅 Red Cluster 状态。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon RDS	CPU 平均利用率 大于 90%，持续 15 分钟，连续 2 次。	$ {RDS:: DBInstance 标识符}: CPUUtilization CloudWatch 警报。
Amazon RDS	的总和 DiskQueueDepth 大于 75%，持续 1 分钟，连续 15 次。	$ {RDS:: DBInstance 标识符}: DiskQueue CloudWatch 警报。
Amazon RDS	平均值 FreeStorageSpace 小于 1,073,741,824 字节，持续 5 分钟，连续 2 次。	$ {RDS:: DBInstance 标识符}: FreeStorageSpace CloudWatch 警报。
Amazon RDS	存储空间不足警报 在为数据库实例分配的存储空间用完时触发。	RDS-EVENT-0007，详情请参阅使用亚马逊 RDS 事件通知。
Amazon RDS	数据库实例失败 由于某个不兼容配置或底层存储问题，数据库实例已失败。从 point-in-time-restore数据库实例开始。	RDS-EVENT-0031，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	未尝试过 RDS -0034 故障切换。 Amazon RDS 不会因为数据库实例上最近出现故障转移而尝试请求故障转移。	RDS-EVENT-0034，请在 Amazon RDS 事件类别和事件消息中查看详情。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon RDS	RDS-0035 数据库实例参数无效 例如，由于该实例类的内存相关参数设置得太高，MySQL 无法启动，因此您的操作是修改内存参数并重启数据库实例。	RDS-EVENT-0035，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	子网 IDs 数据库实例无效 数据库实例处于不兼容的网络中。某些指定的子网 IDs 无效或不存在。	服务事件。RDS-EVENT-0036，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	RDS-0045 数据库实例只读副本错误 在读取复制过程中出错。有关详细信息，请参阅事件消息。有关排查只读副本错误的信息，请参阅 MySQL 只读副本问题疑难解答。	RDS-EVENT-0045，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	RDS-0057 创建 statspack 用户账户时出错 只读副本上的复制已结束。	服务事件。RDS-EVENT-0057，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	RDS-0058 数据库实例读取复制已结束 创建 Statspack 用户账户 PERFSTAT 时出错。在添加 Statspack 选项之前，请先删除账户。	服务事件。RDS-EVENT-0058，请在 Amazon RDS 事件类别和事件消息中查看详情。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon RDS	数据库实例恢复开始 SQL Server 数据库实例正在重新建立其镜像。在镜像重新建立之前，性能将下降。发现具有非 FULL 恢复模式的数据库。恢复模式已更改回完整模式并开始镜像恢复。(<dbname>: <recovery model found>[，...])	服务事件。RDS-EVENT-0066 在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	数据库群集的故障转移已失败。	RDS-EVENT-0069，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	权限恢复无效 S3 存储桶 用于访问您的 Amazon S3 存储桶以执行 SQL Server 本机备份和恢复的 IAM 角色配置不正确。有关更多信息，请参阅设置本机 Backup 和还原。	服务事件。RDS-EVENT-0081 在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	Aurora 无法从 Amazon S3 存储桶复制备份数据。	RDS-EVENT-0082，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	当数据库实例消耗了其分配的存储空间的 90% 以上时，会发出存储空间不足警报。	服务事件。RDS-EVENT-0089 在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	Aurora 无服务器数据库集群扩展失败时的通知服务。	服务事件。RDS-EVENT-0143 在 Amazon RDS 事件类别和事件消息中查看详情。

服务/资源类型	警报来源和触发条件	警报名称和备注
Amazon RDS	数据库实例处于无效状态。无需采取操作。弹性伸缩稍后将重试。	RDS-EVENT-0219，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	数据库实例已达到存储已满阈值，并且数据库已关闭。	RDS-EVENT-0221，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	此事件表示 Amazon RDS 实例存储无法自动扩展，自动扩展失败的原因可能有多种。	RDS-EVENT-0223，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	存储弹性伸缩已触发待处理的扩展存储任务，该任务将达到最大存储阈值。	RDS-EVENT-0224，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	数据库实例的存储类型目前在可用区中不可用。弹性伸缩稍后将重试。	RDS-EVENT-0237，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	Amazon RDS 无法为代理配置容量，因为您的子网中没有足够的 IP 地址。	RDS-EVENT-0243，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon RDS	您的存储空间 AWS 账户 已超过允许的存储配额。	RDS-EVENT-0254，请在 Amazon RDS 事件类别和事件消息中查看详情。
Amazon Redshift 集群	未处于维护模式时集群的运行状况 < 1 持续 5 分钟	RedshiftClusterHealthStatus 有关更多信息，请参阅使用指标监控 Amazon Redshift CloudWatch 。

服务/资源类型	警报来源和触发条件	警报名称和备注
Site-to-Site VPN	VPNTunnel向下 TunnelState <= 0 持续 1 分钟，连续 20 次。	$ {AWS::EC2::VpnConnectionId}- VPNTunnel 向下 TunnelState 当两条隧道都关闭时为 0，当一条隧道都开启时为 .5；当两条隧道都开启时为 1.0。
Systems Manager Agent	EC2 不由 Systems Manager 管理的实例 未安装 SSM 代理。SSM 代理已安装在实例上，但代理服务未运行。SSM 代理没有到 S AWS ystems Manager 服务的网络路由。	还有其他情况会导致 Systems Manager 代理中断；有关更多信息，请参阅托管节点可用性疑难解答。

有关补救工作的信息，请参阅AMS 自动修复警报。

观看安德鲁的视频以了解更多信息 (7:03)

AMS 中的应用程序感知事件通知

使用应用程序感知型自动事件通知，为 AMS 代表您创建的支持案例自定义您的沟通体验。当您使用此功能时，AMS 会从中检索自定义工作负载首选项，使用有关您的应用程序的元数据AWS Service Catalog AppRegistry来丰富您的 AMS 事件通信，并自定义 AMS 代表您创建的支持案例的严重性。要使用此功能，您必须先登录 AWS Service Catalog AppRegistry。

要了解有关 AMS 加速监控默认值的更多信息，请参阅AMS Accelerate 中的监控和事件管理。

加入 AppRegistry 并创建应用程序

要加入 AppRegistry，请参阅《AWS Service Catalog AppRegistry 管理员指南》 AppRegistry中的 “入门”。入职后，使用以下方法之一创建应用程序：

1. AWS 控制台：要了解有关 AppRegistry 通过 AWS 控制台创建应用程序的更多信息，请参阅《AWS Service Catalog AppRegistry 管理员指南》中的创建应用程序。

2. CloudFormation：您可以像定义任何其他资源一样定义 AppRegistry 应用程序。有关更多信息，请参阅《CloudFormation 用户指南》中的 AWS Service Catalog AppRegistry 资源类型参考。
3. AMS 自动化：为了简化应用程序注册流程，AMS 为您提供了 SSM 自动化文档AWSManagedServices-CreateAppRegistryApplication。要使用此方法，请从 AWS Systems Manager 控制台调用文档 https://console.aws.amazon.com/systems-manager/，网址 AWS CLI 为或使用以下示例所述。

```
# The following registers a new application with customized severity
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["normal"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# The following registers a new application with no customizations
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["TAGS"],"AppTagValue":
["MyApp"],"CFNStackNames":[],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
# You can also register applications using CloudFormation stacks
aws ssm start-automation-execution \
  --document-name "AWSManagedServices-CreateAppRegistryApplication" \
  --parameters '{"ResourceAssociationType":["STACKS"],"AppTagValue":
[""],"CFNStackNames":["arn:aws:cloudformation:us-east-1:123456789012:stack/
stack-2343eddq/1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"],"ApplicationName":
["BananaStand"],"ApplicationDescription":["This is my banana stand
 application"],"AppCriticality":["unset"],"AutomationAssumeRole":
["arn:aws:iam::123456789012:role/SSMAdminRole"]}' \
  --region us-east-1
```

创建标签以丰富案例

您必须先为应用程序添加标签，AMS 才能访问应用程序元数据。下表列出了所需的标签。

带有前缀ams:rt:的标签通过资源标记器应用。

标签密钥	标签值
ams 托管	true
ams:rt:ams-managed	true

为您的应用程序自定义 AMS 支持案例的严重性

您可以通过指定您的应用程序对组织的重要程度来自定义 AMS 创建的支持案例的严重程度。此设置由中与您的应用程序关联的属性组控制 AppRegistry。属性组名称的名称必须符合以下模式：

```
AMS.<ApplicationName>.CommunicationOptions
```

在上述模式中，ApplicationName必须与创建应用程序 AppRegistry 时使用的名称相匹配。

示例内容：

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

这决定了您正在使用的架构版本以及可供使用的功能子集。

架构版本	功能
1.0	根据重要性值自定义支持案例的严重性

临界性

此应用程序的重要性决定了 AMS 自动化系统创建的支持案例的严重性。

有效值：

```
low|normal|high|urgent|critical
```

有关严重性级别的更多信息，请参阅 AWS 支持 API 参考SeverityLevel中的。

必需：是

查看所需权限

要使用此功能，AMS 需要访问以下 AWS Identity and Access Management 权限：

- 我是：ListRoleTags
- 我是：ListUserTags
- 资源组标记 api: GetResources
- servicecatalog-appregistry: GetApplication
- servicecatalog-appregistry: ListAssociatedAttributeGroups
- servicecatalog-appregistry: GetAttributeGroup

> **Important**
> 确保没有拒绝上述操作的 IAM 策略或服务控制策略 (SCP)。

API 调用由`ams-access-admin`角色发出。以下是您可能看到的内容的示例：

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

加速警报管理器

AMS Accelerate 使用基于标签的警报管理器对您的 AWS 资源发出警报，以实施基准监控策略，并确保您的所有 AWS 资源都受到监控和保护。通过与基于标签的警报管理器集成，您可以根据 AWS 资源的类型、平台和其他标签自定义资源配置，以确保资源受到监控。在入职期间，警报管理器会部署到您的 Accelerate 账户。

警报管理器的工作原理

当您的账户加入 AMS Accelerate 时，将在您的账户中部署两个 JSON 文档，称为配置文件。AWS AppConfig两个配置文件都位于警报管理器应用程序和 AMS Accelerate 基础设施环境中。

这两个配置文件分别命名AMSManaged为 Alarms（默认配置文件）和 CustomerManagedAlarms（自定义配置配置文件）。

- 默认配置文件：
  - 此配置文件中的配置包含 AMS Accelerate 在所有客户账户中部署的默认配置。此配置包含默认 AMS Accelerate 监控策略，您不应修改该策略，因为 AMS Accelerate 可以随时更新此配置文件，从而删除您所做的任何更改。
  - 如果要修改或禁用这些定义中的任何一个，请参阅修改加速警报默认配置和禁用默认的加速警报配置。
- 自定义配置文件：
  - 此配置文件中的任何配置均完全由您管理；除非您明确要求，否则 AMS Accelerate 不会覆盖此配置文件。
  - 您可以在此配置文件中指定所需的任何自定义警报定义，也可以指定对 AMS Accelerate 管理的默认配置的修改。有关更多信息，请参阅修改加速警报默认配置和禁用默认的加速警报配置。
  - 如果您更新此个人资料，Alarm Manager 会自动在您 AWS 账户中的所有相关资源中强制执行您的更改。请注意，虽然您的更改是自动生效的，但最多可能需要 60 分钟才能生效。
  - 您可以使用 AWS 管理控制台 或 AWS CLI/SDK 工具更新此个人资料。有关更新配置的说明，请参阅《AWS AppConfig 用户指南》。
  - 自定义配置文件最初为空；但是，除了默认配置外，还会强制执行配置文件中放置的所有警报定义。

警报管理器创建的所有 CloudWatch 警报都包含标签键 ams: alarm-manager: managed，标签值为 true。这是为了确保警报管理器仅管理其创建的警报，并且不会干扰您自己的任何警报。您可以使用亚马逊 CloudWatch ListTagsForResourceAPI 查看这些标签。

> **Important**
>
> 如果使用相同的 ConfigurationID 指定自定义警报定义和默认警报定义（请参阅加速配置文件：监控），则自定义定义优先于默认规则。

加速警报管理器入门

默认情况下，当您加入 AMS Accelerate 时，您的配置将部署到 AWS AppConfig，从而为您的资源定义警报基准。警报定义仅适用于带有 ams: rt: * 标签的资源。我们建议使用以下方法应用这些标签加速资源标记器：您设置基本的资源标记器配置，以便让 AMS Accelerate 知道您要管理哪些资源。

使用资源标记器将标签密钥 ams: rt: ams-managed 应用标签值为真的 ams: rt: ams-managed 到您希望 AMS Accelerate 监控的任何资源。

以下是 Resource Tagger 自定义配置文件示例，您可以使用它来选择监控您的所有 Amazon EC2 实例。有关一般信息，请参阅加速资源标记器。

```
{
    "AWS::EC2::Instance": {
        "AMSManageAllEC2Instances": {
            "Enabled": true,
            "Filter": {
                "InstanceId": "*"
            },
            "Tags": [
                {
                    "Key": "ams:rt:ams-managed",
                    "Value": "true"
                }
            ]
        }
    }
}
```

有关如何应用此资源标记器配置的信息，请参阅查看或更改资源标记器配置。

加速警报管理器标签

默认情况下，当您加入 AMS Accelerate 时，您的配置将部署到 AWS AppConfig，从而为您的资源定义警报基准。警报定义仅适用于带有 ams: rt: * 标签的资源。我们建议使用以下方法应用这些标签加速资源标记器：您设置基本的资源标记器配置，以便让 AMS Accelerate 知道您要管理哪些资源。

使用资源标记器将标签密钥 ams: rt: ams-managed 应用标签值为真的 ams: rt: ams-managed 到您希望 AMS Accelerate 监控的任何资源。

主题

- 使用资源标记器加速标签
- 在不使用资源标记器的情况下加速标签
- 使用加速标签 CloudFormation
- 使用 Terraform 加速标签

使用资源标记器加速标签

基于标签的警报管理器管理每个资源 CloudWatch 警报的生命周期；但是，它要求托管的资源具有由 AMS Accelerate 定义的特定标签。要使用资源标记器将默认的 AMS 管理的警报集应用于基于 Linux 和 Windows 的实例，请按照以下步骤操作。

1. 在您的账户中浏览到AppConfig控制台。
2. 选择 ResourceTagger 应用程序。
3. 选择 “配置文件” 选项卡，然后选择CustomerManagedTags。
4. 单击 “创建” 创建新的配置文件。
5. 选择 JSON 并定义您的配置。有关过滤器和平台定义的更多示例，请参阅加速资源标记器。

```
{
"AWS::EC2::Instance": {
   "MonitorAllInstances": {
       "Enabled": true,
       "Filter": {
           "Platform": "*"
       },
       "Tags": [
           {
               "Key": "ams:rt:ams-managed",
               "Value": "true"
           }
       ]
   }
}
}
```

6. 单击 “创建托管配置版本”。
7. 单击 “开始部署”。
8. 定义以下部署细节：

```
Environment: AMSInfrastructure Hosted configuration version: <Select the version
 that you have just created>
              Deployment Strategy: AMSNoBakeDeployment
```

9. 单击 “开始部署”。

您的实例会被贴上标签"ams:rt:ams-managed": "true"，这样可以确保将额外"ams:rt:ams-monitoring-policy": "ams-monitored""ams:rt:ams-monitoring-policy-platform": "ams-monitored-linux"的 and 应用于实例。然后，这些标签会导致为该实例创建相应的警报。有关此过程的更多信息，请参阅 加速中的监控。

观看 Himanshu 的视频以了解更多信息 (11:04)

在不使用资源标记器的情况下加速标签

基于标签的警报管理器管理每个资源 CloudWatch 警报的生命周期；但是，它要求托管的资源具有由 AMS Accelerate 定义的特定标签。AMS Accelerate 提供了一个默认配置文件，该配置文件假设您的标签已由资源标记器应用。

如果您想使用另一种方法将标签应用于资源，例如 CloudFormation 或 Terraform，而不是 Resource Tagger，则需要禁用资源标记器，这样它就不会对您的资源应用标签，也不会与您选择的标记方法竞争。有关更改自定义 Resource Tagger 配置文件以启用只读模式的说明，请参阅阻止资源标记器修改资源。

将资源标记器设置为只读模式并部署配置文件后，根据以下准则，使用您选择的标记方法将标签应用于您的资源：

资源类型	标签密钥	标签值
所有支持的资源（如下表所述）	ams: rt: ams-monitoring-policy	ams 监控
EC2 实例 (Linux)	ams: rt: ams-monitoring-policy-platform	ams-monitored-linux
EC2 实例 (Windows)	ams: rt: ams-monitoring-policy-platform	ams-monitored-windows
OpenSearch 使用 KMS 的域名	ams: rt: ams-monitoring-with-kms	ams-monitored-with-kms
OpenSearch 带有专用主节点的域	ams: rt: ams-monitoring-with-master	ams-monitored-with-master

具有这些标签键和值的资源由 AMS 加速警报管理器管理。

使用加速标签 CloudFormation

> **Note**
>
> 在使用应用标签之前，请务必先将资源标记器设置为只读模式 CloudFormation，否则资源标记器可能会根据配置文件修改标签。有关将 Resource Tagger 设置为只读模式的信息以及提供您自己的标签的指南，请参阅在不使用资源标记器的情况下加速标签。

要使用应用标签 CloudFormation，可以在堆栈级别应用标签（请参阅 CloudFormation 资源标签），也可以在单个资源级别应用标签（例如，请参阅创建 EC2 实例标签）。

以下是如何将 AMS Accelerate 警报管理标签应用于由管理的 Amazon EC2 实例的示例 CloudFormation：

```
Type: AWS::EC2::Instance
Properties:
 InstanceType: "t3.micro"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

以下是如何将 AMS Accelerate 警报管理标签应用于由管理的 Auto Scaling 群组的示例 CloudFormation。请注意，Auto Scaling 组会将其标签传播到由其创建的亚马逊 EC2 实例：

```
Type: AWS::AutoScaling::AutoScalingGroup
Properties:
 AutoScalingGroupName: "TestASG"

 # ...other properties...

 Tags:
   - Key: "aws:rt:ams-monitoring-policy"
     Value: "ams-monitored"
   - Key: "aws:rt:ams-monitoring-policy-platform"
     Value: "ams-monitored-linux"
```

使用 Terraform 加速标签

> **Note**
>
> 在使用应用标签之前，请务必先将资源标记器设置为只读模式 CloudFormation，否则资源标记器可能会根据配置文件修改标签。有关将 Resource Tagger 设置为只读模式的信息以及提供您自己的标签的指南，请参阅在不使用资源标记器的情况下加速标签。

有关如何使用 Terraform 管理资源标签的描述，请参阅 Terraform 文档资源标记。

以下是如何将 AMS 加速警报管理标签应用于 Terraform 管理的亚马逊 EC2实例的示例。

```
resource "aws_instance" "test_linux_instance" {
     # ...ami and other properties...

     instance_type = "t3.micro"

     tags = {
       "aws:rt:ams-monitoring-policy" = "ams-monitored"
       "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
     }
   }
```

以下是如何将 AMS 警报管理标签应用于 Terraform 管理的 Auto Scaling 群组的示例。请注意，Auto Scaling 组会将其标签传播到由其创建的 EC2 实例：

```
 resource "aws_autoscaling_group" "test_asg" {
 name = "terraform-test"
 # ...other properties...

 tags = {
   "aws:rt:ams-monitoring-policy" = "ams-monitored"
   "aws:rt:ams-monitoring-policy-platform" = "ams-monitored-linux"
 }
}
```

加速警报管理器配置文件

当您的账户加入 AMS Accelerate 时，两个名为配置文件的 JSON 文档将部署到您的账户中 AWS AppConfig（参见 What is AWS AppConfig）。两个配置文件都位于警报管理器应用程序和 AMS Accelerate 基础设施环境中。

主题

加速配置文件：监控

默认配置文件文档和自定义配置文件文档遵循相同的结构：

```
{
  "<ResourceType>": {
      "<ConfigurationID>": {
          "Enabled": true,

          "Tag": {
              "Key": "...",
              "Value": "..."
          },
          "AlarmDefinition": {
              ...
          }
      },
      "<ConfigurationID>": {
```

```
            ...
        }
    },
    "<ResourceType>": {
        ...
    }
}
```

- ResourceType: 此密钥必须是以下支持的字符串之一。此 JSON 对象中的配置将仅与指定的 AWS 资源类型相关。支持的资源类型：

```
AWS::EC2::Instance
AWS::EC2::Instance::Disk
AWS::RDS::DBInstance
AWS::RDS::DBCluster
AWS::Elasticsearch::Domain
AWS::OpenSearch::Domain
AWS::Redshift::Cluster
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::ElasticLoadBalancingV2::LoadBalancer::TargetGroup
AWS::ElasticLoadBalancing::LoadBalancer
AWS::FSx::FileSystem::ONTAP
AWS::FSx::FileSystem::ONTAP::Volume
AWS::FSx::FileSystem::Windows
AWS::EFS::FileSystem
AWS::EC2::NatGateway
AWS::EC2::VPNConnection
```

- ConfigurationID：此密钥在配置文件中必须是唯一的，并且对以下配置块进行唯一命名。如果同一个区块中的两个配置ResourceType块具有相同的 C onfigurationID，则配置文件中最新显示的配置块将生效。如果您在自定义配置文件中指定的 ConfigurationID 与默认配置文件中指定的配置文件相同，则自定义配置文件中定义的配置块将生效。
  - 启用：（可选，default=true）指定配置块是否会生效。将其设置为 false 可禁用配置块。禁用的配置块的行为就像配置文件中不存在一样。
  - 标签：指定此警报定义适用的标签。任何具有此标签键和值的资源（相应资源类型）都将使用给定定义创建 CloudWatch 警报。此字段是一个 JSON 对象，包含以下字段：
    - 密钥：要匹配的标签的密钥。请记住，如果您使用资源标记器将标签应用于资源，则标签的密钥将始终以 ams: rt: 开头。
    - 值：要匹配的标签的值。

- AlarmDefinition：定义要创建的警报。这是一个 JSON 对象，其字段按原样传递给 CloudWatch PutMetricAlarm API 调用（伪参数除外；有关更多信息，请参阅加速配置文件：伪参数替换）。有关哪些字段为必填字段的信息，请参阅PutMetricAlarm文档。

  或

  CompositeAlarmDefinition：定义要创建的复合警报。创建复合警报时，您需要为警报指定一个规则表达式，该表达式会考虑您创建的其他警报的警报状态。这是一个 JSON 对象，其字段按原样传递给。CloudWatchPutCompositeAlarm只有当规则的所有条件都得到满足时，复合告警才会进入“ALARM（告警）”状态。在复合告警的规则表达式中指定的告警可以包括指标告警和其他复合告警。有关哪些字段为必填字段的信息，请参阅PutCompositeAlarm文档。

  这两个选项都提供以下字段：

  - AlarmName：指定要为资源创建的警报的名称。该字段的规则与PutMetricAlarm文档中指定的规则完全相同；但是，由于警报名称在一个区域中必须是唯一的，因此警报管理器还有一个额外的要求：您必须在警报名称中指定唯一标识符伪参数（否则，警报管理器会在警报名称的前面附加资源的唯一标识符）。例如，对于AWS::EC2::Instance资源类型，您必须在警报名称${EC2::InstanceId}中指定，或者将其隐式添加在警报名称的开头。有关标识符的列表，请参见加速配置文件：伪参数替换。

    所有其他字段均在PutMetricAlarm或PutCompositeAlarm文档中指定。

  - AlarmRule：指定要评估哪些其他警报以确定此复合警报的状态。对于您引用的每个警报，它们必须存在于您账户的 Alarm Manager 配置文件中 CloudWatch 或在其中指定。

> **Important**
>
> 您可以在 Alarm Manager 配置文档CompositeAlarmDefinition中指定其中一个AlarmDefinition或，但它们不能同时使用。

在以下示例中，当两个指定的指标警报超过其阈值时，系统会创建警报：

```
{
  "AWS::EC2::Instance": {
    "LinuxResourceAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:mylinuxinstance",
```

```
        "Value": "true"
      },
      "CompositeAlarmDefinition": {
        "AlarmName": "${EC2::InstanceId} Resource Usage High",
        "AlarmDescription": "Alarm when a linux EC2 instance is using too much CPU and
 too much Disk",
        "AlarmRule": "ALARM(\"${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}\") AND ALARM(\"${EC2::InstanceId}: CPU Too High\")"
      }
    }
  }
}
```

Important

当 Alarm Manager 由于配置中断而无法创建或删除警报时，它会将通知发送到 Direct-Customer-Alerts SNS 主题。此警报已被调用AlarmDependencyError。
我们强烈建议您确认订阅此 SNS 主题。要接收发布到主题的消息，您必须通过终端节点订阅该主题。有关详细信息，请参阅步骤 1：创建主题。

Note

创建异常检测警报后，警报管理器会自动为指定指标创建所需的异常检测模型。删除异常检测警报后，警报管理器不会删除关联的异常检测模型。
Amazon CloudWatch 限制了您在给定 AWS 区域中可以拥有的异常检测模型的数量。如果您超过了型号配额，则警报管理器不会创建新的异常检测警报。您必须删除未使用的型号，或者与您的 AMS 合作伙伴合作申请提高限额。
AMS Accelerate 提供的许多基准警报定义都将 SNS 主题 MMS 主题列为目标。这用于 AMS Accelerate 监控服务，也是将警报通知发送到 AMS Accelerate 的传输机制。请勿将 MMS-Topic 指定为除基准中提供的警报之外的任何警报的目标（以及该警报的替代项），因为该服务会忽略未知警报。这不会导致 AMS Accelerate 对您的自定义警报采取行动。

加速配置文件：伪参数替换

在任一配置文件中，您可以指定替换的伪参数，如下所示：

- 全局-配置文件中的任何位置：

  - $ {AWS::AccountId}：已替换为您的 AWS 账户 ID
  - $ {AWS::Partition}：替换为资源所在的 AWS 区域 分区（对于大多数区域，这是 “aws”）；有关更多信息，请参阅 ARN 参考中的分区条目。
  - $ {AWS::Region}：替换为资源部署到的区域的区域名称（例如 us-east-1）
- 在AWS::EC2::Instance资源类型块中：
  - $ {EC2::InstanceId}:（标识符）替换为您的 Amazon EC2 实例的实例 ID。
  - $ {EC2::InstanceName}：替换为您的 Amazon EC2 实例的名称。
- 在AWS::EC2::Instance:: Disk 资源块中：
  - $ {EC2::InstanceId}:（标识符）替换为您的 Amazon EC2 实例的实例 ID。
  - $ {EC2::InstanceName}：替换为您的 Amazon EC2 实例的名称。
  - $ {EC2:: Disk:: Device}:（标识符）替换为磁盘的名称。（仅限 Linux，适用于由CloudWatch 代理管理的实例）。
  - $ {EC2:: Disk::FSType}:（标识符）替换为磁盘的文件系统类型。（仅限 Linux，适用于由管理的实例 CloudWatchAgent）。
  - $ {EC2:: Disk:: Path}:（标识符）替换为磁盘路径。在 Linux 上，这是磁盘的装载点（例如，/），而在 Windows 中，这是驱动器标签（例如 c:/）（仅在CloudWatch 代理管理的实例上）。
  - $ {EC2:: Disk:: UUID}:（标识符）必须用生成的 UUID 来唯一标识磁盘，取而代之的是生成的 UUID，必须在警报的名称中指定，因为 AWS::EC2::Instance::Disk 资源类型下的警报将为每个卷创建一个警报。指定 $ {EC2:: Disk:: UUID} 将保持警报名称的唯一性。
- 在AWS::EKS::Cluster资源类型块中：
  - $ {EKS::ClusterName}:（标识符）替换为您的 EKS 集群的名称。
- 在AWS::OpenSearch::Domain资源类型块中：
  - $ {OpenSearch::DomainName}:（标识符）替换为您的 EKS 域名的名称。
- 在AWS::ElasticLoadBalancing::LoadBalancer资源类型块中：
  - $ {ElasticLoadBalancing:::LoadBalancer: Name}:（标识符）替换为您的 V1 Load Balancer 的名称。
- 在AWS::ElasticLoadBalancingV2::LoadBalancer资源类型块中：
  - $ {ElasticLoadBalancingV2:::: Arn}LoadBalancer:（标识符）替换为 V2 Load Balancer 的 ARN。
  - $ {ElasticLoadBalancingV2:::: Name}LoadBalancer:（标识符）替换为您的 V2 Load Balancer 的名称。
  - $ {ElasticLoadBalancingV2::::FullName}LoadBalancer:（标识符）替换为您的 V2 Load Balancer 的全名。

- 在AWS::ElasticLoadBalancingV2::LoadBalancer:: TargetGroup 资源类型块中：
  - $ {ElasticLoadBalancingV2::::FullName}TargetGroup:（标识符）替换为 V2 Load Balancer 的目标组名称。
  - $ {ElasticLoadBalancingV2:::: UUID}TargetGroup:（标识符）替换为您的 V2 Load Balancer 生成的 UUID。
- 在AWS::EC2::NatGateway资源类型块中：
  - $ {NatGateway::NatGatewayId}:（标识符）替换为 NAT 网关 ID。
- 在 A WS:: RDS:: DBInstance 资源类型区块中：
  - $ {RDS:: DBInstance 标识符}:（标识符）替换为您的 RDS 数据库实例标识符。
- 在 A WS:: RDS:: DBCluster 资源类型区块中：
  - $ {RDS:: DBCluster 标识符}:（标识符）替换为您的 RDS 数据库集群标识符。
- 在AWS::Redshift::Cluster资源类型块中：
  - $ {Redshift::ClusterIdentifier}:（标识符）替换为你的 Redshift 集群标识符。
- 在AWS::Synthetics::Canary资源类型块中：
  - $ {Synthetics::CanaryName}:（标识符）替换为你的 Synthetics 金丝雀的名 CloudWatch 字。
- 在 A WS::EC2:: VPNConnection 资源类型区块中：
  - $ {AWS::EC2::VpnConnectionId}:（标识符）替换为您的 VPN ID。
- 在AWS::EFS::FileSystem资源类型块中：
  - $ {EFS::FileSystemId}:（标识符）替换为 EFS 文件系统的文件系统 ID。
- 在AWS::FSx::FileSystem:: ONTAP 资源类型块中：
  - $ {FSx::FileSystemId}:（标识符）替换为 FSX 文件系统的文件系统 ID。
  - $ {FSx::FileSystem: 吞吐量}：替换为 FSX 文件系统的吞吐量。
  - $ {FSx:::FileSystem: Iops}：替换为 FSX 文件系统的 IOPS。
- 在:: ONTAPAWS::FSx::FileSystem:: Volume 资源块中：
  - $ {FSx::FileSystemId}:（标识符）替换为 FSX 文件系统的文件系统 ID。
  - $ {FSx:: ONTAP::VolumeId}:（标识符）替换为卷 ID。
- 在AWS::FSx::FileSystem:: Windows 资源类型块中：
  - $ {FSx::FileSystemId}:（标识符）替换为 FSX 文件系统的文件系统 ID。
  - $ {FSx::FileSystem: 吞吐量}：替换为 FSX 文件系统的吞吐量。

> **Note**
>
> 所有标有标识符的参数都用作已创建警报名称的前缀，除非您在警报名称中指定该标识符。

加速警报配置示例

在以下示例中，系统会为连接到匹配的 Linux 实例的每个磁盘创建警报。

```
{
    "AWS::EC2::Instance::Disk": {
        "LinuxDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mylinuxinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "disk_used_percent",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "device",
                        "Value": "${EC2::Disk::Device}"
                    },
                    {
                        "Name": "fstype",
                        "Value": "${EC2::Disk::FSType}"
                    },
                    {
                        "Name": "path",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
```

```
}
```

在以下示例中，系统会为连接到匹配的 Windows 实例的每个磁盘创建警报。

```
{
     "AWS::EC2::Instance::Disk": {
        "WindowsDiskAlarm": {
            "Tag": {
                "Key": "ams:rt:mywindowsinstance",
                "Value": "true"
            },
            "AlarmDefinition": {
                "MetricName": "LogicalDisk % Free Space",
                "Namespace": "CWAgent",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    },
                    {
                        "Name": "objectname",
                        "Value": "LogicalDisk"
                    },
                    {
                        "Name": "instance",
                        "Value": "${EC2::Disk::Path}"
                    }
                ],
                "AlarmName": "${EC2::InstanceId}: Disk Usage Too High -
 ${EC2::Disk::UUID}"
                ...
            }
        }
    }
}
```

查看您的加速警报管理器配置

AMSManaged警报和都CustomerManagedAlarms可以在中查 AppConfig看GetConfiguration。

以下是该GetConfiguration通话的示例：

```
aws appconfig get-configuration --application AMSAlarmManager --environment
 AMSInfrastructure --configuration AMSManagedAlarms --client-id
      any-string outfile.json
```

- 应用程序： AppConfig这是提供功能的逻辑单元；对于警报管理器来说，这是 AMSAlarmManager
- 环境：这就是 AMSInfrastructure 环境
- 配置：要查看 AMS Accelerate 基准警报，值为AMSManagedAlarms；要查看客户警报定义，配置为 CustomerManagedAlarms
- 客户端 ID：这是一个唯一的应用程序实例标识符，可以是任何字符串
- 可以在指定的输出文件中查看警报定义，在本例中为 outfile.json

您可以通过查看 AMSInfrastructure环境中过去的部署来查看您的账户中部署了哪个版本的配置。

更改加速警报配置

要添加或更新新的警报定义，您可以部署配置文档CloudFormation 用于部署加速配置更改或调用CreateHostedConfigurationVersionAPI。

这是一个 Linux 命令行命令，它在 base64 中生成参数值，这正是 AppConfig CLI 命令所期望的。有关信息，请参阅 AWS CLI 文档 B inary/Blob（二进制大对象）。

例如：

```
aws appconfig create-hosted-configuration-version --application-id application-id --
configuration-profile-id configuration-profile-id --content base64-string
      --content-type application/json
```

- 应用程序 ID：应用程序 AMS 的 ID AlarmManager；您可以通过 ListApplicationsAPI 调用找到这一点。
- 配置文件 ID：配置的 ID CustomerManagedAlarms；您可以通过 ListConfigurationProfilesAPI 调用找到这一点。
- 内容：内容的 Base64 字符串，将通过创建文档并将其编码为 base64 来创建：cat alarms-v2.json | base64（参见 Binary/Blob（二进制大对象））。

  内容类型：MIME 类型，application/json因为警报定义是用 JSON 编写的。

> **Important**
>
> 将StartDeployment和 StopDeploymentAPI 操作的访问权限限制为了解向目标部署新配置的责任和后果的可信用户。

要详细了解如何使用 AWS AppConfig 功能创建和部署配置，请参阅使用 AWS AppConfig。

修改加速警报默认配置

虽然您无法修改默认配置文件，但您可以通过在自定义配置文件中指定与默认配置块相同的 ConfigurationI d 的配置块来覆盖默认配置文件。如果这样做，则整个配置块将覆盖要应用标签配置的默认配置块。

例如，考虑以下默认配置文件：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 5,
                ...
            }
        }
    }
}
```

要将此警报的阈值更改为 10，您必须提供完整的警报定义，而不仅仅是要更改的部分。例如，您可以提供以下自定义配置文件：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                "AlarmName": "${EC2::InstanceId}: AMS Default Alarm",
                "Namespace": "AWS/EC2",
                "MetricName": "CPUUtilization",
                "Dimensions": [
                    {
                        "Name": "InstanceId",
                        "Value": "${EC2::InstanceId}"
                    }
                ],
                "Threshold": 10,
                ...
            }
        }
    }
}
```

Important

请记得在更改配置后再进行部署。在 SSM 中 AppConfig，您必须在创建配置后部署新版本的配置。

部署加速警报配置更改

完成自定义后，需要使用 AppConfig 或对其进行部署 CloudFormation。

主题

- AppConfig 用于部署加速警报配置更改
- CloudFormation 用于部署加速配置更改

AppConfig 用于部署加速警报配置更改

自定义完成后，使用 AppConfig 来部署您的更改StartDeployment。

```
  aws appconfig start-deployment --application-id application_id
   --environment-id environment_id Vdeployment-strategy-id
   deployment_strategy_id --configuration-profile-id configuration_profile_id --
configuration-version 1
```

- 应用程序 ID：应用程序的 IDAMSAlarmManager，您可以通过 ListApplicationsAPI 调用找到它。
- 环境 ID：您可以通过 ListEnvironmentsAPI 调用找到它。
- 部署策略 ID：您可以通过 ListDeploymentStrategiesAPI 调用找到它。
- 配置文件 ID：的 IDCustomerManagedAlarms；您可以通过 ListConfigurationProfilesAPI 调用找到它。
- 配置版本：要部署的配置文件的版本。

> **Important**
>
> 警报管理器应用配置文件中指定的警报定义。您使用 AWS 管理控制台 或 CloudWatch CLI/SDK 对 CloudWatch 警报进行的任何手动修改都会自动恢复，因此请确保您的更改是通过警报管理器定义的。 要了解哪些警报是由警报管理器创建的，您可以查找带有值的ams:alarm-manager:managed标签true。
>
> 将StartDeployment和 StopDeploymentAPI 操作的访问权限限制为了解向目标部署新配置的责任和后果的可信用户。

要详细了解如何使用 AWS AppConfig 功能创建和部署配置，请参阅 AWS AppConfig 文档。

CloudFormation 用于部署加速配置更改

如果您希望使用部署CustomerManagedAlarms配置文件 CloudFormation，则可以使用以下 CloudFormation 模板。在AMSAlarmManagerConfigurationVersion.Content字段中输入所需的 JSON 配置。

在 CloudFormation 堆栈或堆栈集中部署模板时，如果您未遵循配置所需的 JSON 格式，则AMSResourceTaggerDeployment资源部署将失败。有关预期格式加速配置文件：监控的详细信息，请参阅。

有关将这些模板部署为 CloudFormation 堆栈或堆栈集的帮助，请参阅以下相关 AWS CloudFormation 文档：

- 在 AWS CloudFormation 控制台上创建堆栈
- 使用 AWS CLI 创建堆栈
- 创建堆栈集

> **Note**
>
> 如果您使用其中一个模板部署配置版本，然后删除 CloudFormation 堆栈/堆栈集，则该模板配置版本将保持当前部署的版本，并且不会进行其他部署。如果您希望恢复到默认配置，则需要手动部署空配置（即只是 {}），或者将堆栈更新为空配置，而不是删除堆栈。

JSON

```
{
  "Description": "Custom configuration for the AMS Alarm Manager.",
  "Resources": {
    "AMSAlarmManagerConfigurationVersion": {
      "Type": "AWS::AppConfig::HostedConfigurationVersion",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "Content": "{}",
        "ContentType": "application/json"
      }
    },
    "AMSAlarmManagerDeployment": {
      "Type": "AWS::AppConfig::Deployment",
      "Properties": {
        "ApplicationId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-ApplicationId"
        },
        "ConfigurationProfileId": {
```

```
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-
ProfileID"
        },
        "ConfigurationVersion": {
          "Ref": "AMSAlarmManagerConfigurationVersion"
        },
        "DeploymentStrategyId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-Deployment-StrategyID"
        },
        "EnvironmentId": {
          "Fn::ImportValue": "AMS-Alarm-Manager-Configuration-EnvironmentId"
        }
      }
    }
  }
}
```

YAML

```
Description: Custom configuration for the AMS Alarm Manager.
Resources:
  AMSAlarmManagerConfigurationVersion:
    Type: AWS::AppConfig::HostedConfigurationVersion
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      Content: |
        {

        }
      ContentType: application/json
  AMSAlarmManagerDeployment:
    Type: AWS::AppConfig::Deployment
    Properties:
      ApplicationId:
        !ImportValue AMS-Alarm-Manager-Configuration-ApplicationId
      ConfigurationProfileId:
        !ImportValue AMS-Alarm-Manager-Configuration-CustomerManagedAlarms-ProfileID
      ConfigurationVersion:
        !Ref AMSAlarmManagerConfigurationVersion
      DeploymentStrategyId:
```

```
        !ImportValue AMS-Alarm-Manager-Configuration-Deployment-StrategyID
      EnvironmentId:
        !ImportValue AMS-Alarm-Manager-Configuration-EnvironmentId
```

回滚加速警报更改

您可以通过相同的部署机制回滚警报定义，方法是指定先前的配置文件版本并运行 StartDeployment。

保留加速警报

删除 AMS 监控的资源后，警报管理器会自动删除警报管理器为这些资源创建的所有警报。如果您出于审计、合规性或历史目的需要保留某些警报，请使用 Alarm Manager 保留标记功能。

要在警报的监控资源被删除后仍保留警报，请在警报的自定义配置中添加"ams:alarm-manager:retain" 标签，如以下示例所示。

```
{
  "AWS::EC2::Instance": {
    "AMSCpuAlarm": {
      "Enabled": true,
      "Tag": {
        "Key": "ams:rt:ams-monitoring-policy",
        "Value": "ams-monitored"
      },
      "AlarmDefinition": {
        "AlarmName": "${EC2::InstanceId}: CPU Too High",
        "AlarmDescription": "AMS Baseline Alarm for EC2 CPUUtilization",
        [...]
        "Tags": [
          {
            "Key": "ams:alarm-manager:retain",
            "Value": "true"
          }
        ]
      }
    }
  }
}
```

当监控的资源终止时，Alarm Manager 不会自动删除使用"ams:alarm-manager:retain"标签配置的警报。保留的警报会 CloudWatch 无限期保留，直到您使用手动将其删除。 CloudWatch

禁用默认的加速警报配置

AMS Accelerate 根据基准警报在您的账户中提供默认配置文件。但是，可以通过覆盖任何警报定义来禁用此默认配置。 您可以通过覆盖自定义配置文件中规则的 C onfigurationID 并指定值为 false 的启用字段来禁用默认配置规则。

例如，如果默认配置文件中存在以下配置：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": true,
            "Tag": {
                "Key": "ams:rt:ams-monitoring-policy",
                "Value": "ams-monitored"
            },
            "AlarmDefinition": {
                ...
            }
        }
    }
```

您可以通过在自定义配置文件中包含以下内容来禁用此标记规则：

```
{
    "AWS::EC2::Instance": {
        "AMSManagedBlock1": {
            "Enabled": false
        }
    }
}
```

要进行这些更改，必须使用 JSON 配置文件文档调用 CreateHostedConfigurationVersionAPI（请参阅更改加速警报配置），然后必须进行部署（请参阅部署加速警报配置更改）。请注意，在创建新的配置版本时，还必须在 JSON 配置文件文档中包含您想要的任何先前创建的自定义警报。

> **Important**
>
> 当 AMS Accelerate 更新默认配置文件时，它不会根据您配置的自定义警报进行校准，因此，当您在自定义配置配置文件中覆盖默认警报时，请查看对默认警报的更改。

为加速创建其他 CloudWatch 警报

您可以使用自定义 CloudWatch 指标为 AMS Accelerate 创建其他 CloudWatch 警报，也可以为 Amazon EC2 实例创建警报。

生成您的应用程序监控脚本和自定义指标。有关更多信息和访问示例脚本的权限，请参阅监控 Amazon EC2 Linux 实例的内存和磁盘指标。

Linux Amazon EC2 实例的 CloudWatch 监控脚本演示了如何生成和使用自定义 CloudWatch 指标。这些示例 Perl 脚本包含一个功能完备的示例，用于报告 Linux 实例的内存、交换文件和磁盘空间使用率指标。

> **Important**
>
> AMS Accelerate 不会监控您创建的 CloudWatch 警报。

查看警报管理器监控的加速资源数量

Alarm Manager 每小时向`AMS/AlarmManager`命名空间中的 Amazon CloudWatch 发送指标。仅针对警报管理器支持的资源类型发出指标。

指标名称	Dimensions	说明
ResourceCount	组件，ResourceType	在该区域部署的（指定资源类型的）资源数量。 单位：计数
ResourcesMissingManagedAlarms	组件，ResourceType	需要管理警报，但 Alarm Manager 尚未应用警报的资源（指定资源类型）的数量。 单位：计数
UnmanagedResources	组件，ResourceType	警报管理器未对其应用任何托管警报的资源（指定资源类型）的数量。通常，这些资源与任何 Alarm Manager 配置块都不匹配，或者被明确排除在配置块之外。 单位：计数

指标名称	Dimensions	说明
MatchingResourceCount	组件、 ResourceType、 ConfigClauseName	与 Alarm Manager 配置块相匹配的资源（指定资源类型）的数量。要使资源与配置块匹配，必须启用该块，并且该资源必须具有在配置块中指定的相同标签。 单位：计数

这些指标也可以在 AM S-Alarm-Manager-Reporting-Dashboard 中以图表形式查看。要查看控制面板，请从 AWS CloudWatch 管理控制台中选择 AMS-Alarm-Manager-Reporting- Dashboard。默认情况下，此控制面板中的图表显示前 12 小时的数据。

AMS Accel CloudWatch erate 会向您的账户部署警报，以检测非托管资源数量的显著增加，例如，AMS Alarm Manager 不管理的资源。AMS Operations 将调查非托管资源的增加情况，这些资源超过三个相同类型的资源，或者在相同类型的所有资源基础上增加 50%。如果变更似乎不是故意的，AMS Operations 可能会与您联系以审查变更。

AMS 自动修复警报

经过验证后，AWS Managed Services (AMS) 会根据本节中描述的特定条件和流程自动修复某些警报。

警报名称	说明	阈值	操作
状态检查失败	可能的硬件故障或实例的故障状态。	在过去 15 分钟内，系统至少检测到一次故障状态。	AMS 自动补救首先验证实例是否可访问。如果无法访问该实例，则该实例将停止并重新启动。停止和启动允许实例迁移到新的底层硬件。有关更多信息，请参阅以下 “EC2 状态检查失败补救自动化” 部分。
AMSLinuxDiskUsage	当您的 EC2 实例上 1 个挂载点（卷上的指定空	在过去 30 分钟内，该阈值高于定义值的 6 次。	AMS 自动修复首先会删除临时文件。如果这不能释放足够的磁盘空间，则会

警报名称	说明	阈值	操作
	间）的磁盘使用量已满时触发。		扩展音量以防止在卷已满时停机。
AMSWindowsDiskUsage	当您的 EC2 实例上 1 个装载点（卷上的指定空间）的磁盘使用量已满时。	在过去 30 分钟内，阈值高于定义值的 6 次。	AMS 自动修复首先会删除临时文件。如果这不能释放足够的磁盘空间，则会扩展音量以防止在卷已满时停机。
RDS-EVENT-0089	数据库实例已使用其分配的存储空间的 90% 以上。	已分配的存储空间超过 90%。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能：`"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

警报名称	说明	阈值	操作
RDS-EVENT-0007	为数据库实例分配的存储空间已用完。要解决这个问题，请分配额外的存储空间。	存储空间已百分之百分配。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能：`"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

警报名称	说明	阈值	操作
RDS-EVENT-0224	请求的分配存储空间达到或超过配置的最大存储阈值。	数据库实例的最大存储阈值已用尽或大于或等于请求的分配存储空间。	AMS 自动补救首先会验证请求的 RDS 存储量是否会超过最大存储阈值。如果得到确认，AMS 会尝试使用 CloudFormation 变更集将最大存储阈值提高 30%，或者如果未通过配置资源，则直接使用 RDS API。 CloudFormation 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".

警报名称	说明	阈值	操作
RDS 存储容量	为数据库实例分配的存储空间剩余不到 1GB。	存储空间分配了 99%。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".

EC2 状态检查失败：补救自动化注意事项

AMS 自动修复如何处理 EC2 状态检查失败问题：

- 如果您的 Amazon EC2 实例变得无法访问，则必须停止并重新启动该实例，这样才能将其迁移到新硬件并进行恢复。
- 如果问题的根源在于操作系统（fstab 中缺少设备、内核损坏等），则自动化无法恢复您的实例。
- 如果您的实例属于 Auto Scaling 组，则自动化不会执行任何操作—— AutoScalingGroup 扩展操作会取代实例。
- 如果您的实例启用了 EC2 自动恢复，则修复不会采取任何措施。

EC2 音量使用补救自动化

AWS Managed Services (AMS) 自动修复如何处理 EC2 卷使用问题：

- 自动化首先会验证是否需要音量扩展，以及是否可以执行音量扩展。如果认为扩展是适当的，则自动化可以增加卷容量。这种自动化流程在增长需求与受控的有限扩张之间取得平衡。
- 在扩展卷之前，自动化会对实例执行清理任务（Windows：磁盘清理器，Linux：Logrotate + Simple Service Manager 代理日志删除），以尝试释放空间。

> **Note**
>
> 清理任务不在 EC2 “T” 系列实例上运行，因为它们依赖于 CPU 积分来持续运行。

- 在 Linux 上，自动化仅支持扩展 EXT2 EXT3、 EXT4 和 XFS 类型的文件系统。
- 在 Windows 上，自动化仅支持新技术文件系统 (NTFS) 和弹性文件系统 (RefS)。
- 自动化不会扩展属于逻辑卷管理器 (LVM) 或 RAID 阵列的卷。
- 自动化不会扩展实例存储容量。
- 如果受影响的音量已经大于 2 TiB，则自动化不会采取任何行动。
- 通过自动化进行的扩展限制为每周最多三次，在系统的整个生命周期内最多只能进行五次。
- 如果上一次扩展是在过去六小时内进行的，则自动化不会扩大音量。

当这些规则阻止自动化采取行动时，AMS 会通过出站服务请求与您联系，以确定下一步要采取的行动。

Amazon RDS 存储不足事件补救自动化

AWS Managed Services (AMS) 自动修复如何处理 Amazon RDS 存储不足事件问题：

- 在尝试扩展 Amazon RDS 实例存储空间之前，自动化会执行多项检查，以确保 Amazon RDS 实例处于可修改且可用或存储空间已满的状态。
- 如果检测到 CloudFormation 堆栈偏差，则通过 Amazon RDS API 进行补救。
- 在以下情况下，修复操作不会运行：
  - Amazon RDS 实例的状态不是 “可用” 或 “存储空间已满”。
  - Amazon RDS 实例存储目前不可修改（例如，在过去六小时内修改了存储空间时）。
  - Amazon RDS 实例已启用自动缩放存储空间。
  - Amazon RDS 实例不是 CloudFormation 堆栈中的资源。
- 补救仅限于每六小时进行一次扩展，在连续的十四天内不超过三次扩展。
- 当这些情况发生时，AMS 会与您联系，告知出站事件，以确定下一步行动。

在 AMS 中使用亚马逊 EventBridge 托管规则

AMS Accelerate 使用亚马逊 EventBridge 托管规则。托管规则是一种与 AMS 直接关联的独特规则类型。这些规则匹配传入的事件并将其发送到目标进行处理。托管规则由 AMS 预定义，包括服务管理客户账户所需的事件模式，除非另有定义，否则只有拥有的服务才能使用这些托管规则。

AMS 加速托管规则与`events.managedservices.amazonaws.com`服务主体相关联。这些托管规则通过AWSServiceRoleForManagedServices_Events服务相关角色进行管理。要删除这些规则，需要客户特别确认。有关更多信息，请参阅删除 AMS 托管规则。

有关规则的更多信息，请参阅 Amazon EventBridge 用户指南中的规则。

AMS 部署的 Amazon EventBridge 托管规则

亚马逊 EventBridge 托管规则

规则名称	说明	定义

AmsAccessRolesRule	此规则用于监听特定 AMS Accelerate 角色和策略中的修改。	{
		"source": ["aws.iam"],
		"detail-type": ["AWS API Call via CloudTrail"],
		"detail": {
		"eventName": [
		"DeleteRole",
		"DeletePolicy",
		"CreatePolicyVersion",
		"AttachRolePolicy",
		"DetachRolePolicy"
		],
		"requestParameters": {
		"$or": [
		{
		"roleName": [
		"ams-access-admin",
		"ams-access-admin-operations",
		"ams-access-operations",
		"ams-access-read-only",
		"ams-access-security-analyst",
		"ams-access-security-analyst-read-only"
		]

规则名称	说明	定义

```
            },
            {
                "policyArn": [
                    "arn:*:iam::*:policy/ams-ac
cess-allow-pass-role",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-cloudshell-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-operations-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-deny-update-iam-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-ssr-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-read-only-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-security-analyst-extended-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-policy",
                    "arn:*:iam::*:policy/ams-ac
cess-admin-operations-policy"
                ]
            },
         ]
       },
   },
}
```

规则名称	说明	定义

AMSCore规则	该规则会将亚马逊 CloudWatch 事件转发 AWS Config 给 AMS Config 补救和 AMS 监控服务。AWS Config 事件创建并解决 AWS Systems Manager OpsItems。Amazon CloudWatch 事件监控 CloudWatch 警报。	<pre>{
		    {
		        "source": ["aws.config", "aws.cloudwatch"],
		        "detail-type": ["Config Rules Compliance Change", "CloudWatch Alarm State Change"],
		    }
		}</pre>

为 AMS 创建托管规则

您无需手动创建 Amazon EventBridge 托管规则。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时，AMS 会为您创建它们。 AWS CLI

编辑 AMS 的托管规则

AMS 不允许您编辑托管规则。每个托管规则的名称和事件模式均由 AMS 预定义。

删除 AMS 的托管规则

您无需手动删除托管规则。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时，AMS 会为您清理资源并删除 AMS 拥有的所有托管规则。 AWS CLI

如果 AMS 在离职期间未能删除托管规则，您也可以使用 Amazon EventBridge 控制台、 AWS CLI 或 AWS API 手动删除托管规则。为此，您必须先退出 AMS，然后强制删除托管规则。

AMS 中值得信赖的修正者

Trusted Remediator 是一种 AWS Managed Services 解决方案，可自动执行补救措施AWS Trusted Advisor和建议。AWS Compute Optimizer当 Trusted Advisor Compute Optimizer 向您指出降低成本、提高系统可用性、优化性能或弥合安全漏洞的机会时，Trusted Remediator 会创建建议。 AWS 账户借助 Trusted Remediator，您可以使用既定的最佳实践，以安全、标准化的方式解决这些安全、性能、成本优化、容错和服务限制建议的问题。Trusted Remediator 允许您配置修复解决方案，并按照您创建的计划自动运行，从而简化了修复过程。这种简化的方法可以一致、高效地解决问题，且无需人工干预。

可信修正者的主要优点

以下是 Trusted Remediator 的主要优点：

- 提高安全性、性能和成本优化：Trusted Remediator 可帮助您增强账户的整体安全状况，优化资源利用率并降低运营成本。
- 自助服务设置和配置：您可以将 Trusted Remediator 配置为与您的要求和首选项保持一致。
- 自动 Trusted Advisor 检查和 AWS Compute Optimizer 建议修复：配置完成后，Trusted Remediator 会自动为选定的检查运行修复操作。这种自动化消除了手动干预的需求。
- 最佳实践实施：补救措施基于既定的最佳实践，因此以标准化和有效的方式解决问题。
- 计划执行：您可以选择与您的 day-to-day操作工作流程一致的补救时间表。

Trusted Remediator 使您能够主动解决 AWS 环境中已发现的问题，帮助您遵守最佳实践，维护安全、高性能且经济实惠的云基础架构。

可信修正者的工作原理

以下是 “可信修正者” 工作流程的示例：

Trusted Remediator 会 AWS 账户 为您评估 Trusted Advisor 和推荐 Compute Optimizer 建议，然后在中创建。 AWS Systems Manager OpsItems OpsCenter然后，您可以使用 Trusted Remediator 自动化文档 OpsItems 自动或手动修复。以下是每种补救措施的详细信息：

- 自动修复：Trusted Remediator 运行自动化文档并监控运行情况。自动化文档完成后，Trusted Remediator 会解析 Opsitem。
- 手动修复：可信修正者会创建 OpsItem 供您查看。审阅完毕后，即可启动自动化文档。

修复日志存储在 Amazon S3 存储桶中。您可以使用 S3 存储桶中的数据来构建用于报告的自定义 QuickSight 仪表板。AMS 还根据要求为可信修正者提供报告。要接收这些报告，请联系您的 CSDM。有关更多信息，请参阅 可信修正者报告。

可信修正者的关键术语

以下是在 AMS 中使用 Trusted Remediator 时需要了解的术语：

- AWS Trusted Advisor 以及 AWS Compute Optimizer：由提供的云优化服务 AWS。 Trusted Advisor Compute Optimizer 会检查您的 AWS 环境并根据以下六个类别的最佳实践提供建议：
  - 成本优化
  - 性能
  - 安全性
  - 容错能力
  - 卓越运营
  - 服务限制

  有关更多信息，请参阅AWS Trusted Advisor和AWS Compute Optimizer。
- 可信修正者：用于Trusted Advisor检查和AWS Compute Optimizer建议的 AMS 补救解决方案。Trusted Remediator 可帮助您使用已知的最佳实践安全地修复 Trusted Advisor 检查和 Compute Optimizer 建议，以提高安全性、性能并降低成本。可信修正器易于设置和配置。您只需配置一次，Trusted Remediator 就会按照您的首选计划（每天或每周）运行修复。
- AWS Systems Manager SSM 文档：一个 JSON 或 YAML 文件，用于定义对您的 AWS 资源 AWS Systems Manager 执行的操作。SSM 文档可作为声明性规范，用于自动执行跨多个 AWS 资源和实例的操作任务。
- AWS Systems Manager OpsCenter OpsItem：云运营问题管理资源，可帮助您跟踪和解决 AWS 环境中的运营问题。 OpsItems 为跨 AWS 服务 资源的运营数据和问题提供集中视图和管理系统。每个都 OpsItem 代表一个操作问题，例如潜在的安全风险、性能问题或操作事件。
- 配置：配置是存储在中的一组属性 AWS AppConfig，其功能为 AWS Systems Manager。中的 Trusted Remediator 应用程序 AWS AppConfig 可帮助在帐户级别配置修复。您可以使用 AWS AppConfig 控制台或 API 来编辑配置。

- 执行模式：执行模式是一个配置属性，用于确定如何针对每个 Trusted Advisor 检查结果运行修复。支持四种执行模式：自动、手动、有条件和非活动。
- 资源覆盖：此功能使用资源标签来覆盖特定资源的配置。
- 修复项目日志：可信修正者修复 S3 日志存储桶中的日志文件。修复项目日志是在创建修复时创建 OpsItems 的。此日志文件包含手动执行补救 OpsItems 和自动执行补救 OpsItems。使用此日志文件跟踪所有补救项目。
- 自动修复执行日志：可信修正者修复 S3 日志存储桶中的日志文件。自动修复执行日志在 SSM 文档的自动运行完成后创建。此日志包含用于自动执行补救 OpsItems的 SSM 执行详细信息。使用此日志文件来跟踪自动修复。

开始使用 AMS 中的可信修复器

可信修正器在 AMS 中可用，无需额外付费。Trusted Remediator 支持单账户和多账户配置。

加入可信修复者

要将您的 AMS 账户注册到 Trusted Remedieator，请发送电子邮件给您的云架构师或云服务交付经理 (CSDMs)。在电子邮件中，请包含以下信息：

- AWS 账户: 十二位数的账户识别码。您要注册到 Trusted Remedieator 的所有账户都必须属于同一个 Accelerate 客户。
  - 委托管理员帐户：用于单个或多个帐户 Trusted Advisor 和 Compute Optimizer 检查配置的帐户。
  - 成员账户：这些账号是指关联到委派管理员账号的账号。这些账户继承委派管理员账户的配置。您可以拥有一个成员账户或多个成员账户。

    > **Note**
    >
    > 成员账号继承委派管理员账号的配置。如果您需要为特定账户配置不同的配置，请使用您的首选配置注册多个委派管理员帐户。在入职之前，请与您的云架构师一起规划账户结构和配置。

- AWS 区域：您的资源所在的位置。 AWS 区域 有关列表 AWS 区域，请参阅AWS 服务 按地区划分。
- 补救时间表和时间：您的首选补救时间表（每天或每周）。Trusted Remediator 会在计划的时间收集 Trusted Advisor 检查并启动修复。例如，您可以将补救计划设置为每周星期日凌晨 1:00（澳大利亚东部标准时间）。

- 通知电子邮件：Trusted Remediator 使用通知电子邮件每天通知您是否有补救措施。通知电子邮件的主题是 “可信修正者补救摘要”，其内容提供有关过去 24 小时内运行的可信修正者修正的信息。

> **Note**
>
> 每次计划修复后，请检查您的应用程序和资源。如需其他支持，请联系 AMS。

在您向 CA 或 CSDM 提交包含所需详细信息的入会申请后，AMS 会将您的账户登录到 Trusted Remediator。Trusted AWS AppConfig Remediator 使用（一种功能）来定义 Trusted Advisor 检查的配置。 AWS Systems Manager这些配置是存储在中的一组属性 AWS AppConfig。为防止对您的资源进行未经授权的费用，当账户加入可信修正者时，所有支持的 Trusted Advisor 检查都将设置为 “非活动”。入职后，您可以使用 AWS AppConfig 控制台或 API 来管理配置。这些配置可帮助您自动修复特定的 Trusted Advisor 检查，或者评估和手动修复剩余的检查。这些配置是高度可定制的，允许您为每项 Trusted Advisor 检查应用配置。有关更多信息，请参阅 在可信修正器中配置 Trusted Advisor 检查修复。

选择要修复的检查和建议

默认情况下，您的配置中的所有 Trusted Advisor 检查和 Compute Optimizer 建议的修复执行模式均为 “非活动”。这样可以防止未经授权的补救并保护资源。AMS 提供精心策划的 SSM 自动化文档，用于 Trusted Advisor 支票补救。

要选择要使用可信修正者修复的检查，请完成以下步骤：

1. 查看支持的建议Trusted Advisor 和 Compute Optimizer 建议列表或关联的 SSM 自动化文档的名称，以决定要使用 Trusted Remediator 修复哪些检查和建议。
2. 更新您的配置以启用所选 Trusted Advisor 检查的补救功能。有关如何选择支票的说明，请参阅在可信修正器中配置 Trusted Advisor 检查修复。

在 “可信修正者” 中跟踪您的补救措施

更新账户级别配置后，Trusted Remediator 会 OpsItems 为每项补救措施创建。Trusted Remediator 会 OpsItems 根据您的补救计划运行 SSM 文档进行自动修复。有关如何 OpsItems 从 Systems Manager OpsCenter 控制台查看所有补救措施的说明，请参阅在 “可信修正者” 中跟踪补救措施。

在 “可信修正器” 中运行手动修复

您可以手动修复 Trusted Advisor 检查。当您启动手动修复时，可信修正者会创建手动执行 OpsItem。您必须查看并启动 SSM 自动化文档才能修复。 OpsItems有关更多信息，请参阅 在 “可信修正器” 中运行手动修复。

受信任修正者支持的 Compute Optimizer 建议

下表列出了支持的 Compute Optimizer 建议、SSM 自动化文档、预配置的参数以及自动化文档的预期结果。在启用 SSM 自动化文档进行支票补救之前，请查看预期结果，以帮助您根据业务需求了解可能的风险。

确保每个 Compute Optimizer 检查的相应配置规则适用于要为其启用修复的受支持检查。有关更多信息，请参阅选择使用 AWS Compute Optimizer 支 Trusted Advisor 票。

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
规模优化		
亚马逊 EC2 实例建议	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation 根据 Compute Optimizer 的建议更新了亚马逊 EC2 实例类型。如果存在最佳选项，则选择最佳选项，同时保持相同的平台参数（架构、虚拟机管理程序、网络接口、虚拟化类型等）。	• MinimumDaysSinceLastChange：用于指定自上次实例类型更改以来的最小天数的参数。默认值为 7 天。 没有限制 • 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请设置为 “True”。要不创建备份，请将其设置为 “False”。默认为 “真”。 没有限制
Amazon EBS 卷建议	AWSManagedServices-ModifyEBSVolume Amazon EBS 卷是根据 Compute Optimizer 的建议修改的。修改可能	• CreateSnapshot：要在修改卷之前创建快照，请设置为 “True”。要不创建快照，请将其设置为 “False”。默认值为 “真”。 没有限制

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
	包括卷类型、大小、IOPS、卷生成（gp2、gp3 等）。	• VolumeType：所需的卷类型。如果未指定类型，则保留现有类型。 没有限制 • VolumeSize：所需的卷大小，以 GiB 为单位。目标卷大小必须大于或等于该卷的现有大小。如果未指定大小，则保留现有大小。 没有限制 • Iops：请求的每秒 I/O 操作数 (IOPS)。此参数仅对 io1、io2 和 gp3 卷有效。 没有限制 • 吞吐量：为卷预配置的吞吐量，最大为 1000 MiB/s。此参数仅对 gp3 卷有效。 没有限制 • RemediateStackDrift：要启动漂移补救，如果任何漂移是由音量修改引起的，请将其设置为 “True”。要不尝试漂移补救，请将其设置为 “False”。默认为 “真”。 没有限制
Lambda 函数推荐	AWSManagedServices-TrustedRemediatorOptimizeLambdaMemory AWS Lambda 根据 Compute Optimizer 的建议对函数内存进行了优化。	RecommendedMemorySize ：自定义内存大小（如果与推荐的选项不同）。 没有限制
闲置资源		

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
闲置亚马逊 EBS 交易量	AWSManagedServices-DeleteUnusedEBSVolume 未连接的 Amazon EBS 卷将被删除。	• CreateSnapshot：要在删除卷之前创建快照，请设置为 “True”。要不创建快照，请将其设置为 “False”。默认值为 “真”。 没有限制 • MinimumUnattachedDays：删除 Amazon EBS 卷的最短未连接天数，最长为 62 天。默认值为 7。 没有限制
空闲的亚马逊 EC2 实例	AWSManagedServices-StopEC2 实例 闲置的 Amazon EC2 实例将被停止。	ForceStopWithInstanceStore：要强制停止使用实例存储的实例，请设置为 “True”。要不强制停止，请设置为 “False”。默认值为 “False” 可防止实例停止。 没有限制
空闲的亚马逊 RDS 实例	AWSManagedServices-StopIdleRDSInstance 停止闲置的 Amazon RDS 实例。支持的引擎有：MariaDB、微软 SQL Server、MySQL、Oracle、PostgreSQL。本文档不适用于 Aurora MySQL 和 Aurora PostgreSQL。该实例将在最多 7 天内停止并自动重新启动。	不允许使用预配置的参数。 没有限制

Trusted Advisor 受信任修正者支持的检查

下表列出了支持的 Trusted Advisor 检查、SSM 自动化文档、预配置的参数以及自动化文档的预期结果。在启用 SSM 自动化文档进行支票补救之前，请查看预期结果以帮助您根据业务需求了解可能的风险。

对于要为其启用补救功能的受支持检查，请确保每 Trusted Advisor 项检查都有相应的配置规则。有关更多信息，请参阅查看由支持的 AWS Trusted Advisor 支票 AWS Config。如果支票有相应的 AWS Security Hub CSPM 控件，请确保启用了 Security Hub 控件。有关更多信息，请参阅在 Sec urity Hub 中启用控件。有关管理预配置参数的信息，请参阅 Trusted Rem ediator 中的配置 Trusted Advisor 检查修复。

Trusted Advisor 可信修正者支持的成本优化检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Z4 AUBRNSmz 未关联的弹性 IP 地址	AWSManagedServices-TrustedRemediatorReleaseElasticIP 释放未与任何资源关联的弹性 IP 地址。	不允许使用预配置的参数。 没有限制
c18d2gz 150-亚马逊实例已停止 EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime-停止天数的 Amazon EC2 实例终止。	• 创建AMIBefore终止：要在终止 Amazon EC2 实例之前创建实例 AMI 作为备份，请选择`true`。要在终止之前不创建备份，请选择`false`。默认值为 `true`。 • AllowedDays：实例在终止之前处于停止状态的天数。默认值为 30。 没有限制
c18d2gz128 未对生命周期策略进行配置的 Amazon ECR 存储库	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 如果生命周期策略尚不存在，则为指定的存储库创建生命周期策略。	ImageAgeLimit：Amazon ECR 存储库中 “任何” 图像的最大保存期限（以天为单位）(1-365)。 没有限制
DAvU99Dc4C 未充分利用的 Amazon EBS 卷	AWSManagedServices-DeleteUnusedEBSVolume	• CreateSnapshot：如果设置为`true`，则自动化会在删除 Amazon EBS 卷之前创建该卷的

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
	如果过去 7 天内未连接未充分利用的 Amazon EBS 卷，则删除这些卷。默认情况下会创建 Amazon EBS 快照。	快照。默认设置为 `true`。有效值为`true`和`false`（区分大小写）。 • MinimumUnattachedDays：删除 EBS 卷的最少未连接天数，最多 62 天。如果设置为`0`，则 SSM 文档不会检查未连接的时段，如果该卷当前处于未连接状态，则会删除该卷。默认值为`7`。 没有限制
hj m8 LMh88u 闲置的负载均衡器	AWSManagedServices-DeleteIdleClassicLoadBalancer 如果闲置的 Classic Load Balancer 未使用且未注册任何实例，则将其删除。	IdleLoadBalancerDays：Classic Load Balancer 在考虑处于空闲状态之前有 0 个请求的连接的天数。默认值为七天。 如果启用了自动执行，则如果没有活跃的后端实例，则自动化会删除闲置的 Classic 负载均衡器。对于所有具有活跃后端实例但后端实例运行状况不佳的闲置经典负载均衡器，不会使用自动修复，而是创建 OpsItems 用于手动补救的自动修复。
ti39Halfu8 Amazon RDS 闲置数据库实例	AWSManagedServices-StopIdleRDSInstance 过去七天一直处于空闲状态的 Amazon RDS 数据库实例已停止。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
COr6dfpM05 AWS Lambda 内存大小过度配置的函数	AWSManagedServices-ResizeLambdaMemory AWS Lambda 函数的内存大小已调整为由 Trusted Advisor提供的推荐内存大小。	RecommendedMemorySize：Lambda 函数的推荐内存分配。值范围介于 128 和 10240 之间。 如果在自动化运行之前修改了 Lambda 函数的大小，则该自动化可能会使用推荐的值覆盖这些设置。 Trusted Advisor
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-StopEC2Instance（自动和手动执行模式下的默认 SSM 文档。） 使用率低的 Amazon EC2 实例已停止。	ForceStopWithInstanceStore：设置为`true`以强制停止使用实例存储的实例。否则，设置为 `false`。默认值为`false`可防止实例停止。有效值为真或假（区分大小写）。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-ResizeInstanceByOneLevel 在相同的 EC2 实例系列类型中，Amazon 实例按向下调整一个实例类型的大小。实例在调整大小操作期间停止并启动，并在 SSM 文档运行完成后恢复到初始状态。此自动化不支持调整 Auto Scaling 组中的实例的大小。	• MinimumDaysSinceLastChange：自上次实例类型更改以来的最短天数。如果在指定时间内修改了实例类型，则不会更改实例类型。0用于跳过此验证。默认值为 7。 • 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请选择true。要不创建备份，请选择false。默认值为 false。有效值为true和false（区分大小写）。 • ResizeIfStopped：要继续更改实例大小，即使实例处于停止状态，也请选择true。要在实例处于停止状态时不自动调整其大小，请选择false。有效值为true和false（区分大小写）。 没有限制
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-TerminateInstance 如果未加入 Auto Scaling 组且未启用终止保护，则低利用率的 Amazon EC2 实例将被终止。默认情况下会创建 AMI。	创建AMIBefore终止：将此选项设置false为true或可在终止实例之前创建实例 AMI 作为备份。 EC2 默认值为 true。有效值为true和false（区分大小写）。 没有限制
g31sq1e9U Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster 亚马逊 Redshift 集群已暂停。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1cj39rr6v Amazon S3 未完成分段上传中止配置	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 存储桶配置了生命周期规则，用于中止某些天后仍未完成的分段上传。	DaysAfterInitiation：Amazon S3 停止未完成的分段上传的天数。默认设置为 7 天。 没有限制
c1z7kmr00n Amazon 针对实例 EC2 的成本优化建议	使用来自的亚马逊 EC2 实例建议和空闲的亚马逊 EC2 实例受信任修正者支持的 Compute Optimizer 建议。	不允许使用预配置的参数。 没有限制
c1z7kmr02n Amazon EBS 针对卷的成本优化建议	使用来自的 Amazon EBS 交易量建议和空闲亚马逊 EBS 交易量。受信任修正者支持的 Compute Optimizer 建议	不允许使用预配置的参数。 没有限制
c1z7kmr03n Amazon RDS 针对数据库实例的成本优化建议	使用来自的空闲的 Amazon RDS 实例受信任修正者支持的 Compute Optimizer 建议。	不允许使用预配置的参数。 没有限制
c1z7kmr05n AWS Lambda 函数的成本优化建议	使用来自的 Lambda 函数建议。受信任修正者支持的 Compute Optimizer 建议	不允许使用预配置的参数。 没有限制

Trusted Advisor 受信任修正者支持的安全检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 公开的 IAM 访问密钥已停用。	不允许使用预配置的参数。 使用公开的 IAM 访问密钥配置的应用程序无法进行身份验证。
Hs4ma3G127-应启用 API Gateway REST WebSocket 和 API 执行日志记录 相应的 AWS Security Hub CSPM 支票：APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging API 阶段已启用执行日志记录。	LogLevel: 用于启用执行日志记录的日志级别，ERROR-仅对错误启用日志记录。 INFO-已为所有事件启用日志功能。 要启用执行日志，您必须授予 API Gateway 读取和写入账户日志的权限，有关详细信息，请参阅 APIs 在 API Gateway 中设置 REST CloudWatch 日志记录。 CloudWatch
Hs4ma3G129-API Gateway REST API 阶段应该启用追踪 AWS X-Ray 相应的 AWS Security Hub CSPM 支票：APIGateway.3	AWSManagedServices-EnableApiGateWayXRayTracing 在 API 阶段已启用 X 射线追踪。	不允许使用预配置的参数。 没有限制
Hs4Ma3G202-API Gateway	AWSManagedServices-EnableAPIGatewayCacheEncryption	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
REST API 缓存数据应静态加密 相应的 AWS Security Hub CSPM 支票：APIGateway.5	如果 API Gateway REST API 阶段启用了缓存，则为 API Gateway REST API 缓存数据启用静态加密。	
Hs4ma3G177- 相应的 AWS Security Hub CSPM 检查-与负载均衡器关联的 Auto Scaling 组应使用负载均衡器运行状况检查。AutoScaling1	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck 已为 Auto Scaling 组启用了 Elastic Load Balancing 运行状况检查。	HealthCheckGracePeriod：Auto Scaling 在检查已投入使用的亚马逊弹性计算云实例的运行状况之前等待的时间，以秒为单位。 如果连接到 Auto Scaling 组的任何 Elastic Load Balancing 负载均衡器报告运行状况不佳，则启用 Elastic Load Balancing 运行状况检查可能会导致替换正在运行的实例。有关更多信息，请参阅将 Elastic Load Balancing 负载均衡器附加到您的 Auto Scaling 组
Hs4ma3G245-CloudFormation 堆栈应与亚马逊简单通知服务集成 相应的 AWS Security Hub CSPM 支票：CloudFormation.1	AWSManagedServices-EnableCFNStackNotification 将 CloudFormation 堆栈与 Amazon SNS 主题关联以获得通知。	通知ARNs：要与 ARNs 选定 CloudFormation 堆栈关联的 Amazon SNS 主题。 要启用 auto 修复，必须提供`NotificationARNs` 预配置的参数。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G210-CloudFront 发行版应该启用日志记录 相应的 AWS Security Hub CSPM 支票：CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging 已为 Amazon CloudFront 分配启用日志记录。	• BucketName：您要在其中存储访问日志的 Amazon S3 存储桶的名称。 • S3KeyPrefix：亚马逊 CloudFront 分配日志在 S3 存储桶中的位置的前缀。 • IncludeCookies：表示是否在访问日志中包含 Cookie。 要启用 auto 修复，必须提供以下预配置的参数： • BucketName • S3KeyPrefix • IncludeCookies 有关修正限制，请参阅如何为我的 CloudFront 分配开启日志记录？
Hs4ma3G109-应启用 CloudTrail 日志文件验证 相应的 AWS Security Hub CSPM 支票：CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation 启用 CloudTrail 跟踪日志验证。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G108 —— CloudTrail 轨迹应与亚马逊日志集成 CloudWatch 相应的 AWS Security Hub CSPM 支票：CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 已与 CloudWatch 日志集成。	• CloudWatchLogsLogGroupName：将 CloudWatch 日志传送到的日志 CloudTrail 日志组的名称。您必须使用账户中存在的日志组。 • CloudWatchLogsRoleName：CloudWatch 日志终端节点要代入的写入用户日志组的 IAM 角色的名称。您必须使用账户中存在的角色。 要启用 auto 修复，必须提供以下预配置的参数： • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName
Hs4ma3G217-CodeBuild 项目环境应该有日志配置 AWS 相应的 AWS Security Hub CSPM 支票：CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig 启用 CodeBuild 项目日志记录。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G306-Neptune 数据库集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：documen tDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot 从 Amazon DocumentDB 手动集群快照中移除公共访问权限。	不允许使用预配置的参数。 没有限制
Hs4ma3G308-亚马逊 DocumentDB 集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：documen tDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection 为亚马逊文档数据库集群启用删除保护。	不允许使用预配置的参数。 没有限制
Hs4ma3G323-DynamoDB 表应该启用删除保护 相应的 AWS Security Hub CSPM 检查：dynam odB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection 为非 AMS DynamoDB 表启用删除保护。	不允许使用预配置的参数。 没有限制
eps02jt06w-亚马逊 EBS 公开快照	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot 已禁用 Amazon EBS 快照的公共访问权限。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G118-VPC 默认安全组不应允许入站或出站流量 相应的 AWS Security Hub CSPM 支票：EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG 默认安全组中的所有入口和出口规则都将被删除。	不允许使用预配置的参数。 没有限制
Hs4Ma3G117-附加的 EBS 卷应在静态状态下进行加密 相应的 AWS Security Hub CSPM 支票：EC2.3	AWSManagedServices-EncryptInstanceVolume 实例上附加的 Amazon EBS 卷已加密。	• KMSKeyID：用于加密卷的 AWS KMS 密钥 ID 或 ARN。 • DeleteStaleNonEncryptedSnapshotBackups：一个标志，用于决定是否应删除未加密的旧卷的快照备份。 作为修复的一部分，实例将重新启动，如果`DeleteStaleNonEncryptedSnapshotBackups` 将其设置为有助于恢复，则可以进行`false`回滚。
Hs4ma3G120-应在指定的时间段后移除已停止的 EC2 实例 相应的 AWS Security Hub CSPM 支票：EC2.4	AWSManagedServices-TerminateInstance（auto 和手动执行模式的默认 SSM 文档） 停止 30 天的 Amazon EC2 实例将被终止。	创建AMIBefore终止:. 要在终止实例之前创建实例 AMI 作为备份，请选择`true`。 EC2 要在终止之前不创建备份，请选择`false`。默认值为`true`。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G120-应在指定的时间段后移除已停止的 EC2 实例 相应的 AWS Security Hub CSPM 支票：EC2.4	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime-在 Security Hub 中定义的停止天数（默认值为 30）的亚马逊 EC2 实例将被终止。	创建AMIBefore终止：要在终止实例之前创建实例 AMI 作为备份，请选择`true`。 EC2 要在终止之前不创建备份，请选择`false`。默认值为`true`。 没有限制
Hs4ma3G121-应启用 EBS 默认加密 相应的 AWS Security Hub CSPM 支票：EC2.7	AWSManagedServices-EncryptEBSByDefault 默认情况下，Amazon EBS 加密是针对特定的 AWS 区域	不允许使用预配置的参数。 默认加密是区域特定的设置。如果您为某个区域启用该功能，则无法为该区域的单个卷或快照禁用该功能。
Hs4Ma3G124-EC2 亚马逊实例应使用实例元数据服务版本 2 () IMDSv2 相应的 AWS Security Hub CSPM 支票：EC2.8	AWSManagedServices-TrustedRemediator启用EC2实例 IMDSv2 Amazon EC2 实例使用实例元数据服务版本 2 (IMDSv2)。	• IMDSv1MetricCheckPeriod：分析 IMDSv1 使用情况指标的天数 (42-455) CloudWatch。如果 Amazon EC2 实例是在指定时间段内创建的，则分析将从实例的创建日期开始。 • HttpPutResponseHopLimit：实例元数据令牌允许的最大网络跳数。可以在1和2跳数之间配置此值。跳跃限制为将令牌访问1限制为直接在实例上运行的进程，而跳跃限制为则2允许从实例上运行的容器进行访问。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G207-EC2 子网不应自动分配公有 IP 地址 相应的 AWS Security Hub CSPM 支票：EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4个地址 VPC 子网配置为不自动分配公有 IP 地址。	不允许使用预配置的参数。 没有限制
Hs4ma3G209-未使用的网络访问控制列表已删除 相应的 AWS Security Hub CSPM 支票：EC2.16	AWSManagedServices-DeleteUnusedNACL 删除未使用的网络 ACL	不允许使用预配置的参数。 没有限制
Hs4ma3G215-应移除未使用的 EC2 亚马逊安全组 相应的 AWS Security Hub CSPM 支票：EC2.22	AWSManagedServices-DeleteSecurityGroups 删除未使用的安全组。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G247-Amazon Transit G EC2 ateway 不应自动接受 VPC 连接请求 相应的 AWS Security Hub CSPM 支票：EC2.23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach-禁用自动接受指定非 AMS Amazon T EC2 ransit Gateway 的 VPC 连接请求。	不允许使用预配置的参数。 没有限制
Hs4Ma3G235-ECR 私有存储库应配置标签不可变性 相应的 AWS Security Hub CSPM 支票：ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability 将指定存储库的图像标签可变性设置设置为 IMMUTABLE。	不允许使用预配置的参数。 没有限制
Hs4Ma3G216-ECR 存储库应至少配置一个生命周期策略 相应的 AWS Security Hub CSPM 支票：ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 存储库已配置生命周期策略。	LifecyclePolicyText：要应用于存储库的 JSON 存储库策略文本。 要启用 auto 修复，必须提供以下预配置的参数： LifecyclePolicyText

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G325-EKS 集群应启用审核日志记录 相应的 AWS Security Hub CSPM 支票：EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog 已为 EKS 集群启用审核日志。	不允许使用预配置的参数。 没有限制
Hs4Ma3G183-应用程序负载均衡器应配置为丢弃 HTTP 标头 相应的 AWS Security Hub CSPM 支票：ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer 配置为无效的标头字段。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G184-应启用应用程序负载均衡器和经典负载均衡器日志记录 相应的 AWS Security Hub CSPM 支票：ELB.5	AWSManagedServices-EnableELBLogging（auto 和手动执行模式的默认 SSM 文档） 应用程序负载均衡器和经典负载均衡器日志记录已启用。	• BucketName：存储桶名称（不是 ARN）。确保已正确配置存储桶策略以进行日志记录。 • S3KeyPrefix：Elastic Load Balancing 日志在 Amazon S3 存储桶中的位置的前缀。 要启用 auto 修复，必须提供以下预配置的参数： • BucketName • S3KeyPrefix Amazon S3 存储桶必须具有存储桶策略，该策略授予 Elastic Load Balancing 将访问日志写入存储桶的权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G184-应启用应用程序负载均衡器和经典负载均衡器日志记录 相应的 AWS Security Hub CSPM 支票：ELB.5	AWSManagedServices-EnableELBLoggingV2 应用程序负载均衡器和经典负载均衡器日志记录已启用。	• TargetBucketTagKey：用于标识目标 Amazon S3 存储桶的标签名称（区分大小写）。使用它`TargetBucketTagValue` 来标记将用作访问日志的目标存储桶的存储桶。 • TargetBucketTagValue：用于标识目标 Amazon S3 存储桶的标签值（区分大小写）。使用它 `TargetBucketTagKey` 来标记将用作访问日志的目标存储桶的存储桶。 • S3BucketPrefix：Amazon S3 存储桶的前缀（逻辑层次结构）。您指定的前缀不得包含字符串 `AWSLogs`。要获取更多信息，请参阅使用前缀整理对象。 要启用 auto 修复，必须提供以下预配置的参数： • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Amazon S3 存储桶必须具有存储桶策略，该策略授予 Elastic Load Balancing 将访问日志写入存储桶的权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G326-应启用亚马逊 EMR 屏蔽公开访问设置 相应的 AWS Security Hub CSPM 支票：EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess 该账户的 Amazon EMR 屏蔽公开访问设置已开启。	不允许使用预配置的参数。 没有限制
Hs4ma3G135-AWS KMS 密钥不应无意中删除 相应的 AWS Security Hub CSPM 支票：KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 密钥删除已取消。	不允许使用预配置的参数。 没有限制
Hs4ma3G299-Amazon DocumentDB 手动集群快照不应公开 相应的 AWS Security Hub CSPM 支票：Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection 为 Amazon Neptune 集群启用删除保护。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G319-Network Firewall 防火墙应该启用删除保护 相应的 AWS Security Hub CSPM 支票：NetworkFirewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection-为 AWS Network Firewall 启用删除保护。	不允许使用预配置的参数。 没有限制
Hs4ma3G223-OpenSearch 域名应加密节点之间发送的数据 相应的 AWS Security Hub CSPM 支票：OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 已为域启用节点到节点加密。	不允许使用预配置的参数。 启用 node-to-node加密后，您无法禁用该设置。取而代之的是，手动拍摄加密域的快照，创建另一个域，迁移您的数据，然后删除旧域名。
Hs4ma3G222-应该启用记录到日志的 OpenSearch 域名错误 CloudWatch 相应的 AWS Security Hub CSPM 支票：Opensearch.4	AWSManagedServices-EnableOpenSearchLogging 已为该 OpenSearch 域启用错误日志记录。	CloudWatchLogGroupArn：亚马逊 CloudWatch 日志组的 ARN。 要启用 auto 修复，必须提供以下预配置的参数：CloudWatchLogGroupArn。 Amazon CloudWatch 资源策略必须配置权限。有关更多信息，请参阅 Amazon OpenSearch 服务用户指南中的启用审计日志

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G221-OpenSearch 域名应启用审核日志 相应的 AWS Security Hub CSPM 支票：Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 域配置为启用审核日志。	CloudWatchLogGroupArn：要向其发布 CloudWatch 日志的日志组的 ARN。 要启用 auto 修复，必须提供以下预配置的参数：CloudWatchLogGroupArn Amazon CloudWatch 资源策略必须配置权限。有关更多信息，请参阅 Amazon OpenSearch 服务用户指南中的启用审计日志
Hs4Ma3G220-与 OpenSearch 域名的连接应使用 TLS 1.2 进行加密 相应的 AWS Security Hub CSPM 支票：Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 策略设置为 “policy-min-tls-1-2-2019-07”，并且只允许通过 HTTPS (TLS) 进行加密连接。	不允许使用预配置的参数。 使用 TLS 1.2 需要与 OpenSearch 域建立连接。加密传输中数据可能会影响性能。使用此功能测试您的应用程序，以了解 TLS 的性能状况和影响。
Hs4ma3G194-亚马逊 RDS 快照应该是私有的 相应的 AWS Security Hub CSPM 支票：RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公共访问已禁用。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G192-RDS 数据库实例应禁止公共访问，具体取决于配置 PubliclyAccessible AWS 相应的 AWS Security Hub CSPM 支票：RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance 在 RDS 数据库实例上禁用公共访问权限。	不允许使用预配置的参数。 没有限制
Hs4Ma3G189-为亚马逊 RDS 数据库实例配置了增强监控 相应的 AWS Security Hub CSPM 支票：RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring 为 Amazon RDS 数据库实例启用增强监控	• MonitoringInterval：为数据库实例收集增强监控指标的时间间隔，以秒为单位。有效间隔为 0、1、5、10、15、30 和 60。要禁用收集增强监控指标，请指定 0。 • MonitoringRoleName：允许 Amazon RDS 向 Amazon L CloudWatch ogs 发送增强型监控指标的 IAM 角色的名称。如果未指定角色，`rds-monitoring-role` 则使用或创建默认角色（如果该角色不存在）。 如果在自动化执行之前启用了增强监控，则此自动化可能会使用在预配置参数中配置的 MonitoringInterval 和 MonitoringRoleName 值来覆盖这些设置。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G190-Amazon RDS 集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection 已为 Amazon RDS 集群启用删除保护。	不允许使用预配置的参数。 没有限制
Hs4Ma3G198-Amazon RDS 数据库实例应启用删除保护 相应的 AWS Security Hub CSPM 支票：RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection 已为 Amazon RDS 实例启用删除保护。	不允许使用预配置的参数。 没有限制
Hs4Ma3G199-RDS 数据库实例应将日志发布到日志 CloudWatch 相应的 AWS Security Hub CSPM 支票：RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports 已为 RDS 数据库实例或 RDS 数据库集群启用 RDS 日志导出。	不允许使用预配置的参数。 需要服务相关角色 AWSServiceRoleForRDS。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G160-应为 RDS 实例配置 IAM 身份验证 相应的 AWS Security Hub CSPM 支票：RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management 已为 RDS 实例启用身份验证。	ApplyImmediately: 表示是否尽快异步应用此请求中的修改和任何待处理的修改。要立即应用更改，请选择`true`。要在下一个维护时段安排更改，请选择`false`。 没有限制
Hs4Ma3G161-应为 RDS 集群配置 IAM 身份验证 相应的 AWS Security Hub CSPM 支票：RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication 已为 RDS 集群启用了 IAM 身份验证。	ApplyImmediately: 表示是否尽快异步应用此请求中的修改和任何待处理的修改。要立即应用更改，请选择`true`。要在下一个维护时段安排更改，请选择`false`。 没有限制
Hs4Ma3G162-应启用 RDS 自动次要版本升级 相应的 AWS Security Hub CSPM 支票：RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS 的自动次要版本升级配置已启用。	不允许使用预配置的参数。 Amazon RDS 实例必须处于`available` 状态才能进行此修复。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G163-RDS 数据库集群应配置为将标签复制到快照 相应的 AWS Security Hub CSPM 支票：RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagtosnapshot Amazon RDS 集群的设置已启用。	不允许使用预配置的参数。 Amazon RDS 实例必须处于可用状态才能进行此修复。
Hs4Ma3G164-RDS 数据库实例应配置为将标签复制到快照 相应的 AWS Security Hub CSPM 支票：RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot Amazon RDS 的设置已启用。	不允许使用预配置的参数。 Amazon RDS 实例必须处于可用状态才能进行此修复。
rss93 HQwa1 Amazon RDS 公有快照	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公共访问已禁用。	不允许使用预配置的参数。 没有限制
Hs4ma3G103-亚马逊 Redshift 集群应禁止公众访问 相应的 AWS Security Hub CSPM 支票：Redshi ft.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster 亚马逊 Redshift 集群上的公共访问已禁用。	不允许使用预配置的参数。 禁用公共访问会阻止所有来自互联网的客户端。而且，Amazon Redshift 集群在几分钟内处于修改状态，同时修复会禁用集群上的公共访问权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G106-亚马逊 Redshift 集群应启用审核日志 相应的 AWS Security Hub CSPM 支票：Redshi ft.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging 在维护时段内，您的 Amazon Redshift 集群启用了审核日志。	不允许使用预配置的参数。 要启用 auto 修复，必须提供以下预配置的参数。 BucketName: 存储桶必须位于同一个桶中 AWS 区域。集群必须具有读取存储桶和放置对象权限。 如果在自动化执行之前启用了 Redshift 集群日志记录，则该自动化可能会使用在预配置参数中配置的 `BucketName` 和`S3KeyPrefix` 值覆盖日志设置。
Hs4ma3G105-Amazon Redshift 应该启用自动升级到主要版本的功能 相应的 AWS Security Hub CSPM 支票：Redshi ft.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-在维护时段内，主要版本升级会自动应用于集群。Amazon Redshift 集群不会立即停机，但是如果升级到主要版本，您的 Amazon Redshift 集群可能会在其维护时段内停机。	不允许使用预配置的参数。 没有限制
Hs4ma3G104-亚马逊 Redshift 集群应使用增强型 VPC 路由 相应的 AWS Security Hub CSPM 支票：Redshi ft.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting 亚马逊 Redshift 集群已启用增强型 VPC 路由。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G173-S3 阻止公共访问设置应在存储桶级别启用 相应的 AWS Security Hub CSPM 支票：S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Amazon S3 存储桶采用存储桶级别的公共访问封禁。	不允许使用预配置的参数。 此补救措施可能会影响 S3 对象的可用性。有关 Amazon S3 如何评估访问权限的信息，请参阅阻止公众访问您的 Amazon S3 存储。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G230-S3 存储桶服务器访问日志应启用 相应的 AWS Security Hub CSPM 支票：S3.9	AWSManagedServices-EnableBucketAccessLogging（auto 和手动执行模式的默认 SSM 文档） Amazon S3 服务器访问日志已启用。	• TargetBucket：用于存储服务器访问日志的 S3 存储桶的名称。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式（值区分大小写）。要对日志对象使用 S3 密钥的简单格式，请选择`SimplePrefix` 。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。`PartitionedPrefixEventTime` 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。`PartitionedPrefixDeliveryTime` 有效值为 `SimplePrefix` 、`PartitionedPrefixEventTime` 和 `PartitionedPrefixDeliveryTime` 。 要启用 auto 修复，必须提供以下预配置的参数：TargetBucket。 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G230 — 应启用 S3 存储桶服务器访问日志记录 相应的 AWS Security Hub CSPM 支票：S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2-已启用 Amazon S3 存储桶日志记录。	• TargetBucketTagKey：用于标识目标存储桶的标签名称（区分大小写）。使用此和标记TargetBucketTagValue要用作访问日志记录的目标存储桶的存储桶。 • TargetBucketTagValue：标签值（区分大小写），用于标识目标存储桶、使用该值以及标记TargetBucketTagKey要用作访问日志记录的目标存储桶的存储桶。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式（值区分大小写）：要使用日志对象的 S3 密钥的简单格式，请选择SimplePrefix。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。PartitionedPrefixEventTime要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。PartitionedPrefixDeliveryTime默认值为 PartitionedPrefixEventTime。 要启用 auto 修复，必须提供以下参数：TargetBucketTagKey 和TargetBucketTagValue。 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Pfx0 RwqBli Amazon S3 存储桶权限	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess 阻止公有访问	不允许使用预配置的参数。 此检查由多个警报标准组成。这种自动化修复了公共访问问题。 Trusted Advisor 不支持修复标记为的其他配置问题。此修复确实支持修复 AWS 服务 已创建的 S3 存储桶（例如 cf-templates-000000000000）。
Hs4Ma3G272-用户不应拥有笔记本实例的根访问权限 SageMaker 相应的 AWS Security Hub CSPM 支票：SageMaker.3	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess 对于 SageMaker 笔记本实例，用户的 root 访问权限已禁用。	不允许使用预配置的参数。 如果 SageMaker 笔记本实例 InService 处于状态，则此补救措施会导致中断。
Hs4Ma3G179-SNS 话题应使用静态加密 AWS KMS 相应的 AWS Security Hub CSPM 支票：SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest SNS 主题配置了服务器端加密。	KmsKeyId：适用于 Amazon SNS 的 AWS 托管客户主密钥 (CMK) 或用于服务器端加密 (SSE) 的自定义 CMK 的 ID。默认值设置为`alias/aws/sns`。 如果使用自定义 AWS KMS 密钥，则必须为其配置正确的权限。有关更多信息，请参阅 Amazon SNS 主题的启用服务器端加密 (SSE)

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G158-SSM 文档不应公开 相应的 AWS Security Hub CSPM 支票：SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing-禁用 SSM 文档的公开共享。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G136-亚马逊 SQS 队列应在静态时加密 相应的 AWS Security Hub CSPM 支票：SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest 亚马逊 SQS 中的消息经过加密。	• SqsManagedSseEnabled：设置`true`为使用Amazon SQS拥有的加密密钥启用服务器端队列加密，设置`false`为使用密钥启用服务器端队列加密。 AWS KMS • KMSKeyID：Amazon SQS 的 AWS 托管客户主密钥 (CMK) 或用于队列服务器端加密的自定义 CMK 的 ID 或别名。如果未提供，alias/aws/sqs则使用。 • KmsDataKeyReusePeriodSeconds：在再次调用之前，Amazon SQS 可以重复使用数据密钥来加密或解密消息的时间长度，以秒为单位。 AWS KMS 一个表示秒数的证书，介于 60 秒（1 分钟）和 86400 秒（24 小时）之间。如果设置为，`SqsManagedSseEnabled` 则忽略此设置`true`。 匿名 SendMessage 和对加密队列的 ReceiveMessage 请求将被拒绝。针对启用了 SSE 的队列的所有请求都必须使用 HTTPS 和 Signature Version 4。

Trusted Advisor 可信修正者支持的容错检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz138 亚马逊 DynamoDB 恢复 Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR 启用 DynamoDB 表的 point-in-time恢复。	不允许使用预配置的参数。 没有限制
r365s2qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Amazon S3 存储桶版本控制已启用。	不允许使用预配置的参数。 此修复不支持修复 AWS 服务 已创建的 S3 存储桶（例如 cf-templates-000000000000）。
BueAdj7nrp Amazon S3 存储桶日志记录	AWSManagedServices-EnableBucketAccessLogging 已启用 Amazon S3 存储桶日志记录。	• TargetBucket：用于存储服务器访问日志的 S3 存储桶的名称。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式，要使用日志对象的 S3 密钥的简单格式，请选择`SimplePrefix` 。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。`PartitionedPrefixEventTime` 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。`PartitionedPrefixDeliveryTime` 默认值为 `PartitionedPrefixEventTime` 。有效值为`SimplePrefix` 、`PartitionedPrefixEventTime` 和`PartitionedPrefixDeliveryTime` （区分大小写）。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
		要启用 auto 修复，必须提供以下预配置的参数： • TargetBucket 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。
f2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ 已启用多可用区部署。	不允许使用预配置的参数。 在此更改期间，性能可能会降低。
H7 IgTzj TYb Amazon EBS Snapshots	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot 亚马逊 EBSsnapshots 已创建。	不允许使用预配置的参数。 没有限制
op QPADk zvH RDS 备份	AWSManagedServices-EnableRDSBackupRetention 已为数据库启用 Amazon RDS 备份保留功能。	• BackupRetentionPeriod：保留自动备份的天数 (1-35)。 • ApplyImmediately：表示是否尽快异步应用 RDS 备份保留期更改和任何待处理的修改。`true`选择立即应用更改，或者`false`将更改安排到下一个维护时段。 如果将`ApplyImmediately` 参数设置为`true`，则数据库上待处理的更改将与 RDSBackup 保留设置一起应用。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt013 Amazon RDS 数据库实例已关闭存储自动扩缩功能	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling-已为 Amazon RDS 数据库实例启用存储自动扩展。	• MaxAllocatedStorageIncrease Percentage: 电流的增加百分比 AllocatedStorage，用于设置 MaxAllocatedStorage。默认值设置为26。 您必须将最大存储阈值设置为比当前分配的存储空间至少多 10%。最佳做法是将最大存储阈值设置为至少 26%。有关详细信息，请查看使用 Amazon Relational Database Service 存储自动扩展功能自动管理容量。 没有限制
7q GXs KIUw Classic Load Balancer Connection 耗尽	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Classic Load Balancer 已启用连接耗尽功能。	ConnectionDrainingTimeout：取消注册实例之前保持现有连接打开状态的最长时间（以秒为单位）。默认设置为300秒。 没有限制
c18d2gz106 计划中 AWS Backup 未包含亚马逊 EBS	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS 已包含在 AWS Backup 计划中。	补救措施使用以下标签对标记 Amazon EBS 卷。标签对必须符合的基于标签的资源选择标准。 AWS Backup • TagKey • TagValue 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz107 计划中未包含亚马逊 DynamoDB 表 AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan 计划中包含亚马逊 DynamoDB 表。AWS Backup	补救措施使用以下标签对标记 Amazon DynamoDB。标签对必须符合的基于标签的资源选择标准。 AWS Backup • TagKey • TagValue 没有限制
c18d2gz117 AWS Backup 计划中未包含亚马逊 EFS	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS 包含在 AWS Backup 计划中。	补救措施使用以下标签对 Amazon EFS 进行标记。标签对必须符合的基于标签的资源选择标准。 AWS Backup • TagKey • TagValue 没有限制
c18d2gz105 网络负载均衡器跨区域负载均衡	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing 在 Network Load Balancer 上启用了跨区域负载平衡。	不允许使用预配置的参数。 没有限制
c1qf5bt026 亚马逊 RDS `synchronous_commit` 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数`synchronous_commit` 已开启。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt030 亚马逊 RDS `innodb_flush_log_at_trx_commit` 参数不是 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 对`innodb_flush_log_at_trx_commit` 于 Amazon RDS1，参数设置为。	不允许使用预配置的参数。 没有限制
c1qf5bt031 亚马逊 RDS `sync_binlog` 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数`sync_binlog` 已开启。	不允许使用预配置的参数。 没有限制
c1qf5bt036 Amazon RDS `innodb_default_row_format` 参数设置不安全	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 对`innodb_default_row_format` 于 Amazon RDS`DYNAMIC`，参数设置为。	不允许使用预配置的参数。 没有限制
c18d2gz144 未启用 Amazon EC2 详细监控	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring 已为 Amazon 启用详细监控 EC2。	不允许使用预配置的参数。 没有限制

Trusted Advisor 可信修正者支持的性能检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
COr6dfpM06 AWS Lambda 内存大小的函数配置不足	AWSManagedServices-ResizeLambdaMemory Lambda 函数的内存大小已调整为提供的建议内存大小。 Trusted Advisor	RecommendedMemorySize：Lambda 函数的推荐内存分配。值范围介于 128 和 10240 之间。 如果在自动执行之前修改了 Lambda 函数的大小，则此自动化可能会使用推荐的值覆盖设置。 Trusted Advisor
ZRxQlPsb6c 高利用率 Amazon EC2 实例	AWSManagedServices-ResizeInstanceByOneLevel 在相同的 EC2 实例系列中，Amazon 实例按一种实例类型向上调整大小。在调整大小操作期间，实例将停止并启动，并在执行完成后返回到初始状态。此自动化不支持调整 Auto Scaling 组中的实例的大小。	• MinimumDaysSinceLastChange：自上次实例类型更改以来的最短天数。如果在指定时间内修改了实例类型，则不会更改实例类型。0用于跳过此验证。默认值为 7。 • 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请选择true。要不创建备份，请选择false。默认值为 false。有效值为true和false（区分大小写）。 • ResizeIfStopped：要继续更改实例大小，即使实例处于停止状态，也请选择true。要在实例处于停止状态时不自动调整其大小，请选择false。有效值为true和false（区分大小写）。 没有限制
c1qf5bt021 使用小于最佳值的 Amazon RDS	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
innodb_change_buffering 参数	对于 Amazon RDS，innodb_change_buffering 参数NONE的值设置为。	
c1qf5bt025 亚马逊 RDS autovacuum 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数autovacuum 已开启。	不允许使用预配置的参数。 没有限制
c1qf5bt028 亚马逊 RDS enable_indexonlyscan 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数enable_indexonlyscan 已开启。	不允许使用预配置的参数。 没有限制
c1qf5bt029 亚马逊 RDS enable_indexscan 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数enable_indexscan 已开启。	不允许使用预配置的参数。 没有限制
c1qf5bt032 亚马逊 RDS innodb_stats_persistent 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数innodb_stats_persistent 已开启。	不允许使用预配置的参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt037 亚马逊 RDS general_logging 参数已开启	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 亚马逊 RDS 的参数general_logging 已关闭。	不允许使用预配置的参数。 没有限制

Trusted Advisor 受信任修正者支持的服务限制检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
ln7rr0l7j9 EC2-VPC 弹性 IP 地址	AWSManagedServices-UpdateVpcElasticIPQuota 请求对 EC2-VPC 弹性 IP 地址设置新的限制。默认情况下，该限制会增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
km7qq0l7j9 VPC 互联网网关	AWSManagedServices-IncreaseServiceQuota-请求对 VPC 互联网网关设置新的限制。默认情况下，该限制增加三个。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
jl7pp0l7j9 VPC	AWSManagedServices-IncreaseServiceQuota 请求对 VPC 设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
fw7hh0l7j9	AWSManagedServices-IncreaseServiceQuota	增量：要增加当前配额的数字。默认值为 3。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Auto Scaling 组	请求对 Auto Scaling 组设置新的限制。默认情况下，该限制增加 3。	如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
3njm0 DJQO9 RDS 选项组	AWSManagedServices-IncreaseServiceQuota 请求对 Amazon RDS 选项组设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
EM8b3yLRTr ELB Application Load Balancer	AWSManagedServices-IncreaseServiceQuota 请求对 ELB 应用程序负载均衡器设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
8wiQ K YSt25 ELB Network Load Balancer	AWSManagedServices-IncreaseServiceQuota 请求对 ELB 网络负载均衡器设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用0K状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。

Trusted Advisor 可信修正者支持的卓越运营检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz125 Amazon API Gateway 未记录执行日志	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging API 阶段已启用执行日志记录。	不允许使用预配置的参数。 要启用执行日志，您必须授予 API Gateway 读取和写入账户日志的权限，有关详细信息，请参阅 APIs

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
		在 API Gateway 中设置 REST CloudWatch 日志记录。 CloudWatch
c18d2gz168 没有为负载均衡器启用 Elastic Load Balancing 删除保护	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection-Elastic Load Balancer 的删除保护已开启。	不允许使用预配置的参数。 没有限制
c1qf5bt012 Amazon RDS Performance Insights	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights 亚马逊 RDS 的 Performance Insights 已开启。	• PerformanceInsightsRetentionPeriod：保留 Performance Insights 数据的天数。有效值：7或月 * 31，其中月是 1-23 之间的月数。示例：93（3 个月 * 31）、341（11 个月 * 31）、589（19 个月 * 31）或731。 • PerformanceInsightsKMSKeyID：Performance Insights 数据加密的密 AWS KMS 钥 ID。如果您没有为 PerformanceInsights KMSKey ID 指定值，则 Amazon RDS 将使用您的默认 AWS KMS 密钥。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1fd6b96l4 已启用 Amazon S3 访问日志	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 Amazon S3 存储桶访问日志已启用。	• TargetBucketTagValue：标签值（区分大小写），用于标识目标存储桶、使用该值以及标记 TargetBucketTagKey 要用作访问日志记录的目标存储桶的存储桶。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式（值区分大小写）。要对日志对象使用 S3 密钥的简单格式，请选择`SimplePrefix` 。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。`PartitionedPrefixEventTime` 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。`PartitionedPrefixDeliveryTime` 有效值为 `SimplePrefix` 、`PartitionedPrefixEventTime` 和 `PartitionedPrefixDeliveryTime` 。 要启用 auto 修复，必须提供以下预配置的参数：TargetBucketTagKey 和。TargetBucketTagValue 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。

在可信修正器中配置 Trusted Advisor 检查修复

配置 AWS AppConfig 作为可信修正者应用程序的一部分存储在中。每个 Trusted Advisor 检查类别都有单独的配置文件。有关 Trusted Advisor 类别的更多信息，请参阅查看支票类别。

您可以基于每个资源或每个 Trusted Advisor 检查来配置修复。您可以使用资源标签来应用例外。

> **Note**
>
> 目前使用配置了对 Trusted Advisor 发现结果的补救 AWS AppConfig，目前已完全支持此功能。AMS 预计，这种情况将来会改变。最佳做法是避免构建依赖的自动化 AWS AppConfig，因为这种方法可能会发生变化。请注意，为了兼容性，将来可能需要更新或修改围绕当前 AWS AppConfig 实现构建的自动化。
> Compute Optimizer-> EC2 实例功能标志有额外的参数：
>
> - allow-upscal e 允许配置不足但未经过优化的高档实例。 EC2 默认值为“false”。
> - min-savings-opportunity-percentage自动修复的最低节省百分比机会。默认值为 10%

默认补救配置

单个 Trusted Advisor 检查的配置存储为 AWS AppConfig 标志。旗帜名称与支票名称相匹配。每个检查配置都包含以下属性：

- 执行模式：确定可信修正者如何执行默认修复：
  - 自动：Trusted Remediator 通过创建资源来自动修复资源 OpsItem，运行 SSM 文档，然后在成功执行 OpsItem 后解决问题。
  - 手动： OpsItem 已创建，但是 SSM 文档不会自动执行。您可以在 AWS Systems Manager OpsCenter 控制台中查看并手动运行 SSM 文档。 OpsItem
  - 有条件的：默认情况下，修正处于禁用状态。您可以使用标签为特定资源启用它。有关更多信息，请参阅以下各节使用资源标签自定义补救措施和使用资源覆盖标签自定义补救措施。
  - 非活动：不会进行修复， OpsItem 也不会创建任何修复。对于设置为非活动状态的 Trusted Advisor 支票，您无法覆盖其执行模式。
- 预配置参数：输入自动修复所需的 SSM 文档参数的值，格式为，用逗号 (`Parameter=Value,`) 分隔。有关每Trusted Advisor 受信任修正者支持的检查项检查的关联 SSM 文档支持的预配置参数，请参阅。

- alternative-automation-document：此属性有助于用另一个支持的文档覆盖现有的自动化文档（如果可用于特定检查）。默认情况下，此属性处于未选中状态。

> **Note**
>
> 该`alternative-automation-document`属性不支持自定义自动化文档。您可以使用中列出的现有受支持的可信修正者自动化文档。Trusted Advisor 受信任修正者支持的检查
> 例如，为了便于检查`Qch7DwouX1`，有三个关联的 SSM 文档： AWSManagedServices-StopEC2Instance AWSManagedServices-ResizeInstanceByOneLevel、和。AWSManagedServices-TerminateInstance的值`alternative-automation-document`可以是 AWSManagedServices-ResizeInstanceByOneLevel 或 AWSManagedServices-TerminateInstance （AWSManagedServices-StopEC2Instance 是要修复`Qch7DwouX1`的默认 SSM 文档）。

每个属性的值必须与该属性的约束条件相匹配。

> **Tip**
>
> 在为 Trusted Advisor 检查应用默认配置之前，最好考虑使用以下各节中描述的资源标记和资源覆盖功能。默认配置适用于账户内的所有资源，这可能并非在所有情况下都是理想的。

以下是控制台屏幕截图示例，其中执行模式设置为 “手动”，且属性与其约束条件相匹配。

使用资源标签自定义补救措施

校验配置中的automated-for-tagged-only和manual-for-tagged-only属性允许您指定资源标签，说明如何修复单个检查。当您需要对共享相同标签的一组资源应用一致的修复行为时，最好使用此方法。以下是这些标签的描述：

- automated-for-tagged-only：指定资源标签（一个或多个标签对，以逗号分隔），以便检查自动修复，无论默认执行模式如何。
- manual-for-tagged-only：为无论默认执行模式如何，都应手动执行的修复指定资源标签（一个或多个标签对，以逗号分隔）。

例如，如果您要为所有非生产资源启用自动修复并对生产资源强制执行手动修复，则可以按以下方式设置配置：

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

在您的资源上设置了上述配置后，检查修复行为如下所示：

- 标有 “环境=非生产” 的资源会自动修复。
- 标有 “环境=生产” 的资源需要手动干预才能进行修复。
- 没有 “环境” 标签的资源遵循默认的执行模式（在本例中为 “条件”）。 因此，不会对剩余资源采取任何行动）。

要获得有关配置的更多支持，请联系您的云架构师。

使用资源覆盖标签自定义补救措施

资源覆盖标签允许您自定义单个资源的修复行为，无论其标签如何。通过向资源添加特定标签，可以覆盖该资源和 Trusted Advisor 检查的默认执行模式。资源覆盖标签优先于默认配置和资源标记设置。因此，如果您使用资源覆盖标签将资源的默认执行模式设置为 “自动”、“手动” 或 “有条件”，则它将覆盖默认执行模式和任何资源标记配置。

要覆盖资源的执行模式，请完成以下步骤：

1. 确定要覆盖其修复配置的资源。
2. 确定要 Trusted Advisor 改写的支票的支票编号。您可以在中找到支持的签 IDs 入的 Trusted Advisor 支票Trusted Advisor 受信任修正者支持的检查。
3. 使用以下键和值为资源添加标签：

   - 标签密钥:TR-*Trusted Advisor check ID*-Execution-Mode（区分大小写）

     在前面的标签密钥示例中，`Trusted Advisor check ID`替换为要覆盖的 Trusted Advisor 支票的唯一标识。
   - 标签值：使用以下值之一作为标签值：
     - 自动：受信任的修正者会自动修复此 Trusted Advisor 检查的资源。
     - 手动：已 OpsItem 为资源创建，但不会自动执行修复。您可以从中手动查看并运行补救措施 OpsItem。

- 非活动：未对此资源和指定的 Trusted Advisor 检查执行修复和 OpsItem 创建。

例如，要使用 Trusted Advisor 支票编号自动修复 Amazon EBS 卷，请向 EBS 卷DAvU99Dc4C添加标签。标签键为TR-DAvU99Dc4C-Execution-Mode，标签值为Automated。

以下是显示标签部分的控制台示例：

执行模式决策工作流程

有多个级别可以为您的资源和每项 Trusted Advisor 检查配置执行模式。下图显示了 Trusted Remediator 如何根据您的配置决定使用哪种执行模式：

配置补救教程

以下教程提供了在 Trusted Remediator 中创建常见补救措施的示例

手动修复所有资源

此示例为 Trusted Advisor 支票编号为 DAv U99Dc4C（未充分利用的亚马逊 EBS 卷）的所有亚马逊 EBS 卷配置手动修复。

为支票编号 DAv为 U99dc4C 的亚马逊 EBS 卷配置手动修复

1. 在 https://console.aws.amazon.com/systems-manager/appconfig 上打开 AWS AppConfig 控制台。

   请务必以委派管理员帐户身份登录。
2. 从应用程序列表中选择 “可信修正者”。
3. 选择成本优化配置文件。
4. 选择 “未充分利用的 Amazon EBS 卷” 标志。
5. 对于执行模式，请选择手动。
6. 确保automated-for-tagged-only和manual-for-tagged-only属性为空。这些属性用于覆盖带有匹配标签的资源的默认执行模式。

   以下是 “属性” 部分的示例，其中automated-for-tagged-onlymanual-for-tagged-only和的值为空，执行模式为手动：

7. 选择 “保存” 以更新该值，然后选择 “保存新版本” 以应用更改。必须选择 “保存新版本”，可信修正者才能识别更改。
8. 确保您的 Amazon EBS 卷没有带有密钥`TR-DAvU99Dc4C-Execution-Mode`的标签。此标签密钥将覆盖该 EBS 卷的默认执行模式。

自动修复所有资源，所选资源除外

此示例为 Trusted Advisor 支票 ID DAv U99Dc4C（未充分利用的 Amazon EBS 卷）的所有 Amazon EBS 卷配置自动修复，但无法修复的指定卷（指定为 “非活动”）除外。

为支票编号为 DAv U99dc4C 的 Amazon EBS 卷配置自动修复，选定的非活动资源除外

1. 在 https://console.aws.amazon.com/systems-manager/appconfig 上打开 AWS AppConfig 控制台。

   请务必以委派管理员帐户身份登录。
2. 从应用程序列表中选择 “可信修正者”。
3. 选择成本优化配置文件。
4. 选择 “未充分利用的 Amazon EBS 卷” 标志。
5. 对于执行模式，请选择自动。
6. 确保automated-for-tagged-only和manual-for-tagged-only属性为空。这些属性用于覆盖带有匹配标签的资源的默认执行模式。

   以下是 “属性” 部分的示例，其中automated-for-tagged-onlymanual-for-tagged-only和的值为空，执行模式为 “自动”：

7. 选择 “保存” 以更新该值，然后选择 “保存新版本” 以应用更改。必须选择 “保存新版本”，可信修正者才能识别更改。

   此时，所有 Amazon EBS 卷都已设置为自动修复。
8. 覆盖对选定的 Amazon EBS 卷的自动修复：

   a. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
   b. 选择弹性区块存储、卷。
   c. 选择标签。

d. 选择管理标签。

e. 添加以下标签：

- 密钥：TR-DAv U99Dc4C-Execution-Mode
- 值：非活动

以下是显示键和值字段的 “标签” 部分的示例：

f. 对要排除在补救范围之外的所有 Amazon EBS 卷重复步骤 2 到 5。

自动修复已标记的资源

此示例为带有 Trusted Advisor 支票 ID DAv U99Dc4C（未充分利用的 Amazon EBS 卷）标签`Stage=NonProd`的所有亚马逊 EBS 卷配置自动修复。没有此标签的所有其他资源都不会被修复。

使用支票 ID DAv U99dc4C 的标签**`Stage=NonProd`**为亚马逊 EBS 卷配置自动修复

1. 在 https://console.aws.amazon.com/systems-manager/appconfig 上打开 AWS AppConfig 控制台。

   请务必以委派管理员帐户身份登录。
2. 从应用程序列表中选择 “可信修正者”。
3. 选择成本优化配置文件。
4. 选择 “未充分利用的 Amazon EBS 卷” 标志。
5. 对于执行模式，请选择 “有条件的”。
6. 将 automated-for-tagged-only 设置为 `Stage=NonProd`。`execution-mode`对于具有匹配标签的资源，此属性会覆盖默认值。确保manual-for-tagged-only属性为空。

   以下是 “属性” 部分的示例，该部分automated-for-tagged-only设置为 Stage= NonProd，执行模式设置为 “条件”：

7. 或者，将预配置参数设置为以下参数之一：

- `CreateSnapshot=false`不要在删除 Amazon EBS 卷之前创建该卷的快照
- `MinimumUnattachedDays=10`将要删除的 Amazon EBS 卷的最小独立天数设置为 10 天
- `CreateSnapshot=false`，`MinimumUnattachedDays=10`对于上述两个

8. 选择 “保存” 以更新该值，然后选择 “保存新版本” 以应用更改。必须选择 “保存新版本”，可信修正者才能识别更改。
9. 确保您的 Amazon EBS 卷没有带有密钥`TR-DAvU99Dc4C-Execution-Mode`的标签。此标签密钥将覆盖该 EBS 卷的默认执行模式。

在 “可信修正者” 中使用补救措施

在 “可信修正者” 中跟踪补救措施

要跟踪 OpsItems 修正情况，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 选择 “运营管理”，OpsCenter。
3. （可选）按 “来源 = 可信修正者” 筛选列表，以便在列表中仅包括受信任的修正者 OpsItems 。

   以下是按来源=可信修正者筛选的 OpsCenter 屏幕示例：

> **Note**
>
> 除了 OpsItems 从中查看之外 OpsCenter，您还可以查看 AMS S3 存储桶中的修复日志。有关更多信息，请参阅 可信修正者中的修复日志。

在 “可信修正器” 中运行手动修复

可信修正者为配置 OpsItems 为手动修复的检查进行创建。您必须查看这些检查并手动开始修复过程。

要手动修复 OpsItem，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 选择 “运营管理”，OpsCenter。
3. （可选）按 “来源 = 可信修正者” 筛选列表，以便在列表中仅包括受信任的修正者 OpsItems 。
4. 选择您 OpsItem 要查看的。
5. 查看的操作数据 OpsItem。操作数据包括以下项目：

- trustedAdvisorCheck类别：支 Trusted Advisor 票编号的类别。例如，容错
- trustedAdvisorCheckID：唯一的 Trusted Advisor 支票编号。
- trustedAdvisorCheck元数据：资源元数据，包括资源 ID。
- trustedAdvisorCheck名称：支 Trusted Advisor 票的名称。
- trustedAdvisorCheck状态：检测到的资源 Trusted Advisor 检查的状态。

6. 要手动修复 OpsItem，请完成以下步骤：

   a. 从 Runbooks 中，选择一个关联的运行手册（SSM 文档）。

   b. 选择执行。

   c. 对于 AutomationAssumeRole ，选择 `arn:aws:iam::AWS ## ID:role/ams_ssm_automation_role`。将 AWS 账户 ID 替换为运行修复的账户 ID。有关其他参数值，请参阅操作数据。

      要手动修复资源，用于向进行身份验证的角色或用户 AWS 账户 必须拥有 IAM 角色`ams-ssm-automation-role`的`iam:PassRole`权限。有关更多信息，请参阅向用户授予将角色传递给 AWS 服务或联系您的云架构师的权限。

   d. 选择执行。

   e. 在 “最新状态和结果” 列中监控 SSM 文档的执行进度。

   f. 文档完成后，选择 “设置状态”、“已解决” 以手动解决问题 OpsItem。如果文档失败，请查看详细信息并重新运行。 SSMdocument要获得其他故障排除支持，请创建服务请求。

   要解决 OpsItem 不经过修正的问题，请选择 “将状态设置为已解决”。

7. 对于所有剩余的手动修复，重复步骤 3 和 4 OpsItems。

对可信修正者中的修正进行故障排除

如需有关手动补救和补救失败的帮助，请联系 AMS。

要查看修复状态和结果，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 选择 “运营管理”，OpsCenter。
3. （可选）按 “来源 = 可信修正者” 筛选列表，以便在列表中仅包括受信任的修正者 OpsItems 。

4. 选择您 OpsItem 要查看的。
5. 在 “自动化执行” 部分中，查看文档名称和状态以及结果。
6. 查看以下常见的自动化故障。如果您的问题未在此处列出，请联系您的 CSDM 寻求帮助。

常见的补救错误

自动化执行中未列出任何执行任务

任何与关联的执行都 OpsItem 可能表示由于参数值不正确而导致执行未能启动。

故障排除步骤

1. 在运营数据中，查看`trustedAdvisorCheckAutoRemediation`属性值。
2. 验证DocumentName和参数值是否正确。要获得正确的值，请查看在可信修正器中配置 Trusted Advisor 检查修复有关如何配置 SSM 参数的详细信息。要查看支持的校验参数，请参阅 Trusted Advisor 受信任修正者支持的检查
3. 验证 SSM 文档中的值是否与允许的模式相匹配。要查看文档内容中的参数详细信息，请在 “运行手册” 部分中选择文档名称。
4. 检查并更正参数后，再次手动运行 SSM 文档。
5. 为防止此错误再次发生，请确保在配置中使用正确的参数值配置补救措施。有关更多信息，请参阅在可信修正器中配置 Trusted Advisor 检查修复。

自动化执行中的执行失败

补救文档包含多个步骤，这些步骤与通过 AWS 服务 执行各种操作进行交互 APIs。要确定故障的具体原因，请完成以下步骤：

故障排除步骤

1. 要查看各个执行步骤，请在 “自动化执行” 部分中选择 “执行 ID” 链接。以下是 Systems Manager 控制台的示例，显示了所选自动化的执行步骤：

2. 选择状态为 “失败” 的步骤。以下是错误消息示例：

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     此错误表示在修正配置的预配置参数中指定的存储桶名称不正确。

要解决此错误，请使用正确的存储桶名称手动运行自动化。为防止此问题再次发生，请使用正确的存储桶名称更新修复配置。

- `DB instance my-db-instance-1 is not in available status for modification.`

  此错误表示由于数据库实例处于无效状态，自动化无法进行预期的更改。

  要解决此错误，请手动运行自动化。

可信修正者中的修复日志

Trusted Remediator 创建 JSON 格式的日志并将其上传到亚马逊简单存储服务。日志文件将上传到 AMS 创建并命名的 S3 存储桶。`ams-trusted-remediator-{your-account-id}-logs`AMS 在委派管理员账户中创建 S3 存储桶。您可以将日志文件导入到中 QuickSight 以生成自定义的修复报告。

有关更多信息，请参阅 可信修正者与 QuickSight。

修复项目日志

可信修正者会在创建修正`Remediation item log` OpsItem 时创建。此日志包含手动修复 OpsItem 和自动修复 OpsItem。您可以使用`Remediation item log`来跟踪所有修正的概述。

Compute Optimizer 建议的修复项目日志位置

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

用于 Trusted Advisor 检查的修正项目日志位置

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`- `*`Resource ID`*`.json`

修复项目日志示例文件 URL

s3:///ams-trusted-remediator-*111122223333*-logs/remediation_items/*2023-02-06*/*1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json*

Compute Optimizer 修复项目日志格式

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 修正项目日志格式

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
   "ExecutionMode": Automated or Manual,
   "OpsItemID": OpsItem ID
}
```

Compute Optimizer 修复项目日志格式示例内容

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 修复项目日志格式示例内容

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

自动修复执行日志、Compute Optimizer 和 Trusted Advisor

Trusted Remediator 会在自动运行 SSM 文档完成Automated remediation execution log时创建。此日志包含 OpsItem 仅用于自动修复的 SSM 运行详细信息。您可以使用此日志文件来跟踪自动修复。

Compute Optimizer 自动修复日志位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//remediation_executions/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Compute Optimizer recommendation ID*.json

Trusted Advisor 自动修复日志位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs//remediation_executions/*remediation creation time in yyyy-mm-dd format*/*10 digits epoch time or unix timestamp*-*Trusted Advisor check ID*-*Resource ID*.json

Compute Optimizer 自动修复日志位置示例

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json

Trusted Advisor 自动修复日志位置示例

s3://ams-trusted-remediator-*111122223333*-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json

自动修复日志格式示例内容

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"}
```

成员账号日志

Trusted Remediator 会在您的账户加入或注销Member accounts log时创建。您可以使用Member accounts log来查找每个成员账户的账户 ID AWS 区域、已注册和执行时间。

成员账号日志位置

s3://ams-trusted-remediator-*delegated-administrator-account-id*-logs/configuration_logs/member_accounts.json

成员账户日志示例文件 URL

s3://ams-trusted-remediator-*111122223333*-logs/configuration_logs/member_accounts.json

成员账户日志格式

```
{
    "delegated_administrator_account_id": Delegated Administrator account id,
    "appconfig_configuration_region": Trusted Remediator AppConfig Region,
    "member_accounts": [
        {
            "account_id": Member account id
            "account_partition": Member account partition (for example, aws),
            "regions": [
                {
                    "execution_time": Remediation execution time in cron schedule
 expression,
                    "execution_timezone": Timezone for the remediation execution time,
                    "region_name": AWS ## name
                }
                ...
            ]
        }
        ...
    ],
    "updated_at": Log update time,
```

```
}
```

成员账户日志格式示例内容

```
{
    "delegated_administrator_account_id": "111122223333",
    "appconfig_configuration_region": "ap-southeast-2",
    "member_accounts": [
        {
            "account_id": "222233334444",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 9 * * 6",
                    "execution_timezone": "Australia/Sydney",
                    "region_name": "ap-southeast-2"
                },
                {
                    "execution_time": "0 5 * * 7",
                    "execution_timezone": "UTC",
                    "region_name": "us-east-1"
                }
            ]
        },
        {
            "account_id": "333344445555",
            "account_partition": "aws",
            "regions": [
                {
                    "execution_time": "0 1 * * 5",
                    "execution_timezone": "Asia/Seoul",
                    "region_name": "ap-northeast-2"
                }
            ]
        }
    ],
    "updated_at": "1730869607"
}
```

可信修正者与 QuickSight

您可以将存储在 Amazon S3 中的可信修复者日志与集成 QuickSight ，以生成自定义的修复报告。QuickSight 集成是可选的。此功能允许您使用日志来构建自定义报告仪表板。要按要求获取可信修正者的报告，请联系您的 CSDM。有关可用的可信修正者报告的更多信息，请参阅可信修正者报告。

有关在中可视化数据的更多信息 QuickSight，请参阅中的可视化数据。 QuickSight

QuickSight 为修复项目日志添加数据集

要 QuickSight 为修正项目日志添加数据集，请执行以下步骤：

1. 登录 QuickSight 控制台。您可以在任何 AWS 区域 QuickSight 支持的 QuickSight 版本中创建报告。但是，为了提高性能和降低成本，最好在 Trusted Remediator 日志存储桶所在的区域创建报告。
2. 选择数据集。
3. 选择 S3。
4. 在新的 S3 数据源中，输入以下值：

   - 数据源名称: `trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-items`.
   - 上传清单文件：创建包含以下内容的 JSON 文件并使用它。创建文件时，在 URIPrefixes 密钥`logging_bucket_name`中替换。

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_items/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- 选择连接。
- 在 “完成数据集创建” 窗口中，选择 “可视化”。
- QuickSight 打开新的分析表页面。现在，您可以使用修正项目日志创建新的分析了。

以下是样本分析：

QuickSight 为自动修复执行日志添加数据集

1. 登录 QuickSight 控制台。您可以在任何 AWS 区域 QuickSight 支持的 QuickSight 版本中创建报告。但是，为了提高性能和降低成本，最好在 Trusted Remediator 日志存储桶所在的区域创建报告。
2. 选择数据集。
3. 选择 S3。
4. 在新的 S3 数据源中，输入以下值：
   - 数据源名称:`trusted-remediator-`*`delegated_administrator_account_id`*`-`*`account_region`*`-remediation-executions`.
   - 上传清单文件：创建包含以下内容的 JSON 文件，然后使用此文件。创建文件时，在 URIPrefixes 密钥`logging_bucket_name`中替换。

```
{
    "fileLocations": [
        {
            "URIPrefixes": [
                "s3://{logging_bucket_name}/remediation_executions/"
            ]
        }
    ],
    "globalUploadSettings": {
        "format": "JSON",
        "delimiter": ",",
        "textqualifier": "'",
        "containsHeader": "true"
    }
}
```

- 选择连接。
- 在 “完成数据集创建” 窗口中，选择 “可视化”。
- QuickSight 打开新的分析表页面。现在，您可以使用修正项目日志创建新的分析了。

以下是样本分析：

《可信修正者》中的最佳实践

以下是帮助您使用可信修正器的最佳实践：

- 如果您不确定补救结果，请从手动执行模式开始。有时，从一开始就对补救应用自动执行可能会导致意想不到的结果。
- 每周对补救措施进行一次回顾 OpsItems ，深入了解可信修复者的结果。
- 成员账户继承委派管理员账户的配置。因此，重要的是要以一种有助于您管理具有相同配置的多个帐户的方式来构建帐户。您可以使用标签将资源排除在默认配置之外。

受信任的修正者 FAQs

以下是有关可信修正者的常见问题：

什么是 Trusted Remedicator？它对我有什么好处？

当 Compute Optimizer 发现违规行为 Trusted Advisor 或发布建议时，Trusted Remediator 会根据您指定的偏好进行响应，方法是应用补救措施、通过手动修正寻求批准，或者在即将到来的月度业务回顾 (MBR) 中报告补救措施。补救将在您的首选补救时间或计划进行。Trusted Remediator 使您能够自助服务并对 Trusted Advisor 支票采取行动，并且可以灵活地单独或批量配置和修复支票。AMS 拥有经过测试的补救文件库，通过应用安全检查和遵循 AWS 最佳实践，不断禁止提高您的账户。只有当您在配置中指定这样做时，您才会收到通知。AMS 用户可以选择加入 Trusted Remediator，无需额外付费。

Trusted Remediator 与其他 AWS 服务人有何关系和协作？

作为现有企业支持计划的一部分，您可以访问 Trusted Advisor 支票和 Compute Optimizer 建议。Trusted Remediator 与 Trusted Advisor Compute Optimizer 集成，可利用现有的 AMS 自动化功能。具体而言，AMS 使用 AWS Systems Manager 自动化文档（运行手册）进行自动修复。 AWS AppConfig 用于配置修复工作流程。您可以通过 Systems Manager OpsCenter 查看所有当前和过去的补救措施。修复日志存储在 Amazon S3 存储桶中。您可以使用日志在中导入和构建自定义报告仪表板 QuickSight。

谁来配置补救措施？

您的账户中的配置归您所有。管理您的配置是您的责任。您可以联系您的 CA 或 CDSM，寻求管理配置的帮助。您也可以通过服务请求与 AMS 联系，以获得配置支持、手动补救和修复失败故障排除。

如何安装 SSM 自动化文档？

SSM 自动化文档会自动共享给已注册的 AMS 账户。

AMS 拥有的资源也会得到补救吗？

可信修正者不会标记 AMS 拥有的资源。Trusted Remediator 只关注您的资源。

AWS 区域 Trusted Remediator 中有哪些可用以及谁可以使用它？

可信修正器适用于 AMS Accelerate 客户。有关支持区域的最新列表，请参阅AWS 服务 按地区划分。

可信修正者会导致资源漂移吗？

由于 SSM 自动化文档直接通过 AWS API 更新资源，因此可能会出现资源偏差。您可以使用标签来隔离通过现有 CI/CD 包创建的资源。您可以将 Trusted Remediator 配置为在修复其他资源的同时忽略已标记的资源。

如何暂停或停止可信修正者？

您可以通过 AWS AppConfig 应用程序关闭 “可信修正者”。要暂停或停止可信修正者，请完成以下步骤：

1. 在 https://console.aws.amazon.com/systems-manager/appconfig 上打开 AWS AppConfig 控制台。
2. 选择可信修正者。
3. 在配置文件上选择设置。
4. 选择 “暂停可信修正者” 标志。
5. 将该`suspended`属性的值设置为。`true`

> **Note**
>
> 使用此过程时要小心，因为这会停止所有关联到委派管理员帐户的账户的 Trusted Remediator。

如何修复可信修正者不支持的检查？

您可以继续通过按需运营 (OOD) 与 AMS 联系，获取不支持的支票。AMS 可帮助您补救这些检查。有关更多信息，请参阅按需操作。

可信修正者与修复有何不同 AWS Config ？

AWS Config 修复是另一种解决方案，可帮助您优化云资源并保持对最佳实践的合规性。以下是这两种解决方案之间的一些操作差异：

- Trusted Remediator 使用 Trusted Advisor 和 Compute Optimizer 作为检测机制。 AWS Config 修正使用 AWS Config 规则作为检测机制。
- 对于 Trusted Remideator，修复将按照您预定义的修复计划进行。在中 AWS Config，补救是实时进行的。
- Trusted Remediator 中每项修复的参数都可以根据您的用例轻松自定义，并且可以通过在资源上添加标签来实现自动修复或手动修复。
- 可信修正者提供报告功能。
- Trusted Remediator 会向您发送一封电子邮件通知，其中包含修正列表和修正状态。

某些 Trusted Advisor 检查和 Compute Optimizer 建议可能有相同的规则。 AWS Config如果存在匹配的 AWS Config 规则和 Trusted Advisor 检查，则最佳做法是仅启用一项补救措施。有关每项 Trusted Advisor 检查 AWS Config 规则的信息，请参阅Trusted Advisor 受信任修正者支持的检查。

Trusted Remediator 会将哪些资源部署到您的账户？

可信修正者在可信修正者委派的管理员帐户中部署以下资源：

- 一个名为 `ams-trusted-remediator-{your-account-id}-logs` 的 Amazon S3 存储桶。Trusted OpsItem Remediator `Remediation item log` 在创建补救措施时以 JSON 格式创建，并将日志文件上传到此存储桶。
- 用于保存支持的 Trusted Advisor 检查和 Compute Optimizer 建议的补救配置的 AWS AppConfig 应用程序。

可信修正者不会在可信修正者成员帐户中部署资源。

AMS Accelerate 中对 Amazon EKS 进行监控和事件管理

Amazon EKS 的监控和事件管理可监控您的 Amazon EKS 资源是否存在故障、性能下降和安全问题。AMS Accelerate 配置和部署适用于 Prometheus 的亚马逊托管服务警报管理器规则，监控警报，然后在触发这些警报时执行事件管理。Amazon EKS 的监控和事件管理依赖 AMS Alarm Manager 并利用原生 AWS 服务，例如适用于 Prometheus 的亚马逊托管服务、亚马逊托管 Grafana、亚马逊和。GuardDuty AWS LambdaAWS Config

> **Note**
>
> 亚马逊 EKS 的监控和事件管理不支持 AWS GovCloud (US) Windows 节点或 Windows 容器。

AMS Accelerate 中对 Amazon EKS 的监控和事件管理是什么？

Amazon EKS 的监控和事件管理提供以下内容：

- 一种默认配置，用于在您的托管账户中为您选择的 Amazon EKS 集群创建、管理和部署监控器和策略。
- 即使您没有为 Amazon EKS 集群配置任何其他监控，也可让您的 Amazon EKS 工作负载提高可用性的监控基准。有关更多信息，请参阅 AMS Accelerate 中的 Amazon EKS 监控和事件管理中的基准警报。
- 由为您的 Amazon EKS 集群配置的基准监控生成的通知。这些通知被称为警报。当出现即将发生的、持续的、正在消失的或潜在的故障、性能下降或安全问题时，就会生成警报。警报的示例包括 Prometheus 警报、事件或来自 AWS 服务（例如亚马逊）的发现。 GuardDuty
- 警报调查，并提供有关您可以采取的适当补救措施的指导。有关更多信息，请参阅 AMS Accelerate 中的事件报告和服务请求。
- 在可能的情况下，经您批准，AMS 运营部门对警报和事件进行补救，以防止或减少对您的应用程序的影响。有关更多信息，请参阅 AMS Accelerate 中的事件报告和服务请求。
- 可选的预定义 Amazon Managed Grafana 控制面板，可让您了解资源利用率、性能、CoreDNS 的运行状况、活动警报和之前已解决的警报。如果您使用 AMS 提供的模板配置亚马逊托管 Grafana，则可以打开亚马逊托管 Grafana 控制台来查看亚马逊 EKS 集群的指标和提醒。

Amazon EKS 的监控和事件管理如何在 AMS Accelerate 中发挥作用

生成：作为 EKS 入职监控和事件管理的一部分，AMS 会为您在托管账户中选择的 Amazon EKS 集群配置基准监控。AMS 结合使用适用于 Prometheus 的亚马逊托管服务警报管理器规则和 CloudWatch 亚马逊事件规则来配置基准监控。集群中配置了 AMS 的 Prometheus 服务器会将你的 Prometheus 指标抓取并远程写入同一地区的亚马逊托管服务 Prometheus 终端节点。当触发 Prometheus 警报管理器规则或生成事件时，基线监控配置会生成警报。 CloudWatch

聚合：AMS 通过将您的资源生成的所有警报定向到由 AMS 管理的 Amazon 简单通知服务主题，将其发送到 AMS 监控系统。

处理和影响分析：AMS 会分析警报，然后根据其潜在影响进行处理。AMS 按以下方式对警报进行分类：

- 具有已知客户影响的警报：对于这些警报，AMS 使用事件管理流程创建新的事件报告。
- 对客户影响不确定的警报：对于这些警报，AMS 会发送事件报告。在许多情况下，这些警报会要求您在 AMS 采取行动之前验证影响。对于此类警报，AMS 会发送包含详细信息的警报通知，并检查警报是否需要采取缓解措施。AMS 在通知中提供了缓解措施的选项。如果您的回复确认警报是事件，AMS 就会触发创建新的事件报告并启动事件管理流程。任何收到 “对客户没有影响” 回复或三天内完全没有回复的服务通知都将被标记为已解决。此外，相应的警报也被标记为已解决。
- 不影响客户的警报：如果 AMS 在评估后确定该警报对客户没有任何影响，则该警报将关闭。

AMS 责任矩阵 (RACI)

负责任、负责、咨询和知情的 AMS 或 RACI 矩阵将各种活动的主要责任分配给客户或 AMS。下表概述了客户和 AMS 在使用 Amazon EKS 监控和事件管理的应用程序中活动的责任。

- R 代表负责完成任务的责任方。
- A 代表责任方。
- C 代表咨询；征求意见的一方，通常是作为主题专家征求意见的一方；以及与之进行双边沟通的一方。
- 我代表知情；通报进展情况的一方，通常只有在任务或可交付成果完成后才会被告知。

活动	Customer	AMS
针对 AMS 要求的发现	我	R

活动	Customer	AMS
为集群访问启用 AMS 权限 (RBAC)	R	C
如果工作节点上还没有 Amazon S EC2 ystems Manager 代理，请将其安装在工作节点上	R	C
根据需要在集群上部署 AMS 组件，例如 Prometheu s、Prometheus Node Exporter 和 AMS 命名空间。 kube-stat e-metrics	C	R
在 AMS 控制平面中为 Prometheus 配置亚马逊托管服务	我	R
在 AMS 控制平面中配置 Prometheus 警报管理器	我	R
提供亚马逊托管 Grafana 模板并协助进行配置	C	R
启用 GuardDuty EKS 审核日志监控	C	R
启用 Amazon EKS 控制平面日志记录	我	R
监控 Amazon EKS 控制平面的运行状况和性能	我	R
监控 Amazon EKS 集群（集群、节点、工作负载、容器、API 服务器和 CoreDNS）的运行状况和性能	我	R

活动	Customer	AMS
为 Amazon EKS 对警报进行分类并提供事件响应	我	R
在事件发生期间运行诊断命令	我	R
在事件期间分析日志（控制平面和 pod 日志）	我	R
AWS 网络问题事件响应	我	R
回应 GuardDuty EKS 审核日志监控结果	我	R
尽可能为客户提供有关补救事件的行动指导	我	R

AMS Accelerate 中的 Amazon EKS 监控和事件管理中的基准警报

验证警报后，AMS 会为 Amazon EKS 启用以下警报，然后对所选的 Amazon EKS 集群进行监控和事件管理。响应时间服务级别协议 (SLAs) 和服务级别目标 (SLOs) 取决于您选择的账户服务级别（Plus、Premium）。有关更多信息，请参阅 AMS Accelerate 中的事件报告和服务请求。

警报和操作

下表列出了 Amazon EKS 警报以及 AMS 采取的相应操作：

警报	阈值	操作
容器 OOM 被杀	在过去 10 分钟内，容器重启的总次数至少为 1，Pod 中的 Kubernetes 容器在过去 10 分钟内已终止，原因为“OOMKilled”。	AMS 会调查 OOM 终止是由于达到容器限制还是内存限制过度使用而导致，然后建议您采取纠正措施。

警报	阈值	操作
Pod Job 失败	Kubernetes 任务无法完成。如果存在至少一个失败的任务状态，则表示失败。	AMS 会调查 Kubernetes 作业或相应的 cron 作业失败的原因，然后建议您采取纠正措施。
StatefulSet 向下	在至少 1 分钟内，准备提供流量的副本数量与每个 StatefulSet 副本的当前数量不匹配。	AMS 通过查看 pod 事件中的错误消息和 pod 日志中的错误日志片段来确定 pod 未准备就绪的原因，然后建议您采取更正措施。
HPA 扩展能力	由于状态条件 “AbleToScale” 在至少 2 分钟内为假，水平吊舱自动扩缩器 (HPA) 无法扩展。	AMS 确定哪个 Kubernetes 水平容器自动扩缩器 (HPA) 无法为其后续工作负载资源（例如部署或）扩展 pod。 StatefulSet
HPA 指标可用性	由于状态条件 “ScalingActive” 在至少 2 分钟内为假，水平吊舱自动扩缩器 (HPA) 无法收集指标。	AMS 确定 HPA 无法收集指标的原因，例如与服务器配置问题或 RBAC 授权问题相关的指标。
吊舱未准备好	Kubernetes Pod 处于非运行状态（例如 “待处理”、“未知” 或 “失败”）的时间超过 15 分钟。	AMS 会调查受影响的 pod 以获取详细信息，查看容器日志中是否存在相关的错误和事件，然后建议您采取纠正措施。
吊舱崩溃循环	Pod 容器至少每 15 分钟重启一次，持续 1 小时。	AMS 会调查 Pod 无法启动的原因，例如资源不足、文件被另一个容器锁定、数据库被另一个容器锁定、服务依赖关系失败、外部服务的 DNS 问题以及配置错误。

警报	阈值	操作
Daemonset 计划错误	至少有一个 Kubernetes Daemonset pod 在 10 分钟内错时调度。	AMS 决定为何将守护进程安排在不应该运行的节点上。当将错误的 pod 应用于 Da nodeSelector/taints/affinities emonset pod 时，或者当节点（节点池）受到污染并且未安排驱逐现有 Pod 时，可能会发生这种情况。
Kubernetes API 错误	在 2 分钟内，Kubernetes API 服务器的错误率超过 3%。	AMS 会分析控制平面日志，以确定导致此警报的错误数量和类型，并识别主节点或 etcd 自动缩放组的任何资源争用问题。如果 API 服务器无法恢复，AMS 会与 Amazon EKS 服务团队合作。
Kubernetes API 延迟	在 2 分钟内，向 Kubernetes API 服务器发出的请求延迟在 99 个百分位数内超过 1 秒。	AMS 分析控制平面日志，以确定导致延迟的错误数量和类型，并识别主节点或 etcd 自动缩放组的任何资源争用问题。如果 API 服务器无法恢复，AMS 会与 Amazon EKS 服务团队合作。
Kubernetes 客户端证书即将到期	用于向 Kubernetes API 服务器进行身份验证的客户端证书将在不到 24 小时后到期。	AMS 发送此通知是为了通知您，您的集群证书将在 24 小时后过期。
节点未就绪	在至少 10 分钟内，节点 “就绪” 状态为假。	AMS 会调查阻止 kubelet 访问 API 服务器的节点状况和事件，例如网络问题。

警报	阈值	操作
节点高 CPU	在 5 分钟内，CPU 负载超过 80%。	AMS 会确定一个或多个 pod 消耗的 CPU 量是否异常高。然后，AMS 会与您核实您的请求、限制和 pod 活动是否符合预期。
检测到节点 OOM 杀死	在 4 分钟的时间段内，该节点至少报告了一次主机 OOM 终止。	AMS 确定 OOM 终止是由于达到容器限制还是节点过度使用而导致。如果应用程序活动正常，AMS 会就超额提交的请求和限制以及修改 Pod 限制向您提供建议。
节点连接限制	在 5 分钟内，当前连接跟踪条目数与最大限制的比率超过 80%。	AMS 会根据每个内核的推荐连接值为您提供建议。Kubernetes 节点将 conntrack 最大值设置为与节点的总内存容量成正比。高负载应用程序，尤其是在较小的节点上，很容易超过 conntrack 的最大值，从而导致连接重置和超时。
节点时钟不同步	2 分钟内的最低同步状态为 0，以秒为单位的最大错误为 16 或更高。	AMS 确定网络时间协议 (NTP) 是否已安装并正常运行。
Pod 高 CPU	容器的 CPU 使用率在 3 分钟内超过 80%，持续至少 2 分钟。	AMS 会调查 pod 日志，以确定消耗大量 CPU 的 pod 任务。
Pod 高内存	容器的内存使用率在 2 分钟内超过其指定内存限制的 80%。	AMS 会调查 pod 日志，以确定消耗大量内存的 pod 任务。

警报	阈值	操作
CoreDNS 关闭	CoreDNS 已经从 Prometheus 的目标发现中消失了超过 15 分钟。	这是一个严重警报，表示内部或外部群集服务的域名解析已停止。AMS 会检查 CoreDNS 容器的状态，验证 CoreDNS 配置，验证指向 CoreDNS 容器的 DNS 端点，验证 CoreDNS 限制，并在您批准后启用 CoreDNS 调试日志。
CoreDNS 错误	CoreDNS 会在 10 分钟内对超过 3% 的 DNS 请求返回 SERVFAIL 错误。	此警报可能表示应用程序存在问题或配置错误。AMS 会检查 CoreDNS 容器的状态，验证 CoreDNS 配置，验证指向 CoreDNS 容器的 DNS 端点，验证 CoreDNS 限制，并在您批准后启用 CoreDNS 调试日志。
CoreDNS 延迟	DNS 请求持续时间的第 99 个百分位数超过 4 秒，持续 10 分钟。	此警报表示 CoreDNS 可能已过载。AMS 会检查 CoreDNS 容器的状态，验证 CoreDNS 配置，验证指向 CoreDNS 容器的 DNS 端点，验证 CoreDNS 限制，并在您批准后启用 CoreDNS 调试日志。

警报	阈值	操作
CoreDNS 转发延迟	CoreDNS 将请求转发到 kube-dns 的响应时间的第 99 个百分位数在 10 分钟内超过 4 秒。	当 CoreDNS 不是权威服务器或者没有域名的缓存条目时，CoreDNS 会将 DNS 请求转发到上游 DNS 服务器。此警报表示 CoreDNS 可能已过载或上游 DNS 服务器可能存在问题。AMS 会检查 CoreDNS 容器的状态，验证 CoreDNS 配置，验证指向 CoreDNS 容器的 DNS 端点，验证 CoreDNS 限制，并在您批准后启用 CoreDNS 调试日志。
CoreDNS 转发错误	超过 3% 的 DNS 查询在 5 分钟内失败。	当 CoreDNS 不是权威服务器或者没有域名的缓存条目时，CoreDNS 会将 DNS 请求转发到上游 DNS 服务器。此警报表示上游 DNS 服务器可能存在配置错误或问题。AMS 会检查 CoreDNS 容器的状态，验证 CoreDNS 配置，验证指向 CoreDNS 容器的 DNS 端点，验证 CoreDNS 限制，并在您批准后启用 CoreDNS 调试日志。

在 AMS Accelerate 中对 Amazon EKS 进行监控和事件管理的要求

这些是 Amazon EKS for AMS Accelerate 监控和事件管理 and/or 所需的支持资源

- 支持的 Kubernetes 版本：请参阅亚马逊 EKS 用户指南中的亚马逊 EKS Kubernetes 版本。
- 节点类型：支持 Amazon EKS 托管节点。不支持 Windows 节点和容器。
- Kubernetes 集群访问权限：AMS 需要系统:masters RBAC 集群角色和集群用户。

- 亚马逊 EC2 节点上的 SSM 代理：Bottle Rocket 和 Amazon EKS AMIs 都预装了 SSM 代理。请确保在您的自定义节点 AMIs 和 Amazon EC2 节点上安装了 SSM 代理。
- 服务配额有关更多信息，请参阅适用于 Prometheus 的亚马逊托管服务和亚马逊托管 Grafana 的服务配额。
- 支持的 AWS 区域：

区域名称	区域	指标存储区域
美国东部（俄亥俄州）	us-east-2	us-east-2
美国东部（弗吉尼亚州北部）	us-east-1	us-east-1
美国西部（俄勒冈州）	us-west-2	us-west-2
亚太地区 (东京)	ap-northeast-1	ap-northeast-1
亚太地区 (首尔)	ap-northeast-2	ap-northeast-2
亚太地区（新加坡）	ap-southeast-1	ap-southeast-1
亚太地区（悉尼）	ap-southeast-2	ap-southeast-2
欧洲地区（法兰克福）	eu-central-1	eu-central-1
欧洲地区（爱尔兰）	eu-west-1	eu-west-1
欧洲地区（伦敦）	eu-west-2	eu-west-2
非洲（开普敦）	af-south-1	eu-west-1 eu-west-2
亚太地区（香港）	ap-east-1	ap-northeast-1 ap-northeast-2

> **Note**
>
> 位于非洲 af-south-1（开普敦）和亚太地区（香港）ap-east-1（香港）的 Amazon EKS 集群的指标将分别导出到 AMS 监控服务。 AWS 区域然后， AWS 区域 这些指标将在 AMS 监控服务中传输到不同的区域，在那里进行处理和存储。有关 AMS 监控服务用于存储指标的区域，请参阅上表。

在 AMS Accelerate 中加入 Amazon EKS 的监控和事件管理

执行以下步骤以加入 Amazon EKS 的监控和事件管理。

1. 启用 Amazon EKS 成本优化标签：请参阅 Amazon EKS 用户指南中的标记资源以进行计费。
2. 启动 EKS 的监控和事件管理入门：请联系您的云服务交付经理 (CSDM)，提供要加入的账户 IDs 和集群名称。
3. 验证要求：您的云架构师 (CA) 将在入职开始之前验证是否满足了所有要求。
4. 更新 Kubernetes 基于角色的访问控制 (RBAC)：AMS 共享命令来实现这些`eksctl`更改。您可以查看这些更改，然后进行部署。您必须部署 RBAC 更新，这样 AMS 才有权代表您运行命令。这些更新包括将 AMS IAM 角色映射到 Kubernetes 用户、为 AMS 创建新的 Kubernetes 集群角色以及将 AMS Kubernetes 集群角色绑定到该用户。
5. 部署集群组件：AMS 在您的集群上的 AMS 管理的命名空间中部署以下组件：
   - Prometheus 服务器
   - Prometheus 节点导出器（不适用于） AWS Fargate
   - kube-state-metrics
6. 执行 Prometheus 配置更新：AMS 将 Prometheu s 配置为启用指标的远程写入。
7. （可选）配置控制面板：您的 CA 可帮助您在账户中配置 Amazon Managed Grafana 控制面板。

> **Note**
>
> 在您的 Amazon EKS 集群加载后，AMS 会分析警报信号并执行基准评估以确定集群中存在的问题。基准评估完成后，AMS 将通过 Trusted Advisor 分享调查结果和补救建议，并提交一份服务请求，您可以使用这些请求来解决集群中的问题。根据评估，AMS 通过调整账户级别的警报阈值，创建特定于您的 EKS 集群的 Amazon EKS 监控基准。为了消除针对这些发现的重复

AMS响应，我们调整了监控以排除这些警报信号。当您的CSDM通知我们潜在问题已得到修复时，我们会重新调整监控，以包括信号。

在 AMS Accelerate 中脱离对 Amazon EKS 的监控和事件管理

使用账户 IDs 和集群名称通知您的云服务交付经理 (CSDM)，开始离职流程。在您离线后，根据适用于 Prometheus 的默认亚马逊托管服务数据保留政策，将暂停警报处理、指标存储和指标查询，并删除指标。

AMS 执行以下离线步骤：

1. AMS 会禁用发送给您和 AMS 运营部门的警报。
2. AMS 从您的亚马逊 EKS 集群中移除 Prometheus 实例。
3. AMS 会移除您账户中安装的其他 AWS 资源，例如 IAM 角色和 AWS Config 规则。

完成这些步骤后，您必须完成以下离职步骤：

1. 用于从中`eksctl`移除 Kubernetes RBAC 权限。`aws-auth ConfigMap`
2. 如果您之前安装了该实例，请删除您配置为连接到 AMS 的 Amazon 托管 Grafana 实例。

AMS 中的连续性管理加速

AMS 利用它 AWS Backup 来集中和自动化跨 AWS 服务备份您的数据。AMS 备份计划为各种用例提供了最佳实践；但是，欢迎您继续使用现有的备份计划。在您加入 AMS 备份管理后，AMS 会提供备份报告，AMS 专家会持续监控您的备份任务，以确保您拥有可靠的备份解决方案。

要了解更多信息，请参阅 AWS Backup：工作原理和支持的 AWS 资源和第三方应用程序。

AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。要快速了解 AMS 如何利用我们的一些关键运营功能（包括全天候服务台、主动监控、安全、补丁、日志记录和备份）来帮助您的团队实现整体卓越运营，请参阅 AMS 参考架构图。 AWS 云

观看 Carl 的视频以了解更多信息 (9:29)

主题

AMS 中连续性管理的工作原理

AMS 备份计划定义了备份数据的频率以及备份的保留政策。AMS 备份保管库可让您的备份数据井井有条。资源与备份计划关联后，将以增量方式备份兼容的资源。第一个备份是完整副本，随后的备份会捕获增量更改。根据所选的资源和 AMS 备份计划，Point-in-time 还原 (PITR) 允许您通过选择恢复时间来倒带资源。要开始使用 AMS Backup Management，只需选择 AMS 备份计划并标记您的资源即可。

> **Note**
>
> 按照以下步骤确保 AWS Backup 为每个账户和资源类型启用该功能：入门 1：服务选择加入。
> AWS 区域
> 您无需继续 “入门 2：在按需备份上创建”。

相关话题来自 AWS Backup

- 处理备份（创建、编辑、复制、恢复、删除）
- 创建按需备份
- 跨创建备份副本 AWS 区域
- AWS Backup 支持的服务
- Point-in-time 恢复
- AWS Backup 功能

选择 AMS 备份计划

AMS 提供三种不同的备份计划和第四种备份计划，以最大限度地降低入职期间的成本。要为每个支持的资源选择 AMS 备份计划，请使用计划的关联标签标记该资源。在您加入 Accelerate 时，AMS 将与您合作，确定最适合您需求的备份计划。

> **Important**
>
> 请勿编辑您的 AMS 默认备份计划，因为您所做的更改可能会丢失。取而代之的是，为您的自定义配置制定新的计划。有关更多信息，请参阅创建备份计划。

默认 AMS 备份计划

AWS Backup 此备份计划未启用连续备份；有关详细信息，请参阅使用 point-in-time还原恢复到指定时间 (PITR)。

标签密钥：`ams:rt:backup-orchestrator`

标签值：`true`

默认 AMS 备份计划	Start Time	保留
每小时备份	不适用	不适用
每日备份	世界标准时间每日 4:00	7 days
每周备份	世界标准时间星期六 2:00	4 个星期
每月备份	本月 1 日，世界标准时间 2:00	26 个星期

默认 AMS 备份计划	Start Time	保留
年度备份	世界标准时间 1 月 1 日 2:00	2 年

增强的备份计划

AWS Backup 在支持的资源上启用了连续备份，保留期最长（31 天）；有关详细信息，请参阅使用 point-in-time还原恢复到指定时间 (PITR) 和支持的 point-in-time还原服务和应用程序 (PITR)。

标签密钥：`ams:rt:backup-orchestrator-enhanced`

标签值：`true`

增强的备份计划	Start Time	保留
每小时备份	不适用	不适用
每日备份	世界标准时间每日 4:00	31 天
每周备份	世界标准时间星期六 2:00	6 个星期
每月备份	本月 1 日，世界标准时间 2:00	26 个星期
年度备份	世界标准时间 1 月 1 日 2:00	2 年

数据敏感备份计划

AWS Backup 在支持的资源上启用了连续备份，保留期最长（31 天）；有关详细信息，请参阅使用 point-in-time还原恢复到指定时间 (PITR) 和支持的 point-in-time还原服务和应用程序 (PITR)。

标签密钥：`ams:rt:backup-orchestrator-data-sensitive`

标签值：`true`

数据敏感备份计划	Start Time	保留
每小时备份	每小时	7 天

数据敏感备份计划	Start Time	保留
每日备份	世界标准时间每日 4:00	31 天
每周备份	世界标准时间星期六 2:00	6 个星期
每月备份	本月 1 日，世界标准时间 2:00	26 个星期
年度备份	世界标准时间 1 月 1 日 2:00	2 年

AMS 加快入职备份计划

AWS Backup 此备份计划未启用连续备份；有关详细信息，请参阅使用 point-in-time还原恢复到指定时间 (PITR)。

标签密钥：`ams:rt:backup-orchestrator-onboarding`

标签值：`true`

AMS 加快入职备份计划	Start Time	保留
每小时备份	每小时	2 个星期
每日备份	不适用	不适用
每周备份	不适用	不适用
每月备份	不适用	不适用
年度备份	不适用	不适用

相关 AWS Backup 话题

- 创建备份计划
- Point-in-time restore (PITR) 支持对支持的资源进行连续备份，并允许您选择特定的恢复时间。有关支持的资源列表，请参阅按资源划分的功能可用性。

标记您的资源以应用 AMS 备份计划

要向 AMS 备份计划分配资源，请使用该计划的标签键值对标记该资源。您可以使用 AMS 资源标记器将 AMS 备份计划应用于您的部分资源或账户中所有支持的资源。如果您想使用其他方法将标签应用于您的资源，例如 AWS CloudFormation 或 Terraform，请关闭资源标记器，这样它就不会与您选择的标记方法发生冲突。有关更多信息，请参阅 阻止资源标记器修改资源。

以下示例演示了如何使用资源标记器将默认 AMS 备份计划应用于账户中的 Amazon Elastic Compute Cloud 实例。对于此备份计划，请应用标签键`ams:rt:backup-orchestrator`和值`true`。要使用其他备份计划，请将密钥更改为与所需备份计划的标签密钥相匹配。要了解 AMS Resource Tagger 并了解如何将以下引用的配置文件与 Accelerate 账户中的当前（已配置）配置文件集成，请参阅加速资源标记器。

1. 在 https://console.aws.amazon.com/systems-manager/appconfig 上打开 AWS AppConfig 控制台。
2. 选择 ResourceTagger 应用程序。
3. 选择 “配置文件” 选项卡，然后选择 CustomerManagedTags
4. 选择 “创建” 以创建新版本。
5. 选择 JSON，然后复制并粘贴以下 JSON 对象：

```
{
    "AWS::EC2::Instance": {
        "AccelerateBackupPlan": {
            "Enabled": true,
            "Filter": {
                "Fn::AND": [
                    {
                        "Platform": "*"
                    }
                ]
            },
            "Tags": [
                {
                    "Key": "ams:rt:backup-orchestrator",
                    "Value": "true"
                }
            ]
        }
    }
}
```

6. 选择创建托管配置版本。
7. 选择开始部署。
8. 定义以下部署细节：

```
Environment: AMSInfrastructure
Hosted configuration version: Select the version that you have just created.
Deployment Strategy: AMSNoBakeDeployment
```

9. 选择开始部署。Resource Tagger 会标记您的实例`ams:rt:backup-orchestrator: true`，确保您的实例按照默认 AMS 备份计划进行备份。

查看 AMS 保管库中的备份

您可以使用标签控制单个存储库级别的备份库通知。您可以通过在特定文件库`True`上添加标签`AMSNotificationOptOut`并将该值设置为，来选择不接收针对特定文件库的通知。要恢复从文件库中获取通知，请移除标签。

要查看您的 AMS 备份列表，请打开AWS Backup 控制台。在导航窗格中，选择 Backup Vaul ts，然后从下表中选择一个 AMS 备份存储库。在 “备份” 部分，查看备份库中所有备份的列表。选择要编辑、删除或恢复的备份。

AMS Backup 计划的保管库

AMS 保管库名称	AMS Backup Plan 标签密钥
ams-automated-backups	ams:rt:backup-orchestrator
ams-automated-enhanced-backups	ams: rt: backup-orchestrator-enhanced
ams-automated-data-sensitive-备份	ams: rt: backup-orchestrator-data-sensitive
ams-onboarding-backups	ams: rt: backup-orchestrator-onboarding

其他 AMS 保管库

AMS 保管库名称	说明
ams-manual-backups	此保管库包含由 AWSManagedServices-StartBackupJob SSM Automation 文档创建的手动启动的备份，以及修补之前由 AMS 自动补丁创建的补丁前备份。
ams-custom-backups	对于在 AMS 备份计划之外创建的备份，建议使用此保管库。

相关 AWS Backup 话题

- 按资源查看备份
- 处理备份

AMS 备份监控和报告

> **Important**
>
> AMS 备份监控和报告仅在 AMS 支持的地区可用。它们是美国东部（弗吉尼亚州）、美国西部（加利福尼亚北部）、美国西部（俄勒冈）、美国东部（俄亥俄州）、加拿大（中部）、南美洲（圣保罗）、欧洲（爱尔兰）、欧洲（法兰克福）、欧洲（伦敦）、欧洲（巴黎）、亚太地区（孟买）、亚太地区（首尔）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）。

AMS 生成每日自助服务报告以及有关资源覆盖率和备份任务状态的月度报告。月度报告在《月度商业评论》(MBRs) 中共享。要了解有关每日备份报告的更多信息，请参阅每日备份报告。

AMS 专家会监控您使用配置的所有备份任务 AWS Backup。如果备份失败，AMS 会调查故障并通知您根本原因和补救选项（如果有）。为了避免警报噪音，在导致您的账户出现大量备份失败的事件中，AMS 会通过您的 CSDM 提出集体建议，而不是就每个故障通知您。

请注意，AMS 不会监控使用 AWS 服务的独立备份功能配置的任何备份。

了解 AMS Accerate 中的补丁管理

Important

加速补丁报告定期部署 AWS Glue 基于资源的策略。请注意，AMS 对修补系统的更新会覆盖现有的基于 AWS Glue 资源的策略。

Important

您可以为托管节点指定备用补丁存储库。在 AMS 实施您请求的补丁配置时，您负责选择和验证所选存储库的安全性。您还必须接受使用这些存储库所带来的任何风险，例如供应链风险。以下是确保补丁管理流程安全性的最佳实践：

- 仅使用可信、经过验证的存储库来源
- 如果可能，默认为标准操作系统供应商存储库
- 定期审核自定义存储库配置

您可以使用 AMS Accelerate 修补系统，即补丁附加组件，使用安全相关更新和其他类型的更新来修补您的实例。加速补丁插件是一项为 AMS 实例提供基于标签的修补的功能。它利用 AWS Systems Manager (SSM) 功能，因此您可以使用基准和您配置的窗口标记实例并修补这些实例。AMS Accelerate 补丁插件是一个入门选项，如果您在加入 Accelerate 账户时未获得，请联系您的云服务交付经理 (CSDM) 获取。

AMS Accelerate 补丁管理使用 Systems Manager 补丁基准功能来控制应用于实例的补丁的定义。补丁基准包含预先批准的补丁列表；例如，所有安全补丁。实例的合规性是根据与其关联的补丁基准来衡量的。默认情况下，AMS Accelerate 会安装所有可用的补丁以使实例保持最新状态。

Note

AMS Accelerate 仅应用操作系统 (OS) 补丁。例如，对于 Windows，仅应用 Windows 更新，不应用微软更新。

有关报告的信息，请参阅AMS 主机管理报告。

AMS Accelerate 提供了一系列运营服务，可帮助您实现卓越运营 AWS。要快速了解 AMS 如何利用我们的一些关键运营功能（包括全天候服务台、主动监控、安全、补丁、日志记录和备份）来帮助您的团队实现整体卓越运营，请参阅 AMS 参考架构图。 AWS 云

主题

修补建议

如果您参与应用程序或基础架构的运营，您就会明白操作系统 (OS) 修补解决方案的重要性，该解决方案要足够灵活且可扩展，可以满足应用程序团队的不同需求。在典型的组织中，一些应用程序团队使用的架构涉及不可变实例，而另一些应用程序团队则在可变实例上部署应用程序。

有关修补 AWS 规范指南的更多信息，请参阅使用自动修补混合云中的可变实例。 AWS Systems Manager

> **Note**
>
> 加速补丁插件是一项为 AMS 实例提供基于标签的修补的功能。它利用 AWS Systems Manager (SSM) 功能，因此您可以使用基准和您配置的窗口标记实例并修补这些实例。AMS Accelerate 补丁插件是一个入门选项，如果您在加入 Accelerate 账户时未获得，请联系您的云服务交付经理 (CSDM) 获取。

补丁责任建议

永久性实例的修补过程应涉及以下团队和操作：

- 应用程序 (DevOps) 团队根据应用程序环境、操作系统类型或其他标准为其服务器定义补丁组。它们还定义了每个补丁组特定的维护窗口。此信息应存储在附加到实例的标签上。推荐的标签名称为“补丁组”和“维护窗口”。在每个补丁周期中，应用程序团队都要为修补做准备，在修补后测试应用程序，并在修补期间对应用程序和操作系统的任何问题进行故障排除。

- 安全运营团队为应用团队使用的各种操作系统类型定义补丁基准，并通过 Systems Manager Patch Manager 提供补丁程序。
- 自动修补解决方案定期运行，并根据用户定义的补丁组和维护时段部署补丁基准中定义的补丁。
- 治理和合规团队定义补丁指南以及例外流程和机制。

有关更多信息，请参阅可变 EC2 实例的修补解决方案设计。

申请团队指南

- 查看并熟悉如何创建和管理维护窗口；要了解更多信息，请参阅AWS Systems Manager 维护窗口和创建 SSM 维护窗口进行修补。了解维护窗口的总体结构和用法，可以帮助您了解如果不是创建维护窗口的人，则需要提供哪些信息。
- 对于高可用性 (HA) 设置，计划为每个可用区和每个环境设置一个维护窗口 (Dev/Test/Prod)。这将确保修补期间的持续可用性。
- 建议的维护时段持续时间为 4 小时，中断时间为 1 小时，外加每 50 个实例增加 1 小时
- 在开发和测试版本之间留出足够的时间进行修补，这样你就可以在生产修补之前识别出任何潜在的问题。
- 通过 SSM 自动化自动执行常见的修补前和修补后任务，并将其作为维护窗口任务运行。请注意，对于修补后的任务，您必须确保分配足够的时间，因为一旦达到截止时间，任务就不会启动。
- 熟悉补丁基准及其功能，尤其是补丁严重性类型的自动批准延迟，这可用于确保日后只有在生产中应用的补丁 Dev/Test 才能在生产中应用。有关详细信息，请参阅关于补丁基准。

安全运营团队指南

- 查看并熟悉补丁基准。补丁批准以自动方式处理，并且具有不同的规则选项。有关更多信息，请参阅关于补丁基准。
- Dev/Test/Prod与应用团队讨论有关修补的需求，并制定多个基准来满足这些需求。

治理和合规团队指南

- 修补应该是一个 “选择退出” 功能。应存在默认维护窗口和自动标记，以确保没有任何未修补的内容。AMS Resource Tagger 可以帮助解决这个问题；请与您的云架构师 (CA) 或云服务交付经理 (CSDM) 讨论此选项，以获取实施指导。

- 申请补丁豁免时应要求提供证明豁免理由的文件。首席信息安全官 (CISO) 或其他审批官应批准或拒绝申请。
- 应通过 Patch Manager 控制台、Security Hub 或漏洞扫描程序定期检查补丁合规性。

高可用性 Windows 应用程序的设计示例

概述：

- 每个可用区一个维护窗口。
- 每个环境都有一组维护窗口。
- 每个环境一个补丁基准：
  - 开发人员：0 天后批准所有严重性和分类。
  - 测试：在 0 天后批准关键安全更新补丁，7 天后批准所有其他严重性和分类。
  - Prod：在 0 天后批准关键安全更新补丁，14 天后批准所有其他严重性和分类。

CloudFormation 脚本：

这些脚本的设置是为了使用上述基准批准设置为两个可用区 Windows HA EC2 应用程序构建维护窗口、基准和修补任务。

- Windows Dev CFN 堆栈示例：ha-patching-dev-stack.json
- Windows 测试 CFN 堆栈示例：ha-patching-test-stack.json
- Windows Prod CFN 堆栈示例：ha-patching-prod-stack.json

补丁建议 FAQs

问：如何处理 “0” 天漏洞的计划外修补？

答：SSM 支持 “立即修补” 功能，该功能使用实例操作系统的当前默认基准。AMS 会部署一组默认的补丁基准，该基准会在 0 天后批准所有补丁。但是，使用 “立即修补” 功能时，不会拍摄修补前的快照，因为此命令运行 AW RunPatchBaseline S-SSM 文档。我们建议您在修补之前进行手动备份。

问：AMS 是否支持修补自动伸缩组 () ASGs 中的实例？

答：不是。 目前，Accelerate 客户不支持 ASG 修补。

问：维护时段是否有任何限制需要记住？

答：是的，您应该注意一些限制。

- 每个账户的维护时段：50
- 每个维护时段的任务数：20
- 每个维护时段的最大并发自动化数量：20
- 并发维护时段的最大数量：5

有关默认 SSM 限制的完整列表，请参阅AWS Systems Manager 终端节点和配额。

在 AMS 中创建补丁维护窗口

补丁维护窗口按设定的计划为目标 Amazon EC2 实例运行 AMS 补丁自动运行。目标由一组实例的一个或多个标签定义。你可以根据星期二补丁前后的日期和时间来设置时间表，也可以使用 cron 表达式定义时间表。有关更多信息，请参阅 AWS Systems Manager 用户指南中的参考：适用于 Systems Manager 的 cron 和 rate 表达式。在修补之前，AMS 会创建每个实例根卷的快照。如果 AMS 检测到修补会影响实例的运行状况，或者如果您将修补对应用程序的影响通知 AMS，则 AMS 会使用此快照将根卷恢复到修补前的状态。

AMS 加速补丁维护时段限制

AMS 修补使用 AWS Systems Manager （Systems Manager）。除了 Systems Manager 的服务限制外，每个补丁维护窗口的 AMS 修补限制为 300 个目标实例。假设每个实例的补丁完成时间一般为 30 分钟，下表提供了维护时段数量和持续时间的示例。

要修补的实例	维护时段持续时间（小时）	需要并行维护窗口
100	1	1
200	1	1
300	2	1
600	3	2
800	4	3

要修补的实例	维护时段持续时间（小时）	需要并行维护窗口
1200	6	4
1500	8	5

> **Important**
>
> 这些示例假设没有其他 Systems Manager 维护窗口处于活动状态，也没有其他自动化程序在运行。

有关限制的更多信息，请参阅AWS Systems Manager 终端节点和配额。

主题

- 从 AMS 控制台创建定期的 “补丁星期二” 维护窗口（推荐）
- 使用 CloudFormation AMS Accelerate 创建补丁维护窗口
- 通过 Systems Manager 控制台为 AMS Accelerate 创建维护窗口
- 使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口

从 AMS 控制台创建定期的 “补丁星期二” 维护窗口（推荐）

Microsoft在每个月的第二个星期二（也称为补丁星期二）发布其操作系统的补丁。通常将 Windows 和 Linux 实例的修补时间安排在周二补丁之上。要将定期补丁维护时间安排在周二补丁之后的第一个或第二个周末，请访问 AMS 控制台并按照以下步骤操作：

1. 为您的补丁维护窗口提供一个名称。
2. [可选] 提供补丁维护窗口的描述。
3. 选择与周二补丁相关的日期。
4. 以 hh: mm 为单位输入补丁维护窗口的开始时间。例如，午夜是 00:00，晚上 11 点是 23:00。然后选择一个时区。
5. [可选] 更改持续时间以满足您的需求。AMS 建议至少持续四小时。
6. 输入目标的补丁标签密钥和值。有关信息，请参阅什么是标签？ 。
7. [可选] 展开可选参数以调整并发度、错误率和维护窗口截止时间。

1. 并发控制同时修补多少目标实例。例如，10 个目标实例的并发度为 50%，一次修补不超过 5 个实例，而 100% 的并发度将同时修补所有 10 个实例。
2. 错误率控制暂停修补程序之前的错误容忍度。例如，如果有 10 个目标实例的错误率为 100%，则无论有多少实例失败，都将修补所有实例，而 50% 的错误率将在 5 个实例无法修补时暂停修补。AMS 建议错误率为 100%。
3. 修补程序维护窗口截止时间通过在补丁维护时段结束前的指定小时暂停新修补活动的开始，从而防止修补程序维护窗口被破坏。例如，截止时间为 1 小时（推荐），则会在补丁维护窗口结束前 1 小时停止新的补丁活动。

> **Important**
>
> 验证下次执行时间。
> 访问 SSM 维护窗口控制台，搜索您新创建的补丁维护窗口，并验证下次执行时间。如果您有任何疑问或需要编辑补丁维护窗口，请创建服务请求以与 AMS 补丁专家交谈

要使用安排基于 Cron 的补丁维护时段 CloudFormation，请参阅。使用 CloudFormation AMS Accelerate 创建补丁维护窗口

使用 CloudFormation AMS Accelerate 创建补丁维护窗口

要使用创建 AMS Accelerate 补丁维护窗口 AWS CloudFormation，请先登录您的 Accelerate 账户，然后选择目标实例所在 AWS 区域 的位置。然后在 https://console.aws.amazon.com/cloudformat ion 上按照以下步骤操作：

1. 从两个自定义 Accelerate 修补 CloudFormation 模板中选择一个。

   - 周二补丁计划：Microsoft在每个月的第二个星期二（也称为补丁星期二）发布其操作系统的补丁，将补丁维护时间安排在补丁周二之后的第一个或第二个周末：登录加速控制台后，使用此链接 PatchTuesdayScheduling CloudFormation 模板。
   - CRON 计划：要使用 CRON 创建补丁维护窗口来定义起始日期，请使用此链接 CRONScheduling CloudFormation 模板。请记住，Systems Manager CRON 编号为 1-7 天（有关 Systems Manager CRON 的详细信息，请参阅参考：Systems Manager 的 Cron 和费率表达式）。

   选择其中一个链接会使模板自动加载到 CloudFormation 控制台上。然后单击 Next（下一步）。

2. 在指定堆栈详细信息页面（创建堆栈页面的第 2 步）上，输入堆栈名称和模板参数（显示的默认参数是 AMS 推荐的默认参数，请为您的用例选择日期和时间）。完成后，单击 Next。
3. 配置堆栈选项（可选）。有关这些选项的信息，请参阅设置 AWS CloudFormation 堆栈选项。完成后，单击 Next。
4. 查看您的堆栈值（可选）。有关查看堆栈详细信息以估算成本的信息，请参阅查看堆栈和估算堆栈成本。准备就绪后，单击 “创建堆栈”。

   堆栈最多可能需要一分钟才能创建。成功创建堆栈后，您的补丁维护窗口将在指定的时间运行。您可以通过创建和执行 CloudFormation 更改集（推荐）（有关执行此操作的详细信息，请参阅使用变更集创建堆栈）或在 Systems Manager 维护窗口控制台上更新补丁维护窗口（ ）来更改补丁维护窗口（ ）。https://console.aws.amazon.com/systems-manager/maintenance-windows

观看 Namrata 的视频以了解更多信息 (5:41)

通过 Systems Manager 控制台为 AMS Accelerate 创建维护窗口

要从 Systems Manager 控制台创建 AMS 加速维护窗口，请执行以下步骤：

1. 在 “变更管理” 区域的左侧导航栏中，单击 “维护窗口”，然后单击屏幕右上角的 “创建维护窗口”。填写表格。有关任何选项的详细信息，请参阅创建维护窗口（控制台）。完成后，单击 “创建维护窗口”。

   维护时段列表页面打开。
2. 选择新创建的维护时段。

   维护时段详细信息页面打开。
3. 转到目标选项卡，然后选择注册目标。

   将打开 “注册目标” 页面。
4. 添加你的加速目标。有关目标的信息，请参阅将目标分配给维护时段（控制台）。完成后，单击 “注册目标”。以后需要时记下目标。

   维护时段详细信息页面在 “目标” 选项卡上重新打开，其中包含新目标的列表。
5. 在维护时段详细信息页面的任务选项卡上，选择注册任务，然后从下拉列表中选择注册自动化任务。填写表格。加速笔记：

   - 提供一个有意义的任务名称。例如： AcceleratePatch。
   - 在自动化文档区域中，单击搜索框，选择所有者，然后选择共享文档。

- 在搜索框中单击并选择文档名称前缀--> 等于，然后键入:，即可选择自动化文档。AWSManagedServices-PatchInstance然后通过选择AWSManagedServices-PatchInstance文档的单选按钮来选择该文档。
- 在 “文档版本” 下，选择 “运行时的默认版本”。
- 在 “目标” 部分中：
  - 将目标设置为：选择已注册的目标组。
  - 在目标列表中，选择您在目标选项卡中注册的目标。
- 在 “输入参数” 部分，填写表单。
  - InstanceId: {{*TARGET_ID*}}
  - StartInactiveInstances: `True` 如果实例在补丁维护窗口期间停止，则启动这些实例。

> **Note**
>
> InstanceId参数值区分大小写，StartInactiveInstances参数值可以为 True 或 False。当被标签定位时，已停止的实例无法启动。有关更多信息，请参阅没有可执行的调用。

- 在 “速率控制” 部分中，选择百分比。AMS A cc el erate 建议并发度为 100%，错误阈值为 100%，以便尝试同时修补所有实例，无论自动化错误如何。例如，如果您希望一次修补一半的目标，以保持负载平衡后面的一半目标实例运行，请将并发设置为 50%。
- 在 IAM 服务角色部分，选择使用自定义服务角色，然后选择 ams_ssm_automation_role。

单击 “注册自动化任务”。

修补维护窗口已创建。在 “描述” 选项卡下，您可以看到下次执行时间。

使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口

要使用命令行界面创建 AMS 加速维护窗口，请执行以下操作：

1. 按照 SSM 教程进行操作：创建和配置维护窗口 (AWS CLI)。对于本教程的每个步骤，以下是用于修补的 CLI 命令示例。

> **Note**
>
> 这些示例特定于 Linux 或 macOS。也可以运行这些命令，使用 AWS CloudShell 这些命令可能比在本地计算机awscli上配置更简单。有关详细信息，请参阅使用 AWS CloudShell。

a. 在本教程的第 1 步中，要创建维护窗口，请执行以下操作：

```
aws ssm create-maintenance-window \
                --name Sample-Maintenance-Window \
                --schedule "cron(0 30 23 ? * TUE#2 *)" \
                --duration 4 \
                --cutoff 1 \
                --allow-unassociated-targets \
                --tags "Key=Environment,Value=Production"
```

成功完成后window-id，返回。

b. 在本教程的第 2 步中，要注册目标节点，请执行以下操作：

```
aws ssm register-target-with-maintenance-window \
                --window-id "mw-xxxxxxxxx" \
                --resource-type "INSTANCE" \
                --target "Key=tag:Environment,Values=Prod"
```

成功完成后，返回 WindowTargetID s。

c. 在本教程的第 3 步中，要注册任务，请执行以下操作：

```
aws ssm register-task-with-maintenance-window \
    --window-id "mw-xxxxxx" \
    --targets "Key=WindowTargetIds,Values=63d4f63c-xxxxxx-9b1d-xxxxxfff" \
    --task-arn "AWSManagedServices-PatchInstance" \
    --service-role-arn "arn:aws:iam::AWS-Account-ID:role/ams_ssm_automation_role"
 \
    --task-invocation-parameters "{\"Automation\":{\"DocumentVersion\":\"\$DEFAULT
\",\"Parameters\":{\"InstanceId\":[\"{{TARGET_ID}}\"],\"StartInactiveInstances\":
[\"True\"]}}}" \
    --max-concurrency 50 \
    --max-errors 50 \
    --name "AutomationExample" \
```

```
    --description "Sample Description" \
    --task-type=AUTOMATION
```

带挂钩的补丁

您可以使用 AMS 补丁挂钩将 AMS 修补配置为在修补之前和之后运行操作系统 (OS) 级别的命令。使用 AMS 补丁挂钩运行 SSM Command 文档以在修补之前停止服务，然后在修补后启动服务，或者运行命令以确认您的应用程序在修补后是否运行正常。

要使用 AMS 补丁挂钩，您需要执行以下操作：

1. 创建 SSM 命令文档以用作补丁挂钩。
2. 创建 AMS 补丁维护窗口，或使用现有的 AMS 补丁维护窗口。有关详细信息，请参阅 AMS 补丁维护窗口。
3. 配置 AMS 补丁维护窗口，以便使用您的 SSM 命令文档来处理 AMS 补丁挂钩。

AMS 补丁挂钩 RACI

负责任、负责、咨询和知情矩阵或 RACI 矩阵将各种活动的主要责任分配给客户或 AMS。下表概述了客户和 AMS 在使用 AMS 补丁挂钩的应用程序中活动的责任。

- R 代表负责完成任务的责任方
- A 代表责任方
- C 代表咨询；征求意见的一方，通常是作为主题专家征求意见的一方；以及与之进行双边沟通的当事人
- 我代表知情；通报进展情况的一方，通常只有在任务或可交付成果完成后才获悉进展情况

活动	Customer	AMS
创建 pre/post 补丁 SSM 命令文档和文档内容	R	C
为 AMS 修补配置补丁挂钩参数	R	C

活动	Customer	AMS
执行 pre/post 补丁 SSM 命令文档	我	R
对补丁挂钩故障进行分类和响应	我	R
通知客户补丁挂钩故障	我	R
如果客户要求，可回滚到补丁前状态	C	R

为补丁挂钩创建 SSM 文档

AMS 补丁挂钩在修补期间使用 Amazon S EC2 ystems Manager (SSM) 文档。使用进行修补的帐户创建 SSM 命令文档或共享现有的 SSM 命令文档。有关 SSM 文档的信息（包括限制），请参阅共享 SSM 文档。

要创建 SSM 命令文档，请执行以下步骤：

1. 创建一个 SSM 文档，文档类型为 “命令”。
2. 在 “内容” 部分中输入您的命令。有关更多信息，请参阅创建 SSM 文档内容。

> **Note**
>
> 也可以使用 AWS CLI 或 CloudFormation创建 AMS 补丁挂钩的 SSM 文档。如果您在为 AMS 补丁挂钩创建 SSM 文档时需要帮助，请联系您的云架构师。

配置 AMS 补丁维护窗口以使用您的 SSM 命令文档作为 AMS 补丁挂钩

AMS 补丁维护窗口是一个 Systems Manager 维护窗口，用于执行您配置的 AMS 补丁自动化。

要编辑 AMS 补丁维护窗口以使用补丁挂钩，请按照以下步骤操作：

1. 在左侧导航窗格的变更管理工具下，选择维护窗口。https://console.aws.amazon.com/systems-manager/

将打开一个列出现有维护窗口的页面。

2. 选择以 mw- 开头的窗口 ID。

将打开该维护窗口的详细信息页面。

3. 选择 “任务” 选项卡和带有任务 ARN 为 AMS- 的窗口任务 ID，PatchInstance然后单击 “编辑”。

4. 向下滚动到 “参数” 部分并更新以下参数。

AMS 补丁挂钩参数：

- PrePatchHook：要在打补丁之前运行的类型为 “命令” 的 SSM 文档的名称。如果您在修补之前没有运行命令，请将其留空或键入 “AWS-noop”（区分大小写）。
- PostPatchHook：打补丁后要运行的 SSM 文档的名称，类型为 “命令”。如果您在修补后没有运行命令，请将其留空或键入 “AWS-noop”（区分大小写）。
- ExecutePatchBasedOnPreHookStatus: 根据运行成功或失败 PrePatchHook 运行补丁，选择一个：
  - OnPreHookSuccess：仅在成功后运行 AMS 补丁自动化。 PrePatchHook
  - 始终：成功和失败时运行 AMS 补丁自动化。 PrePatchHook
  - OnPreHookFailure-仅在 PrePatchHook 失败时运行 AMS 补丁自动化。
  - 从不：不要运行 AMS 补丁自动化。这在测试你的时可能很有用 PrePatchHook。
- ExecutePostHookBasedOnPatchStatus: 根据 AMS 补丁自动化的成功或失败运行补丁后挂钩，选择一个：
  - OnPatchSuccess：仅 PostPatchHook 当 AMS 补丁自动化成功运行时才运行。
  - 始终： PostPatchHook 当 AMS 补丁自动化成功和失败时运行。
  - OnPatchFailure- PostPatchHook 仅在 AMS 补丁自动化失败时运行。

> **Note**
>
> 如果这些变量中的任何一个缺少其文本框，请向上滚动到同一页面上的 “自动化文档” 部分，选择其他文档，然后重新选择原始文档来解决这个问题。这会刷新输入参数，以便您可以对其进行编辑。

AMS 加速补丁基准

补丁基准定义批准在您的实例上安装的补丁。您可以逐个指定批准或拒绝的补丁。也可以创建自动批准规则，指定应自动批准的某些更新类型 (例如重要更新)。拒绝补丁列表将覆盖这些规则和批准列表。

默认补丁基准

当您加入 AMS Accelerate 补丁时，默认补丁基准将被以下操作系统的 AMS Accelerate 默认补丁基准所覆盖。

- Windows
- Amazon Linux 1
- Amazon Linux 2
- CentOS
- Suse
- Rhel
- Ubuntu

> **Important**
>
> 默认补丁基准由 AMS 管理。请勿编辑默认补丁基准，因为您的更改可能会丢失。相反，请创建自定义补丁基准。请参阅 使用 AMS Accelerate 自定义补丁。

> **Note**
>
> 定义为 product = * 的 AMS Accelerate 补丁基准意味着所有补丁都适用于所有安全和分类的实例。

使用 AMS Accelerate 自定义补丁

要在 AMS Accelerate 中使用自定义补丁基准，请先确保您有补丁组，然后创建自定义基准。

有关更多信息，请参阅以下资源：

- 使用补丁组

- 创建自定义补丁基准 (Windows)
- 创建自定义补丁基准 (Linux)
- 更新或删除自定义补丁基准（控制台）

创建 IAM 角色以按需修补 AMS Accelerate

在您的账户加入 AMS Accelerate 补丁后，AMS Accelerate 会部署托管策略，即 amspatchmanagedpolicy。此策略包含使用 AMS 自动化文档`AWSManagedServices-PatchInstance`进行按需修补所需的权限。要使用此自动化文档，账户管理员需要为用户创建一个 IAM 角色。按照以下步骤进行操作：

使用以下方法创建角色 AWS 管理控制台：

1. 登录 AWS 管理控制台 并打开 IAM 控制台。
2. 在控制台的导航窗格中，选择角色，然后选择创建角色。
3. 选择其他 AWS 账户角色类型。
4. 在账户 ID 中，输入您想要授予资源访问权限的 AWS 账户 ID。

   指定账户的管理员可向该账户中的任何 IAM 用户授予担任该角色的权限。为此，管理员向用户或群组附加一个策略，授予 sts: AssumeRole 操作的权限。该策略必须将角色的 Amazon 资源名称 (ARN) 指定为资源。请注意以下几点：

   - 如果您向来自您无法控制的账户的用户授予权限，并且这些用户将以编程方式担任此角色，请选择 “需要外部 ID”。外部 ID 可以是您和第三方账户管理员之间达成一致的任何字词或数字。此选项会自动向信任策略添加一个条件，即只有在请求包含正确的 STS: externalID 时，用户才能代入该角色。有关更多信息，请参阅在向第三方授予对您的 AWS 资源的访问权限时如何使用外部 ID。
   - 如果要将角色限制为使用多重身份验证 (MFA) 登录的用户，请选择需要 MFA。这将向角色的信任策略中添加用于检查 MFA 登录的条件。需要担任角色的用户必须使用配置的 MFA 设备中的临时一次性密码进行登录。没有 MFA 身份验证的用户无法担任该角色。有关 MFA 的更多信息，请参阅中的使用多重身份验证 (MFA)。 AWS
5. 选择下一步: 权限。

   IAM 包含账户中的策略列表。在 “添加权限” 下，在筛选框中输入 amspatchmanagedpolicy，然后选中此权限策略的复选框。单击下一步。
6. 在角色详细信息下，输入角色名称 PatchRole，例如，添加角色描述（推荐），并添加标签以帮助您识别此角色。角色名称不区分大小写，但必须是唯一的 AWS 账户。完成后，单击 “创建角色”。

> **Note**
>
> 角色名称在创建后无法进行编辑。

了解 AMS Accelerate 中的补丁通知和补丁故障

> **Important**
>
> 从 2025 年 2 月 1 日起，AMS 客户将不再在其托管账户中收到补丁维护窗口为空的通知。

补丁服务请求和电子邮件通知

AMS 在下一个补丁维护窗口之前四天创建新的服务请求。例如，在名为 App1 PROD 的补丁维护窗口运行前四天，AMS 为 App1 Prod for Account [账户 ID] 创建了一个名为 “四月补丁维护窗口” 的服务请求。如果您需要调整计划补丁或跳过即将发布的补丁，请使用补丁服务请求与 AMS 沟通。创建服务请求后，系统会向您的补丁通知地址发送一封包含服务请求链接的电子邮件。每当 AMS 更新服务请求时，您都会收到一封额外的电子邮件。

> **Note**
>
> 即使补丁维护窗口是在计划运行前不到四天创建的，AMS 也会创建新的服务请求。修补程序维护窗口必须处于 “启用” 状态才能接收服务请求通知。

在修补开始前一小时，AMS 会通过补丁服务请求通知您。修补完成后，AMS 会使用指向 Patch Manager 控制台的链接更新补丁服务请求。使用该链接查看补丁维护窗口所针对的实例的补丁合规性。

> **Note**
>
> Patch Manager 控制台中的链接显示了实例的当前合规性。如果在 AMS 完成修补和您访问链接之间发布了新补丁，则补丁管理器会将实例显示为不合规。

通过 CloudWatch 事件发送补丁通知

在补丁过程中，AMS 会发送三次 CloudWatch 事件，包括：

- 在补丁维护窗口运行前四天。
- 补丁维护窗口运行前一小时。
- 补丁维护窗口结束时。

以下是补丁维护窗口高级通知事件架构：

```
{
    "version": "0",
    "id": "37004d81-458d-2cef-fe1c-8afa8af30406",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "145917996532",
    "time": "2021-05-20T02:00:00Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {
        "State": "PREEMPTIVE",
        "StartTime": "2021-05-24T02:00:00.000000",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\"}, {\"instanceId\":
 \"i-0000000aaaaaaaaab\"}]"
    }
}
```

下表描述了补丁维护窗口预先通知事件架构：

补丁通知详情

属性名称	说明	样本值
状态	修补维护时段的状态	PREEMPTIVE-补丁窗口计划很快开始

属性名称	说明	样本值
状态	修补维护窗口的状态	成功-所有实例均已修补完毕，未出现故障 失败 — 至少有一个实例无法修补
StartTime	修补维护时段的开始时间，采用 ISO 格式	2021-02-03T 22:14:05 .814 308
WindowArn	修补维护窗口的唯一标识符	arn: aws: ssm: us-east-1 :123456789012: maintance window/mw-00000001235
结果	补丁窗口所针对的实例列表	InstanceId — 目标实例的实例 ID

以下是补丁维护窗口结束事件架构：

```
{"version": "0",
    "id": "0f25add5-44a9-0702-d2bc-bd2102affefe",
    "detail-type": "AMS Patch Window Execution State Change",
    "source": "aws.managedservices",
    "account": "123456789012",
    "time": "2021-02-03T22:14:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/mw-00000001235",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaab"
    ],
    "detail": {"State": "[COMPLETED]",
        "Status": "SUCCESS",
        "StartTime": "2021-02-03T22:12:00.814308",
        "EndTime": "2021-02-03T22:14:05.814309",
        "WindowArn": "arn:aws:ssm:us-east-1:123456789012:maintenancewindow/
mw-00000001235",
        "WindowExecutionId": "e32088eb-c05f-4c63-b766-6866e163c818",
        "Results": "[{\"instanceId\": \"i-0000000aaaaaaaaaa\", \"status\":
 \"Success\", \"missing_critical_patch_count\": 0, \"missing_total_patch_count
```

```
\": 0} }, {\"instanceId\": \"i-0000000aaaaaaaaab\", \"status\": Success},
 \"missing_critical_patch_count\": 0, \"missing_total_patch_count\": 0}]"
    }
}
```

下表描述了补丁维护窗口结束事件架构：

补丁窗口结束细节

属性名称	说明	样本值
状态	修补维护时段的状态	已完成-修补窗口已完成
状态	修补维护窗口的状态	成功-所有实例都已修补完毕，没有出现故障 失败 — 至少有一个实例无法修补
StartTime	修补维护时段的开始时间，采用 ISO 格式	2021-02-03T 22:14:05 .814 308
EndTime	修补维护时段的结束时间，采用 ISO 格式	2021-02-03T 23:14:05 .814 308
WindowArn	修补维护时段的唯一标识符。	arn: aws: ssm: us-east-1 :123456789012: maintance window/mw-00000001235
WindowExecutionId	窗口执行 ID，可以从 SSM 维护窗口控制台中看到	e32088eb-c05f-4c63-b766-6866e163c818
结果	补丁窗口将瞄准的实例列表	InstanceId — 目标实例 ID 状态 — 实例补丁状态 missing_critical_patch_count-实例上缺少的关键补丁数量 missing_total_patch_count-实例上缺失的补丁总数

您可以使用 Events CloudWatch 事件来触发一条 CloudWatch 规则，该规则会在发送修补维护窗口预先通知时通知您。为此，请使用以下配置配置 CloudWatch 规则：

```
{
    "source": [
        "aws.managedservices"
    ],
    "detail-type": [
        "AMS Patch Window Execution State Change"
    ],
    "detail": {
        "State": ["PREEMPTIVE"]
    }
}
```

> **Note**
>
> 不会为操作系统不支持的实例创建补丁失败警报，也不会为在维护时段内停止的实例创建补丁失败警报。

AMS 中的补丁失败调查

AWS Managed Services (AMS) 负责管理补丁并包括补丁故障修复。修补失败时，AMS 运营部门会收到警报，并尝试按照 AWS AMS 最佳实践进行补救以解决问题。

<instance-id>如果补丁失败，AMS 会在账户 OpsItem 中创建一个 SSM，标题如下：AWS Managed Services — 例如补丁实例故障。

然后，AMS进行调查. OpsItem 如果 AMS 可以在没有您干预的情况下纠正故障，那么 AMS 就会解决。 OpsItem如果需要您的干预，AMS 会通过包含调查结果和建议补救步骤的服务请求通知您。如果您不采取措施来解决问题，AMS 会尝试在下一个预定的补丁维护窗口期间修补实例。

> **Note**
>
> 对于操作系统 OpsItems 不支持的实例，或者在补丁维护时段内处于 “已停止” 状态的实例，不会造成补丁失败。

使用 AMS 资源调度器进行成本优化

AMS Resource Scheduler on AWS 解决方案通过停止未使用的资源 AWS 并在需要容量时启动资源来帮助您降低和 AMS 的成本。例如，您可以在开发环境中使用 AMS 资源调度器， AWS 在每天工作时间以外自动停止实例。如果您让所有实例以最大利用率运行，则此解决方案可能会降低实例利用率，从而根据您配置的计划降低总体成本。

使用 AWS Managed Services (AMS) 资源计划程序安排账户中 Auto Scaling 组、Amazon EC2 实例和 Amazon RDS 实例的自动启动和停止。在资源本来不打算全天候运行的情况下，这有助于降低基础设施成本。该解决方案建立在AWS 实例调度器之上，但包含针对 AMS 客户需求的其他功能和自定义设置。自定义包括对安排 Auto Scaling 群组的支持、 CloudWatch Elastic Load Balancing 警报的警报抑制器、对亚马逊多个 AWS Systems Manager 维护窗口的支持 EC2、成本节省估算器以及 AMS 的运营支持。

AMS 资源调度器使用周期和计划。周期定义资源应运行的时间，例如开始时间、结束时间和当月中的几天。计划包含您定义的时间段以及其他配置（SSM 维护时段、时区、休眠等），并指定资源何时运行。您可以使用 AMS 提供的 AWS Systems Manager 自动化运行手册来配置这些时间段和计划。每个计划必须包含至少一个时间段，用于定义实例应运行的时间。一个时间表可以包含多个时段。如果计划中使用了多个时段，则当至少有一个周期规则为真时，实例计划程序会应用相应的启动操作。有关计划和周期的更多详细信息，请参阅 AWS 实例计划程序的解决方案组件。

AMS Resource Scheduler 使用 AWS 资源标签将计划与一个或多个资源相关联，以便将这些资源作为定时启动和停止操作的目标。您可以使用计划程序中配置的标签密钥（默认为`Schedule`）来标记资源，并将计划名称作为值。您可以在 Scheduler 的成本估算器功能中 AWS Cost Explorer 配置与成本分配标签相同的标签密钥，以跟踪和报告成本节省情况。

AMS 资源调度器是一项选择加入功能，您可以按账户启用。

通过 AMS 资源调度器使用资源

Amazon EC2

- 作为 Auto Scaling 组一部分的 Amazon EC2 实例不会单独处理，也不会被 AMS 资源计划程序跳过，即使它们已被标记。
- 如果目标实例根卷使用 AWS KMS 客户主密钥 (CMK) 加密，则需要向您的资源调度器 IAM 角色添加额外的`kms:CreateGrant`权限，以便计划程序能够启动此类实例。为了提高安全性，默认情况下不会向角色添加此权限。如果您需要此权限，则可以通过更新 CloudFormation 堆栈来添加权限`ams-resource-scheduler`，并将 CMK 列表作为`UseCMK`参数的值（使用格式 ARNs 中的一

个或多个 CMK 密钥`arn:partition:kms:region:account-id:key/key-id`而不是 KMS 别名）。

- 如果您的 Amazon EC2 实例配置了特定的软件或由管理的供应商许可证 AWS License Manager，则资源调度器需要获得特定 AWS License Manager 许可证的权限才能启动该实例。您可以通过将许可证 ARN 列表添加到堆栈`ams-resource-scheduler`的许可证管理器许可参数 () AWS License Manager 中， EC2 为资源调度器授予必要的权限。 CloudFormation

Amazon A EC2 uto Scaling

- AMS 资源调度器启动或停止 Auto Scaling 组的自动扩展，而不是组中的单个实例。也就是说，调度器恢复 Auto Scaling 组的大小（开始）或将大小设置为 0（停止）。
- 使用指定的标签为 Auto Scaling 组添加标签，而不是该组中的实例。
- 在停止期间，AMS 资源调度器会存储 Auto Scaling 组的最小、所需和最大容量值，并将最小和所需容量设置为 0。在启动期间，调度器会将 Auto Scaling 组的大小恢复为停止时的状态。因此，Auto Scaling 组实例必须使用适当的容量配置，这样实例的终止和重新启动就不会影响在 Auto Scaling 组中运行的任何应用程序。
- 如果在运行期间修改 Auto Scaling 组（最小或最大容量），则计划程序会存储新的 Auto Scaling 组大小，并在停止计划结束时恢复该组时使用该大小。

Amazon RDS

- 调度器可以在停止 RDS 实例之前拍摄快照（不适用于 Aurora 数据库集群）。此功能默认处于开启状态，创建 RDS 实例快照 AWS CloudFormation 模板参数设置为 true。快照将一直保留到下次停止 Amazon RDS 实例并创建新快照为止。
- 调度器可以是属于集群或 start/stop Amazon RDS Aurora 数据库或多可用区（多可用区）配置的 Amazon RDS 实例。但是，当计划程序无法停止 Amazon RDS 实例（尤其是多可用区实例）时，请检查 Amazon RDS 限制。
- 要安排 Aurora 集群的启动或停止，请使用安排 Aurora 集群模板参数（默认为 t rue）。Aurora 集群（不是集群中的单个实例）必须使用初始配置期间定义的标签键进行标记，并将计划名称作为标签值来调度该集群。

> **Note**
>
> 资源调度器不验证资源是否已启动或停止。它为相关服务发出 API 调用并继续前进。如果 API 调用失败，它会记录错误以供调查。

AMS 资源调度器不支持 AWS Backup 窗口。如果您将 AWS Backup启用了 RDS 实例与资源计划程序计划进行映射，则要使备份按预期运行，备份窗口必须位于计划的运行窗口内。

入门 AMS 资源调度器

当您的账户加入 AMS Accelerate 运营计划时，您的账户不会自动加入 AMS 资源计划程序。但是，作为账户注册加入 AMS Accelerate 运营计划的一部分，或者之后的任何时候，您可以请求您的云服务交付经理 (CSDM) 将该账户加入 AMS 资源计划程序。在您的 CSDM 加入账户后，包含默认配置的 AMS 资源调度器资源的 CloudFormation 堆栈将自动配置到您的账户中。

在您的账户中配置 AMS 资源调度器后，我们建议您查看默认配置，并在需要时根据自己的偏好自定义配置，例如标签密钥、时区、计划服务等。有关推荐的自定义项的详细信息自定义 AMS 资源调度器，请参阅 “下一步”。

自定义 AMS 资源调度器

启动后，AMS 资源调度器将以 CloudFormation 堆栈的形式部署在您的 AMS Accelerate 账户的主要 AWS 区域中`ams-resource-scheduler`，并带有名称。您可以根据自己的偏好通过 CloudFormation 堆栈参数和执行堆栈更新来配置 AMS 资源调度器的属性。有关更新 CloudFormation 堆栈的信息，请参阅直接更新堆栈。

我们建议您自定义以下属性，并将其余属性保留为默认值，以获得最佳功能。

- 标签名称：资源调度器将用于将实例计划与资源关联的标签的名称。默认值为 `Schedule`。
- 要调度的服务：以逗号分隔的资源调度器可以管理的服务列表。默认值为“`ec2,rds,autoscaling`”。有效值为 “ec2”、“rds” 和 “自动缩放”。
- 默认时区：指定资源调度器要使用的默认时区。默认值为 `UTC`。
- 加密 EBS 卷的 CMK：以逗号分隔的 Amazon KMS 客户托管密钥 (CMK) 列表 ARNs ，资源调度器可以被授予访问权限。
- EC2 例如，许可证管理器许可：可以 ARNs 向该资源调度器授予权限的以逗号分隔的 AWS 许可证管理器列表。

Note

AMS 偶尔会发布功能和修复程序，以使您的账户中的 AMS 资源调度器保持最新状态。发生这种情况时，您通过堆栈参数对 AMS 资源调度器堆栈所做的任何自定义都将保留。

我们强烈建议不要直接对 AMS 资源调度程序的任何组件资源进行任何自定义。这样做会影响资源调度程序的功能以及 AMS 使其保持最新状态的能力。

使用 AMS 资源调度器

如何在 AMS 加速账户中使用 AMS 资源调度器周期。

使用以下一组 AWS Systems Manager 自动化运行手册在 AMS 资源计划程序中管理所需的时间表和周期。

Note

这些 SSM 自动化操作手册可在您账户的主要 AWS 区域中找到。

- `AWSManagedServices-AddOrUpdatePeriod`
- `AWSManagedServices-AddOrUpdateSchedule`
- `AWSManagedServices-DeleteScheduleOrPeriod`
- `AWSManagedServices-DescribeScheduleOrPeriods`
- `AWSManagedServices-EnableOrDisableAMSResourceScheduler`

此外，AMS 还规定了一个 AWS Systems Manager 需要和承担的 AWS Identity and Access Management 角色才能使用运行手册。`ams_resource_scheduler_ssm_automation_role`IAM 角色的范围由最低权限内联策略限制，该策略授予 Runbook 功能所需的 SSM 权限。

先决条件

在开始使用 SSM 自动化运行手册和 AMS 资源计划程序之前，请执行以下步骤。

将以下策略附加到您希望允许其使用自动化运行手册管理 AMS 资源计划程序中的计划和周期的相应 IAM 实体（用户、群组或角色）。如果您的 IAM 实体在您的账户中拥有管理员或 PowerUser 权限，则无需使用该政策。

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowPassingResourceSchedulerRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/
ams_resource_scheduler_ssm_automation_role",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Sid": "ListAndDescribeAutomationExecutions",
            "Effect": "Allow",
            "Action": [
                "ssm:GetAutomationExecution",
                "ssm:DescribeAutomationStepExecutions"
            ],
            "Resource": "arn:aws:ssm:*:111122223333:automation-execution/*"
        },
        {
            "Sid": "ListAndDescribeResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:ListDocumentVersions",
                "ssm:DescribeDocument",
                "ssm:ListDocumentMetadataHistory",
                "ssm:DescribeDocumentParameters",
                "ssm:GetDocument",
                "ssm:DescribeDocumentPermission"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdatePeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-AddOrUpdateSchedule",
                "arn:aws:ssm:*::document/AWSManagedServices-
DeleteScheduleOrPeriod",
                "arn:aws:ssm:*::document/AWSManagedServices-
DescribeScheduleOrPeriods",
                "arn:aws:ssm:*::document/AWSManagedServices-
EnableOrDisableAMSResourceScheduler"
            ]
        },
```

```
        {
            "Sid": "AllowExecutionOfResourceSchedulerSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:StartAutomationExecution"
            ],
            "Resource": [
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdatePeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
AddOrUpdateSchedule:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DeleteScheduleOrPeriod:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
DescribeScheduleOrPeriods:*",
                "arn:aws:ssm:*::automation-definition/AWSManagedServices-
EnableOrDisableAMSResourceScheduler:*"
            ]
        },
        {
            "Sid": "AllowListingAllDocuments",
            "Effect": "Allow",
            "Action": "ssm:ListDocuments",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingAllSSMExecutions",
            "Effect": "Allow",
            "Action": "ssm:DescribeAutomationExecutions",
            "Resource": "*"
        },
        {
            "Sid": "AllowListingIAMRolesForStartingExecutionViaConsole",
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        }
    ]
}
```

您可以从 AWS Systems Manager 控制台或使用 AWS CLI 运行自动化。如果使用 AWS CLI，则可能需要安装和配置它或 AWS 工具（如果还没有）。 PowerShell有关信息，请参阅安装或升级 AWS 命令行工具。

观看 Navish 的视频以了解更多信息 (4:52)

在 AWS Managed Services 资源计划程序中处理时间段和计划

您可以使用 AMS 资源调度器在 AMS Accelerate 账户中添加、更新或删除计划或时段。

在 AMS 资源调度器中添加或更新周期

在您的 AMS 账户中添加或更新资源计划周期。

你需要的数据：

- 操作：要执行的操作类型。如果要添加期间，请使用 “添加”；如果要更新现有期间，请使用 “更新”。
- 名称：期间的名称。如果要添加新周期，则必须指定唯一值。
- AutomationAssumeRole： AWS Identity and Access Management (IAM) 角色的 ARN，允许运行手册代表您添加或更新周期。将角色指定为`ams_resource_scheduler_ssm_automation_role`。
- 描述（可选）：对期间的有意义的描述。
- BeginTime（可选）：您要启动资源的时间，采用 HH: MM 格式。
- EndTime（可选）：您要停止资源的时间，采用 HH: MM 格式。
- 月（可选）：以逗号分隔的月份列表或用连字符连接的月份范围，资源应在此期间运行。
- MonthDays（可选）：以逗号分隔的当月天数列表或以连字符表示的资源运行天数范围。
- WeekDays（可选）：以逗号分隔的列表，列出资源应在一周中的几天或一周中的某几天范围。

怎么做：

- 在以下位置查看文档 AWSManagedServices-AddOrUpdatePeriod（您可能需要选择您的入职区域）。

  在输入参数部分中指定要求，然后选择执行。操作完成后，在 “输出” 选项卡中查看结果。
- AWS CLI：

  运行以下命令以启动自动化。*`placeholders`*用您自己的信息替换。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdatePeriod" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"],
    "Description":["DESCRIPTION"],"BeginTime":["TIME"], "EndTime":["TIME"],
    "Months":["MONTH"],"MonthDays":["DAY"], "WeekDays":["DAY"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

示例：

以下示例显示了如何使用 AWS Systems Manager 控制台添加新时段。我们已经命名了周期名称，并将其配置为涵盖每月前 15 天的周一至周五上午 9 点至下午 6 点。

1. 在以下 AWS Systems Manager 位置查看自动化文档 AWSManagedServices-AddOrUpdatePeriod（您可能需要选择已上线的区域）。

2. 为参数提供值。

3. 单击 “执行”，等待自动化完成。

在 AMS 资源调度器中添加或更新计划

在 AMS Accelerate 账户中添加或更新资源计划表。

你需要的数据：

- 操作：要执行的操作类型。如果要添加计划，请使用 “添加”；如果要更新现有计划，请使用 “更新”。
- 名称：时间表的名称。如果要添加新计划，则必须指定唯一值。
- AutomationAssumeRole：允许运行手册代表您添加或更新计划的 AWS Identity and Access Management (IAM) 角色的 ARN。指定角色`ams_resource_scheduler_ssm_automation_role`。
- 描述（可选）：对时间表的有意义的描述。
- 计划（可选）：指定要用于此计划的时段的逗号分隔列表。每个周期都必须已经创建。
- RetainRunning（可选）：如果资源是在运行周期开始之前手动启动的，则指定 “true” 可防止资源调度器在运行周期结束时停止正在运行的资源。默认情况下，资源调度器会停止资源。

- StopNewInstances（可选）：指定 “false” 以防止资源调度器在首次标记资源时停止该资源（如果该资源在运行期之外运行）。默认情况下，资源调度器会停止资源。
- SSMMaintenance窗口（可选）：指定以逗号分隔的 AWS Systems Manager (SSM) 维护时段列表，您要将其添加为计划的运行时段。您还必须将 “” 属性指定UseMaintenanceWindow为 “true”。
- TimeZone（可选）：指定您希望资源调度器使用的时区。默认情况下，资源调度器使用 UTC。
- UseMaintenanceWindow（可选）：如果您希望资源调度器将亚马逊关系数据库服务 (RDS) 维护窗口视为 Amazon RDS 实例计划的运行期，或者将 AWS Systems Manager (SSM) 维护时段作为运行时间添加到亚马逊实例计划中，请指定 “true”。 EC2
- UseMetrics（可选）：指定 “true” 可在计划级别启用 CloudWatch 指标，指定 “false” 则禁用 CloudWatch 指标。指定此属性会覆盖在堆栈级别设置的 CloudWatch 指标设置。

怎么做：

- 在以下位置查看文档 AWSManagedServices-AddOrUpdateSchedule（您可能需要选择您的入职区域）。

  在 “输入参数” 部分中指定要求，然后选择 “执行”。操作完成后，在 “输出” 选项卡中查看结果。

- AWS CLI：

  运行以下命令以启动自动化。*placeholders*用您自己的信息替换。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
AddOrUpdateSchedule" --document-version "\$DEFAULT"
     --parameters '{"Action":["add" or "update"], "Name":["NAME"], "Description":
["DESCRIPTION"],
    "Hibernate":["true or false"],"Enforced":["true or false"],
    "OverrideStatus":["running or stopped"],"Periods":["PERIOD-A, PERIOD-B"],
    "RetainRunning":["true or false"],"StopNewInstances":["true or false"],
    "SSMMaintenanceWindow":["WINDOW-NAME"],"TimeZone":["TIMEZONE"],
    "UseMaintenanceWindow":["true or false"],"UseMetrics":["true or false"],
    "AutomationAssumeRole" : ["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"] }' --region ONBOARDED_REGION
```

示例：

以下示例说明如何为 AMS 资源调度器添加计划。在此示例中，您添加了一个名为的计划，名为 CustomSchedule 使用 CustomPeriod。

1. 在以下 AWS Systems Manager 位置查看自动化文档 AWSManagedServices-AddOrUpdateSchedule（您可能需要选择已上线的区域）。

2. 为参数提供值。

3. 单击 “执行”，等待自动化完成。

在 AMS 资源调度器中删除时间段或计划

要删除 AMS Accelerate 账户中的资源调度器周期或计划，您需要以下数据：

- ConfigurationType：要删除的配置类型。如果要删除期间，请使用 “周期”；如果要删除计划，请使用 “计划”。
- 名称：要删除的计划或期间的名称。
- AutomationAssumeRole： AWS Identity and Access Management (IAM) 角色的 ARN，它允许运行手册代表您删除计划或时段。指定角色`ams_resource_scheduler_ssm_automation_role`。

怎么做：

- 在以下位置查看文档 AWSManagedServices-DeleteScheduleOrPeriod（您可能必须选择您的已上线区域）。

  在输入参数部分中指定要求，然后选择执行。操作完成后，在 “输出” 选项卡中查看结果。

- AWS CLI：

  运行以下命令以启动自动化。*`placeholders`*用您自己的信息替换。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DeleteScheduleOrPeriod" --document-version "\$DEFAULT"
--parameters '{"ConfigurationType":["period" or "schedule"],"Name":["NAME"],
    "AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}' --region ONBOARDED_REGION
```

示例：

以下示例说明如何使用 AWS Systems Manager 控制台删除句点。

1. 在以下 AWS Systems Manager 位置查看自动化文档 AWSManagedServices-DeleteScheduleOrPeriod（您可能需要选择已上线的区域）。

2. 为参数提供值。

3. 单击 “执行”，等待自动化完成。

在 AMS 资源调度器中描述时间段或日程安排

为了描述（查看详情）AMS Accelerate 账户中的资源调度周期或计划，您需要以下数据：

- ConfigurationType：您要描述的配置类型。如果要描述所有时段，请使用 “周期”；如果要描述所有时间表，请使用 “时间表”。
- AutomationAssumeRole： AWS Identity and Access Management (IAM) 角色的 ARN，它允许运行手册代表你描述日程安排或时段。指定角色`ams_resource_scheduler_ssm_automation_role`。

怎么做：

- 在以下位置查看文档 AWSManagedServices-DescribeScheduleOrPeriods（您可能需要选择已上线区域）：
  1. 在 “输入参数” 部分中指定要求，然后选择 “执行”。
  2. 操作完成后，在 “输出” 选项卡中查看结果。
- AWS CLI：
  1. 运行以下命令以启动自动化。*`placeholders`*用您自己的信息替换。

```
aws ssm start-automation-execution --document-name "AWSManagedServices-
DescribeScheduleOrPeriods" --document-version "\$DEFAULT"
                --parameters '{"ConfigurationType":["period" or
 "schedule"],"AutomationAssumeRole":["arn:aws:iam::ACCOUNTID:role/
ams_resource_scheduler_ssm_automation_role"]}'
                --region ONBOARDED_REGION
```

示例：

以下示例显示了如何使用 AWS Systems Manager 控制台描述一个时段。

1. 在以下 AWS Systems Manager 位置查看自动化文档 AWSManagedServices-DescribeScheduleOrPeriods（您可能需要选择已上线的区域）。

2. 为参数提供值。

3. 单击 “执行”，等待自动化完成。

为 AMS 资源调度程序标记资源

为 AMS 资源调度程序标记资源。

向 AMS 资源计划添加计划和周期后，您需要使用资源计划程序标签名称作为标签键，或者使用您自定义的标签键以及计划名称作为标签值来标记资源。有关如何在 AMS Accelerate 账户中标记资源的详细信息，请参阅在 AMS 中添加标签加速。

> **Note**
>
> 如果使用 Resource Tagger 来标记资源，则必须将资源调度器的默认标签键自定义为具有前缀 “ams:rt:”，因为资源标记器应用的所有标签都具有密钥前缀 “”。ams:rt:否则，使用资源标记器标记的资源将不会由资源调度器管理。要了解有关为资源调度器自定义默认标签密钥的更多信息，请参阅。自定义 AMS 资源调度器

AMS 资源调度器中的成本估算器

为了跟踪成本节省情况，AMS 资源调度器具有一个组件，该组件每小时计算由计划程序管理的 Amazon EC2 和 Amazon RDS 资源的估计成本节约。然后，这些成本节省数据将作为 CloudWatch 指标 (AMS/ResourceScheduler) 发布，以帮助您对其进行跟踪。成本节省估算器仅估算实例运行时间节省的时间。它不考虑任何其他成本，例如与资源相关的数据传输成本。

使用资源调度器启用了成本节约估算器。它每小时运行一次，并从中 AWS Cost Explorer检索成本和使用数据。它根据该数据计算出每种实例类型的平均每小时成本，然后预测在未计划的情况下运行一整天的成本。节省的成本是给定日期的预计成本与Cost Explorer的实际报告成本之间的差额。

例如，如果实例 A 的资源调度器配置为从上午 9 点到下午 5 点运行，则在给定一天中运行八个小时。Cost Explorer 将成本报告为 1 美元，使用量报告为 8。因此，每小时的平均成本为0.125美元。如果实例未使用资源调度器进行计划，则该实例将在当天运行 24 小时。在这种情况下，成本将为 24x0.125 = 3美元。资源调度器帮助您节省了2美元的成本。

为了使成本节省估算器仅检索由 Cost Explorer 中的资源调度器管理的资源的成本和使用量，需要在账单控制面板中激活资源调度器用于定位资源的标签密钥作为成本分配标签。如果该账户属于某个组织，则需要在该组织的管理账户中激活标签密钥。有关执行此操作的信息，请参阅激活用户定义的成本分配标签和用户定义的成本分配标签

将标签密钥激活为成本分配标签后，AWS 账单开始跟踪资源调度器管理的资源的成本和使用情况，在这些数据可用之后，成本节省估算器开始计算节省的成本并将数据发布在中的AMS/ResourceScheduler指标命名空间下。 CloudWatch

如果未激活成本分配标签，则即使启用了该指标，估算器也无法计算节省的费用并发布该指标。

> **Note**
>
> 成本节省估算器在计算时不考虑预留实例、储蓄计划等折扣。估算器从 Cost Explorer 中提取使用成本，然后计算资源每小时的平均成本。有关更多详细信息，请参阅 “了解您的 AWS 成本数据集：备忘单”。

AMS 资源调度器中的警报抑制器

AMS 资源调度器附带 CloudWatch 警报抑制器，该抑制器作为名AMSAlarmSuppressor为的单独的 Lambda 函数部署，用于抑制位于 Elastic Load Balancing、Application Load Balancing 或 Network Load Balance 后面的实例的警报。该函数每 5 分钟运行一次，检索账户中存在的所有警报，并根据命名空间对警报进行分组；例如、AWS/ELBAWS/ApplicationELB、AWS/NetworkELB。对于每组警报，抑制器都会找到负载均衡器名称 and/or 目标组（针对ALB/NLB) from alarm dimensions, finds the instances that are registered with the load balancer and/or目标组），并检查实例状态以发现这些实例是否由 AMS 资源调度器调度。如果实例由资源调度器调度，并由资源调度器停止，则抑制器会标记警报以将其禁用。如果注册实例列表中至少有一个实例正在运行，则抑制器会标记相应的警报以启用标记为启用的警报，并禁用标记为禁用的警报。这方面的日志存储在/aws/lambda/AMSAlarmSuppressor日志组中。

AMS Accelerate 中的日志管理

AMS Accelerate 将支持的 AWS 服务配置为收集日志。AMS Accelerate 使用这些日志来确保您的账户内资源的合规性和审计。

AMS Accelerate 提供了一系列运营服务，可帮助您在 AWS 上实现卓越运营。要快速了解 AMS 如何利用我们的一些关键运营功能（包括全天候服务台、主动监控、安全、修补、日志和备份）来帮助您的团队在 AWS 云中实现整体卓越运营，请参阅 AMS 参考架构图。

主题

日志管理 — AWS CloudTrail

AWS CloudTrail是一项用于账户管理的服务：合规性、运营审计和风险审计。借 CloudTrail助，您可以记录、持续监控和保留与整个 AWS 基础架构中的操作相关的账户活动。

AMS Acc AWS CloudTrail elerate 需要登录才能管理您账户中所有资源的审计和合规性。在入职时，您可以选择以下选项之一：

- AMS 已部署跟踪：如果您选择此选项，AMS 将在您的主 AWS 区域创建、部署和管理 CloudTrail 多区域跟踪，独立于您账户中的任何现有跟踪。
- 自带足迹：如果您选择提供自己的账户或组织 CloudTrail跟踪，则必须与您的云架构师 (CA) 合作，确保其满足 Accelerate 所需的配置。如果您选择此选项但不提供自己的跟踪，则 Accelerate 会自动部署自己的 CloudTrail 跟踪，以保持持续的安全和审计覆盖范围。如果您稍后提供自己的跟踪，AMS 会删除其已部署的跟踪，以避免冗余和额外费用。这种方法有助于在您的账户中维护一条活跃的 CloudTrail 跟踪，并防止重复的日志成本。

> **Note**
>
> 如果您的账户已有 CloudTrail 跟踪，并且您在入职期间没有专门配置或请求 AMS 托管跟踪，AMS Accelerate 会自动从您的账户中删除 AMS 部署的跟踪。这样可以防止重复记录，优化资源使用并节省额外成本。

AMS Accelerate 为加速部署的 CloudTrail 跟踪创建一个 Amazon S3 存储桶作为事件传送目的地，并使用 AWS Key Management Service (AWS KMS) 加密。AMS Accelerate 操作员可以访问您的跟踪事件以进行调查和诊断。如果您选择让 Accelerate 在入门期间部署 Accelerate 托管跟踪，则该账户已启用现有 CloudTrail 跟踪，则此跟踪除此之外。

AMS Accelerate 部署 AWS Config 规则来确保您的 CloudTrail 账户跟踪（包括加速部署的 CloudTrail 跟踪）得到正确设置和加密。要了解更多信息，请参阅AWS Config。以下是使用的规则，以描述这些规则的 AWS 文档的链接形式呈现：

- multi-region-cloudtrail-enabled。 检查 AMS Acc CloudTrail elerate 的设置是否正确且配置正确。
- cloud-trail-encryption-enabled。 配置 AWS CloudTrail 为使用服务器端加密 (SSE) 和 AWS KMS 客户主密钥 (CMK) 加密的检查。
- cloud-trail-log-file-已启用验证。启用后，会检查是否 AWS CloudTrail 创建带有日志的已签名摘要文件。我们强烈建议您在所有跟踪上启用文件验证。
- s3-bucket-default-lock-enabled。启用后，将检查 Amazon S3 存储桶是否已启用锁定。
- s3-bucket-logging-enabled。启用后，将检查 Amazon S3 存储桶是否启用了日志记录。

AMS Ac AWS KMS celerate 用于加密您账户中加速部署的 CloudTrail 跟踪记录的事件。此密钥由账户管理员、AMS Accelerate 操作员和控制并可供其访问 CloudTrail。有关的更多信息 AWS KMS，请参阅AWS Key Management Service 功能产品文档。

访问和审核 CloudTrail 日志

CloudTrail AMS Accelerate 部署的 CloudTrail 跟踪的日志存储在您账户中的 Amazon S3 存储桶中。存储在 Amazon S3 存储桶中的跟踪数据使用 CloudTrail 资源配置时创建的 AWS KMS 密钥进行加密。

Amazon S3 存储桶使用 ams-a-***aws account id***cloudtrail-***AWS Region***（例如：ams-a123456789--1a）的命名模式，所有事件都以 AWS/ 前缀存cloudtrail-us-east储。CloudTrail对主存储桶的所有访问都将被记录下来，并对日志对象进行加密和版本控制，以供审计。

有关跟踪更改和查询日志的更多信息，请参阅跟踪您的 AMS Accelerate 账户中的更改。

保护和保留 CloudTrail 日志

AMS Accelerate 允许使用治理模式锁定 Amazon S3 对象，用于加速部署的 CloudTrail 跟踪，以确保用户在没有特殊权限的情况下无法覆盖或删除对象版本或更改其锁定设置。有关更多信息，请参阅 Amazon S3 对象锁定。

默认情况下，此存储桶中的所有日志都将无限期保存。如果您想更改保留期，可以通过 Cent AWS 支持 er 提交服务请求以设置不同的保留政策。

访问亚马逊 EC2 日志

您可以使用访问 Amazon EC2 实例日志 AWS 管理控制台。实例和 AWS 服务生成的日志可在 CloudWatch 日志中找到，AMS Accelerate 管理的每个账户中都可用。有关访问日志的信息，请参阅 CloudWatch 日志文档。

保留 Amazon EC2 日志

默认情况下，Amazon EC2 实例日志会无限期保存。如果您想更改保留期，可以通过 Cent AWS 支持 er 提交服务请求以设置不同的保留政策。

日志管理 — Amazon EC2

AMS Accelerate 会在您确定为 AMS 加速托管的所有亚马逊 EC2 实例上安装 CloudWatch 代理。该代理将系统级日志发送到 Amazon CloudWatch 日志。有关信息，请参阅什么是 Amazon CloudWatch 日志？

以下日志文件将发送到 Lo CloudWatch gs，并将其发送到与日志同名的日志组中。在每个日志组中，将为每个 Amazon EC2 实例创建一个日志流，该日志流根据亚马逊 EC2 实例 ID 命名。

Linux

- /var/log/amazon/ssm/amazon-ssm-agent.log
- /var/log/amazon/ssm/errors.log
- /var/log/audit/audit.log
- /var/log/auth.log
- /var/log/cloud-init-output.log
- /var/log/cron
- /var/log/dnf.log
- /var/log/dpkg.log
- /var/log/maillog
- /var/log/messages
- /var/log/secure

- /var/log/spooler
- /var/log/syslog
- /var/log/yum.log
- /var/log/zypper.log

有关更多信息，请参阅手动创建或编辑 CloudWatch 代理配置文件。

Windows

- Amazon SSMAgent 日志
- AmazonCloudWatchAgentLog
- Amazon SSMError 日志
- AmazonCloudFormationLog
- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEvent日志
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog

有关更多信息，请参阅快速入门：允许运行 Windows Server 2016 的 Amazon EC2 实例使用 CloudWatch 日志代理向 CloudWatch 日志发送日志。

日志管理 — 亚马逊 VPC 流日志

VPC 流日志是一项功能，可捕获有关进出您的 VPC 中网络接口的 IP 流量的信息。流日志数据可以发布到亚马逊 CloudWatch 日志或 Amazon S3。流日志数据收集不会影响网络吞吐量或延迟。您可以创建或删除流日志，而不会对网络性能产生任何影响。

流日志可帮助您处理多种任务，例如：

- 诊断过于严格的安全组规则
- 监控到达您的实例的流量

- 确定在网络接口上往返的流量的方向

您不必在加速账户中为每个新创建的 VPC 启用 VPC 流日志。AMS 将使用 ams-nist-cis-vpc-flow-logs-enabled Config 规则自动检测 VPC 是否有流日志。如果未启用 VPC 流日志，AMS 将通过创建带有自定义字段的 VPC 流日志来自动对其进行修复。增加这些字段将使 AMS 和客户能够更好地监控 VPC 流量、了解网络依赖关系、解决网络连接问题并识别网络威胁。

有关查看和搜索流日志的信息，请参阅使用流日志。

跟踪您的 AMS Accelerate 账户中的更改

Important

自 2025 年 7 月 1 日起，变更记录服务已被弃用。
新账户无法加入 “更改记录” 服务。
要查询您的 AMS Accelerate 账户中的 CloudTrail 数据，您可以使用以下服务：

- 在中 AWS CloudTrail，选择事件历史记录并使用查找属性筛选事件。您可以使用时间范围过滤器，选择按`s3.amazon.aws.com`指定事件源筛选事件历史记录，也可以选择按用户名筛选事件历史记录。有关更多信息，请参阅使用 CloudTrail 事件历史记录。
- 使用 AWS CloudTrail Lake 通过查询收集数据。在中 AWS CloudTrail 选择 “湖泊”，然后选择 “查询”。您可以创建自己的查询、使用查询生成器或使用示例查询来收集基于事件的数据。例如，您可以询问上周谁删除了 Amazon EC2 实例。有关更多信息，请参阅通过 AWS CloudTrail 源和CloudTrailLake 查询创建数据湖。
- AWS CloudTrail 在中创建 Amazon Athena 表，并将存储位置设置为与您的跟踪关联的 Amazon S3 存储桶。验证您的跟踪的主区域和 Amazon S3 存储桶是否相同。在 Amazon Athena 中，使用查询编辑器运行 Accelerate 提供的与 Athena 控制台配合使用的默认查询。有关如何创建 Athena 表来 CloudTrail 查询日志的更多信息，请参阅查询日志。 AWS CloudTrail

主题

AWS Managed Services 使用亚马逊 Athena（At hena）控制台和 AMS 加速日志管理提供可查询的界面，帮助您跟踪 AMS 加速运营团队和 AMS 加速自动化所做的更改。

Athena 是一项交互式查询服务，您可以使用标准结构化查询语言 (SQL) 来分析 Amazon S3 中的数据（参见 Amazon Athena 的 SQL 参考）。Athena 没有服务器，没有要管理的基础设施，只需为运行的查询付费。AMS Accelerate 创建包含每日日志分区 CloudTrail 的 Athena 表，并提供有关您的 AWS 主要区域和工作组内部的查询。ams-change-record您可以选择任何默认查询并根据需要运行它们。要了解有关 Athena 工作组的更多信息，请参阅工作组的工作原理。

> **Note**
>
> 只有当加速与您的组织跟踪集成时，Accelerate 才能使用 Athena 查询 CloudTrail 您的 Accelerate 账户 CloudTrail 的事件，除非您的组织管理员部署了 IAM 角色，以便在入职期间使用 Athena 查询和 CloudTrail 分析您账户中的事件。

使用更改记录，您可以轻松回答以下问题：

- 谁（AMS 加速系统或 AMS 加速运营商）访问了您的账户
- AMS Accelerate 对您的账户进行了哪些更改
- AMS Accelerate 是什么时候对你的账户进行更改的
- 去哪里查看账户中所做的更改
- 为什么 AMS Accelerate 需要对你的账户进行更改
- 如何修改查询以获得所有非 AMS 变更问题的答案

查看您的变更记录

要使用 Athena 查询，请登录管理控制台并 AWS 导航到主区域中的 Athena 控制台。 AWS

> **Note**
>
> 如果您在执行任何步骤时看到 Amazon Athena 入门页面，请单击“开始”。即使您的“更改记录”基础架构已经到位，您也可能会看到此信息。

1. 从 Athena 控制台的上方导航面板中选择“工作组”。
2. 选择ams-change-record工作组，然后单击“切换工作组”。
3. ams-change-record-database从“数据库”组合框中进行选择。ams-change-record-database包括ams-change-record-table表格。
4. 从上方的导航面板中选择“已保存的查询”。
5. “已保存的查询”窗口显示 AMS Accelerate 提供的查询列表，您可以运行这些查询。从“已保存的查询”列表中选择要运行的查询。例如，ams_session_access_v1 查询。

   有关预设 AMS 加速查询的完整列表，请参阅默认查询。
6. 根据需要调整查询编辑器框中的日期时间过滤器；默认情况下，查询仅检查与上一天相比的更改。

7. 选择运行查询。

默认查询

AMS Accelerate 提供了几个默认查询，您可以在 Athena 控制台中使用。下表列出了默认查询。

> **Note**
>
> - 所有查询都接受日期时间范围作为可选筛选条件；默认情况下，所有查询都在过去 24 小时内运行。有关预期的输入，请参阅以下小节修改查询中的日期时间过滤器。
> - 可以或需要更改的参数输入*<PARAMETER_NAME>*与角大括号一样显示在查询中。用您的参数值替换占位符和角括号。
> - 所有过滤器都是可选的。在查询中，一些可选的过滤器在行首用双破折号 (--) 注释掉。所有查询都将在没有它们的情况下运行，并使用默认参数。如果要为这些可选筛选器指定参数值，请删除该行开头的双破折号 (--)，然后根据需要替换参数。
> - 所有查询都返回IAM PincipalIdIAM SessionId并在输出中
> - 运行查询的计算费用取决于为该账户生成的 CloudTrail 日志数量。要计算成本，请使用 AWS Athena 定价计算器。

预设查询

目的/描述	输入	输出
查询名称：ams_access_session_query_v1		
跟踪 AMS 加速访问会话 提供有关特定 AMS 加速访问会话的信息。该查询接受 IAM 委托人 ID 作为可选筛选条件，并返回事件时间、访问账户的业务需求、请求者等。 您可以通过取消注释行并在查询编辑器中将占	（可选）IAM PrincipalId ：尝试访问的资源的 IAM 委托人标识符。格式为*UNIQUE_ID ENTIFIER :RESOURCE_NAME* 。有关详细信息，请参阅唯一标识符。您可以在不使用此筛选条件的情况下运行查询，以确定	• EventTime: 获得访问权限的时间 • EventName: AWS 活动名称 (AssumeRole) • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID • BusinessNeed 类型：访问账户的业务原因类型。允许的值为： SupportCase、 OpsItem、问题、文本。

目的/描述	输入	输出
位符*IAM Principal Id* 替换为特定 ID 来筛选特定 IAM 委托人 ID。 您还可以通过删除查询的 WHERE 子句中的用户代理筛选器行来列出非 AMS 访问会话。	要筛选 PrincipalId 的确切 IAM。	• BusinessNeed: 业务需要访问该账户。例如，Support Case ID、Ops Item ID 等。 • 请求者：访问该账户的操作员 ID 或访问该账户的自动化系统。 • RequestAccessType: 请求者类型（系统、、OpsApi OpsConsole、未设置）
查询名称：ams_events_query_v1		
跟踪 AMS Accelerate 完成的所有变异动作 返回使用该 AMS Accelerate 角色筛选器对账户完成的所有写入操作。 您还可以通过从查询的 WHERE 子句中删除 useridentity.arn 筛选器行来跟踪非 AMS 角色所做的变更操作。	（可选） 仅限日期时间范围。请参阅修改查询中的日期时间过滤器。	• AccountId: AWS 账户 ID • RoleArn: RoleArn 对于请求者 • EventTime: 获得访问权限的时间 • EventName: AWS 活动名称 (AssumeRole) • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID • RequestParameters：请求的请求参数 • ResponseElements：响应的响应元素。 • UserAgent: AWS CloudTrail 用户代理
查询名称：ams_instance_access_sessions_query_v1		

目的/描述	输入	输出
通过 AMS Accelerate 追踪实例访问情况 返回 AMS Accelerate 实例访问列表；每条记录都包括事件时间、事件区域、实例 ID、IAM 委托人 ID、IAM 会话 ID、SSM 会话 ID、SSM 会话 ID。您可以使用 IAM 委托人 ID 通过 At `ams_access_sessions_query_v1` hena 查询获取有关访问实例的业务需求的更多详细信息。您可以使用 SSM 会话 ID 来获取有关实例访问会话的更多详细信息，包括会话的开始和结束时间、日志详细信息以及使用实例 AWS 区域中的 AWS 会话管理器控制台。 用户还可以通过删除查询 WHERE 子句中的用户身份筛选器行来列出非 AMS 实例访问权限。	仅限 `datetime range`。请参阅修改查询中的日期时间过滤器。	• InstanceId: 实例 ID • SSMSession ID：SSM 会话 ID • RoleArn: RoleArn 对于请求者 • EventTime: 获得访问权限的时间 • EventName: AWS 活动名称 (AssumeRole) • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID
查询名称：`ams_privilege_escalation_events_query_v1`		

目的/描述	输入	输出
跟踪 AMS 和非 AMS 用户的许可（升级）事件 提供可能直接或可能导致权限升级的事件列表。该查询接受 ActionedBy 为可选过滤器 EventName，并返回 EventId EventTime、、等。还会返回与该事件关联的所有字段。如果不适用于该事件，则字段为空。默认情况下，ActionedBy 过滤器处于禁用状态；要启用该过滤器，请从该行中删除“--”。 默认情况下， ActionedBy 筛选器处于禁用状态（它将显示所有用户的权限升级事件）。要显示特定用户或角色的事件，请从 WHERE 子句的用户身份筛选器行中删除双破折号 (--)，并将占位符*ACTIONEDBY_PUT_USER_NAME_HERE* 替换为 IAM 用户或角色名称。您可以在不使用筛选器的情况下运行查询，以确定要筛选的确切用户。	（可选）ACTIONEDBY_PUT_USER_NAME ：ActionedBy 用户的用户名。这可以是 IAM 用户或角色。例如 ams-access-admin。 （可选）datetime range。请参阅修改查询中的日期时间过滤器。	• AccountId: 账户编号 • ActionedBy用户名 ActionedBy ： • EventTime: 获得访问权限的时间 • EventName: AWS 事件名称 (AssumeRole)。 • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID
查询名称：ams_resource_events_query_v1		

目的/描述	输入	输出
跟踪特定资源 AMS 或非 AMS 的写入事件 提供在特定资源上完成的事件的列表。查询接受资源 ID 作为筛选器的一部分（替换查询的 WHERE 子句*RESOURCE_INFO* 中的占位符），并返回对该资源执行的所有写入操作。	（必填）RESOURCE_INFO ：资源标识符可以是账户中任何 AWS 资源的 ID。不要将其与资源 ARNs混淆。例如，实例的实例 ID、DynamoDB 表的表名 logGroupName 、日志的表 CloudWatch 名等。EC2 （可选）datetime range。请参阅修改查询中的日期时间过滤器。	• AccountId: 账户编号 • ActionedBy用户名 ActionedBy ： • EventTime: 获得访问权限的时间 • EventName: AWS 事件名称 (AssumeRole)。 • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID
查询名称：ams_session_events_query_v1		
跟踪 AMS Accelerate 在特定会话期间执行的写入操作 提供在特定会话中完成的事件列表。该查询接受 IAM 委托人 ID 作为筛选条件的一部分（替换查询的 WHERE 子句*PRINCIPAL_ID* 中的占位符），并返回对该资源执行的所有写入操作。	（必填）PRINCIPAL_ID ：会话的主人 ID。格式为*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* 。有关详细信息，请参阅唯一标识符。你可以运行查询 “ams_session_ids_by_requester_v1” 来获取请求者的 IAM 委托人列表。 IDs 您也可以在不使用此筛选条件的情况下运行查询，以确定 PrincipalId 要筛选的确切 IAM。 （可选）datetime range。请参阅修改查询中的日期时间过滤器。	• AccountId: 账户编号 • ActionedBy用户名 ActionedBy ： • EventTime: 获得访问权限的时间 • EventName: AWS 活动名称 (AssumeRole) • EventRegion: 收到请求的 AWS 区域 • EventId: CloudTrail 事件 ID

目的/描述	输入	输出
查询名称：ams_session_ids_by_requester_v1		
跟踪特定请求 Principal/Session IDs 者的 IAM。 该查询接受 “请求者”（替换查询的 WHERE 子句*Requester* 中的占位符），并返回该请求者在指定时间范围内的所有 IAM 委托人 ID。	（必填）Requester ：访问账户的操作员 ID（例如：操作员的别名）或访问该账户的自动化系统（例如： OsConfiguration AlarmManager、等）。 （可选）datetime range。请参阅修改查询中的日期时间过滤器。	• IAM PrincipalId -会话的 IAM 委托人 ID。格式为*UNIQUE_ID ENTIFIER* :*RESOURCE_NAME* ．有关详细信息，请参阅唯一标识符。您可以在不使用此筛选条件的情况下运行查询，以确定 PrincipalId 要筛选的确切 IAM。 • IAM SessionId -访问会话的 IAM 会话 ID • EventTime: 获得访问权限的时间

修改查询中的日期时间过滤器

所有查询都接受日期时间范围作为可选过滤器。默认情况下，所有查询都是在过去一天内运行的。

日期时间字段使用的格式为yyyy/MM/dd（例如：2021/01/01）。请记住，它只存储日期，而不是整个时间戳。对于整个时间戳，请使用 e vent ime 字段，该字段以 ISO 8601 格式存储时间戳 yyyy-MM-dd T HH: mm: ss Z（例如：2021-01-01T23：59:59 Z）。但是，由于表是在日期时间字段上进行分区的，因此您需要将日期时间和事件时间过滤器同时传递给查询。请见以下 示例。

> **Note**
>
> 要查看所有可接受的修改范围的方法，请参阅基于当前用于日期和时间函数和运算符的 Athena 引擎版本的最新 Presto 函数文档，了解修改范围的所有可接受的方式。

日期级别：过去 1 天或过去 24 小时（默认）示例：如果 CURRENT_DATE='2021/01/01'，则筛选器将从当前日期中减去一天并将其格式化为日期时间 > '2020/12/31'

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
```

日期级别：过去 2 个月示例：

```
datetime > date_format(date_add('month', - 2, CURRENT_DATE), '%Y/%m/%d')
```

日期级别：2 个日期之间示例：

```
datetime > '2021/01/01'
      AND
      datetime < '2021/01/10'
```

时间戳级别：过去 12 小时示例：

将分区数据扫描到最近 1 天，然后筛选过去 12 小时内的所有事件

```
datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND
      eventtime > date_format(date_add('hour', - 12, CURRENT_TIMESTAMP), '%Y-%m-%dT%H:
%i:%sZ')
```

时间戳级别：在 2 个时间戳之间示例：

获取在 2021 年 1 月 1 日下午 12:00 至 2021 年 1 月 10 日下午 3:00 之间的活动。

```
datetime > '2021/01/01' AND datetime < '2021/01/10'
      AND
      eventtime > '2021-01-01T12:00:00Z' AND eventtime < '2021-01-10T15:00:00Z'
```

默认查询示例

ams_access_session_query_v1

```
Name: ams_access_session_query_v1

Description: >-
   The query provides more information on specific AMS access session.
   The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   By default; the query filter last day events only, the user can change the datetime
 filter to search for more wide time range.
   By default; the IAM PrincipalId filter is disabled. To enable it, remove "-- " from
 that line.

AthenaQueryString: |-
```

```
  /*
    The query provides list of AMS access sessions during specific time range.
    The query accepts IAM Principal Id as an optional filter and returns event time,
business need for accessing the account, requester, ... etc.

    By default, the query filters the last day's events only; you can change the
"datetime" filter to search for a wider time range.

    By default; the IAM Principal ID filter is disabled (it shows access sessions for
all IAM principals).
    If you want to only show access sessions for a particular IAM principal ID, remove
the double-dash (--) from
    the "IAM Principal ID" filter line in the WHERE clause of the query, and replace
the placeholder "<IAM PrincipalId>" with the specific ID that you want.
    You can run the query without the filter to determine the exact IAM PrincipalId
you want to filter with.

    By default; the query only shows AMS access sessions. If you also want to show
non-AMS access sessions,
    remove the "useragent" filter in the WHERE clause of the query.

    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries
  */

  SELECT
     json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
PrincipalId",
     json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
SessionId",
     eventtime AS "EventTime",
     eventname AS "EventName",
     awsregion AS "EventRegion",
     eventid AS "EventId",
     json_extract_scalar(requestparameters, '$.tags[0].value') AS "BusinessNeed",
     json_extract_scalar(requestparameters, '$.tags[1].value') AS "BusinessNeedType",
     json_extract_scalar(requestparameters, '$.tags[2].value') AS "Requester",
     json_extract_scalar(requestparameters, '$.tags[3].value') AS "AccessRequestType"
  FROM
      "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
  WHERE
     datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
     AND eventname = 'AssumeRole'
     AND useragent = 'access.managedservices.amazonaws.com'
```

```
      -- AND  json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId')
 = '<IAM PrincipalId>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of AMS access sessions during specific time range.
   # The query accepts IAM Principal Id as an optional filter and returns event time,
 business need for accessing the account, requester, ... etc.
   #
   # By default; the IAM Principal ID filter is disabled (it shows access sessions for
 all IAM principals).
   # If you want to only show access sessions for a particular IAM principal ID, remove
 the # (#) from
   # the "IAM Principal ID" filter of the query, and replace the placeholder "<IAM
 PrincipalId>" with the specific ID that you want.
   # You can run the query without the filter to determine the exact IAM PrincipalId
 you want to filter with.
   #
   # By default; the query only shows AMS access sessions. If you also want to show
 non-AMS access sessions,
   # remove the "useragent" filter from the query.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter eventName="AssumeRole" AND userAgent="access.managedservices.amazonaws.com"
   # | filter responseElements.assumedRoleUser.assumedRoleId= "<IAM PrincipalId>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      requestParameters.tags.0.value as BusinessNeed,
      requestParameters.tags.1.value as BusinessNeedType,
      requestParameters.tags.2.value as Requester,
      requestParameters.tags.3.value as AccessRequestType
```

ams_events_query_v1

```
ams_events_query_v1.yaml
/*
  The query provides list of events to track write actions for all AMS changes.
  The query returns all write actions done on the account using that AMS role filter.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  You can also track mutating actions done by non-AMS roles by removing the
 "useridentity.arn" filter lines from the WHERE clause of the query.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   useridentity.arn AS "RoleArn",
   eventid AS "EventId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventsource AS "EventService",
   eventtime AS "EventTime",
   requestparameters As "RequestParameters",
   responseelements AS "ResponseElements",
   useragent AS "UserAgent"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   readonly <> 'true'
   AND
   (
      LOWER(useridentity.arn) LIKE '%/ams%'
      OR LOWER(useridentity.arn) LIKE '%/customer_ssm_automation_role%'
   )
ORDER BY eventtime
```

ams_instance_access_sessions_query_v1

```
ams_instance_access_sessions_query_v1
/*
  The query provides list of AMS Instance accesses during specific time range.

  The query returns the list of AMS instance accesses; every record includes the event
 time, the event AWS Region, the instance ID, the IAM session ID, and the SSM session
 ID.
  You can use the IAM Principal ID to get more details on the business need for
 accessing the instance by using ams_access_session_query_v1 athena query.
  You can use the SSM session ID to get more details on the instance access session,
 including the start and end time of the session and log details, using the AWS Session
 Manager Console in the instance's AWS Region.

  You can also list non-AMS instance accesses by removing the "useridentity" filter
 line in the WHERE clause of the query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   json_extract_scalar(requestparameters, '$.target') AS "InstanceId",
   json_extract_scalar(responseelements, '$.sessionId') AS "SSM SessionId",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventsource AS "EventService",
   eventtime AS "EventTime"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   useridentity.sessionContext.sessionIssuer.arn like '%/ams_%'
   AND eventname = 'StartSession'
ORDER BY eventtime
```

ams_privilege_escalation_events_query_v1

```
ams_privilege_escalation_events_query_v1.yaml
/*
  The query provides list of events that can directly or potentially lead to a
 privilege escalation.

  The query accepts ActionedBy as an optional filter and returns EventName, EventId,
 EventTime, ... etc.
  All fields associated with the event are also returned. Some fields are blank if not
 applicable for that event.
  You can use the IAM Session ID to get more details about events happened in that
 session by using ams_session_events_query_v1 query.

  By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

  By default, the ActionedBy filter is disabled (it shows privilege escalation events
 from all users).
  To show events for a particular user or role, remove the double-dash (--) from the
 useridentity filter line in the WHERE clause of the query
  and replace the placeholder "<ACTIONEDBY_PUT_USER_NAME_HERE>" with an IAM user or
 role name.
  You can run the query without the filter to determine the exact user you want to
 filter with.

  For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes in
 your AMS Accelerate accounts -> Default Queries
*/

SELECT
   useridentity.principalId AS "IAM PrincipalId",
   useridentity.accesskeyid AS "IAM SessionId",
   useridentity.accountid AS "AccountId",
   reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
   eventname AS "EventName",
   awsregion AS "EventRegion",
   eventid AS "EventId",
   eventtime AS "EventTime",
   json_extract_scalar(requestparameters, '$.userName') AS "UserName",
   json_extract_scalar(requestparameters, '$.roleName') AS "RoleName",
   json_extract_scalar(requestparameters, '$.groupName') AS "GroupName",
   json_extract_scalar(requestparameters, '$.policyArn') AS "PolicyArn",
   json_extract_scalar(requestparameters, '$.policyName') AS "PolicyName",
```

```
   json_extract_scalar(requestparameters, '$.permissionsBoundary') AS
 "PermissionsBoundary",
   json_extract_scalar(requestparameters, '$.instanceProfileName') AS
 "InstanceProfileName",
   json_extract_scalar(requestparameters, '$.openIDConnectProviderArn') AS
 "OpenIDConnectProviderArn",
   json_extract_scalar(requestparameters, '$.serialNumber') AS "SerialNumber",
   json_extract_scalar(requestparameters, '$.serverCertificateName') AS
 "ServerCertificateName",
   json_extract_scalar(requestparameters, '$.accessKeyId') AS "AccessKeyId",
   json_extract_scalar(requestparameters, '$.certificateId') AS "CertificateId",
   json_extract_scalar(requestparameters, '$.newUserName') AS "NewUserName",
   json_extract_scalar(requestparameters, '$.newGroupName') AS "NewGroupName",
   json_extract_scalar(requestparameters, '$.newServerCertificateName') AS
 "NewServerCertificateName",
   json_extract_scalar(requestparameters, '$.name') AS "SAMLProviderName",
   json_extract_scalar(requestparameters, '$.sAMLProviderArn') AS "SAMLProviderArn",
   json_extract_scalar(requestparameters, '$.sSHPublicKeyId') AS "SSHPublicKeyId",
   json_extract_scalar(requestparameters, '$.virtualMFADeviceName') AS
 "VirtualMFADeviceName"
FROM
   "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
WHERE
   (
     -- More event names can be found at https://docs.aws.amazon.com/IAM/latest/
UserGuide/list_identityandaccessmanagement.html
     eventname LIKE 'Add%' OR
     eventname LIKE 'Attach%' OR
     eventname LIKE 'Delete%' AND eventname != 'DeleteAccountAlias' OR
     eventname LIKE 'Detach%' OR
     eventname LIKE 'Create%' AND eventname != 'CreateAccountAlias' OR
     eventname LIKE 'Put%' OR
     eventname LIKE 'Remove%' OR
     eventname LIKE 'Update%' OR
     eventname LIKE 'Upload%' OR
     eventname = 'DeactivateMFADevice' OR
     eventname = 'EnableMFADevice' OR
     eventname = 'ResetServiceSpecificCredential' OR
     eventname = 'SetDefaultPolicyVersion'
   )
   AND eventsource = 'iam.amazonaws.com'
ORDER BY eventtime
```

ams_resource_events_query_v1

```
Name: ams_resource_events_query_v1

Description: >-
   The query provides list of events done on specific resource.
   The query accepts resource id as part of the filters, and return all write actions
 done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of events done on specific resource.

     The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the WHERE clause of the query),
     and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
     Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventid AS "EventId",
      eventsource AS "EventService",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
```

```
      AND
      (
         requestparameters LIKE '%<RESOURCE_INFO>%'
         OR responseelements LIKE '%<RESOURCE_INFO>%'
      )
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of events done on specific resource.
   #
   # The query accepts the resource ID as part of the filters (replace the placeholder
 "<RESOURCE_INFO>" in the filter of the query),
   # and returns all write actions done on that resource. The resource ID can be an ID
 for any AWS resource in the account.
   # Example: An instance ID for an EC2 instance, table name for a DynamoDB table,
 logGroupName for a CloudWatch Log, etc.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries

   filter readOnly=0
   | parse @message '"requestParameters":{*}' as RequestParameters
   | parse @message '"responseElements":{*}' as ResponseElements
   # | filter RequestParameters like "RESOURCE_INFO" or ResponseElements like
 "<RESOURCE_INFO>"
   | fields
      userIdentity.principalId as IAMPrincipalId,
      userIdentity.accessKeyId as IAMSessionId,
      userIdentity.accountId as AccountId,
      userIdentity.arn as ActionedBy,
      eventName as EventName,
      awsRegion as EventRegion,
      eventID as EventId,
      eventSource as EventService,
      eventTime as EventTime
   | display IAMPrincipalId, IAMSessionId, AccountId, ActionedBy, EventName,
 EventRegion, EventId, EventService, EventTime
   | sort eventTime desc
```

ams_session_events_query_v1

```
Name: ams_session_events_query_v1
```

```
Description: >-
   The query provides list of events done on specific session.
   The query accepts IAM Principal Id as part of the filters, and return all write
 actions done on that resource.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides a list of events executed on a specific session.

     The query accepts the IAM principal ID as part of the filters (replace the
 placeholder "<PRINCIPAL_ID>" in the WHERE clause of the query),
     and returns all write actions done on that resource.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.

     For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      useridentity.principalId AS "IAM PrincipalId",
      useridentity.accesskeyid AS "IAM SessionId",
      useridentity.accountid AS "AccountId",
      reverse(split_part(reverse(useridentity.arn), ':', 1)) AS "ActionedBy",
      eventname AS "EventName",
      awsregion AS "EventRegion",
      eventsource AS "EventService",
      eventtime AS "EventTime",
      requestparameters As "RequestParameters",
      responseelements AS "ResponseElements",
      useragent AS "UserAgent"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate   WHERE
      useridentity.principalid = '<PRINCIPAL_ID>'
      AND datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND readonly <> 'true'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides a list of events executed on a specific session.
   #
```

```
  # The query accepts the IAM principal ID as part of the filters (replace the
placeholder "<PRINCIPAL_ID>" in the filter of the query),
  # and returns all write actions done on that resource.
  #
  # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
in your AMS Accelerate accounts -> Default Queries

  filter readOnly=0 AND userIdentity.principalId = "<IAM Principal>"
  | sort eventTime desc
  | fields
     userIdentity.accessKeyId as IAMSessionId,
     userIdentity.principalId as IAMPrincipalId,
     userIdentity.accountId as AccountId,
     userIdentity.arn as ActionedBy,
     eventName as EventName,
     awsRegion as EventRegion,
     eventSource as EventService,
     eventTime as EventTime,
     userAgent as UserAgent
  | parse @message '"requestParameters":{*}' as RequestParameters
  | parse @message '"responseElements":{*}' as ResponseElements
```

ams_session_ids_by_requester_v1

```
Name: ams_session_ids_by_requester_v1

Description: >-
   The query provides list of IAM Principal/Session Ids for specific requester.
   The query accepts requester and return all IAM Principal/Session Ids by that
 requester during specific time range.
   By default; the query list the accesses for last day, the user can change the time
 range by changing the datetime filter.

AthenaQueryString: |-
   /*
     The query provides list of IAM Principal IDs for a specific requester.

     The query accepts the requester (replace placeholder "<Requester>" in the WHERE
 clause of the query),
     and returns all IAM Principal IDs by that requester during a specific time range.

     By default, the query filters the last day's events only; you can change the
 "datetime" filter to search for a wider time range.
```

```
    For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   */

   SELECT
      json_extract_scalar(responseelements, '$.assumedRoleUser.assumedRoleId') AS "IAM
 PrincipalId",
      json_extract_scalar(responseelements, '$.credentials.accessKeyId') AS "IAM
 SessionIId",
      eventtime AS "EventTime"
   FROM
       "{DATABASE NAME HERE}".{TABLENAME HERE} <- This should auto-populate
   WHERE
      datetime > date_format(date_add('day', - 1, CURRENT_DATE), '%Y/%m/%d')
      AND json_extract_scalar(requestparameters, '$.tags[2].value') = '<Requester>'
   ORDER BY eventtime

InsightsQueryString: |-
   # The query provides list of IAM Principal IDs for a specific requester.
   #
   # The query accepts the requester (replace placeholder "<Requester>" in the filter
 of the query),
   # and returns all IAM Principal IDs by that requester during a specific time range.
   #
   # For expected inputs and scenarios, refer to AMS Documentation -> Tracking changes
 in your AMS Accelerate accounts -> Default Queries
   filter eventName="AssumeRole" AND requestParameters.tags.2.value="<Requester>"
   | sort eventTime desc
   | fields
      responseElements.assumedRoleUser.assumedRoleId as IAMPrincipalId,
      responseElements.credentials.accessKeyId as IAMSessionId,
      eventTime as EventTime
```

更改记录权限

运行更改记录查询需要以下权限：

- Athena
  - 雅典娜：GetWorkGroup
  - 雅典娜：StartQueryExecution

  - 雅典娜：ListDataCatalogs
  - 雅典娜：GetQueryExecution
  - 雅典娜：GetQueryResults
  - 雅典娜：BatchGetNamedQuery
  - 雅典娜：ListWorkGroups
  - 雅典娜：UpdateWorkGroup
  - 雅典娜：GetNamedQuery
  - 雅典娜：ListQueryExecutions
  - 雅典娜：ListNamedQueries
- AWS KMS
  - kms:Decrypt
  - AWS KMS 的 AMSCloudTrailLogManagement密钥 ID 或您的 AWS KMS 密钥 ID（如果 Accelerate 使用您的 CloudTrail 跟踪事件 Amazon S3 存储桶数据存储，则使用 SSE-KMS 加密）。
- AWS Glue
  - 胶水：GetDatabase
  - 胶水：GetTables
  - 胶水：GetDatabases
  - 胶水：GetTable
- 亚马逊 S3 读取权限
  - 亚马逊 S3 存储桶 CloudTrail 数据存储：ams-a *AccountId*-cloudtrail-，或者*primary region*你的亚马逊 S3 存储桶名称，跟踪事件 Ama CloudTrail zon S3 存储桶数据存储。
- 亚马逊 S3 写入权限
  - Athena 事件查询结果 Amazon S3 存储桶：ams-a athena-results-*AccountId primary region*

AWS Systems Manager 在 “加速”

AWS Systems Manager 文档（SSM 文档）定义了 Systems Manager 对您的 AWS 资源执行的操作。Systems Manager 包含十几个预先配置的文档，您可以通过在运行时指定参数来使用这些文档。文档使用 JavaScript 对象表示法 (JSON) 或 YAML，它们包括您指定的步骤和参数。

AWS Managed Services (AMS) 是值得信赖的 SSM 文档发布商。AMS 拥有的 SSM 文档仅与已注册的 AMS 账户共享，始终以保留的前缀（AWSManagedServices-*）开头，并显示在 Systems Manager 控制台中，归亚马逊所有。AMS 的 SSM 文档开发和发布流程遵循 AWS 最佳实践，需要在整个文档生命周期中进行多次同行评审。有关共享 SSM 文档的 AWS 最佳实践的更多信息，请访问共享 SSM 文档的最佳实践。

可用的 AMS 加速 SSM 文档

AMS Accelerate SSM 文档仅向 AMS Accelerate 客户提供，用于自动化操作工作流程以操作您的账户。

要查看可用的 AMS 加速 SSM 文档， AWS 管理控制台请访问：

1. 在控制台打开系统管理器控制AWS Systems Manager 台。
2. 选择 “与我共享”。
3. 在搜索栏中，按文档名称前缀筛选，然后按 “等于” 进行筛选，然后将值设置为 “AWSManaged服务-”。

   有关 AWS CLI 说明，请参阅使用共享 SSM 文档。

AMS 加速 SSM 文档版本

SSM 文档支持版本控制。AMS Accelerate SSM 文档无法从客户的账户中修改，也无法重新共享。它们由 AMS Accelerate 集中管理和维护，以便操作账户。

在特定 AWS 区域中，版本号会随着文档的更新而增加。随着新区域的推出，两个区域中的相同文档内容可能具有不同的版本号；这是典型的，并不意味着它们的行为会有所不同。如果您想比较两个 AMS Accelerate SSM 文档，我们建议将它们的哈希值与以下内容进行比较： AWS CLI

```
aws ssm describe-document \
```

```
    --name AWSManagedServices-DOCUMENTNAME \
    --output text --query "Document.Hash"
```

如果两个 SSM 文档的哈希值匹配，则它们是相同的。

Systems Manager 定价

AMS 加速 SSM 文档访问不收取任何费用。运行时间成本因 SSM 文档的类型、步骤和运行时长而异。有关更多信息，请参阅定AWS Systems Manager 价。

AMS Accelerate 用户指南的文档历史记录

下表描述了《AMS Accelerate 用户指南》每个版本中的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
更新了日志管理- AWS CloudTrail 部分	有关 AWS CloudTrail 日志的新信息和注意事项。	2025年9月25日
新增了 4 项受可信修正者支持 Trusted Advisor 的成本优化检查	添加了以下成本优化检查： • c1z7kmr00n-亚马逊针对实例的成本优化建议 EC2 • c1z7kmr02n-亚马逊 EBS 关于批量的成本优化建议 • c1z7kmr03n-针对数据库实例的 Amazon RDS 成本优化建议 • c1z7kmr05n-函数的成本优化建议 AWS Lambda	2025年9月22日
更新了 Change Record 服务的弃用说明	更新了 Change Record 服务的弃用说明，并提供了其他解决方案。	2025年9月11日
更新了受信任修正者支持 Trusted Advisor 的安全检查	更新了支票 Hs4ma3G108 支持的预配置参数和约束条件——跟踪 CloudTrail 应与 Amazon Logs 集成 CloudWatch	2025 年 9 月 5 日
更新了受信任修正者支持 Trusted Advisor 的安全检查	更新了 Trusted Advisor 安全检查以添加 Hs4Ma3G184 版本 2-应启用应用程序负载均衡器和经典负载均衡器日志记录	2025 年 9 月 5 日

更新了由 “可信修正者” 部分支持的卓越 Trusted Advisor 运营检查	更新了 Trusted Remediator 支持的卓越 Trusted Advisor 运营检查，添加了新的支持检查 c1fd6b96l4 Amazon S3 访问日志已启用。	2025 年 8 月 28 日
更新了 “可信修正者” 部分，加入了 Compute Optimizer 的新内容	更新了 “可信修正者” 部分，加入了支持的 AWS Compute Optimizer 建议的新内容。	2025 年 8 月 18 日
已移除 TOC 词汇表链接	AWS 词汇表。	2025 年 8 月 8 日
已移除 TOC 词汇表链接	AWS 词汇表。	2025 年 8 月 8 日
每日补丁报告中的新字段	实例标签：与 Amazon EC2 实例 ID 关联的标签。	2025 年 8 月 8 日
新的可信修正者检查	Trusted Advisor 成本优化检查由 Trusted Remedieator Hs4ma3G120— AWSManagedServices-TerminateEC 2 InstanceStoppedForPeriodOfTime、Hs4ma3G230—2 和 c18d2gz150—2 和 c18d2gz150—2 支持的受信任修复者 Trusted Advisor 安全检查支持。AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	2025 年 8 月 8 日
在第 3.2 点中更新 IAM 标准	澄清了措辞并删除了对标签的提及。	2025 年 7 月 25 日

在 Accelerate 中更新了资源标记器配置文件	在 “加速” 的资源标记器配置文件中添加了新的 AvailabilityZone 过滤器。	2025 年 7 月 25 日
在 Accelerate 中更新了事件报告、服务请求和账单问题。	将对 Plus 和 Premium 服务等级的引用替换为服务 SLA 链接。	2025 年 7 月 25 日
更新了 Accelerate 中的事件管理。	更新了有关运营中心的信息。	2025 年 7 月 25 日
使用正确的链接更新了 AMS 模式页面。	修复了 SLA 和 SLO 链接。	2025 年 7 月 25 日
警报选择退出选项的更新	添加标签允许您选择退出另外两个警报。	2025 年 7 月 25 日
备份的新功能	使用新标签自定义备份保管库的通知。	2025 年 7 月 25 日
更新了 “加速” 中支持的配置部分	更新了 Accelerate 中支持的操作系统和支持的终止支持 (EOS) 操作系统的支持配置。	2025 年 6 月 26 日
在 Accelerate 中删除了管理补丁管理标签的页面	删除了 Accelerate 中管理补丁管理标签的页面，因为此功能已被弃用。	2025 年 6 月 19 日
补丁管理备用补丁存储库的重要安全注意事项。	在 AMS Accelerate 中使用备用补丁存储库的重要安全说明和最佳实践。	2025 年 6 月 10 日
AMS 加快更改记录的弃用。	AMS Accelerate Change Record 服务将于 2025 年 7 月 1 日起被弃用。	2025 年 5 月 27 日
支持的操作系统更新。	AMS Accelerate 支持的操作系统已更新，有些已添加，有些已删除。	2025 年 5 月 22 日

中东（阿联酋）地区支持的服务注意事项。	中东（阿联酋）地区对某些服务的支持有限。	2025 年 5 月 22 日
仅限内部。 APIs	仅限内部 APIs ，出现在某些 CloudWatch 日志中。	2025 年 5 月 22 日
添加了缺失的日志位置。	添加了一些缺失的 Windows 日志位置。	2025 年 5 月 22 日
AMS 加速可信修复器更新。	如何使用新参数在 Trusted `preconfigured-parameters` Remediator 中自定义 Trusted Advisor 检查。	2025 年 5 月 22 日
AMS 加速可信修复者常见问题解答和更新。	对支持的 Trusted Advisor 检查进行了多项更新，Trusted Remediator 常见问题解答（已添加 “Trusted Remediator 向您的账户部署了哪些资源？”），以及更多。另请参阅可信修正者支持的Trusted Advisor 检查。	2025 年 5 月 8 日
AMS 加速标准安全控制更新。	添加了 “安全组共享” 控件。	2025 年 5 月 8 日
加快监控警报的更新。	添加了其他警报，并在备注列中添加了警报名称。	2025 年 4 月 28 日
加快资源库存。	资源清单电子表格文件（压缩）已更新。	2025 年 4 月 24 日
加快日志位置。	添加了其他日志位置。	2025 年 4 月 24 日
加快安全事件响应的新角色和职责 (RACI)。	用于安全事件响应的 RACI。	2025 年 3 月 27 日
加快新的 Amazon RDS 自动修复提醒。	警报 ID：-0224，当请求的分配存储空间达到或超过配置的最大存储阈值时触发。	2025 年 3 月 27 日

加快入职角色模板更新。	AMS Accelerate 入职角色模板已更新，可支持 AWS GovCloud 区域。	2025 年 3 月 25 日
加快新的自动修复 RDS 警报。	RDS-EVENT-0224 已添加。	2025 年 3 月 17 日
加速新功能：事件通知。	您可以使用 AppRegistry 创建应用程序并自定义这些应用程序的事件通知。	2025 年 3 月 13 日
加快更新到 RDS 警报监控阈值。	RDS 平均 CPU 使用率警报阈值已从 75% 更改为 90%。	2025 年 2 月 20 日
加速更新 AMS 警报自动修复表。	警报补救表已扩展为新内容。	2025 年 2 月 20 日
加速新功能：保留警报。	您可以将警报管理器配置为保留警报 CloudWatch 而不是自动删除。	2025 年 2 月 20 日
更新了自助服务报告，增加了用于查看汇总报告的新数据选项	为以下自助服务报告添加了数据选项`Admin Account ID`，以包括新的字段名:**`aws_admin_account_id`** 、数据集字段名:**`Trusted AWS Organization account enabled by the customer`**和定义: : • 补丁报告（每日） • Backup 报告（每日） • 事件报告（每周） • 资源标记器控制面板 • 安全配置 Rules 控制面板	2025 年 1 月 28 日

添加了受信任修正者支持的其他 AWS Trusted Advisor 检查	可信修正者现在支持以下 Trusted Advisor 检查：
	• 成本优化
	  • c1cj39rr6v-Amazon S3 未完成的分段上传中止配置
	• 安全性
	  • Hs4Ma3G199-RDS 数据库实例应将日志发布到日志 CloudWatch
	  • Hs4ma3G326-应启用亚马逊 EMR 屏蔽公开访问设置
	  • Hs4Ma3G272-用户不应拥有 AI 笔记本实例的 root 访问权限 SageMaker
	  • Hs4ma3G325-EKS 集群应启用审核日志记录
	  • HHs4Ma3G118-VPC 默认安全组不应允许入站或出站流量
	  • Hs4ma3G127-应启用 API Gateway REST WebSocket 和 API 执行日志记录
	  • Hs4Ma3G124- EC2 亚马逊实例应使用实例元数据服务版本 2 () IMDSv2
	• 容错能力
	  • c1qf5bt013-Amazon RDS 数据库实例已关闭存储自动扩展
		2025 年 1 月 28 日

    - 7q GXs KIUw -Classic Load Balancer Connection Draining
    - c18d2gz106-计划中不包括亚马逊 EBS AWS Backup
    - c18d2gz107-计划中不包括亚马逊 DynamoDB 表格 AWS Backup
    - cc18d2gz117-计划中不包括亚马逊 EFS AWS Backup
    - c18d2gz105-Network Load Balancer 交叉负载平衡
    - c1qf5bt026-亚马逊 RDS synchronous_commit 参数已关闭
    - c1qf5bt030-亚马逊 RDS innodb_flush_log_at_trx_commit 参数不是 1
    - c1qf5bt031-亚马逊 RDS sync_binlog 参数已关闭
    - c1qf5bt036-亚马逊 RDS innodb_default_row_format 参数设置不安全
    - c18d2gz144-未启用亚马逊详细监控 EC2
- 卓越运营
    - c18d2gz125-亚马逊 API Gateway 未记录执行日志
    - c18d2gz168-负载均衡器未启用弹性负载保护 BalancingDeletion

	• c1qf5bt012-亚马逊 RDS Performance Insights 已关闭 • 性能 • c1qf5bt021-使用小于最佳值的 Amazon RDS innodb_change_buffering 参数 • c1qf5bt025-亚马逊 RDS 自动真空参数已关闭 • c1qf5bt028-亚马逊 RDS enable_indexonlyscan 参数已关闭 • c1qf5bt029-亚马逊 RDS enable_indexscan 参数已关闭 • c1qf5bt032-亚马逊 RDS innodb_stats_persistant 参数已关闭 • c1qf5bt037-Amazon _logging 参数已开启 RDSgeneral	
更新了资源清单电子表格	更新了资源清单电子表格。	2025 年 1 月 23 日
AMS 新功能：聚合自助服务报告	聚合自助服务报告 (SSR) 为您提供在组织层面、跨账户汇总的现有自助服务报告的视图。	2025 年 1 月 21 日
新的加速补丁功能：补丁挂钩	使用此功能使用 SSM Command 文档配置 “挂钩”，以便在修补之前或之后运行操作系统级别的命令。	2025 年 1 月 16 日

“监控工作原理” 部分的更新	添加了有关新功能的信息，即按资源或实例 ID 而不是按事件配置警报通知。	2025 年 1 月 8 日
EKS 监控和事件管理的 “入职” 部分的更新	更新了入职程序说明，以明确警报信号何时暂停和恢复。	2024 年 12 月 19 日
成员账户日志已添加到 “可信修正者”	您可以使用成员账户日志来查找每个成员账户的账户 ID AWS 区域、注册时间和执行时间。	2024 年 12 月 19 日
使用 SSM 代理的先决条件	有关屏蔽出站流量的内容已更新。	2024 年 12 月 4 日
亚太地区（香港）现已支持 EKS 的加速监控和事件管理 AWS 区域	亚太地区（香港）现在由 EKS 的 “加速监控和事件管理” 支持	2024 年 11 月 21 日
更新了按需运营产品表	支持以下操作系统进行就地升级： • 微软 Windows 2016 到微软 Windows 2022 及更高版本	2024 年 11 月 11 日
非洲（开普敦）现在支持 EKS 的加速监控和事件管理 AWS 区域。	非洲（开普敦）现在受到 EKS 加速监控和事件管理的支持	2024 年 11 月 4 日

更新了按需运营产品表	支持以下操作系统进行就地升级： • 微软 Windows 2012 R2 到微软 Windows 2016 及更高版本 • 红帽企业 Linux 7 到红帽企业 Linux 8 • 红帽企业 Linux 8 到红帽企业 Linux 9 • 甲骨文 Linux 7 到甲骨文 Linu	2024 年 11 月 1 日
更新了快速入门模板	更新了图表、模板参数和 yaml 模板文件。	2024 年 10 月 28 日

Trusted Advisor 已向 AMS 中的可信修正者添加支票	现在，可信修正器中提供了以下 Trusted Advisor 检查： • Z4 AUBRNSmz -未关联的弹性 IP 地址 • c18d2gz128-未配置生命周期策略的 Amazon ECR 存储库 • c18d2gz138-DynamoDB 恢复 Point-in-time • Hs4ma3G323-Dynamo 应该启用删除保护 DBtables • Hs4ma3G247-Amazon Transit G EC2 ateway 不应自动接受 VPC 连接请求 • Hs4ma3G308-亚马逊 DocumentDB 集群应启用删除保护 • Hs4ma3G299-Neptune 数据库集群应启用删除保护 • Hs4ma3G306-Amazon DocumentDB 手动集群快照不应公开 • Hs4ma3G109-应启用 CloudTrail 日志文件验证 • Hs4ma3G217 — CodeBuild 项目环境应该有日志记录 AWS Configuration4 • Hs4ma3G158-SSM 文档不应公开 • Hs4ma3G319-Network Firewall 防火墙应该启用删除保护	2024 年 10 月 25 日

更新了支持的配置	将支持的 Oracle Linux 操作系统更新到 9.0-9.3、8.0-8.9、7.5-7.9。	2024 年 10 月 24 日
AMS Accelerate 在 Offboard 中添加	有关如何使用 AMS Accelerate 的 Offboard 中添加的警报管理器和资源标记器依赖项下线的说明。	2024 年 10 月 24 日
资源标记器仪表板现已可用。	资源标记器仪表板现已在自助服务报告中提供。	2024 年 9 月 26 日
现在，您可以在基于标签的警报中包含多个电子邮件地址。	基于标签的警报现在支持多个电子邮件地址。	2024 年 9 月 20 日
AMS 加速限制现已包含在 AMS 补丁管理中。	AMS Accelerate 限制包含在补丁管理中-创建补丁维护窗口。	2024 年 8 月 30 日
AMS 加速账户发现更新	已在 “账户发现” 中为亚马逊 EC2 实例评估添加了一个新部分。	2024 年 8 月 29 日
AMS Accelerate 默认补丁基准现已适用于 Ubuntu 操作系统。	AMS Accelerate 默认补丁基准现已适用于 Ubuntu 操作系统。	2024 年 8 月 22 日
AMS 加速账户发现更新	操作检查表的 “ AWS CloudTrail 评估” 部分中添加了四个新的 AWS API 调用。	2024 年 8 月 2 日
Trusted Remediator 现在支持额外检查	Trusted Remediator 现在支持安全检查 Hs4Ma3G192-RDS 数据库实例应禁止公共访问。	2024 年 7 月 30 日
AMS 现在支持 Amazon Route 53 解析器 DNS 防火墙	AMS 现在支持 Amazon Route 53 解析器 DNS 防火墙	2024 年 7 月 30 日

AMS Accelerate onboarding_role_minimal.zip 现在包含 terraform 代码	AMS Accelerate onboarding_role_minimal.zip 现在包含 Terraform 代码。	2024 年 7 月 30 日
安全配置 Config 规则控制面板	Security Config 规则控制面板现已在自助服务报告中提供。	2024 年 7 月 24 日
AMS Accelerate 现在支持 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	AMS Accelerate 现在支持 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	2024 年 7 月 5 日
AMS 加速账户发现流程已更新。	登录 AMS Accelerate AWS 账户 时使用的账户发现流程已更新。	2024 年 7 月 1 日
可信修正者现已可用。	Trusted Remediator 是一款可自动修复 AWS Trusted Advisor 支票的 AWS Managed Services 解决方案，现已上市。	2024 年 6 月 24 日
安全事件响应中的 Amazon Route 53 解析器 DNS 防火墙事件。	AMS 现在可以在安全事件响应中监控 Amazon Route 53 解析器 DNS 防火墙事件	2024 年 6 月 21 日
已更新支持的操作系统	AMS Accelerate 现在支持 AlmaLinux 8.3-8.9、9.0-9.2（AlmaLinux 仅支持 x86 架构）	2024 年 6 月 19 日
现在，如果满足默认值，则自动增加实例配置文件限制。	现在，如果达到 10 的默认限制，AMS 会将默认实例配置文件限制增加到 20。	2024 年 6 月 18 日
默认情况下，AMS SSM 代理自动安装功能现已启用。	默认情况下，AMS SSM 代理自动安装功能对于 2024 年 3 月 6 日之后注册的账户启用。	2024 年 6 月 7 日

安全管理中添加了安全常见问题解答。	安全常见问题解答现已推出，其中涵盖了有关 AMS 运营工程师或自动化人员访问您的账户时使用的安全最佳实践、控制、访问模型和审计机制的常见问题。	2024 年 6 月 3 日
Amazon EKS 的监控和事件管理现在支持其他 AWS 区域。	Amazon EKS 的监控和事件管理现在支持另外三个 AWS 区域。	2024 年 5 月 23 日
现在，服务请求补丁通知会在补丁维护窗口之前发送。	AMS Accelerate 修补会在补丁维护窗口开始前 4 天创建新的服务请求。您可以使用服务请求与 AMS 沟通以调整补丁或跳过补丁。	2024 年 5 月 3 日
警报阈值已添加到 AMS 加速 EKS 监控基线警报表中。	Amazon EKS 监控的基准警报表中现在提供了详细的警报阈值。	2024 年 5 月 3 日
更新：警报管理器配置文件。	添加了有关使用警报管理器创建异常检测警报的注释。	2024 年 4 月 25 日
资源标记器配置配置文件的新增内容。	DynamoDB 表和 Amazon S3 存储桶现已在 Resource Tagger 中提供	2024 年 4 月 25 日
添加了计划活动管理 (PEM) 信息部分。	有关 PEM 服务的详细信息现已在 AMS Accelerate 用户指南中提供。	2024 年 4 月 25 日
AMS 支持红帽企业 Linux (RHEL) 9.x。	AMS 支持红帽企业 Linux (RHEL) 9.x。	2024 年 4 月 25 日
AMS Accelerate 支持报告所有 AWS 区域配置。	AMS Accelerate 支持所有 AWS 区域配置的 SSM 库存报告。	2024 年 4 月 25 日

更新： AWS 托管策略。	AWSManagedServices DeploymentToolkitPolicy 使用新的 ECR 权限更新了。	2024 年 4 月 4 日
更新：资源标记器配置文件部分	已AWS::EFS::FileSystem 添加到ResourceType列表中。	2024 年 3 月 21 日
更新：“加速” 部分中的事件报告和服务请求。	在 Accelerate 中将主题标题更改为事件报告、服务请求和账单问题。添加了新部分 “账单问题”。	2024 年 3 月 21 日
更新：服务请求管理的工作原理部分。	添加了对 AMS 如何处理包含功能请求或错误的服务请求的说明。	2024 年 3 月 21 日
更新：使用部分创建 aws_managedservices_onboarding_role 角色 CloudFormation	添加了用于创建角色的命令 AWS CloudShell。	2024 年 3 月 21 日
更新：（可选）快速入门模板	添加了从中下载模板的命令 AWS CloudShell。	2024 年 3 月 21 日
警报管理器配置文件可用的新资源类型。	在 Alarm Manager 配置文件中添加了 Amazon FSx、Amazon EFS 和 Elasticsearch 的资源类型。	2024 年 3 月 21 日
可用于配置文件的其他伪参数替换。	添加了 Amazon EFS 和亚马逊 FSx 伪参数替换。	2024 年 3 月 21 日
在 “服务描述” 主题中的 “功能” 中添加了新部分。	在 AMS Accelerate 功能下添加了新的服务请求管理部分。	2024 年 3 月 21 日

自助服务报告每周事件报告中添加了新列	每周事件报告中添加了新列，因此您可以根据事件创建或解决的季度、月、周或日期筛选事件。	2024 年 3 月 11 日

早期更新

下表描述了 2024 年 3 月之前 AMS 加速指南文档的重要更改。

更改	描述	日期
AMS 的改进加速 CloudTrail 试用入门	AMS 加速 CloudTrail 试用版入门的改进： • 将所有存储桶策略收集到一个区块中 • 删除政策声明中的第二个 AWS 组织 ID • 阐明客户环境要求 有关更多信息，请参阅 查看并更新您的配置，让 AMS Accelerate 能够使用您的 CloudTrail 跟踪。	2024 年 2 月 23 日
已更新：账户注册流程。	重组了账户注册流程部分，使步骤更加清晰。还为入门功能添加了可选的快速入门模板。 请参阅（可选）加速中的快速入门模板。	2024 年 2 月 22 日
更新：下线 AMS 加速。	更新了 “AMS Accelerate 离线注意事项” 部分，以表明离线流程不会删除ams-access-management CloudFormation 堆栈和 ams-access-management IAM 角色。 请参阅AMS 加速下机效果。	2024 年 2 月 22 日
更新：加速中的配置合规性。	将 “事件报告” 更改为 “服务请求”（如适用），以避免对这些条款产生混淆。 请参阅加速中的配置合规性。	2024 年 2 月 22 日

更改	描述	日期
更新：“加速” 中的账号发现。	在 Accelerate 中重新组织了账户发现，以便通过相关部分更好地对先决条件进行分组。 请参阅第 1 步：在 “加速” 中发现账户。	2024 年 2 月 22 日
已重命名：向 AMS 主机管理部门报告 AMS 补丁。	将 AMS 补丁报告重命名为 AMS 主机管理层，并将补丁详细信息报告重命名为 SSM 代理覆盖率报告。 请参阅AMS 主机管理报告。	2024 年 2 月 22 日
更新了按需操作目录	更新了 Operations on Demand 产品目录表，删除了中对 “健康” 的提法`Amazon EKS cluster maintenance` 。 请参阅按需请求 AMS 操作。	2024 年 2 月 22 日
更新了 AMS 事件路由器	更新了 `AMSCoreRule` AMS 事件路由器部分中的。 请参阅在 AMS 中使用亚马逊 EventBridge 托管规则。	2024 年 2 月 22 日
更新了支持的操作系统。	更新了支持的操作系统以包括 SUSE Linux 企业服务器 15 SP5。 请参阅支持的配置。	2024 年 2 月 22 日
更新了 EC2 批量使用补救自动化	使用正确的 EC2 容量扩展计划更新了卷使用情况修正自动化部分。 请参阅EC2 音量使用补救自动化。	2024 年 2 月 22 日
更新：查看并更新您的配置以允许 Accelerate 使用您的 CloudTrail跟踪	更新了 AMS 加速组织 CloudTrail S3 存储桶策略部分。请参阅 查看并更新您的配置，让 AMS Accelerate 能够使用您的 CloudTrail 跟踪。	2024 年 2 月 15 日

更改	描述	日期
新增功能：SSM Agent auto 自动安装	为 SSM Agent auto 自动安装添加了新章节 请参阅SSM 代理自动安装。	2024 年 1 月 26 日
更新：支持的配置	添加了有关支持的版本的信息 AWS Control Tower 请参阅支持的配置。	2024 年 1 月 26 日
更新：AMS 补丁报告。	从 AMS 补丁报告中删除了三个部分： • 补丁实例详细信息摘要报告 • 补丁详细信息报告 • 报告错过补丁的实例 请参阅AMS 主机管理报告。	2023 年 12 月 22 日
更新：加快入职先决条件。	更新了加载 AMS Accelerate 所需的支持计划。 请参阅加快入职先决条件。	2023 年 12 月 15 日
更新：创建补丁维护窗口。	删除了 “默认补丁周期” 部分，因为此功能已被弃用。 请参阅在 AMS 中创建补丁维护窗口。	2023 年 12 月 13 日
更新：加速中的通知设置。	澄清了哪个电子邮件用于通知。 请参阅加速中的通知设置了解更多信息。	2023 年 12 月 12 日
更新：AMSAccelerateCustomerAccessPolicies 模板。	更新了AMSAccelerateCustomerAccessPolicies 模板以更正语法错误。 请参阅使用 AMS 功能的权限了解更多信息。	2023 年 12 月 12 日

更改	描述	日期
新增：变更请求安全审查	在 “安全管理” 下新增了 “更改请求安全审查” 部分。 请参阅更改请求安全审查了解更多信息。	2023 年 12 月 11 日
已更新：resource_inventory.xlsx	已更新 resource_inventory.xlsx 以包含安全分析师角色。 请参阅用于加速的资源清单了解更多信息。	2023 年 11 月 17 日
更新： ams-access-admin-operations角色描述	更新了ams-access-admin-operations描述。 有关更多信息，请参阅 AMS 访问您的账户的原因和时间 和 在 AMS 加速中使用身份进行身份验证。	2023 年 11 月 17 日
更新：AMS 加速离职注意事项	更新了 “安全” 部分，以阐明亚马逊提供的内容 GuardDuty 以及下线后的 AWS Config 规则。 请参阅AMS 加速下机效果了解更多信息。	2023 年 11 月 17 日
新增：Amazon EKS 的监控和事件管理	Amazon EKS 的监控和事件管理可监控您的 Amazon EKS 资源是否存在故障、性能下降和安全问题。 请参阅AMS Accelerate 中对 Amazon EKS 进行监控和事件管理了解更多信息。	2023 年 11 月 14 日
更新：标记	添加了有关客户提供的标签的信息。 请参阅Accelerate 中客户提供的标签了解更多信息。	2023 年 11 月 7 日

更改	描述	日期
更新：资源标记器配置配置文件	已添加 AWS::AutoScaling::AutoScalingGroup, AWS::EKS::Cluster, AWS::Elasticsearch ::Domain, and AWS::FSx::FileSystem 到 “过滤器” 部分。 请参阅AMS 中的资源标记器配置文件加速了解更多信息。	2023 年 10 月 27 日
更新：服务说明	在支持的操作系统中添加了 Ubuntu 22.04。请参阅 服务描述。	2023 年 9 月 29 日
更新：AMS 加速入职前提条件	在 AMS 加速 VPC 终端节点中添加了注释以包含 CloudFormation 模板。请参阅加快入职先决条件。	2023 年 9 月 29 日
更新：检测	从 AMS 加速安全响应中删除了端点保护类型。请参阅Detect。	2023 年 9 月 29 日
更新：来自 AMS 基线监控的警报	已添加 AWS Outposts 到 “来自基线监控的警报” 表中。请参阅Detect monitoring-default-metrics。	2023 年 9 月 29 日
更新：使用创建 aws_managedservices_onboarding_role 角色 CloudFormation	更新了 “指定堆栈详细信息” 的屏幕截图。请参阅为加速aws_managedservices_onboarding_role CloudFormation 而创作。	2023 年 9 月 29 日
更新：AMS Accelerate 部署的亚马逊 EventBridge 托管规则	添加了新的 AMS 加速 Amazon EventBridge 托管AMSCore规则规则。 更新了 AMS Accel EventBridge erate Amazon 托管规则AMSAccessRolesRule以添加新角色。 请参阅AMS 部署的 Amazon EventBridge 托管规则 了解更多信息。	2023 年 9 月 19 日

更改	描述	日期
更新：警报管理器配置文件	添加了 AWS Outposts 伪参数替换标识符。请参阅AMS Accelerate 中的监控和事件管理。	2023 年 9 月 11 日
更新：资源标记器配置配置文件	添加了 AWS Outposts 资源类型。请参阅加速配置文件：伪参数替换。	2023 年 9 月 11 日
更新：支持的服务	在 “ CloudWatch 警报监控的服务” 部分中添加了 Amazon Elastic File S ystem。 请参阅服务描述了解更多信息。	2023 年 9 月 6 日
更新：补丁监控和故障修复	在 “使用 Patch Orchestrator” 部分中添加了以下注释： “不会为操作系统不支持的实例创建补丁失败警报，也不会为在维护时段内停止的实例创建补丁失败警报” 请参阅了解 AMS Accerate 中的补丁管理了解更多信息。	2023 年 9 月 6 日
更新：澄清了对恶意软件事件的响应运行手册	澄清了针对安全事件响应的恶意软件事件响应操作手册。请参阅AMS 中的安全事件响应 了解更多信息。	2023 年 9 月 6 日
更新：将你的加速账户与 Transit Gateway 关联起来	阐明了将新的 Accelerate 账户 VPC 连接到 AMS 多账户着陆区网络（创建 TGW VPC 附件）的步骤：有关更多信息，请参阅将您的加速账户与 Transit Gateway 连接起来。	2023 年 9 月 5 日
更新：来自 AMS 基线监控的警报	删除了对两个已弃用警报的引用 AMSReadLatencyAlarm 和。 AMSWrite LatencyAlarm请参阅来自 AMS 基线监测的警报了解更多信息。	2023 年 9 月 5 日
新增：AMS 事件路由器	添加了 AMS 事件路由器的文档有关在 AMS 中使用亚马逊 EventBridge 托管规则更多信息，请参阅。	2023 年 9 月 5 日

更改	描述	日期
更新：警报管理器伪参数列表。	更新了警报管理器伪参数列表。 EC2 实例名称参数已添加到 EC2 实例和 EC2 磁盘警报配置中。请参阅加速配置文件：伪参数替换了解更多信息。	2023 年 8 月 29 日
新增：AMS Access 下线	增加了退出 AMS Access 时的注意事项。请参阅AMS 加速下机效果。	2023 年 8 月 24 日
新增：AMS 安全事件响应	添加了有关使用 AMS 安全事件响应的文档。请参阅AMS 中的安全事件响应 。	2023 年 8 月 18 日
更新：AMS 加速访问角色	更正了角色名称中的一个错字。请参阅AWS Identity and Access Management 在 AMS 中加速。	2023 年 8 月 10 日
更新：政策声明	用通配符替换了硬编码的角色名称。请参阅查看并更新您的配置，让 AMS Accelerate 能够使用您的 CloudTrail 跟踪。	2023 年 8 月 10 日
更新：带有 EFS 警报的受监控服务列表。	使用适用于 AMS 基准监控的新 EFS 警报更新了监控服务列表。添加了 4 种新的 EFS 警报类型。请参阅来自 AMS 基线监测的警报了解更多信息。	2023年8月3日
更新：加速资源清单表	已移除 ams-backup-config-rule-stack 和相关资源。请参阅用于加速的资源清单。	2023 年 7 月 18 日
更新：AMS 加速访问角色	<8-digit hash>删除了角色 ams-backup-config-rule-st-amsBackupAlert ConfigRule-<8-digit hash>和 ams-backup-config-rule-st-amsBackupPlan ConfigRule H-。请参阅AWS Identity and Access Management 在 AMS 中加速。	2023 年 7 月 18 日

更改	描述	日期
更新：受监控的 RDS 警报列表。	更新了 AMS 基线监控的 RDS 警报列表。添加了 9 种新的 RDS 警报类型，删除了 3 种现有的 RDS 警报类型。请参阅来自 AMS 基线监测的警报了解更多信息。	2023 年 6 月 19 日
新增：AMS 加速访问角色	为 AMS Security 添加了新的访问角色。	2023 年 6 月 16 日
新增：AMS 加速 CloudTrail 日志管理现在可以使用客户 CloudTrail 跟踪。	更新了 Accerate 支持的 CloudTrail 日志管理选项，包括加速部署的跟踪或与客户托管 CloudTrail 账户或组织跟踪的集成。请参阅查看并更新您的配置，让 AMS Accelerate 能够使用您的 CloudTrail 跟踪了解更多信息。	2023年6月9日
更新：AMS Accelerate Config 规则响应配置报告。	更新了 AWS Config Rules 响应配置报告的应要求报告。请参阅加快按需报告的更新。请参阅AMS Config 规则响应配置报告。	2023 年 5 月 26 日
更新：服务计费开始日期政策。	更新了中账单开始日期的定义AMS 关键术语。	2023 年 5 月 15 日
更新： AWS 托管策略。	AWSManagedServicesDeploymentToolkitPolicy 使用新的 CFN 和 ECR 权限更新了，并使用通配符缩小了现有操作的范围。请参见加快服务相关角色的更新。请参阅加快服务相关角色的更新。	2023年5月9日
更新：访问角色策略链接。	现在可以直接从 Accelerate S3 存储桶位置下载访问角色。 请参阅 AMS 访问您的账户的原因和时间和AWS Identity and Access Management 在 AMS 中加速。	

更改	描述	日期
更新：月度账单自助服务报告。	新增说明：月度账单报告仅适用于管理付款人账户（AMS Advanced 多账户登陆区），但适用于所有关联的 AMS Accelerate 管理的账户。 请参阅账单报告（每月）。	2023 年 4 月 13 日
更新：警报列表。	已删除 CloudTrail 参考文献。 请参阅AMS Accelerate 中的日志管理。	2023 年 4 月 13 日
更新：警报列表。	添加了三个新的 SSM 代理警报。 请参阅来自 AMS 基线监测的警报。	2023 年 4 月 13 日
更新：加速先决条件。	澄清说，Accelerate 需要四个 AWS Support 计划中的一个，但不包括开发人员计划。 请参阅加快入职先决条件。	2023 年 4 月 13 日
更新：加速服务相关角色策略。	联系人服务政策 zip 文件已更新。 请参阅AWS AMS 加速的托管策略。	2023 年 4 月 13 日
更新：AMS 资源调度器。	角色名称不正确 AWSManagedServices-DescribeScheduleOrPeriod，已更正为 AWSManagedServices-DescribeScheduleOrPeriods。请参阅使用 AMS 资源调度器进行成本优化。	2023 年 4 月 13 日
更新： AWS 托管策略。	更新自定义调查结果响应了在单个或多个账户中更新自定义回复的说明。	2023 年 4 月 13 日
更新：资源标记	添加了有关 “为新配置指定名称（SampleConfigurationBlock 在提供的示例中），因为您可能会无意中使用相同名称覆盖由 AMS 管理的配置” 的警告。请参阅AMS Accelerate 中的资源标记器用例。	2023 年 3 月 16 日

更改	描述	日期
更新：补丁 RACI	对 RACI 进行了几次更新和澄清，以进行修补。请参阅服务描述。	2023 年 3 月 16 日
更新：部署工具包 SLR JSON 中的操作	更新了政策和行动。请参阅：在 AMS Accelerate 中使用服务相关角色。	2023 年 3 月 16 日
更新：自动修复	移除了对 EC2 音量自动化的LVM支持。请参阅：AMS 自动修复警报。	2023 年 3 月 16 日
更新：加快入门速度。	阐明了角色的使用，尤其是最小角色的用法。创建 AMS 角色的模板	2023 年 3 月 16 日
更新：自助报告。	每日备份报告现在支持主要和次要区域。两者都在 “资源区域” 字段中报告Backup 报告（每日）。	2023 年 3 月 16 日
更新：修补指南	添加了警告，要求不要自定义默认的修补基准，这些基准由 AMS 管理。而是创建新的自定义补丁基准。请参阅：默认补丁基准和使用 AMS Accelerate 自定义补丁。	2023 年 3 月 16 日
更新了服务终止政策。	更新了中服务终止和服务终止日期的定义AMS 关键术语。终止通知必须在您最后一个完整月的前一个月的第 20 天之前发出。	2023 年 3 月 16 日
更新： AWS 托管策略。	明确的策略名称:联系人 AMS Accelerate 的服务相关角色.	2023年2月16日
新增： AWS 托管策略。	新增政策:联系人 AMS Accelerate 的服务相关角色.	2023年2月16日
更新：配置合规性。	修复了拼写错误的单词:. 加速中的配置合规性	2023年2月16日
新内容：不支持 OSes	已添加有关 AMS 为不支持的操作系统提供哪些服务的信息（OSes），请参阅Accelerate 中针对不支持的操作系统的功能。	2023年2月16日

更改	描述	日期
更新：创建补丁窗口	添加了用于 CloudShell 的链接使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口。	2023年2月16日
更新内容：入职管理资源	更新了中压缩的 JSON 模板。创建 AMS 角色的模板	2023年2月16日
新内容：配置合规性	添加了一个新主题:自定义调查结果响应.	2023年2月16日
新增： AWS 托管策略。	新增政策:Amazon EventBridge 规则 AMS Accelerate 的服务相关角色.	2023年2月7日
更新： AWS 托管策略。	`AWSManagedServicesDeploymentToolkitPolicy` 使用新的 S3 权限更新了。请参阅加快服务相关角色的更新。	2023年1月30日
新的选择加入区域：CPT。	AMS Accelerate 现已在开普敦 (CPT) 选择加入区域推出。要选择加入，请参阅管理 AWS 区域。	2023年1月12日
更新：服务说明。	向中添加了由 CloudWatch 警报监控的 FSx 服务服务描述。	2023年1月12日
更新：监控默认指标。	向添加了 6 个 FSx 警报来自 AMS 基线监测的警报。	2023年1月12日
更新：AMS 模式。	添加了自定义 Cloudwatch 警报通知。AMS 模式	2023年1月12日
更新：入职管理资源。	更新了模板表，在 in `ams-onboarding-ssm-execution-role` 中添加了一行创建 AMS 角色的模板。	2023年1月12日
更新：配置合规性。	有关请求自定义补救的更多详细信息（在“重要”框中）。加速中的配置合规性	2023年1月12日

更改	描述	日期
更新： Service-linked-role权限。	已删除较旧或重复的权限。请参阅在 AMS Accelerate 中使用服务相关角色。	2022年12月15日
更新：补丁管理、维护窗口。	在控制台说明步骤 5 中添加了有关创建维护窗口的指南。请参阅通过 Systems Manager 控制台为 AMS Accelerate 创建维护窗口。	2022年12月15日
新增：补丁管理部分。	为星期二补丁维护窗口添加了一个部分。请参阅从 AMS 控制台创建定期的 “补丁星期二” 维护窗口（推荐）。	2022年12月15日
更新：AMS 资源调度器。	更新了 CloudFormation 堆栈名称。请参阅通过 AMS 资源调度器使用资源。	2022年12月15日
更新：标记您的资源以进行备份。	添加了使用 AMS 资源标记器的指南。请参阅标记您的资源以应用 AMS 备份计划。	2022年12月15日
更新：选择备份计划。	指明哪些计划提供持续备份。请参阅选择 AMS 备份计划。	2022年12月15日
更新：AMS 资源调度器。	更新了删除时间段或计划的 AWS CLI 示例。请参阅在 AWS Managed Services 资源计划程序中处理时间段和计划。	2022年12月15日
更新： AWS 托管策略。	添加了`AWSManagedServicesDeploymentToolkitPolicy` 。请参阅AWS AMS 加速的托管策略。	2022年12月15日
新增：添加了描述 AMS 新服务相关角色的章节。`AWSServiceRoleForManagedServices_DetectiveControlsConfig`	添加了 GovCloud 区域和权限。请参阅Detective 控制 AMS Accerate 的服务相关角色。	2022年12月15日

更改	描述	日期
新增： AWS-托管策略	添加了描述服务相关角色策略 AWSManagedServices_AlarmManager _ ServiceRolePolicy 中如何使用 AWS托管策略来限制服务相关角色创建的 IAM 角色权限的章节。 AWSManagedServices_AlarmManagerPermissionsBoundary AWSServiceRoleForManagedServices_AlarmManager请参阅AWS AMS 加速的托管策略。	2022年12月15日
更新：按需操作。	新增产品： EC2 运营上的 SQL Server 以及 AMI 构建和自动售货。请参阅按需运营。	2022年11月10日
更新：监控和事件管理。	更新了服务通知和事件报告的说明。请参阅监控的工作原理。	2022年11月10日
更新：服务相关角色区域	添加了 GovCloud 区域和权限。请参阅在 AMS Accelerate 中使用服务相关角色。	2022年11月10日
新增：服务关联角色。	添加了新角色:`AWSServiceRoleForAMSDetectiveControls` . 请参阅Detective 控制 AMS Accerate 的服务相关角色。	2022年11月10日
更新：访问管理。	使用改进的说明更新了小节。请参阅AMS 中的访问管理加速。	2022年11月10日
更新：服务描述。	更新了 RACI 矩阵中的 AMS 模式。请参阅服务描述。	2022年11月10日
更新：AMS 模式。	客户负责模式部署。请参阅AMS 模式。	2022年11月10日
更新：离职。	添加了有关在离线期间特定 Backup 和 Monitoring 资源会发生什么情况的详细信息。请参阅退出 AMS Accelerate。	2022年11月10日

更改	描述	日期
更新：补丁管理...	更新并缩短了有关 IAM 政策的指南。请参阅创建 IAM 角色以按需修补 AMS Accelerate。	2022年11月10日
新增：架构图链接。	为各种主题添加了 AMS 参考架构图的链接。有关示例，请查看 AMS Accelerate 中的监控和事件管理。	2022年11月10日
全新：按需运营产品	添加了 “着陆区加速器行动”。请参阅按需运营。	2022年10月13日
更新：监控管理。警报生成事件报告，而不是服务请求	监控的工作原理.	2022年10月13日
新增：使用加速自定义 CFN 模板创建补丁维护窗口	CloudFormation 补丁窗口配置模板。请参阅在 AMS 中创建补丁维护窗口。	2022年9月15日
更新：离职	强调 Accelerate 中的备份计划在下线后不再起作用。请参阅退出 AMS Accelerate。	2022年9月15日
更新： CloudWatch 配置变更详情	更正了 Windows 和 Linux 示例中的一个错误。请参阅CloudWatch 配置变更详情。	2022年9月15日
更新：使用 AMS 资源调度器	添加了有关成本分配标签的指南。请参阅AMS 资源调度器中的成本估算器。	2022 年 9 月 15 日
更新：AMS Config 规则库	在规则表中添加了两条`ams-eks-`配置规则。请参阅AMS Config 规则库。	2022 年 9 月 15 日
更新：Backup 管理	从备份计划标题和描述中删除了误导性标签 PITR (point-in-time-recovery)。请参阅选择 AMS 备份计划。	2022 年 9 月 15 日
更新：加速服务说明	更新了配置规则和加那利群岛的描述。请参阅服务描述。	2022 年 9 月 15 日

更改	描述	日期
更新：服务描述、支持的配置	已删除 Windows 2008 R2 的 end-of-service日期。加速不支持 Windows 2008。请参阅支持的配置。	2022 年 8 月 11 日
更新：服务描述、角色和职责	更新了 RACI 表。从 “网络” 部分的最后一行中删除了 ELB 访问日志。我们不为 Accelerate 客户启用 ELB 访问日志。请参阅角色和责任。	2022 年 8 月 11 日
更新：配置合规性	更正了 “规则表，框架” 列中的一个错字。NIST-CSF 被错误地列为 NIST-CIS。请参阅加速中的配置合规性。	2022 年 8 月 11 日
新增内容：加速离职	离职的注意事项和流程。请参阅下线 AMS 加速。	2022 年 8 月 11 日
更新：预安装的 SSM 代理操作系统列表	将 “Ubuntu Linux 18.04 和 20.04” 添加到列表中。请参阅加载 EC2 实例以加速。	2022 年 8 月 11 日
新增：资源调度器	使用 AMS 资源调度器通过仅在需要时停止和启动资源来优化成本。请参阅使用 AMS 资源调度器进行成本优化。	2022 年 7 月 14 日
更新：资源调度器的服务描述	针对新的资源调度器产品更新了服务描述的几个部分。请参阅服务描述。	2022 年 7 月 14 日
新增：AMS 模式	AMS 提供模式模板，这是一种通用解决方案，可解决 AMS 托管环境中的一系列用例。提供的第一种图案:AMS 模式.	2022 年 7 月 14 日
新增：成本优化说明	添加了一个注释，解释了成本如何随着资源使用而增加。请参阅用于加速的资源清单。	2022 年 7 月 14 日
更新：AMS Config 规则	重组了中的表格。AMS Config 规则库为了便于一目了然，HTML 表格的列数较少。可下载的电子表格还有其他列可以进行排序和筛选。	2022 年 7 月 14 日

更改	描述	日期
更新：访问管理	更新了中的示例 CloudFormation 模板使用 AMS 功能的权限。该AMSAccelerateAdminAccess 策略现在包括AmsResourceSchedulerPassRolePolicy 和IAMReadOnlyPolicy 策略。	2022 年 7 月 14 日
更新：自助报告	添加了使用 KMS 密钥加密 AWS Glue 元数据的说明。参见标有 “重要” 的方框自助报告。	2022 年 7 月 14 日
更新：AMS 基线监测	添加了 DeleteRecoveryPoint 备份警报。 来自 AMS 基线监测的警报	2022 年 7 月 14 日
更新：支持的操作系统	增加了亚马逊 Linux 2 的终止支持日期。 服务描述	2022 年 7 月 14 日
更新：AMS 报告	添加了有关选择加入区域的注释。 报告和选项	2022 年 7 月 14 日
资源调度程序	添加了有关入职和使用 AMS 资源调度器通过安排资源停止和开始时间来帮助优化成本的信息。此外，还更新了 Accelerate 服务描述，增加了对资源调度程序的提及。此外，将亚马逊 Linux 2 支持的终止支持日期更新为 2024 年。请参阅使用 AMS 资源调度器进行成本优化和服务描述。	2022 年 6 月 30 日
新警报	添加了 AWS Backup 警报。 来自 AMS 基线监测的警报	2022 年 6 月 21 日
新增内容	添加了服务关联角色内容。 在 AMS Accelerate 中使用服务相关角色	2022 年 6 月 16 日
	AWS Network Firewall Operations 已添加到按需运营 (OOD) 产品目录中。 按需运营	2022 年 6 月 16 日
	添加了问题管理功能描述。 服务描述	2022 年 6 月 16 日

更改	描述	日期
	添加了有关特定选择加入区域不支持的配置规则集的注释。 加速中的配置合规性	2022 年 6 月 16 日
更新了内容	配置合规性。“AMS Config 规则库”-> “规则表”已更新并移除为仅限 ZIP。 加速中的配置合规性	2022 年 6 月 16 日
	删除了升级电子邮件。 升级路径	2022 年 6 月 16 日
	将主题列表移至开头段落下方。 什么是 AMS 加速？	2022 年 6 月 16 日
	更新了 auto 重定内容。 AMS 自动修复警报	2022 年 6 月 16 日
更新内容：服务说明	将 EKS 添加到中由 AMS Config 规则监控的服务列表中受支持的服务。 更新了 RACI 表中的角色和责任监控描述。	2022 年 5 月 12 日
更新内容：配置合规性	添加了与 EKS 相关的配置规则。请参阅加速中的配置合规性。	2022 年 5 月 12 日
更新内容：入门、账号发现	在中添加了该 AwsAccountDiscoveryCli 脚本的更新版本（在账户发现变更日志 zip 文件中）。第 1 步：在 “加速” 中发现账户	2022 年 5 月 12 日
更新内容：监控、默认指标	更新了 ALB 相关指标的触发条件。请参阅来自 AMS 基线监测的警报。	2022 年 5 月 12 日
更新内容：修补新手入门	添加了明确的修补先决条件：您需要选择加入 EBS。请参阅Accelerate 中的入门补丁。	2022 年 5 月 12 日
更新内容：加速资源清单表	更改了 ams-detective-controls-config-rules-cdk 规则，添加了-cdk 和-cdk 的规则。 ams-detective-controls-recorder ams-detective-controls-infrastructure请参阅用于加速的资源清单。	2022 年 4 月 14 日

更改	描述	日期
更新内容：配置合规性	行业标准、配置规则和响应类型简介。强调客户不会选择单独的配置规则或响应。 加速中的配置合规性。	2022 年 4 月 14 日
更新内容：服务说明	将现有的 “变更范围” 部分移至 “角色和职责” 下。请参阅角色和责任。	2022 年 4 月 14 日
更新内容：标记和监控	已`AWS::Synthetics:Canary` 添加到允许标记和监控的资源类型列表中。请参阅 AMS 中的资源标记器配置文件加速和加速配置文件：伪参数替换。	2022 年 4 月 14 日
更新内容：加速先决条件	向添加了 SSM 必需的存储桶权限。加速中的 Amazon EC2 Systems Manager	2022 年 4 月 14 日
新内容：修补和监控	添加了使用 Cloudformation 部署标记和监控配置的示例代码。请参阅 使用 for Accelerat CloudFormation e 部署配置文件和CloudFormation 用于部署加速配置更改。	2022 年 3 月 10 日
更新内容：补丁维护控制台	重新排序了步骤通过 Systems Manager 控制台为 AMS Accelerate 创建维护窗口以匹配控制台界面。	2022 年 3 月 10 日
更新内容：补丁维护 CLI	更新了 CLI 参数（计划、持续时间和截止时间）使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口	2022 年 3 月 10 日
新内容：自动实例 Config	添加了`AMSInstanceProfileBasePolicy` 的定义 IAM 权限变更详情	2022 年 3 月 10 日
新内容：入职	在 Linux 命令中添加了一个示例 加速中的出站互联网连接	2022 年 3 月 10 日
新内容：入职	向添加了最低权限选项。创建 AMS 角色的模板	2022 年 3 月 10 日

更改	描述	日期
更新内容：加快升级指令	添加了指南、链接和电子邮件联系人 升级路径	2022 年 3 月 10 日
更新内容：支持的配置	AMS预计将于2023年3月14 CentOs 日终止对RHEL 6的支持。请参阅 支持的配置。	2022 年 3 月 10 日
更新内容：资源表	在用于加速的资源清单资源表中添加了 AMS 访问权限 IAM 角色	2022 年 3 月 10 日
更新内容：入职和 Backup	添加了有关选择加入和 AWS Backup 的在 “加速” AWS Backup 中入职说明 AMS 中的连续性管理加速	2022 年 3 月 10 日
更新内容：访问管理	已从 “加速” 指南中移除特定于高级的说明。如何以及何时在 AMS 中使用 root 用户账户	2022 年 3 月 10 日
更新内容：支持的配置	AMS 现在支持 Oracle Linux 8.3 和 Ubuntu 18.04 和 20.04。请参阅支持的配置。	2022 年 2 月 28 日
更新内容：服务等级协议	更新了中可下载的服务等级协议。受支持的服务	2022 年 2 月 28 日
更新内容：访问管理	更新了 AMS 如何访问您的账户 AMS 操作员控制台角色并警告不要修改或删除它们。 FAQs	2022 年 2 月 28 日
更新内容：警报管理器	已更新 加速配置文件：监控。警报管理器不再局限于单指标警报。	2022 年 2 月 28 日
更新内容：入门	已更新 第 2 步：Accelerate 中的入职管理资源。添加了一个 IAM 角色，该角色对入职资源的访问权限最小。	2022 年 2 月 28 日
新内容：服务说明变更范围	添加了一个新部分AMS Accelerate 执行的变更范围，重点介绍了 AMS Accelerate 无法执行的界限和动作。	2022 年 2 月 10 日

更改	描述	日期
更新内容：入门	新的入职流程从设置默认功能和配置开始，然后再进行自定义。小节包含特定功能的目标和相关链接。请参阅AMS 入门加速。	2022 年 2 月 10 日
更新内容：AMS Backup 管理。	为了便于阅读，缩短并重新组织了AMS 中的连续性管理加速章节。	2022 年 2 月 10 日
更新内容：标记	添加了 “标记工具” 部分，以容纳 CloudFormation 和其他工具的代码示例。请参阅在 AMS 中添加标签加速。	2022 年 2 月 10 日
更新内容：基线监控	改善了 RedShift 集群警报的触发条件，减少了维护期间的误报。请参阅来自 AMS 基线监测的警报。	2022 年 2 月 10 日
更新内容：修补	更新了示例 CLI 命令以注册维护窗口。请参阅使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口。	2022 年 2 月 10 日
更新内容： AWS Config 规则清单。	`ams-nist-cis-ec2-security-group-attached-to-eni` 从 Config Rules 清单表中移除了已弃用的 AWS 配置规则。请参阅规则表。	2022 年 1 月 27 日
新内容：创建补丁维护窗口。	添加了指向 SSM 教程的链接以及用于从命令行创建补丁维护窗口的示例命令。请参阅使用 AMS Accelerate 的 Systems Manager 命令行界面 (CLI) 创建维护窗口。	2022 年 1 月 27 日
新内容：资源标记器可识别新的 Auto Scaling Groups (ASG) 资源类型。	将 Auto Scaling 组添加到可使用资源标记器配置配置文件筛选的资源类型中。请参阅语法和结构。	2022 年 1 月 13 日
新内容：其他备份计划和存储库。	添加了新的备份计划和保管库，以缓解包括勒索软件攻击在内的高风险情况。请参阅 查看 AMS 保管库中的备份和查看 AMS 保管库中的备份。	2022 年 1 月 13 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。