AMS 高级账户注册信息

AMS 高级入职指南

版本 September 25, 2025

AMS 高级入职指南: AMS 高级账户注册信息

Table of Contents

AWS Managed Services 入职简介

欢迎使用 AWS Managed Services (AMS)。AMS 是一项企业服务，可为您的 AWS 基础设施提供持续管理。本指南旨在帮助您开始使用 AMS，包括如何为 AMS 设置新账户、设置网络和访问 AMS，以及如何验证您的入门设置。

它适用于负责准备和执行将 AMS 服务注册到新 AWS 账户所需任务的 IT 管理员。加入 AMS 服务需要特殊权限才能设置 Active Directory 信任和完成其他网络级别的任务。要在决定使用多账号着陆区账户还是单账号着陆区账户时获取帮助，请访问选择单个 MALZ 还是多个。 MALZs

> **Important**
>
> 本指南在本介绍之后分为两部分：一部分用于多账号着陆区账户，另一部分用于单账号着陆区账户。两者的入职方式大不相同，请前往指南中适用于您的情况的部分旁边。

主题

了解 AMS

要更好地了解 AMS，请参阅以下 AMS 用户指南部分：

- 什么是 AWS Man aged Services 介绍了 AMS 服务，并描述了主要功能、操作和接口以及典型的 AMS 托管网络架构。本章还提供有关访问管理的信息，包括如何访问您的 AMS 管理的资源和使用堡垒。
- 关键术语提供了 AMS 术语的定义和解释。

- 了解 AMS 默认值提供 AMS 使用的默认值，包括基本环境组件、IAM 和代理 EC2、受监控指标、日志记录、端点安全 (EPS)、备份和修补的默认值。
- 变更管理详细介绍了变更请求 (RFCs) 和变更类型 (CTs) 的工作原理，并包括使用 AMS 的示例 RFCs。
- 其他几章涵盖了使用 AMS 变更管理系统访问 AWS 控制台、AMS CLI、AMS SKMS、安全、服务请求、事件、监控、日志、EPS、备份和补丁管理。

要了解有关 AMS 多账户 landing zone 架构的更多信息，请参阅多账户着陆区网络架构

要了解有关 AMS 单账户着陆区架构的更多信息，请参阅单账户着陆区网络架构

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。

AMS 模式

根据您想要的灵活性和规范性管理组合，使用它来帮助您选择合适的 AWS Managed Services (AMS) 模式来托管应用程序，以实现业务成果。

此信息的目标受众是：

- 客户团队负责其 landing zone 的策略和治理。这些信息将帮助该团队为AMS管理的着陆区奠定基础，以及他们希望向内部和外部客户提供的AMS模式。
- 负责将其应用程序迁移到 AMS 的企业和应用程序所有者。这些信息将有助于规划应用程序迁移，并为 migrate/host 其应用程序提供相应的 AMS 模式。请注意，在软件开发生命周期 (SDLC) 生命周期的不同阶段，同一应用程序可以在多个 AMS 模式下托管。
- AMS 合作伙伴的任务是指导客户选择构建和迁移到 AMS 的不同选项。

此信息假设您已经决定利用 AMS 来加速您的云之旅。在云迁移之旅的两个时刻参考这篇论文：首先，在设置 AMS 托管平台的基础阶段。其次，当你从云采用之旅的基础阶段过渡到迁移阶段时，就在向 AMS 的入职完成并专注于应用程序治理和运营之后。

AMS 模式和应用程序或工作负载

在选择正确的模式时，请考虑应用程序的运营和管理要求，方法是申请新的应用程序帐户或将应用程序托管在现有应用程序帐户中。为每个应用程序或工作负载选择适当的 AMS 模式取决于以下因素：

- 环境将提供的 SDLC 生命周期功能类型（例如，包含未经审核更改的沙箱、具有一些频繁更改的 UAT、更改最少且受到严格监管的生产）
- 所需的治理政策（通过 SCPs OU 级别强制执行）
- 运营模式（如果您想承担运营责任或想将其外包给AMS）
- 预期的业务成果，例如在云端运营的时间和运营成本。

> **Note**
>
> 有关每个 AMS 服务的模式类型的描述，请参阅 AMS 中的模式和账户类型。
> 有关不同模式的真实用例，请参阅 AMS 模式的真实世界用例

下表概述了应用程序所有者在决定最合适的 AMS 模式时需要考虑的关键因素。应用程序所有者应在应用程序迁移之前加入评估阶段，以充分了解哪种模式适用于他们的特定应用程序。示例：对于基于云原

生服务或无服务器架构的应用程序，最好的选择可能是在开发人员模式下开始构建和迭代，然后使用 AMS Managed — SSP 模式部署最终的基础设施即代码。在这种情况下，可能需要进行轻度重构，以确保为自动部署创建的任何 CloudFormation 模板都符合 AMS 制定的采集指南。此外，任何 IAM 权限都需要获得 AMS Security 的批准，以确保它们遵循最低权限模式。

为托管应用程序而选择的 AMS 模式可以帮助您朝着所需的云运营模式进行构建。

> **Note**
>
> 根据为托管应用程序而选择的不同 AMS 模式，单个 AMS 托管着陆区中可以存在多个云运营模式。

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
运营准备就绪						
记录、监控和事件管理	AMS 负责所有托管基础架构			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	客户负责
连续性管理	AMS 负责执行客户选择的备份计划			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
实例级访问管理	AMS 通过本地域的单向 AD 信任进行管理。需要托管基础设施才能加入 AMS 域			不适用	负责使用开发者 IAM 角色在 AMS CM 系统之	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
					外配置资源的客户	
安全管理和账户级别访问管理	AMS 对所有托管账户负责			AMS 负责所有托管账户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
补丁管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
变更管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
资源调配管理	针对 AMS 中提供的配置选项进行了规范和标准化	按照 AMS 规范性标准，可以灵活地直接使用适用于 AWS Service Catalog 的 AWS 服务 API	按照 AMS 规范性标准灵活地直接使用 AWS 服务 API	可以灵活地直接使用 AWS 服务 APIs 提供 SSP 服务	可以灵活地直接使用 AWS 服务 API 进行配置	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
事件管理和审计	AMS 负责所有托管账户				负责使用开发者 IAM 角色在 AMS 变更管理系统之外配置资源的客户	
GuardRails 以及共享基础架构（网络）和安全框架	利用 AMS 核心账户的规范性和标准化					灵活定制利用 AMS 核心账户
应用程序就绪						
应用程序重构	需要轻量化重构				需要轻量级重构（如果使用 AMS 标准 CM 进行配置）	无需重构
对 AWS 服务的支持	仅限于 AMS 支持的内容					不限
业务注意事项						
是时候做好运营准备了	三到六个月			6 个月以上，具体取决于客户的应用程序操作能力		6-18 个月视客户基础架构和应用程序操作能力而定

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
成本	$$$$			$$$	$$	$
应用示例	具有 3 层堆栈的 Web 服务器、符合合规性和监管要求的应用程序			使用 API Gateway 的 Web 服务器、利用 ECS/EKS 的容器化应用程序	对使用 Lambda、Glue、Athena 等的数据湖应用程序进行迭代/优化	accounts/applications 像沙盒一样去中心化、第三方托管的应用程序

* Operations On Demand (OOD) 为使用标准 CM 模式的客户提供了通过专用资源管理管理其变更的服务。有关更多详细信息，请参阅按需运营产品目录，并咨询您的云服务交付经理 (CSDM)。

> **Note**
>
> SSP 模式和开发者模式之间的价格比较假设预配置了相同的 AWS 服务。

将 AMS 模式与业务和 IT 目标进行比较

如图所示，如果您正在为应用程序寻找高度可控和标准化的监管模式，那么 AMS 管理的标准变更、AWS Service Catalog 或直接变更模式最为合适。如果您需要以应用程序创新为重点的定制治理模型，而无需做好运营准备，请选择客户管理模式。在 Customer Managed 模式下，您可能需要更长的时间才能运行应用程序，因为您有责任建立人员、流程和工具来支持操作功能，例如事件管理、配置管理、配置管理、安全管理、补丁管理等。

AMS 账户后规范性指导

随着组织采用分布式运营和 DevOps 实践，在部署工作负载之前，应将一组核心运营能力应用于每个客户，以满足 Well Architected 的支柱。

此链接下载包含 Word 文档的 ZIP 文件以及包含脚本和示例的 ZIP 文件。自动账户设置是一组用于自动设置或引导新应用程序帐户设置的脚本。

出售新账户后，在部署任何工作负载之前，为了使账户从运营、安全和管理的角度做好准备，您需要设置默认备份计划、补丁窗口和加密（等等）。为了帮助提高应用程序帐户设置的敏捷性、一致性和响应能力，提供了以下 “操作方法” 示例，供您参考。

自动账户设置。

我们做什么，不做什么

AMS 为您提供部署 AWS 基础设施的标准化方法，并提供必要的持续运营管理。有关角色、职责和支持的服务的完整描述，请参阅服务描述。

> **Note**
>
> 要请求 AMS 提供其他 AWS 服务，请提交服务请求。有关更多信息，请参阅提出服务请求。

- 我们做什么：

  完成入职后，AMS 环境可以接收变更请求 (RFCs)、事件和服务请求。您与 AMS 服务的交互围绕着应用程序堆栈的生命周期。新堆栈是从预先配置的模板列表中订购的，启动到特定的虚拟私有云 (VPC) 子网，在运行期间通过更改请求 (RFCs) 对其进行修改，并全天候监控事件和事件。

  主动应用程序堆栈由 AMS 监控和维护，包括修补，除非需要更改或堆栈已停用，否则在堆栈的生命周期内无需采取任何进一步的操作。AMS 检测到的影响堆栈运行状况和功能的事件会生成通知，可能需要也可能不需要您采取措施来解决或验证。可以通过提交服务请求来提出操作方法问题和其他查询。

  此外，AMS 还允许您启用不由 AMS 管理的兼容 AWS 服务。有关兼容 AWS-AMS 的服务的信息，请参阅自助服务配置模式。

- 我们不做什么：

  虽然 AMS 通过提供许多手动和自动选项来简化应用程序部署，但您需要负责应用程序的开发、测试、更新和管理。AMS 为影响应用程序的基础设施问题提供故障排除帮助，但 AMS 无法访问或验证您的应用程序配置。

AMS 出口流量管理

默认情况下，AMS 私有子网和客户应用程序子网的目标 CIDR 为 0.0.0.0/0 的路由将网络地址转换 (NAT) 网关作为目标。AMS TrendMicro 服务和补丁是必须具有互联网出口访问权限的组件，这样 AMS 才能提供其服务， TrendMicro 并且操作系统可以获取更新。

AMS 支持通过客户管理的出口设备将出口流量转移到互联网，前提是：

- 它充当隐式（例如，透明）代理。

  以及

- 它允许 AMS HTTP 和 HTTPS 依赖关系（在本节中列出），以便能够持续修补和维护 AMS 托管基础架构。

部分示例包括：

- 公交网关 (TGW) 的默认路由，通过多账户着陆区网络账户中的 AWS Direct Connect 连接指向客户管理的本地防火墙。
- TGW 有一个默认路由，指向利用 AWS 的多账户着陆区出口 VPC 中的 AWS 终端节点，指向另一个 PrivateLink AWS 账户中的客户管理的代理。
- TGW 的默认路由指向另一个 AWS 账户中的客户管理的防火墙， site-to-siteVPN 连接作为多账户着陆区 TGW 的附件。

AMS 已经确定了相应的 AMS HTTP 和 HTTPS 依赖关系，并不断开发和完善这些依赖关系。请参阅 egressMgmt.zip。除了 JSON 文件外，ZIP 还包含一个自述文件。

> **Note**
>
> - 此信息并不全面，此处未列出一些必需的外部站点。
> - 请勿在拒绝列表或屏蔽策略下使用此列表。
> - 此列表旨在作为出口过滤规则集的起点，期望使用报告工具来精确确定实际流量与列表的偏离位置。

要询问有关筛选出口流量的信息，请发送电子邮件至 CSDM：ams-csdm@amazon.com。

AMS 中的 IAM 用户角色

IAM 角色与 IAM 用户类似，因为它是一个具有权限策略的 AWS 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，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。

目前，对于标准 AMS 账户，有一个 AMS 默认用户角色`Customer_ReadOnly_Role`，还有一个角色适用于使用托管 Active Directory 的 AMS 账户。`customer_managed_ad_user_role`

角色策略设置了 Amazon S3 日志操作的权限、AMS 控制台访问权限、对大多数控制台的只读限制 AWS 服务、对账户 S3 控制台的限制访问以及 AMS 更改类型访问权限。 CloudWatch

此外，还`Customer_ReadOnly_Role`具有可变的预留实例权限，允许您预留实例。它具有一些节省成本的价值，因此，如果您知道在很长一段时间内将需要一定数量的 Amazon EC2 实例，则可以调用这些 APIs实例。要了解更多信息，请参阅 Amazon EC2 预留实例。

> **Note**
>
> 除非要重复使用现有策略，否则为 IAM 用户创建自定义 IAM 策略的 AMS 服务级别目标 (SLO) 为四个工作日。如果您想修改现有的 IAM 用户角色或添加新角色，请分别提交 IAM：更新实体或 IAM：创建实体 RFC。

如果您不熟悉 Amazon IAM 角色，请参阅 IAM 角色了解重要信息。

多账户着陆区 (MALZ)：要查看 AMS 多账户着陆区默认、未自定义的用户角色政策，请参阅下文。MALZ：默认 IAM 用户角色

MALZ：默认 IAM 用户角色

默认多账户 AMS 多账户 landing zone 用户角色的 JSON 政策声明。

> **Note**
>
> 用户角色是可自定义的，并且可能因每个账户而异。提供了有关如何找到您的角色的说明。

以下是默认 MALZ 用户角色的示例。要确保设置了所需的策略，请运行 AWS 命令`get-role`或登录 AWS 管理-> IAM 控制台，然后在导航窗格中选择角色。

OU 账户的核心

核心账户是 MALZ 管理的基础设施账户。AMS 多账户 landing zone Core 账户包括一个管理账户和一个网络账户。

OU 核心 OU 账户：常见角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess（公共 AWS 托管策略）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupport访问权限（公有 AWS 托管策略）。
AWSManagedServicesChangeManagementRole（核心账户版本）	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

核心 OU 账户：管理账户角色和政策

角色	政策或政策
AWSManagedServicesBillingRole	AMSBilling政策（AMSBilling政策）。
AWSManagedServicesReadOnlyRole	ReadOnlyAccess（公共 AWS 托管策略）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupport访问权限（公有 AWS 托管策略）。
AWSManagedServicesChangeManagementRole（管理账户版本）	ReadOnlyAccess
	AWSSupport访问

角色	政策或政策
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

核心 OU 账户：网络账户角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess（公共 AWS 托管策略）。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupport访问权限（公有 AWS 托管策略）。
AWSManagedServicesChangeManagementRole（网络账户版本）	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

应用程序账户角色

应用程序账户角色适用于您的应用程序专用账户。

应用程序账户：角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess（公共 AWS 托管策略）。
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupport访问权限（公有 AWS 托管策略）。 该政策提供对所有支持操作和资源的访问权限。有关信息，请参阅 AWS Support 入门。
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSSupport访问示例 该政策提供对所有支持操作和资源的访问权限。 AWSCertificateManagerFullAccess 信息，（公共 AWS 托管政策） AWSWAFFullAccess 信息，（公共 AWS 托管政策）。此政策授予对 AWS WAF 资源的完全访问权限。 AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole（应用程序账号版本）	ReadOnlyAccess AWSSupport访问权限（公有 AWS 托管策略）。 该政策提供对所有支持操作和资源的访问权限。有关信息，请参阅 AWS Support 入门。 AMSSecretsManagerSharedPolicy AMSChangeManagementPolicy

角色	政策或政策
	AMSReservedInstancesPolicy
	AMSS3Policy
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFull访问
	AMSS3Policy
	AMSReservedInstancesPolicy

策略示例

提供了大多数使用的策略的示例。要查看该 ReadOnlyAccess 政策（只要它提供对所有 AWS 服务的只读访问权限，则为页面），如果您有活跃的 AWS 账户，则可以使用此链接：ReadOnlyAccess。此外，此处还包括精简版。

AMSBilling政策

```
AMSBillingPolicy
```

您的会计部门可以使用新的账单角色来查看和更改管理账户中的账单信息或账户设置。要访问诸如备用联系人之类的信息、查看账户资源使用情况、查看账单甚至修改付款方式，您可以使用此角色。这个新角色包含 AWS 账单 IAM 操作网页中列出的所有权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
```

```
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
```

```
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

查看所有 AMS 变更类型以及请求更改类型的历史记录的权限。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

请求 Deployment | Managed landing zone | 管理账户 | 创建应用程序账户（使用 VPC）更改类型的权限。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

请求 Deployment | Managed landing zone | 网络账户 | 创建应用程序路由表更改类型的权限。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy（管理层 | 其他 | 其他 CTs）

请求 “管理” | “其他” | “其他” | “创建” 和 “管理” | “其他” | “其他” | “更新” 更改类型的权限。

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

查看 AMS 通过 passwords/hashes 共享的机密的权限 AWS Secrets Manager （例如，用于审计的基础设施密码）。

创建与 AMS 共享 password/hashes 的密钥的权限。（例如，需要部署的产品的许可证密钥）。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

AMSChangeManagementPolicy

请求和查看所有 AMS 变更类型的权限，以及请求的更改类型的历史记录。

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

管理亚马逊 EC2 预留实例的权限；有关定价信息，请参阅亚马逊 EC2 预留实例。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
  ]
 }]
}
```

AMSS3政策

AMSS3Policy

在现有 Amazon S3 存储桶中创建和删除文件的权限。

> **Note**
>
> 这些权限不授予创建 S3 存储桶的权限；必须使用部署 | 高级堆栈组件 | S3 存储 | 创建更改类型来完成。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupport访问权限

AWSSupportAccess

完全访问权限 支持。有关信息，请参阅入门 支持。有关 Premium Support 的信息，请参阅支持。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions（公共 AWS管理政策）

订阅、取消订阅和查看订 AWS Marketplace 阅的权限。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

完全访问权限 AWS Certificate Manager。有关更多信息，请参阅 AWS Certificate Manager。

`AWSCertificateManagerFullAccess`信息，（公共 AWS 托管政策）。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFull访问权限

AWSWAFFullAccess

完全访问权限 AWS WAF。有关更多信息，请参阅 AWS WAF -Web 应用程序防火墙。

AWSWAFFullAccess信息，（公共 AWS 管理政策）。此政策授予对 AWS WAF 资源的完全访问权限。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

ReadOnlyAccess

ReadOnlyAccess

对 AWS 控制台上所有 AWS 服务和资源的只读访问权限。 AWS 启动新服务时，AMS 会更新 ReadOnlyAccess 政策，为新服务添加只读权限。更新的权限会应用于策略附加到的所有主体实体。

这并不能授予登录 EC2 主机或数据库主机的权限。

如果您有激活的政策 AWS 账户，则可以使用此ReadOnlyAccess链接查看整个 ReadOnlyAccess 政策。只要它为所有人提供只读访问权限，整个 ReadOnlyAccess 策略就会持续很长时间 AWS 服务。以下是该 ReadOnlyAccess 政策的部分摘录。

单账户着陆区 (SALZ)：要查看 AMS 单账户着陆区默认、未自定义的用户角色策略，请参阅 “下一步”。SALZ：默认 IAM 用户角色

SALZ：默认 IAM 用户角色

默认 AMS 单账户 landing zone 用户角色的 JSON 政策声明。

> **Note**
>
> SALZ 默认用户角色是可自定义的，可能因每个账户而异。提供了有关如何找到您的角色的说明。

以下是默认 SALZ 用户角色的示例。要确保已为您设置了策略，请运行`get-role`命令。或者，登录 AWS Identity and Access Management 控制台 https://console.aws.amazon.com/iam/，然后选择 “角色”。

客户只读角色是多个策略的组合。以下是该角色的细分 (JSON)。

Managed Services 审计政策：

托管服务 IAM ReadOnly 政策

Managed Services 用户政策

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
           "encrypted/",
           "encrypted/app/*"
```

```
          ]
        }
      }
    },
    {
      "Sid": "BasicAccessRequiredByS3Console",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid": "AllowCustomerToGetLogs",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
```

```
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
```

```
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
```

```
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
```

```
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
```

```
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

客户 Secrets Manager 共享政策

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
```

```
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

客户市场订阅政策

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

默认访问防火墙规则

这些是访问您的实例所需的默认防火墙规则。

> **Note**
>
> 有关建立 AD 单向信任所需的防火墙规则和端口的信息，请前往 AWS Artifact 控制台-> “报告”选项卡并搜索 AWS Managed Services，查看 AMS 安全指南。

Linux 堆栈实例端口

这些规则是您对 AMS Linux 堆栈进行身份验证所必需的。

Linux 实例端口规则从：Linux 堆栈实例到：CORP 域控制器

端口	协议	服务	方向
389	TCP	LDAP	入口
389	UDP	LDAP	入口
88	TCP	Kerberos	入口
88	UDP	Kerberos	入口

Windows 堆栈实例端口

这些规则是您对 AMS Windows 堆栈进行身份验证所必需的。

从：Windows Stack 实例到：CORP 域控制器

端口	协议	服务	方向
88	TCP | UDP	Kerberos	入口和出口
135	TCP | UDP	DCE/RPC 定位器服务	入口和出口
389	TCP | UDP	LDAP	入口和出口
3268	TCP | UDP	msft-gc，微软全球目录（包含来自 Active Directory 森林的数据的 LDAP 服务）	入口和出口
445	TCP	微软 DS Active Directory，Windows	入口和出口
49152 - 65535	TCP	无法向 IANA 注册的动态或私有端口。此范围用于私有或定制服务或临时用途，也用于临时端口的自动分配。	入口和出口

AWS Managed Services 中的服务管理

主题

AMS 服务如何为您服务。

AWS Managed Services 中的账户管理

本节介绍 AMS 账户管理。

您被指定为云服务交付经理 (CSDM)，负责在整个 AMS 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 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。

在 AWS Managed Services 中开始提供服务

服务开始：AWS Managed S ervices 账户的服务开始日期是第一个日历月的第一天，在此之后，AWS 会通知您该 AWS Managed Services 账户的入职要求中规定的活动已经完成；前提是，如果 AWS 在某个日历月的第 20 天之后发出此类通知，则服务开始日期为该通知之日后第二个日历月的第一天。

服务开始

- R 代表负责任的一方，负责完成任务。
- 我代表知情；一个通报进展情况的当事方，通常只有在任务或可交付成果完成后才会被告知。

服务开始

步骤 #	步骤标题	说明	Custome	AMS
1.	移交客户 AWS 账户	客户创建一个新的 AWS 账户并将其移交给 AWS Managed Services	R	我
2.	AWS Managed Services 账户-设计	完成 AWS Managed Services 账户的设计	我	R
3.	AWS Managed Services 账户-构建	AWS Managed Services 账户是按照步骤 2 中的设计创建的	我	R

客户关系管理 (CRM)

AWS Managed Services (AMS) 提供了客户关系管理 (CRM) 流程，以确保与您建立和维持明确的关系。这种关系的基础是AMS对您的业务需求的洞察。CRM 流程有助于准确、全面地理解：

- 您的业务需求以及如何满足这些需求
- 你的能力和限制
- AMS 和您的不同责任和义务

CRM 流程允许 AMS 使用一致的方法向您提供服务，并管理您与 AMS 的关系。CRM 流程包括：

- 确定您的主要利益相关者
- 组建治理团队
- 与您举行和记录服务审查会议
- 提供带有上报程序的正式服务投诉程序
- 实施和监控您的满意度和反馈流程

- 管理您的合同

CRM 流程

CRM 流程包括以下活动：

- 识别和了解您的业务流程和需求。您与 AMS 的协议确定了您的利益相关者。
- 定义要提供的服务以满足您的需求和要求。
- 在服务审查会议上与您会面，讨论 AMS 服务范围、SLA、合同和您的业务需求的任何变化。可能会与您举行临时会议，讨论绩效、成就、问题和行动计划。
- 使用我们的客户满意度调查和会议反馈来监控您的满意度。
- 在内部衡量的月度绩效报告中报告绩效。
- 与您一起审查服务，以确定改进的机会。这包括就所提供的 AMS 服务的水平和质量与您进行频繁沟通。

CRM 会议

AMS 云服务交付经理 (CSDMs) 定期与您开会，讨论服务轨道（运营、安全和产品创新）和高管方向（SLA 报告、满意度衡量标准和业务需求的变化）。

会议	用途	Mode	参与者
每周状态回顾（可选）	未解决的问题或事件、补丁、安全事件、问题记录 12 周运营趋势 (+/-6) 应用程序操作员关注的问题 周末日程安排	现场客户 location/ Telecom/Chime	AMS：CSDM 和云架构师 (CA) 客户分配的团队成员（例如：云/基础架构、Application Support、架构团队等）
每月业务回顾	查看服务级别性能（报告、分析和趋势） 财务分析	现场客户 location/ Telecom/Chime	AMS：CSDM、云架构师 (CA)、AMS 客户

会议	用途	Mode	参与者
	产品路线图 CSAT		团队、AMS 技术产品经理 (TPM)（可选）、AMS 运营经理（可选） 您：应用程序运营商代表
季度业务回顾	记分卡和服务级别协议 (SLA) 绩效和趋势（6 个月） 即将到来的 12 年 3 月 6 日/9 月计划/迁移 风险和风险缓解 关键改进举措 产品路线图项目 未来方向一致的机会 金融 成本节约举措 业务优化	现场客户位置	AMS：CSDM、云架构师、AMS 客户团队、AMS 服务总监、AMS 运营经理 您：应用程序运营商代表、服务代表、服务主管

CRM 会议安排

AMS CSDM 负责记录会议，包括：

- 创建议程，包括行动项目、议题和与会者名单。
- 创建每次会议上审查的措施项目列表，以确保项目按计划完成和解决。
- 在会议结束后的一个工作日内通过电子邮件向与会者分发会议纪要和行动项目列表。
- 将会议记录存储在相应的文档存储库中。

在CSDM缺席的情况下，主持会议的AMS代表编写和分发会议记录。

> **Note**
>
> 您的 CSDM 会与您合作建立您的账户管理。

CRM 月度报告

您的 AMS CSDM 准备并发送每月服务绩效演示文稿。演讲包括以下方面的信息：

- 举报日期
- 摘要和见解：
  - Key Call Outs：堆栈总数和活跃堆栈数、堆栈补丁状态、账户入职状态（仅限入职期间）、客户特定问题摘要
  - 性能：事件解决、警报、修补、变更请求 (RFCs)、服务请求以及控制台和 API 可用性的统计信息
  - 问题、挑战、疑虑和风险：客户特定的问题状态
  - 即将推出的项目：客户特定的入职培训或事件解决计划
- 托管资源：堆栈的图表和饼图
- AMS 指标：监控和事件指标、事件指标、AMS SLA 遵守指标、服务请求指标、变更管理指标、存储指标、连续性指标、Trusted Advisor 指标和成本摘要（以多种方式呈现）。功能请求。联系信息。

> **Note**
>
> 除了上述信息外，您的 CSDM 还会告知您范围或条款的任何重大变化，包括AMS使用分包商进行运营活动。
>
> AMS 会生成有关修补和备份的报告，您的 CSDM 将这些报告包含在您的月度报告中。作为报告生成系统的一部分，AMS 会为您的账户添加一些您无法访问的基础设施：
>
> - 一个 S3 存储桶，报告了原始数据
> - 一个 Athena 实例，带有用于查询数据的查询定义
> - 用于从 S3 存储桶读取原始数据的 Glue 爬行器

AWS Managed Services 中的成本优化

AWS Managed Services 每月都会在您的每月业务评估中向您提供详细的成本利用率和节省报告（MBRs）。

AMS 遵循一套标准的流程和机制来确定您的托管账户中的成本节约途径，并帮助您规划和推出变更以优化 AWS 支出。

> **Note**
>
> AMS 正在开发一段有助于成本优化的视频。第一步是为您提供一份包含成本优化最佳实践的 PDF 和 Excel 电子表格。要访问这些资源，请打开成本优化快速指南 ZIP 文件。

成本优化框架

AMS 采用三阶段方法来优化您的 AWS 成本：

1. 确定托管环境中的成本优化途径
2. 向您提交成本优化计划
3. 以可衡量的方式协助实现成本优化

确定托管环境中的成本优化途径

AMS 利用成本资源管理器和 Trusted Advisor 等 AWS 原生工具，同时利用架构优化、 EC2 实例和以 AWS 客户为中心的优化中的 20 多种成本节省模式，为您制定量身定制的成本节约建议。

一些优化建议包括以下内容。

架构优化建议：

- S3 存储类的最佳使用：Amazon S3 提供了一系列存储类别，以满足基于数据访问权限、弹性和成本的各种工作负载要求。基于工作负载需求的 S3 智能分层和 S3 存储类分析使您能够高效地管理 S3 成本。
- 使用缓存架构：在适用的情况下，利用缓存实例可以帮助您替换某些数据库实例，同时满足 IOPS 要求。
- EBS 升级节省开支：将 EBS 卷从 gp2 迁移到 gp3 可节省高达 20% 的成本，无论卷大小如何，您都可以利用可预测的 3,000 IOPS 基准性能和 125 MiB/s。

- 使用弹性： AWS 提供的自动缩放功能允许有效的资源利用率和成本优化的途径。根据需要定期审查和更新实例扩展策略，可以进一步节省成本。

EC2 以实例为重点的建议

- 调整实例大小：建议侧重于根据使用情况调整实例大小和优化配置。建议还包括使用 Amazon A EC2 uto Scaling 功能，在适用的情况下将 EC2 实例替换为 Amazon S3 上的静态网页内容等。 AWS Lambda
- 实例调度：使用 AMS 资源调度器根据时间表自动启动和停止实例有助于控制成本，特别是对于非工作时间未使用的非生产实例。
- 订阅储蓄计划：储蓄计划是节省 AWS 使用量的最简单方法。与按需定价相比，Instance Savings Plans 可为您的亚马逊 EC2 实例使用量节省高达 72% 的费用。 EC2 Amazon SageMaker AI Savings Plans 可为您的亚马逊 A SageMaker I 服务使用量节省高达 64% 的费用。AMS 会根据您的 AWS 资源使用情况提供相应的储蓄计划建议。
- 预留实例 (RI) 使用和消费指南：与按需定价相比，Amazon EC2 Reserved Instances (RI) 可提供大幅折扣（高达 75%），并且在特定可用区域中使用时会提供容量预留。
- 竞价型实例使用率：容错工作负载可以利用竞价型实例并将价格降低多达 90%。
- 空闲实例终止：识别并报告处于空闲状态或利用率低且可以终止的实例。

以账户为中心的推荐

- 账户清理：在账户层面，AMS 还会识别未使用的 EBS 卷、重复的 CloudTrail 跟踪、带有未使用资源的空账户等，并提供清理建议。
- SLA 建议：此外，AMS 会定期审查您的高级版和高级版账户，并建议为这些账户选择正确的 SLA 级别。
- AMS 自动化优化：AMS 不断优化用于提供 AMS 服务的 AMS 自动化和基础设施。

向客户演示并协助规划

AMS每月与主要的客户利益相关者进行业务审查 (MBRs)，并介绍已确定的成本节约途径、机制和建议以及潜在的成本节约。我们将进一步与您合作，计划所需的更改。

协助实施建议并衡量成本影响

AMS 有助于实现和衡量成本影响和优化变更。

您可以评估所建议更改的应用程序影响、风险和成功标准，并通过 AMS 控制台提出相应的更改请求 (RFCs)。AMS 与您合作，在您的托管账户中实施与成本优化相关的变更。AMS衡量成本影响，并在月度业务评估中包括实现的节省（MBRs）。

成本优化责任矩阵

AMS 成本优化方面的职责。

成本优化 RACI

活动	Customer	AMS
编制节省成本的建议并准备报告	我	R
提交成本节约报告	C	R
与成本节约相关的计划变更	R	C
评估变更的影响和风险	R	C
RFCs 为实施变更筹款	R	C
审查 RFCs 并实施变更	C	R
测试应用程序并验证变更实施	R	C

活动	Customer	AMS
衡量变更后的成本影响并提交给客户	我	R

AWS Managed Services 中的服务时间

功能	AMS 高级版
	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
监控和提醒	全天候
自动申请变更 (RFC)	全天候
非自动变更请求 (RFC)	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

在 AWS Managed Services 中获取帮助

AMS 全年 365 天、每周 7 天、每天 24 小时为您提供事件管理、服务请求管理和变更管理方面的支持（根据适用于该账户的 AMS 服务等级协议）。

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 控制台并提交事件报告。有关详细信息，请参阅报告事件。有关 AMS 事件管理的一般信息，请参阅事件响应。

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。有关详细信息，请参阅创建服务请求。有关 AMS 服务请求的一般信息，请参阅服务请求管理。

更改管理模式

AWS Managed Services (AMS) 使用变更管理模式对 AMS Advanced 中的更改进行防护。变更管理模式可帮助您保持环境的高运营标准，并控制风险和防止不利影响。AMS Advanced 有不同的模式，可提供不同级别的控制和风险。除客户管理模式外，所有模式均由 AMS 管理。以下是可用的变更管理模式：

- RFC 模式（前身为标准 CM 模式）：提供 “更改请求” (RFC) 系统和 AMS 自定义更改类型 () CTs
- 直接更改模式：与 RFC 模式相同，还可使用 AWS APIs 和控制台创建 AMS 管理的资源
- AMS 上的 AWS Service Catalog：与 “直接更改” 模式类似，但不是使用 AMS 变更管理系统 (RFCs)，而是使用 S AWS ervice Catalog 来创建由 AMS 管理的资源。
- 开发者模式：与 Direct Change 模式相同，只有您使用 AWS APIs 和控制台创建的资源不受 AMS 管理——您负责管理这些资源
- 自助服务配置 (SSP) 模式：与开发者模式相同，唯一的不同是无法访问 AMS 变更管理系统（否 RFCs）
- 客户管理模式：AMS 为您提供多账户 landing zone landing zone，但所有资源管理均由您负责

AWS Managed Services (AMS) 变更管理系统使用变更管理 (CM) API，为多账户着陆区 (MALZRFCs) 和单账户着陆区 (SALZ) 账户提供创建和管理变更请求 () 的操作。

变更请求 (RFC) 是您或 AMS 通过 AMS 接口创建的对托管环境进行更改的请求，包括特定操作的更改类型 (CT) ID。

AMS 变更管理 (CM) API 提供用于创建和管理变更请求 (RFCs) 的操作。您可以创建、更新、提交、批准、拒绝和取消 RFCs。AMS 运营商可以创建、更新、提交、批准、拒绝、取消和标记 RFCs 为已关闭。

有关不得在标签或其他名称中使用的 AMS 保留前缀的列表，请参阅保留前缀。

有关每种变更类型的信息，包括架构和示例，请参阅 AMS 变更类型参考。

> **Note**
>
> 所有变更管理 API 调用都记录在 AWS 中 CloudTrail。有关更多信息，请参阅访问您的日志。

模式概述

根据您想要的灵活性和规范性监管组合，使用这些信息来帮助您选择合适的 AWS Managed Services (AMS) 模式来托管应用程序，以实现业务成果。

此信息的目标受众是：

- 客户团队负责其 landing zone 的策略和治理。这些信息将帮助该团队为AMS管理的着陆区奠定基础，以及他们希望向内部和外部客户提供的AMS模式。
- 负责将其应用程序迁移到 AMS 的企业和应用程序所有者。这些信息将有助于规划应用程序迁移，并为 migrate/host 其应用程序提供相应的 AMS 模式。请注意，在软件开发生命周期 (SDLC) 生命周期的不同阶段，同一应用程序可以在多个 AMS 模式下托管。
- AMS 合作伙伴的任务是指导客户选择构建和迁移到 AMS 的不同选项。

这些信息在设置 AMS 托管平台的基础阶段最有用，当你从云采用之旅的基础阶段过渡到迁移阶段时，刚刚完成向 AMS 的入职并专注于应用程序治理和运营。

AMS 中的模式和账户类型

AWS Managed Services (AMS) 模式可以定义为在每种模式的特定管理框架下与 AMS 服务进行交互的方式。记录了着陆区的区别、多账户着陆区（MALZ）和单账户着陆区（SALZ）。

> **Note**
>
> 有关应用程序部署和选择正确的 AMS 模式的详细信息，请参阅 AMS 模式和应用程序或工作负载。
> 有关不同模式的真实用例，请参阅 AMS 模式的真实世界用例

下表描述了每个 AMS 服务的模式。

AMS 功能	RFC 模式（以前是标准 CM 模式）/OOD *	直接更改模式	AWS Service Catalog	自助服务配置/开发者模式	客户管理
着陆区配置	MALZ 和 SALZ	MALZ 和 SALZ		MALZ 和 SALZ	

AMS 功能	RFC 模式（以前是标准 CM 模式）/OOD *	直接更改模式	AWS Service Catalog	自助服务配置/开发者模式	客户管理
变更管理	变更计划、查看手动变更和变更记录	与 RFC 模式相同，适用于高风险更改，例如 IAM 或安全组	无		
记录、监控、防护和事件管理	是（支持的资源）			否	
连续性管理	是（支持的资源）			不适用/否	否
安全管理	实例级安全控制和账户级别控制			账户级别控制	AWS 组织级别控制
补丁管理	是			不适用/否	否
事件和问题管理	AMS 支持的资源的响应和解决方案 SLA			对由此产生的资源做出响应 SLA	否
报告	是			否	
服务请求管理	是			仅限 Support 请求	否

* Operations On Demand (OOD) 为使用 RFC 模式的客户提供了通过专用资源管理变更的服务。有关更多详细信息，请参阅按需运营产品目录，并咨询您的云服务交付经理 (CSDM)。

> **Note**
>
> AMS 中的自助服务配置模式而且两者AMS 高级开发者模式似乎都适合具有植根于原生 AWS 服务的复杂架构的应用程序。在设计工作负载时，您需要根据业务环境在卓越运营和敏捷性之

间进行权衡。这是考虑为应用程序选择 SSP 模式或开发者模式的好方法。选择也可能根据应用程序的 SDLC 阶段而变化。例如：当应用程序已做好生产准备时，SSP 模式可能更合适，因为该模式下的 AMS 护栏更加严格。防护措施以预防性控制的形式强制执行，例如基于 RFC 的 IAM 更新和 SCPs 应用程序 OU 级别的变更控制。这些业务决策可以推动您的工程优先事务。您可以进行优化，以提高处于 “预生产” 阶段的应用程序所有者的灵活性，但会牺牲治理和运营支持。

MALZ 架构和相关的 AMS 模式

AMS 多账户 landing zone (MALZ) 允许您选择在默认组织单位 (OU) 下自动配置应用程序帐户（或资源帐户）：客户管理的 OU、托管 OU 或开发 OU。在每个账户下创建的应用程序账户中配置的基础架构受这些 OUs 基础 OUs架构提供的特定 AMS 模式的约束。通常在同一个应用程序帐户中混合使用两种或多种模式。例如：RFC 模式和 SSP 模式可以共存于 AMS 托管账户中，该账户托管管管道架构，包括用于触发函数的 API Gateway 和 Lambda EC2，以及用于摄取和编排的 S3 和 SQS。在这种情况下，SSP 模式将适用于 Lambda 和 API Gateway。

图 1 显示了 AMS OUs 中如何通过 “基础” 提供不同的模式。在 AMS 中申请新的应用程序账户时，必须为该账户选择 OU。

MALZ 架构和相关的 AMS 模式

AMS 利用 OUs 基于 AWS 最佳实践的基础知识，使用服务控制策略 () SCPs 对账户进行逻辑管理。这是在每个 AMS 模式下强制执行治理框架的一种方式。应用于基础的任何治理和安全护栏（以形式 SCPs）OUs 也会自动应用于基础。 custom/child OUs SCPs 可以要求为孩子提供额外服务 OUs。重要的是要明白，应用程序帐户与模式不同。模式适用于在账户中配置的基础设施，并定义了 AMS 和客户之间的运营责任。

图 1：MALZ 架构和相关的 AMS 模式

> **Note**
>
> “限制性” 意味着您可以为这些策略申请自定义策略 OUs，这些策略由AMS批准，以确保它们不会干扰AMS提供卓越运营的能力。 case-by-case有关 AMS 护栏的详细列表，请参阅用户指南中的 AMS Guardrail s。

AMS 模式和应用程序或工作负载

在选择正确的模式时，请考虑应用程序的运营和管理要求，方法是申请新的应用程序帐户或将应用程序托管在现有应用程序帐户中。为每个应用程序或工作负载选择适当的 AMS 模式取决于以下因素：

- 环境将提供的 SDLC 生命周期功能类型（例如，包含未经审核更改的沙箱、具有一些频繁更改的 UAT、更改最少且受到严格监管的生产）
- 所需的治理政策（通过 SCPs OU 级别强制执行）
- 运营模式（如果您想承担运营责任或想将其外包给AMS）
- 预期的业务成果，例如在云端运营的时间和运营成本。

> **Note**
>
> 有关每个 AMS 服务的模式类型的描述，请参阅 AMS 中的模式和账户类型。
> 有关不同模式的真实用例，请参阅 AMS 模式的真实世界用例

下表概述了应用程序所有者在决定最合适的 AMS 模式时需要考虑的关键因素。应用程序所有者应在应用程序迁移之前加入评估阶段，以充分了解哪种模式适用于他们的特定应用程序。示例：对于基于云原生服务或无服务器架构的应用程序，最好的选择可能是在开发人员模式下开始构建和迭代，然后使用 AMS Managed — SSP 模式部署最终的基础设施即代码。在这种情况下，可能需要进行轻度重构，以确保为自动部署创建的任何 CloudFormation 模板都符合 AMS 制定的采集指南。此外，任何 IAM 权限都需要获得 AMS Security 的批准，以确保它们遵循最低权限模式。

为托管应用程序而选择的 AMS 模式可以帮助您朝着所需的云运营模式进行构建。

> **Note**
>
> 根据为托管应用程序而选择的不同 AMS 模式，单个 AMS 托管着陆区中可以存在多个云运营模式。

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
运营准备就绪						

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
记录、监控和事件管理	AMS 负责所有托管基础架构			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	客户负责
连续性管理	AMS 负责执行客户选择的备份计划			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
实例级访问管理	AMS 通过本地域的单向 AD 信任进行管理。需要托管基础设施才能加入 AMS 域			不适用	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
安全管理和账户级别访问管理	AMS 对所有托管账户负责			AMS 负责所有托管账户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
补丁管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
变更管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
资源调配管理	针对 AMS 中提供的配置选项进行了规范和标准化	按照 AMS 规范性标准，可以灵活地直接使用适用于 AWS Service Catalog 的 AWS 服务 API	按照 AMS 规范性标准灵活地直接使用 AWS 服务 API	可以灵活地直接使用 AWS 服务 APIs 提供 SSP 服务	可以灵活地直接使用 AWS 服务 API 进行配置	
事件管理和审计	AMS 负责所有托管账户				负责使用开发者 IAM 角色在 AMS 变更管理系统之外配置资源的客户	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
GuardRails 以及共享基础架构（网络）和安全框架	利用 AMS 核心账户的规范性和标准化					灵活定制利用 AMS 核心账户
应用程序就绪						
应用程序重构	需要轻量化重构				需要轻量级重构（如果使用 AMS 标准 CM 进行配置）	无需重构
对 AWS 服务的支持	仅限于 AMS 支持的内容					不限
业务注意事项						
是时候做好运营准备了	三到六个月			6 个月以上，具体取决于客户的应用程序操作能力		6-18 个月视客户基础架构和应用程序操作能力而定
成本	$$$$			$$$	$$	$

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
应用示例	具有 3 层堆栈的 Web 服务器、符合合规性和监管要求的应用程序			使用 API Gateway 的 Web 服务器、利用 ECS/EKS 的容器化应用程序	对使用 Lambda、Glue、Athena 等的数据湖应用程序进行迭代/优化	accounts/ applications 像沙盒一样去中心化、第三方托管的应用程序

* Operations On Demand (OOD) 为使用标准 CM 模式的客户提供了通过专用资源管理管理其变更的服务。有关更多详细信息，请参阅按需运营产品目录，并咨询您的云服务交付经理 (CSDM)。

> **Note**
>
> SSP 模式和开发者模式之间的价格比较假设预配置了相同的 AWS 服务。

将 AMS 模式与业务和 IT 目标进行比较

如图所示，如果您正在为应用程序寻找高度可控和标准化的监管模式，那么 AMS 管理的标准变更、AWS Service Catalog 或直接变更模式最为合适。如果您需要以应用程序创新为重点的定制治理模型，而无需做好运营准备，请选择客户管理模式。在 Customer Managed 模式下，您可能需要更长的时间才能运行应用程序，因为您有责任建立人员、流程和工具来支持操作功能，例如事件管理、配置管理、配置管理、安全管理、补丁管理等。

AMS 模式的真实用例

检查这些内容以帮助确定如何使用 AMS 模式。

- 用例 1，企业必须通过时间敏感的数据中心退出来降低成本：具有引人注目的业务事件（例如数据中心退出）的企业有兴趣在云上重新托管其本地应用程序。大多数本地库存都包含混合操作系统版本的 Windows 和 Linux 服务器。在这样做的过程中，客户还希望利用迁移到云端所带来的成本节约，并改善其应用程序的技术和安全状况。客户想要快速行动，但尚未具备内部云运营专业知识。客户必须

在重构之间找到平衡，在时间紧迫的情况下，过多的重构可能会带来风险。但是，通过一些重构，例如更新操作系统版本和优化数据库，应用程序可以实现更高的性能水平。在此示例中，客户可以选择 AMS 管理的 RFC 模式来重新托管其大部分应用程序。AMS 提供基础设施运营，同时还指导客户运营团队了解在云端安全运营的最佳实践。

AMS 管理的 AWS Service Catalog 和 AMS 管理的 Direct Change 模式为客户提供了额外的灵活性，同时实现了相同的业务成果和目标。此外，客户可以使用 AMS 按需运营 (OOD) 产品让专门的 AMS 运营工程师来优先执行变更请求 (RFCs)。

在将无差别的基础设施运营任务（修补、备份、账户管理等）转移给 AMS 的同时，客户可以继续专注于优化其应用程序，增强内部团队的云运营能力。AMS 每月向客户提供成本节约报告，并就资源优化提出建议。在此用例中，如果客户决定不进行重构的旧操作系统版本（如Windows 2003和2008）上托管了 end-of-life应用程序，则这些应用程序也可以迁移到 AMS 并托管在利用客户管理模式的帐户中。

- 用例 2，在安全 AMS 边界内使用 Lambda、Glue、Athena 构建数据湖：一家企业希望建立数据湖以满足 AMS 中多个应用程序的报告需求。客户希望使用 S3 存储桶来存储数据集，并使用 AWS Athena 来查询每个报告的数据集。S3 和 AWS Athena 将部署在单独的 AMS 托管账户中。使用 S3 的账户还有其他服务，例如 Glue、Lambda 和 Step Functions，可用于构建数据摄取管道。在这种情况下，Glue、Lambda、Athena 和 Step Functions 被视为自助配置 (SSP) 服务。客户还在账户中部署了一个充当临时 tooling/scripting 服务器的 EC2 实例。客户首先请求 AMS 在其 AMS 托管账户中启用 SSP 服务。一旦该角色加入客户的联合解决方案，AMS 就会为客户可以担任的每项服务配置一个 IAM 角色。为便于管理，客户还可以将各个 IAM 角色的策略合并到一个自定义角色中，从而无需在 AWS 服务之间切换角色。在账户中启用该角色后，客户就可以根据自己的要求配置服务。但是，客户必须使用 AMS 变更管理系统来申请额外权限，具体取决于他们的用例。

  例如，要访问 Glue Crawlers，Glue 需要额外的权限。还需要其他权限才能为 Lambda 创建事件源。客户将与 AMS 合作更新 IAM 角色，以允许 Athena 跨账户访问查询 S3 存储桶。还需要通过 AMS 变更管理更新服务角色或服务相关角色，让 Lambda 调用 Step Functions 服务，Glue 才能读取和写入所有 S3 存储桶。AMS 与客户合作，确保遵循最低权限访问模式，并且请求的 IAM 更改不会过于宽松，从而使环境面临不必要的风险。客户的数据湖团队花时间规划特定于客户架构的服务所需的所有 IAM 权限，并请求 AMS 启用这些权限。这是因为所有 IAM 更改都是手动处理的，并经过 AMS 安全团队的审查。应用程序部署计划中应考虑处理这些请求所需的时间。

  由于 SSP 服务已在账户中运行，因此客户可以通过 AMS 事件管理和服务请求请求支持和报告问题。但是，AMS 不会主动监控 Lambda 的性能和并发指标，也不会主动监控 Glue 的作业指标。客户有责任确保为 SSP 服务启用适当的日志记录和监控。账户中的 EC2 实例和 S3 存储桶完全由 AMS 管理。

- 用例 3，在 AMS 中快速灵活地设置 CICD 部署管道：一位客户希望建立一个基于 Jenkins 的 CICD 管道，以便将代码管道部署到 AMS 中的所有应用程序帐户。客户可能会发现最适合在 AMS 管理的 Direct Change 模式 (DCM) 或 AMS 管理的开发者模式下托管此 CICD 管道，因为它使他们能够灵活地设置 Jenkins 服务器，开启所需的自定义配置 EC2，拥有所需的 IAM 访问权限 CloudFormation 和托管工件存储库的 S3 存储桶。虽然这也可以在 AMS 管理的 RFC 模式下完成，但客户团队需要为 IAM 角色创建多个手册 RFCs ，以迭代许可程度最低的已批准权限集，这些权限由 AMS 手动审核。DCM 允许客户在 AWS 上实现运营目标，同时在使用 AMS 管理的 RFC 模式时，无需为 IAM 角色创建多个手册 RFCs 来迭代许可性最低的已批准权限集，这些权限由 AMS 手动审核。要提高 AMS 流程和工具，客户需要时间和教育。使用开发人员模式，客户可以从 “开发人员角色” 开始，使用原生 AWS 配置基础设施 APIs。设置此管道的最快、最灵活的方法是使用 AMS 托管开发者模式。开发人员模式提供了最快、最简单的方法，同时影响了操作集成，而 DCM 不那么灵活，但提供的操作支持级别与 RFC 模式相同。
- 用例 4，AMS 基金会内部的定制运营模式：客户正在考虑最后期限驱动的数据中心退出，他们的一个企业应用程序完全由第三方 MSP 管理，包括应用程序运营和基础设施运营。假设客户没有时间在计划中重构此应用程序以使其可以由 AMS 运行，那么客户管理模式是一个合适的选择。客户可以利用 AMS 管理的着陆区的自动快速设置。他们可以利用集中式账户管理，通过集中式网络账户控制账户销售和连接。它还通过AMS Payer账户合并所有客户管理账户的费用，从而简化了他们的账单。客户可以灵活地设置定制的访问管理模式，将 MSP 与 AMS 托管账户使用的标准访问管理分开。这样，使用客户管理模式，他们可以设置 AMS 托管环境，同时满足腾出本地环境的业务需求。在这种情况下，如果客户还有要迁移到云端的基于Windows的应用程序，并选择将其迁移到客户管理的帐户，则客户负责创建云运营模式。这可能很复杂、昂贵且耗时，具体取决于客户转变传统 IT 流程和培训人员的能力。通过将此类工作负载 “转移并转移” 到 AMS 托管账户，并将基础设施运营转移给 AMS，客户可以节省时间和成本。

> **Note**
>
> 客户有时可能会觉得有必要在 RFC 或 SSP 模式的治理框架和开发者模式之间转移应用程序帐户。例如，作为初始迁移和轮班迁移的一部分，客户可能以 AMS 管理模式托管应用程序，但随着时间的推移，客户希望重写该应用程序以针对云原生 AWS 服务对其进行优化。他们可以将预生产账户的模式从 AMS 管理的 RFC 更改为 AMS 管理的开发者模式，从而为他们提供配置基础设施的灵活性和敏捷性。但是，一旦使用 “开发人员角色” 对基础设施配置进行了更改，就无法将相同的基础设施移回 AMS 管理的 RFC 模式。这是因为 AMS 无法保证在 AMS 变更管理系统之外配置的基础设施的运行。客户可能需要创建一个提供 AMS 管理的 RFC 模式的新应用程序账户，然后通过 CloudFormation 模板或自定义 AMIs 采集到 AMS 管理的账户中重新部署 “优化” 的基础架构配置。这是部署生产就绪配置的简洁方法。

部署后，该应用程序将处于规范性的 AMS 管理和运营之下。这同样适用于在客户管理模式和 AMS 管理模式之间切换模式。

RFC 模式

RFC 模式是 AMS 高级运营计划客户的默认模式。它包括一个变更管理系统，其中包含变更请求或，RFCs 以及用于请求对账户进行所需添加或更改的变更类型目录。此变更管理系统在限制谁可以更改您的帐户方面提供一定程度的安全性。

有关 AMS 高级更改类型的详细信息，请参阅什么是 AMS 更改类型？ 。

有关加入 AMS Advanced 的详细信息，请参阅 AWS Managed Services 入门简介。

有关更改类型示例演练，请参阅 “按分类划分的 AMS 高级更改类型参考变更类型” 部分中相关变更类型的 “其他信息” 部分。

> **Note**
>
> RFC 模式以前被称为 “变更管理模式” 或 “标准 CM 模式”。

主题

- 了解有关 RFCs
- 什么是变更类型？
- 对 AMS 中的 RFC 错误进行故障排除

了解有关 RFCs

变更请求或 RFCs以双重方式起作用。首先，RFC 本身需要一些参数。这些是 `CreateRfc` API 中的选项。其次，RFC 的操作需要参数（执行参数）。要了解这些`CreateRfc`选项，请参阅《AMS API 参考》的CreateRfc部分。这些选项通常显示在 “创建 RFC” 页面的 “其他配置” 区域中。

您可以使用 `CreateRfc` API、`aws amscm create-rfc` CLI 或使用 AMS 控制台创建 RFC 页面创建和提交 RFC。有关创建 RFC 的教程，请参阅创建 RFC。

主题

什么是 RFCs？

变更请求（RFC）是指您如何在 AMS 管理的环境中进行更改，或者让 AMS 代表您进行更改。要创建 RFC，您可以从 AMS 更改类型中进行选择，选择 RFC 参数（例如计划），然后使用 AMS 控制台或 API 命令CreateRfc提交请求。SubmitRfc

RFC 包含两个规范，一个用于 RFC 本身，另一个用于变更类型 (CT) 参数。在命令行中，您可以使用内联 RFC 命令或 JSON 格式的标准 CreateRfc 模板，该模板与您创建的 CT JSON 架构文件（基于 CT 参数）一起填写并提交。CT 名称是对 CT 的非正式描述。CSIO（类别、子类别、项目、操作）是对 CT 的更正式的描述。创建 RFC 时只需要指定 CT ID。

当更改成功完成（成功）或未成功（失败）时，AMS 会通知您。

> **Note**
>
> 有关排除 RFC 故障的信息，请参阅对 AMS 中的 RFC 错误进行故障排除。

下图描述了您提交的 RFC 的工作流程。

使用 AMS API/CLI 时进行身份验证

使用 AMS API/CLI 时，必须使用临时证书进行身份验证。要为联合用户申请临时安全证书，请使用 cal、 GetFederationTokenAssumeRole、AssumeRoleWithSAML 或 AssumeRoleWithWebIdentityAWS 安全令牌服务 (STS) APIs。

常见的选择是 SAML。设置完成后，您可以为所调用的每个操作添加一个参数。例如：`aws --profile saml amscm list-change-type-categories`。

SAML 2.0 配置文件的一个快捷方式是在每个 API/CLI 配置文件的开头设置配置文件变量`set AWS_DEFAULT_PROFILE=saml`（对于 Windows；对于 Linux 则是这样`export AWS_DEFAULT_PROFILE=saml`）。有关设置 CLI 环境变量的信息，请参阅配置 AWS 命令行界面，环境变量。

了解 RFC 安全评论

AWS Managed Services (AMS) 变更管理批准流程可确保我们对您的账户中所做的更改进行安全审查。

AMS 根据 AMS 技术标准评估所有变更请求 (RFCs)。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。在安全审查期间，AMS 会重点介绍相关风险，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 RFC。还对所有变化进行评估，以评估对AMS运营能力的不利影响。如果发现潜在的不利影响，则需要在AMS内部进行额外的审查和批准。

AMS 技术标准

AMS 技术标准定义了最低安全标准、配置和流程，以建立账户的基本安全性。AMS 和您都必须遵守这些标准。

任何可能因偏离技术标准而可能降低您账户安全状况的变更都要经过风险接受流程，AMS会强调相关风险，并由您的授权安全人员接受或拒绝。还要对所有这些变化进行评估，以评估是否会对AMS的账户运营能力产生任何不利影响，如果是，则需要在AMS内部进行额外的审查和批准。

RFC 客户安全风险管理 (CSRM) 流程

当您的组织中的某人请求更改您的托管环境时，AMS 会审查更改，以确定该请求是否会超出技术标准，从而恶化您账户的安全状况。如果请求确实降低了账户的安全状况，AMS 会将相关风险通知您的安全团队联系人并执行变更；或者，如果变更给环境带来了高或非常高的安全风险，AMS 将以风险接受的形式寻求您的安全团队联系人的明确批准（详见下文）。AMS 客户风险接受流程旨在：

- 确保清楚地识别风险并将其传达给正确的所有者

- 将已识别的环境风险降至最低
- 获得并记录了解贵组织风险状况的指定安全联系人的批准
- 减少已识别风险的持续运营开销

如何获得技术标准以及高风险或非常高的风险

我们已将 AMS 技术标准文档https://console.aws.amazon.com/artifact/作为报告提供给您参考。在提交变更申请 (RFC) 之前，请使用 AMS 技术标准文档，了解变更是否需要您的授权安全联系人接受风险。

使用默认值登录后，在 “报告” 选项卡搜索栏中搜索 “AWS Managed Services (AMS) 技术标准”，即可找到技术标准 AWS Artifact 报告AWSManagedServicesChangeManagementRole。

> **Note**
>
> 单账户 landing zone 中的 Customer_ ReadOnly _Role 可以访问 AMS 技术标准文档。在多账户 landing zone 中，安全管理员 AWSManagedServicesChangeManagementRole 使用和应用团队 AWSManagedServicesAdminRole 使用的登录区域可用于访问文档。如果您的团队使用自定义角色，请创建一个 Other | Other RFC 来请求访问权限，我们将更新指定的自定义角色。

了解 RFC 变更类型分类

您在提交 RFC 时使用的变更类型分为两大类：

- 部署：此分类用于创建资源。
- 管理：此分类用于更新或删除资源。管理类别还包含访问实例、加密或共享以及启动、停止 AMIs、重启或删除堆栈的更改类型。

了解 RFC 操作和活动状态

`RfcActionState`(API)/活动状态（控制台）可帮助您了解 RFC 上人为干预或操作的状态。主要用于手动 RFCs，`RfcActionState`可帮助您了解您或 AMS 运营部门何时需要采取行动，并帮助您了解 AMS 运营部门何时正在积极处理您的 RFC。这提高了 RFC 在其生命周期中所采取行动的透明度。

`RfcActionState`(API)/活动状态（控制台）定义：

- AwsOperatorAssigned: AWS 运营商正在积极处理您的 RFC。

- AwsActionPending：预计 AWS 会做出回应或采取行动。
- CustomerActionPending: 预计客户会做出回应或采取行动。
- NoActionPending：AWS 或客户均无需采取任何行动。
- NotApplicable：此状态不能由 AWS 运营商或客户设置，只能用于 RFCs 在此功能发布之前创建的状态。

RFC 操作状态会有所不同，具体取决于提交的变更类型是否需要人工审核以及是否将计划设置为 “尽快”。

- 在审核、批准和启动具有延迟计划的手动变更类型期间 RFC ActionState更改：
  - 在您提交手册、预定的 RFC 后，ActionState系统会自动更改AwsActionPending为，表示操作员需要审核和批准 RFC。
  - 当操作员开始积极审查您的 RFC 时，ActionState更改为。AwsOperatorAssigned
  - 当运营商批准您的 RFC 后，RFC 状态将更改为 “已计划”，并ActionState自动更改为。NoActionPending
  - 到达 RFC 的预定开始时间后，RFC 状态将更改为 InProgress，并ActionState自动更改为，表示AwsActionPending需要指派一名操作员来审查 RFC。
  - 当操作员开始主动运行 RFC 时，他们会将其更改ActionState为。AwsOperatorAssigned
  - 完成后，操作员将关闭 RFC。这会自动将更改ActionState为NoActionPending。

> **Important**
>
> - 您无法设置操作状态。它们要么根据 RFC 中的更改自动设置，要么由 AMS 操作员手动设置。
> - 如果您向 RFC 添加信件，则会自动设置为。ActionStateAwsActionPending
> - 创建 RFC 时，会ActionState自动设置为。NoActionPending
> - 提交 RFC 后，会ActionState自动设置为。AwsActionPending
> - 当 RFC 被拒绝、已取消或已完成且状态为 “成功” 或 “失败” 时，会自动重置ActionState为NoActionPending。
> - 自动和手动操作状态均启用 RFCs，但手动操作状态最重要， RFCs 因为这些类型的操作 RFCs 通常需要通信。

查看 RFC 操作状态用例示例

用例：手动 RFC 流程的可见性

- 提交手动 RFC 后，RFC 操作状态会自动更改为AwsActionPending，表示操作员需要审核和批准 RFC。当操作员开始积极查看您的 RFC 时，RFC 操作状态将更改为。AwsOperatorAssigned
- 以手动 RFC 为例，该手动 RFC 已获得批准并已安排好开始运行。一旦 RFC 状态更改为InProgress，RFC 操作状态就会自动更改为。AwsActionPendingAwsOperatorAssigned当操作员开始积极运行 RFC 时，它将再次更改为。
- 手动 RFC 完成后（以“成功”或“失败”的形式关闭），RFC 操作状态将NoActionPending更改为，表示客户或操作员无需采取进一步的行动。

用例：RFC 通信

- 如果是手动 RFCPending Approval，AMS 操作员可能需要您提供更多信息。运营商将向 RFC 发布信件，并将 RFC 操作状态更改为。CustomerActionPending当您通过添加新的 RFC 通信来回应时，RFC 操作状态会自动更改为。AwsActionPending
- 当自动或手动 RFC 失败时，您可以在 RFC 详细信息中添加对应信息，询问 AMS 操作员 RFC 失败的原因。添加信件后，RFC 操作状态将自动设置为。AwsActionPending当 AMS 操作员拿起 RFC 查看您的信件时，RFC 操作状态将更改为。AwsOperatorAssigned当操作员通过添加新的 RFC 通信来做出回应时，RFC 操作状态可以设置为CustomerActionPending，表示预期的客户还有另一个回应，或者设置为NoActionPending，表示不需要或预计客户不需要或预计不需要任何回应。

了解 RFC 状态码

RFC 状态代码可帮助您跟踪您的请求。在 RFC 运行期间，您可以在 CLI 输出中观察这些状态代码，也可以通过刷新控制台中的 RFC 列表页面来观察这些状态代码。

您还可以在该 RFC 的详细信息页面上查看 RFC 的代码，可能如下所示：

你可能会在列表中看到一个你没有提交的 RFC。当 AMS 操作员使用仅限内部的 CT 时，他们会在 RFC 中提交并显示在您的 RFC 列表中。有关更多信息，请参阅 仅限内部的变更类型。

> **Important**
>
> 您可以请求 RFC 状态变更通知。有关详细信息，请参阅 RFC 状态更改通知。

RFC 状态码

成功	Failure
编辑：RFC 已创建但尚未提交 PendingApproval /已提交：RFC 已提交，系统正在确定是否需要批准，并在需要时获得批准 AWS 批准/客户批准：RFC 已获得批准。自动 RFCs 由 AWS 批准，手动 RFCs 由操作员批准，有时还需要客户批准 已计划：RFC 已通过语法和要求检查并计划运行 InProgress: RFC 正在运行， RFCs 请注意，配置多个资源或资源长期运行 UserData，需要更长的时间才能运行 已执行：RFC 已运行 成功/成功：RFC 已成功完成	已拒绝： RFCs 通常因为验证失败而被拒绝；例如，指定了不可用的资源，即子网 已取消： RFCs 之所以取消，通常是因为它们在配置的开始时间过去之前未通过验证 失败：RFC 已失败；有关失败原因，请参阅输出 StatusReason 中的，AMS 操作会自动创建故障单并根据需要与您沟通

> **Note**
>
> 取消或拒绝 RFCs 可使用重新提交 UpdateRfc；另更新 RFCs请参阅。

如果 RFC 通过了所有必要条件（例如，指定了所有必需的参数），则状态将更改为`PendingApproval`（即使是自动也 CTs 需要批准，如果语法和参数检查通过，则会自动进行审批）。如果未通过，则状态将更改为`Rejected`。`StatusReason`提供有关拒绝的信息；`ExecutionOutput`字段提供有关批准和完成的信息。错误代码包括：

- InvalidRfcStateException: RFC 的状态不允许执行被调用的操作。例如，如果 RFC 已变为 “已提交” 状态，则无法再对其进行修改。
- InvalidRfcScheduleException: StartTime EndTime、或 TimeoutInMinutes 参数被破坏。
- InternalServerError: 系统遇到了问题。
- InvalidArgumentException：参数指定不正确；例如，使用了不可接受的值。
- ResourceNotFoundException: 找不到堆栈 ID 等值。

如果计划请求的开始和结束时间（也称为变更运行窗口）发生在更改获得批准之前，RFC 状态将`Canceled`更改为。如果更改获得批准，则 RFC 状态将`Scheduled`更改为。ASAP 的变更运行窗口 RFCs 是提交时间加上 CT 的`ExpectedExecutionDuration`值。

在变更运行窗口到来之前的任何时候，都可以修改或取消计划变更（`RequestedStartTime`在 CLI 中使用提交）。如果计划更改被修改，则必须重新提交。

当更改开始时间（计划或尽快）到来且批准完成后，状态将更改为，无法进行任何修改。`InProgress`如果更改在指定的变更运行窗口内完成，则状态将更改为`Success`。如果更改的任何部分失败，或者变更运行窗口结束时更改仍在进行中，则状态将更改为`Failure`。

> **Note**
>
> 在`InProgress`、`Success`或`Failure`更改状态期间，无法修改或取消 RFC。

下图说明了从 CreaterFC 调用到解析的 RFC 状态。

了解 RFC 更新 CTs 和 CloudFormation 模板偏差检测

在 AMS 中配置的资源使用修改后的 CloudFormation 模板。如果资源的参数通过服务的 AWS 管理控制台直接更改，则该资源的 CloudFormation 创建记录将不同步。如果发生这种情况，并且您尝试使用 AMS 更新更改类型来更新 AMS 中的资源，则 AMS 将引用原始资源配置并可能重置更改的参数。此重置可能会造成损害，因此，如果检测到任何额外的 AMS 配置更改，AMS 将不允许 RFCs 更新更改类型。

要查看更新更改类型的列表，请使用控制台筛选器。

漂移补救 FAQs

有关 AMS 漂移补救的问题和答案。您可以使用两种更改类型来启动偏差补救，一种是执行模式=手动或 “需要审查”，另一种是执行模式=自动。

支持漂移修复的资源 (ct-3kinq0u4l33zf)

这些是漂移修复更改类型 (ct-3kinq0u4l33zf) 支持的资源。 要修复任何资源，请改用 “需要审查” (ct-34sxfo53yuzah) 更改类型。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

漂移补救更改类型

有关使用 AMS 漂移补救变更类型的问题与解答。

有关漂移修复功能支持的资源列表，请参阅支持漂移修复的资源 (ct-3kinq0u4l33zf)。

> **Important**
>
> 漂移修复会修改堆栈模板 and/or 参数，并且必须更新您的本地模板存储库或任何正在更新这些堆栈的自动化以使用最新的堆栈模板和参数。在不进行同步的情况下使用旧的模板 and/or 参数可能会对底层资源造成破坏性更改。

无需审查、自动化 CT（ct-3kinq0u4l33zf）仅支持每个 RFC 修复 10 个资源。要在 10 个批次中修复剩余的资源，请创建新的资源， RFCs 直到所有资源都已修复。

我应该使用哪种漂移补救更改类型？

我们建议在以下情况下使用无需复查的自动 CT（ct-3kinq0u4l33zf）：

- 您尝试使用自动 CT 对现有堆栈资源执行更新，但 RFC 按堆栈原样被拒绝。`DRIFTED`
- 你过去使用过 Update CT，但由于堆栈已漂移，它失败了。您无需再次尝试更新，可以改用所需的审核、手动、CT。

我们建议仅在漂移补救不支持漂移资源类型（无需审查）、自动、CT（ct-3kinq0u4l33zf）或漂移补救无需审查、自动化、CT（ct-3kinq0u4l33zf）或漂移补救无需审查、自动化、CT 失败时才使用所需的审查（ct-34sxfo53yuzah）。

修复期间对堆栈进行了哪些更改？

修复需要更新堆栈模板 and/or 参数，具体取决于偏移的属性。修复还会在修复期间更新堆栈的堆栈策略，并在修复完成后将堆栈策略恢复到之前的值。

我们怎样才能看到对堆栈模板 and/or 参数所做的更改？

在对 RFC 的回复中，提供了包含以下信息的变更摘要：

- `ChangeSummaryJson`：包含作为偏差补救一部分的堆栈模板 and/or 参数的更改摘要。补救分多个阶段执行。此变更摘要包含各个阶段的更改。如果修复成功，请检查最后一个阶段的更改。有关按顺序执行的阶段，请参阅 ExecutionPlan JSON 中的。例如，存在时 RestoreReferences 段总是在最后执行，并且包含用于修复后更改的 JSON。如果在 DryRun 模式下运行修复，则这些更改都不会应用于堆栈。
- `PreRemediationStackTemplateAndConfigurationJson`：包含在 CloudFormation 堆栈上触发修复 StackPolicyBody 之前的堆栈配置快照，包括模板、参数、输出。

执行修复后我需要做什么？

> **Important**
>
> 您需要使用 RFC 摘要中提供的最新模板和参数来更新本地模板存储库或任何将更新已修复堆栈的自动化。这样做非常重要，因为使用旧的模板 and/or 参数可能会对堆栈资源造成进一步的破坏性更改。

在此补救期间，我的应用程序会受到影响吗？

补救是一个离线过程，只能在 CloudFormation 堆栈配置上执行。不对底层资源执行任何更新。

修复后，我能否继续使用管理 | 其他 | 其他 RFCs 来更新资源？

我们建议您始终使用可用的自动更新来更新堆栈资源 CTs。如果可用的更新 CTs 不支持您的用例，请使用管理 | 其他 | 其他请求。

修复是否会在堆栈中创建任何新资源？

修复不会在堆栈中创建任何新资源。但是，修复会创建新的输出并更新堆栈模板元数据部分以存储修复摘要供您参考。

补救总是成功吗？

修复需要仔细分析和验证模板配置，以确定是否可以执行。在这些验证失败的情况下，修复过程将停止，并且不会对堆栈模板或参数进行任何更改。此外，只能对支持的资源类型执行修复。

如果修复不成功，如何更新堆栈资源？

你可以使用 “管理 | 其他 | 其他 | 更新 CT” (ct-0xdawir96cy7k) 来请求更改。AMS 对此类情况进行监控，并努力改进补救解决方案。

我能否修复同时具有受支持和不支持的资源类型的堆栈？

是。但是，只有在堆栈中发现支持的资源类型存在漂移时，才会执行修复。如果有任何不受支持的资源类型为 DRIFTED，则修复不会继续。

我能否请求对通过非 CFN Ingest 创建的堆栈进行补救？ CTs

是。无论用于创建堆栈的更改类型如何，都可以对堆栈执行修复。

我能否知道在补救之前会对堆栈执行哪些更改？

是。两种更改类型都提供了一个DryRun选项，您可以使用该选项来请求在堆栈修复后将要执行的更改。但是，最终的补救更改可能会有所不同，具体取决于补救时堆栈上存在的偏差。

日程安排 RFCs

“日程安排” 功能允许您选择的开始时间 RFCs。“日程安排” 功能中提供了以下选项：

- 尽快执行此更改：AMS 一经批准，就会立即运行 RFC。大多数 CTs 都是自动批准的。如果不希望 RFC 在特定时间启动，请使用此选项。

- 安排此更改：设置 RFC 运行的日期、时间和时区。对于自动变更类型，最佳做法是在计划提交 RFC 后至少 10 分钟后申请开始时间。要查看必需的变更类型，您需要在计划提交 RFC 后至少 24 小时内申请开始时间。如果 RFC 在配置的开始时间之前未获得批准，则 RFC 将被拒绝。

设置 RFC 时间表

要安排 RFC，请使用以下方法之一：

尽快执行此更改：

- 主机：什么都不做。这使用默认的 RFC 时间表。
- API 或 CLI：删除 “创建 RFC” 操作中的`RequestedStartTime`和`RequestedEndTime`选项。

如果在提交后的三十天内未获得批准，ASAP “需要审核” RFCs 将自动被拒绝。

安排此更改：

- 控制台：选择 “安排此更改” 单选按钮。将打开 “开始时间” 区域。手动输入日期或使用日历控件选择日期。输入以 ISO 8601 格式表示的 UTC 时间，然后使用下拉列表选择地点。默认情况下，AMS 使用 ISO 8601 格式 YYYYMMDDThhmmss Z 或:mm: ss YYYY-MM-DDThh z，这两种格式都被接受。

> **Note**
>
> 默认结束时间是从您输入的开始时间算起 4 小时。要将计划更改的结束时间设置为 4 小时以上，请使用 API 或 CLI 运行更改。

- API 或 CLI：在 “创建 RFC” 操作中提交`RequestedStartTime`和`RequestedEndTime`参数的值。传递配置`RequestedEndTime`并不能停止已经启动的自动更改类型的运行。对于 “需要审核” 的变更类型，如果在 AMS 运营研究仍在进行期间达到，并且您正在与 AMS 沟通，则可以申请延期，或者可能会要求您重新提交 RFC。`RequestedEndTime`

> **Tip**
>
> 有关世界标准时间读数的示例，请参阅 Time-is 网站上的 UTC。下午 2 点 20 分 date/time 值为 2016-12-05 的 ISO 8601 格式示例：2016-12-05T14：20:00 Z 或 20161205T142000Z。

如果你提供...

- 只有 aRequestedStartTime，RFC 被视为已定时RequestedEndTime的，并使用该ExecutionDurationInMinutes值填充。
- 只有 aRequestedEndTime，我们扔一个 InvalidArgumentException。
- 两者RequestedStartTime兼而有之RequestedEndTime，我们RequestedEndTime用指定的开始时间加上该ExecutionDurationInMinutes值覆盖。
- RequestedStartTime也不是RequestedEndTime，我们将这些值保留为空，并且 RFC 被视为 ASAP RFC。

> **Note**
>
> 对于所有已安排的时间 RFCs，将未指定的结束时间写成指定的时间RequestedStartTime加上已提交的更改类型的ExpectedExecutionDurationInMinutes属性。例如，如果ExpectedExecutionDurationInMinutes为 “60”（分钟），指定RequestedStartTime为2016-12-05T14:20:00Z（2016 年 12 月 5 日凌晨 4:20），则实际结束时间将设置为 2016 年 12 月 5 日凌晨 5:20。要查找ExpectedExecutionDurationInMinutes特定更改类型的，请运行以下命令：
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

使用 RFC 优先级选项

使用execution mode = manual变更类型中的 “优先级” 选项提醒 AMS 运营部门注意请求的紧迫性。

优先级选项位于execution mode = manual：

将手动 RFC 的优先级指定为 “高”、“中” 或 “低”。 RFCs 在 RFC 服务级别目标 (SLOs) 及其提交时间的前提下，在 RFCs 归类为 “中” 之前要经过审核和批准。 RFCs 如果指定了低优先级或未指定优先级，则按提交顺序进行处理。

批准或拒绝 RFCs

RFCs 提交时需要批准（手动） CTs 必须获得您或 AMS 的批准。系统会自动处理预先批准 CTs 。有关更多信息，请参阅 CT 批准要求。

> **Note**
>
> 使用 “需要审核” 时 CTs，AMS 建议您使用 “尽快安排” 选项（在控制台中选择 “尽快”，在 AP I/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

如果 AMS 成功提交了需要批准的 RFC，则必须得到您的明确批准。或者，如果您提交需要批准的 RFC，则必须获得 AMS 的批准。如果您需要批准 AMS 提交的 RFC，则会向您发送电子邮件或其他预先确定的通信，请求批准。通信包括 RFC ID。发送通信后，请执行以下任一操作：

- 控制台批准或拒绝：使用 RFC 详细信息页面查看相关 RFC：

- API/CLI 批准：将更改ApproveRfc标记为已批准。如果所有者和操作者都需要，则必须同时采取行动。以下是 CLI 批准命令的示例。在以下示例中，将 RFC_ID 替换为相应的 RFC ID。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI 拒绝：将更改RejectRfc标记为已拒绝。以下是 CLI 拒绝命令的示例。在以下示例中，将 RFC_ID 替换为相应的 RFC ID。

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

申请 RFC 限制运行期

以前称为封锁日，您可以请求限制某些时间段。在这段时间内无法进行任何更改。

要设置限制运行时段，请使用 UpdateRestrictedExecutionTimesAPI 操作并以 UTC 为单位设置特定的时间段。您指定的时间段会覆盖之前指定的任何时段。如果您在指定的受限运行时间内提交 RFC，则提交失败并显示错误 “RFC 计划无效”。您最多可以指定 200 个受限时间段。默认情况下，未设置限制期限。以下是请求命令示例（配置了 SAML 身份验证）：

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

您也可以通过运行 ListRestrictedExecutionTimesAPI 操作来查看当前 RestrictedExecutionTimes 设置。示例：

```
aws amscm  --profile saml list-restricted-execution-times
```

如果您想在指定的受限执行时间内提交 RFC，请添加值为的 OverrideRestrictedTimeRanges，然后像往常一样提交 RFC。RestrictedExecutionTimesOverrideId最佳做法是仅将此方法用于关键或紧急 RFC。有关更多信息，请参阅的 API 参考SubmitRfc。

创建、克隆、更新、查找和取消 RFCs

以下示例将引导您完成各种 RFC 操作。

主题

- 创建 RFC
- 使用 AMS 控制台进行克隆 RFCs （ 重新创建 ）
- 更新 RFCs
- 查找 RFCs
- 取消 RFCs

创建 RFC

使用控制台创建 RFC

以下是 AMS 控制台中 RFC 创建流程的第一页，其中快速卡片已打开，浏览更改类型处于活动状态：

以下是 AMS 控制台中 RFC 创建流程的第一页，按类别选择处于活动状态：

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。

2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 创建 RFC

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何CreateRfc参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数（内联提供执行参数时使用转义引号）发出 create RFC 命令，然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：：

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

模板创建：

> **Note**
>
> 此创建 RFC 的示例使用了 Load Balancer (ELB) 堆栈更改类型。

1. 找到相关的 CT。以下命令在 CT 分类摘要中搜索项目名称中包含 “ELB” 的摘要，并以表格形式创建类别、项目、操作和 ChangeType ID 的输出（两者的子类别均为Advanced stack components）。

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ------------------------------------------------------------------------
   |                            CtSummaries                               |
   +------------+---------------------------+---------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   +------------+---------------------------+---------------------------+
   ```

2. 查找 CT 的最新版本：

   ChangeTypeIdandChangeTypeVersion：本演练的更改类型 ID 是ct-123h45t6uz7jl（创建 ELB），要查找最新版本，请运行以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. 了解选项和要求。以下命令将架构输出到名为 CreateElbParams .json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 修改并保存执行参数 JSON 文件。此示例将文件命名为 CreateElbParams .json。

   对于配置 CT，包含 StackTemplateId 在架构中，并且必须在执行参数中提交。

   对于 TimeoutInMinutes，在 RFC 失败之前允许创建堆栈多少分钟，此设置不会延迟 RFC 的执行，但您必须留出足够的时间（例如，不要指定 “5”）。对于 CTs 长时间运行 UserData：创建 EC2 和创建 ASG，有效值为 “60” 到 “360”。我们建议所有其他配置 CTs的最大允许值为 “60”。

   提供您要在其中创建堆栈的 VPC 的 ID；您可以使用 CLI 命令获取 VPC ID aws amsskms list-vpc-summaries。

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. 将 RFC JSON 模板输出到当前文件夹中名为 CreateElbRfc .json 的文件中：

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. 修改并保存 CreateElbRfc .json 文件。由于您在单独的文件中创建了执行参数，因此请删除该ExecutionParameters行。例如，你可以用这样的东西替换内容：

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. 创建 RFC。以下命令指定执行参数文件和 RFC 模板文件：

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

> **Note**
>
> 您可以使用 AMS 创建 RFC API/CLI ，而无需创建 RFC JSON 文件或 CT 执行参数 JSON 文件。为此，您可以使用`create-rfc`命令并将所需的 RFC 和执行参数添加到命令中，这称为“Inline Create”。请注意，所有配置 CTs 都在`execution-parameters`区块中包含一个包含资源参数的`Parameters`数组。参数必须使用反斜杠 (\) 对引号进行转义。
>
> 另一种记录在案的创建 RFC 的方法叫做“模板创建”。在这里，您可以为 RFC 参数创建一个 JSON 文件，为执行参数创建另一个 JSON 文件，然后使用`create-rfc`命令提交这两个文件。这些文件可以用作模板并在将来 RFCs重复使用。
>
> RFCs 使用模板创建时，您可以使用命令通过发出如下所示的命令来创建包含所需内容的 JSON 文件。这些命令使用显示的内容创建一个名为“parameters.json”的文件；你也可以使用这些命令来创建 RFC JSON 文件。

使用 AMS 控制台进行克隆 RFCs （重新创建）

您可以使用 AMS 控制台克隆现有的 RFC。

要使用 AMS 控制台克隆或重新创建 RFC，请执行以下步骤：

1. 找到相关的 RFC。在左侧导航栏中，单击RFCs。

   RFCs 仪表板打开。

2. 滚动浏览页面，直到找到要克隆的 RFC。使用 “筛选” 选项缩小列表范围。选择要克隆的 RFC。

   RFC 详细信息页面打开。

3. 单击 “创建副本”。

   将打开 “创建更改请求” 页面，所有选项的设置都与原始 RFC 中的设置相同。

4. 根据需要进行更改。要设置其他选项，请将 “基本” 选项更改为 “高级”。设置完所有选项后，选择提交。

   活动的 RFC 详细信息页面打开时会显示克隆的 RFC 的新 RFC ID，克隆的 RFC 将显示在 RFC 控制面板中。

更新 RFCs

您可以通过更新 RFC 然后提交或重新提交来重新提交已被拒绝或尚未提交的 RFC。请注意，大多数 RFCs 都被拒绝，因为指定的值在提交前`RequestedStartTime`已通过，或者指定的值 TimeoutInMinutes 不足以运行 RFC（由于 TimeoutInMinutes 不会延长成功的 RFC，因此对于长期运行的 Amazon EC2 或 Amazon A EC2 uto Scaling 组，我们建议始终将其设置为至少 “60”，最多设置为 “360”）。 UserData本节介绍如何使用`UpdateRfc`命令的 CLI 版本使用新的 RFC 参数更新 RFC，或者使用字符串化的 JSON 或更新的参数文件来更新 RFC。

此示例介绍如何使用 CLI 版本的 AMS UpdateRfc API（参见更新 RFC）。虽然有些更改类型可用于更新某些资源（DNS 私有和公有、负载均衡器堆栈以及堆栈修补配置），但没有 CT 可以更新 RFC。

我们建议您一次提交一个 UpdateRfc 操作。如果您提交多个更新（例如在 DNS 堆栈上），则尝试同时更新 DNS 时，更新可能会失败。

必填数据:`RfcId`: 您正在更新的 RFC。

可选数据:`ExecutionParameters`: 除非你要更新非必填字段，比如`Description`，否则你需要提交修改后的执行参数来解决导致 RFC 被拒绝或取消的问题。所有提交的非空值都会覆盖原始 RFC 中的这些值。

1. 找到相关的已拒绝或已取消的 RFC，您可以使用以下命令（可以将值替换为`Canceled`）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 您可以修改以下任何 RFC 参数：

```
{
    "Description": "string",
    "ExecutionParameters": "string",
    "ExpectedOutcome": "string",
    "ImplementationPlan": "string",
    "RequestedEndTime": "string",
    "RequestedStartTime": "string",
    "RfcId": "string",
    "RollbackPlan": "string",
    "Title": "string",
    "WorstCaseScenario": "string"}
```

更新描述字段的命令示例：

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
 --region us-east-1
```

更新 ExecutionParameters VpcId 字段的命令示例：

```
aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
 "RFC_ID" --region us-east-1
```

使用包含更新的执行参数文件更新 RFC 的命令示例；参见步骤 2 中的示例执行参数文件：EC2 stack | Creat e:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. 使用`submit-rfc`与首次创建 RFC 时相同的 RFC 编号重新提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，则您不会在命令行收到任何确认或错误消息。

4. 要监控请求的状态并查看执行输出，请运行以下命令。

```
aws amscm get-rfc --rfc-id RFC_ID
```

查找 RFCs

使用控制台查找变更请求 (RFC)

要使用 AMS 控制台查找 RFC，请按照以下步骤操作。

> **Note**
>
> 此过程仅适用于未使用 ASAP 选项的已计划 RFCs。 RFCs

1. 在左侧导航栏中，单击RFCs。

   RFCs 仪表板打开。
2. 滚动浏览列表或使用 “筛选” 选项来细化列表。

   根据筛选标准，RFC 列表会发生变化。
3. 选择所需的 RFC 的 “主题” 链接。

   将打开该 RFC 的 RFC 详细信息页面，其中包含包括 RFC ID 在内的信息。
4. 如果仪表板 RFCs 中有许多内容，则可以使用 “筛选器” 选项按 RFC 进行搜索：

   - 主题：创建 RFC 时向其提供的主题行或标题（在 API/CLI 中）。
   - RFC ID：RFC 的标识符。
   - 活动状态：如果您知道 RFC 状态，则可以在AwsOperatorAssigned表示操作员当前正在查看 RFC（AwsActionPending即 AMS 操作员必须在 RFC 执行之前执行某项操作）或CustomerActionPending表示您需要在 RFC 执行之前采取一些操作之间进行选择。
   - 状态：如果您知道 RFC 状态，则可以在以下选项中进行选择：
     - 已计划： RFCs 那是预定的。
     - 已取消： RFCs 已取消。
     - 进行中： RFCs 进行中。
     - 成功： RFCs 成功执行。
     - 已拒绝： RFCs 已被拒绝。

  - 编辑： RFCs 正在编辑中。
  - 失败： RFCs 失败了。
  - 待批准：在 AMS 或您批准之前， RFCs 这无法继续进行。通常，这表示您需要批准 RFC。您将在服务请求列表中收到有关此问题的服务通知。
- 更改类型：选择 “类别”、“子类别”、“物料” 和 “操作”，系统将为您检索更改类型 ID。
- 请求的开始时间或请求的结束时间：此筛选选项允许您选择 “之前” 或 “之后”，然后输入日期，也可以输入时间（可选）（hh: mm 和时区）。此过滤器只能按计划成功运行 RFCs （不是 ASAP RFCs）。
- 状态：“已计划”、“已取消”、“进行中”、“成功”、“已拒绝”、“正在编辑” 或 “失败”。
- 主题：您向 RFC 提供的主题（或标题，如果 RFC 是使用 API/CLI 创建的）。
- 变更类型 ID：使用与 RFC 一起提交的变更类型的标识符。

  搜索允许您添加过滤器，如以下屏幕截图所示。

5. 点击所需的 RFC 的 “主题” 链接。

   将打开该 RFC 的 RFC 详细信息页面，其中包含包括 RFC ID 在内的信息。

使用 CLI 查找变更请求 (RFC)

您可以使用多个筛选器来查找 RFC。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

如果您没有写下 RFC ID，需要稍后查找，则可以使用 AMS 变更管理 (CM) 系统进行搜索并使用筛选器或查询来缩小结果范围。

1. CM API ListRfcSummaries操作具有过滤器。您可以根据Attribute和Value组合在逻辑 AND 运算中筛选结果，也可以基于AttributeCondition、a 和筛选结果Values。

   RFC 过滤

属性	有效值	有效条件	默认条件	备注
ActualEndTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
ActualStartTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
AutomationStatusId	手动、自动	Equals	Equals	只有两种自动化状态
ChangeTypeId	任何有效的更改类型 ID；例如，ct-123h45t6uz7jl	Equals	Equals	查找变更类型或 CSIO
ChangeTypeVersion	任何有效的更改类型 ID；例如 1.0	Equals	Equals	查找变更类型或 CSIO
CreatedBy	任何字符串（允许的最大长度为 2048 个字符）	包含	包含	RFC 的 CreatedBy 字段包含创建它的用户的 ARN

属性	有效值	有效条件	默认条件	备注
CreatedTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
LastModifiedTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
LastSubmittedTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
RequestedEndTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期

属性	有效值	有效条件	默认条件	备注
RequestedStartTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
RfcStatusId	已取消、正在编辑、失败、 InProgress、PendingApproval、已拒绝、已计划、成功	Equals	Equals	刷新 AMS 控制台中的 RFC 列表或运行 GetRfc
职务	任何有效的 RFC 标题	包含	包含	不支持每个字段中的正则表达式。不区分大小写的搜索

示例：

要查找所有与 SQS RFCs 相关的（其中 SQS 包含在 CT 的项目部分），可以使用以下命令： IDs

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

它返回的结果是这样的：

```
-------------------------------------------------------------------------
|                          ListRfcSummaries                             |
+----------+---------------------------------+-------+-------+----------------+
|Deployment| Advanced Stack Components       |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+----------------+
```

另一个可用的过滤器`list-rfc-summaries`是`AutomationStatusId`，寻找 RFCs 自动或手动的过滤器：

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

另一个可用的过滤器`list-rfc-summaries`是`Title`（控制台中的主题）：

```
 Attribute=Title,Value=RFC-TITLE
```

JSON 中的新请求结构示例，其返回 RFCs 位置为：

- （标题包含 “Windows 2012” 或 “亚马逊 Linux” 这句话）和
- （RfcStatusId 等于 “成功” 或 InProgress “”）和
- (20170101T000000Z <= RequestedStartTime <= 20170103T000000Z) 和 (ActualEndTime <= 20170103T000000Z)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> 在更高级的版本中`Filters`，AMS 打算在即将发布的版本中弃用以下字段：
>
> - 值：“值” 字段是 “筛选器” 字段的一部分。使用支持更多高级功能的 “值” 字段。
> - RequestedEndTimeRange: 使用支持更高级功能的 “过滤器” 字段 RequestedEndTime 内部
> - RequestedStartTimeRange：使用支持更高级功能的 “过滤器” 字段 RequestedStartTime 内部。

有关使用 CLI 查询的信息，请参阅如何使用--query 选项过滤输出和查询语言参考JMESPath 规范。

2. 如果您使用的是 AMS 控制台：

   转到RFCs列表页面。如果需要，您可以在 RFC 主题上进行筛选，这是您在创建 RFC `Title` 时输入的内容。

提示

> **Note**
>
> 此过程仅适用于未使用 ASAP 选项的已计划 RFCs。 RFCs

取消 RFCs

您可以使用控制台或 AMS API/CLI 取消 RFC。

要使用控制台取消 RFC，请在您的 RFC 列表中找到 RFC，将其打开，单击 “取消”。

所需数据：

- `Reason`: 你为什么要取消 RFC。
- `RfcId`: 您要取消的 RFC。

1. 通常，您会在提交 RFC 后立即将其取消（因此 RFC ID 应该很方便）；否则，除非您安排了它并且在指定的开始时间之前，否则您将无法取消它。如果需要查找 RFC ID，则可以使用以下命令（可以Value用PendingApproval替换手动批准的 RFC）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. 取消 RFC 的命令示例：

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
region us-east-1
```

将 AMS 控制台与 RFCs

AMS 控制台提供的功能可帮助您成功创建和提交 RFCs。

使用 RFC 列表页面（控制台）

AMS 控制台RFCs列表页面为您提供以下选项：

- 通过过滤器进行高级 RFC 搜索。有关信息，请参阅查找 RFCs。
- 查找 RFC 上次修改的时间。此值表示上次更改 RFC 状态的时间。
- 使用 RFC 主题查看 RFC 详细信息。选择此链接将打开该 RFC 的详细信息页面。
- 查看 RFC 状态。有关信息，请参阅。了解 RFC 状态码

使用 RFC 快速创建（控制台）

使用 RFC 快速创建卡片或列表表，或者 RFCs 按分类选择更改类型。

要了解更多信息，请参阅创建 RFC。

添加 RFC 信件和附件（控制台）

您可以在 RFC 提交后和获得批准之前向其添加信件；例如，当它处于 “PendingApproval” 状态时。在 RFC 获得批准（处于 “已计划” 或 InProgress “” 状态）后，无法添加信件，因为它可能被解释为对请求的更改。RFC 完成后（处于 “已取消”、“已拒绝”、“成功” 或 “失败” 状态），将再次启用通信，但在 RFC 关闭超过 30 天后，通信将被禁用。

> **Note**
>
> 每封信件不得超过 5,000 个字符。

附件的限制：

- 每封信件只有三个附件。
- 每个 RFC 限制五十个附件。
- 每个附件的大小必须小于 5 MB。
- 仅接受文本文件，例如纯文本 (`.txt`)、逗号分隔值 ()、JSON (`.csv`) 或 YAM `.json` L ()。`.yaml`如果是 YAML 格式，则必须使用文件扩展名`.yaml`附加文件。

  > **Note**
  >
  > 禁止包含 XML 内容的文本文件。如果您有 XML 内容要与 AMS 共享，请使用服务请求。

- 文件名限制为 255 个字符，只能包含数字、字母、空格、破折号 (-)、下划线 (_) 和点 (.)。
- 目前不支持在 RFC 上更新和删除附件。

要向 RFC 添加信件和附件，请执行以下步骤：

1. 在 AMS 控制台中，在 RFC 的 RFC 详细信息页面上，找到页面底部的 “通信” 部分。

   在任何通信之前：

   经过一番信件后：

2. 要添加新的信件，请在回复文本框中键入您的消息。要附加与信件相关的文件，请选择 “添加附件”，然后选择所需的文件。

3. 完成后，选择 “提交”。

   新的信件以及所附文件的链接出现在RFC详细信息页面的信件列表中。

配置 RFC 电子邮件通知（控制台）

AMS 控制台的 “更改请求创建” 页面为您提供了添加电子邮件地址以接收 RFC 状态变更通知的选项：

此外，您可以将通知的电子邮件地址添加到任何更改类型，例如：

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

在请求的 RFC 参数部分，而不是参数部分，向任何更改类型内联或模板请求添加类似的行 (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`)。

了解常用 RFC 参数

以下是您需要提交的 RFC 参数以及中 RFCs常用的参数：

- 更改类型信息： ChangeTypeId 和 ChangeTypeVersion。有关更改类型 IDs 和版本号的列表，请参阅更改类型参考。

  使用`query`参数`list-change-type-classification-summaries`在 CLI 中运行以缩小结果范围。例如，缩小结果范围以更改`Item`名称中包含 “Access” 的类型。

  ```
  aws amscm list-change-type-classification-summaries --query
   "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
  ```

  运行`get-change-type-version`并指定更改类型 ID。以下命令获取 ct-2tylseo8rxfsc 的 CT 版本。

  ```
  aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
  ```

- 标题：RFC 的名称；它成为 AMS 控制台 RFC 列表中 RFC 的主题，你可以使用`GetRfc`命令和过滤器对其进行搜索 `Title`
- 计划：如果您想要预定的 RFC，则必须包含`RequestedStartTime`和`RequestedEndTime`参数，或者使用 “安排此更改” 控制台选项。对于 ASAP RFC（在获得批准后立即运行），在使用 CLI 时，

请保留RequestedStartTime并RequestedEndTime为 null。使用控制台时，请接受 “尽快” 选项。

如果错过RequestedStartTime，则 RFC 将被拒绝。

- 配置 CTs：执行参数，或者Parameters是配置资源所需的特定设置。根据 CT 的不同，它们差异很大。
- 非预配 CTs： CTs 未配置资源（例如访问权限 CTs 或其他 | 其他）或删除堆栈的执行参数最少且没有Parameters阻塞。
- 有些 RFCs 还要求您在 RFC 失败之前指定创建堆栈的时间或允许多少分钟。TimeoutInMinutes对于长时间运行 UserData，有效值为 60（分钟）到 360。如果在超过之前无法完成执行，则 TimeoutInMinutes RFC 将失败。但是，此设置不会延迟 RFC 的执行。
- RFCs 创建实例（例如 S3 存储桶或 ELB）通常会提供允许您添加最多七个标签（键/值对）的架构。您可以使用部署 | 高级堆栈组件 | 标签 | 创建更改类型 (ct-3cx7we852p3af) 提交 RFC，从而向 S3 存储桶添加更多标签。 EC2、EFS、RDS 和多层（HA 双层和 HA 单层）架构最多允许 50 个标签。标签是在架构的ExecutionParameters部分中指定的。提供标签可能非常有价值。有关更多信息，请参阅标记您的 Amazon EC2 资源。

  使用 AMS 控制台时，必须打开其他配置区域才能添加标签。

  > **Tip**
  >
  > 许多 CT 架构的架构顶部附近都有一个Description和Name字段。这些字段用于命名堆栈或堆栈组件，它们不会命名您正在创建的资源。有些架构提供参数来命名你正在创建的资源，有些则没有。例如，Create EC2 堆栈的 CT 架构不提供用于命名 EC2 实例的参数。为此，您必须使用密钥为 “Name” 和您想要的名称的值创建一个标签。如果您未创建此类标签，则您的 EC2 实例将在 EC2 控制台中显示，但不带名称属性。

使用 RFC AWS 区域选项

AMS API 和 CLI（amscm和amsskms）端点已在us-east-1。如果您使用安全断言标记语言 (SAML) 进行联合，则会在入门时为您提供将您的区域设置为 us-east-1 的脚本。 AWS 如果您使用 SAML，则在发出命令时无需指定该--region选项。如果您的 SAML 配置为使用 us-east-1，但您的账户不 AWS 在该区域内，则在发出其他命令（例如）时，您必须指定您的账户已注册区域。 AWS aws s3

> **Note**
>
> 本指南中提供的大多数命令示例都不包含该`--region`选项。

注册 RFC 每日电子邮件

您可以使用 RFC 摘要功能注册每日一封电子邮件，总结过去 24 小时内您账户中的 RFC 活动。RFC 摘要功能是一个简化的流程，可减少您收到的有关您账户的电子邮件通知的 RFCs数量。RFC 摘要可能会降低您错过等待回复的操作的可能性。

要打开 RFC 摘要功能，请联系您的 AMS 云服务交付经理 (CSDM)。CSDM 会为您订阅。您可以请求将最多 20 个电子邮件地址（或别名）添加到 RFC 摘要电子邮件列表中。当前的电子邮件时间表固定在 09:00 UTC-8。

要关闭 RFC 摘要功能，请联系您的 CSDM 并提出您的请求。

如果您没有设置 RFC 摘要并想要有关您的通知 RFCs，或者您想要的信息 RFCs 比 RFC 摘要提供的内容更详细，请使用变更管理系统为您想要了解的每个 RFC 设置 CloudWatch 事件通知或电子邮件通知。有关设置 RFC 通知的信息，请参阅 RFC 状态更改通知。

RFC 摘要中包含的主题包括以下内容：

- 等待买家批准： RFCs 处于PendingApproval状态正在等待您批准的列表
- 待处理的买家回复： RFCs 正在等待您回复 RFC 信件的清单
- 待定 AWS 批准或回复：等待 AMS 回复或批准的清单 RFCs
- 已完成：列表状态 RFCs 为成功、失败、已取消和已拒绝

以下是 RFC 摘要示例：

什么是变更类型？

变更类型是指 AWS Managed Services (AMS) 变更请求 (RFC) 执行的操作，包括变更操作本身，以及变更类型（手动与自动）。AMS 拥有大量未被其他 Amazon 网络服务使用的变更类型。在提交变更请求 (RFC) 以部署、管理或访问资源时，您可以使用这些更改类型。

主题

自动和手动 CTs

对更改类型的限制是它们是自动还是手动的，这是更改类型AutomationStatusId属性，在 AMS 控制台中称为执行模式。

自动变更类型具有预期的结果和执行时间，并通过AMS自动化系统运行，通常在一小时或更短的时间内（这在很大程度上取决于CT配置的资源）。手动更改类型并不常见，但它们的处理方式有所不同，因为它们要求 AMS 操作员在运行 RFC 之前对其进行操作。这有时意味着要与 RFC 提交者沟通，因此，手动更改类型需要不同的时间才能完成。

对于所有已安排的时间 RFCs，将未指定的结束时间写成指定的时间RequestedStartTime加上已提交的更改类型的ExpectedExecutionDurationInMinutes属性。例如，如果ExpectedExecutionDurationInMinutes为 “60”（分钟），指定RequestedStartTime为2016-12-05T14:20:00Z（2016 年 12 月 5 日凌晨 4:20），则实际结束时间将设置为 2016 年 12 月 5 日凌晨 5:20。要查找ExpectedExecutionDurationInMinutes特定更改类型的，请运行以下命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> 在控制台中， RFCs 使用执行模式 = 手动进行调度，必须设置为将来至少 24 小时运行。此注意事项不适用于 AMS API/CLI，但 RFCs 至少提前 8 小时安排手动计划仍然很重要。

> **Note**
>
> 使用 “需要审核” 时 CTs，AMS 建议您使用 “尽快安排” 选项（在控制台中选择 “尽快”，在 AP I/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

AMS 的目标是在四小时内对手动 CT 做出回应，并将尽快对应，但是 RFC 可能需要更长的时间才能真正运行。

有关手动 CTs 且需要 AMS 审核的内容的列表，请参阅控制台开发者资源页面上的更改类型 CSV 文件。

YouTube 视频：如何查找 AMS 的自动变更类型 RFCs？

要在 AMS 控制台中查找 CT 的执行模式，必须使用浏览更改类型搜索选项。结果显示匹配的变更类型或变更类型的执行模式。

要使用 AMS CLI 查找特定更改类型的，请运行以下命令：`AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

您还可以在 AMS 变更类型参考中查找变更类型，该参考提供了有关所有 AMS 变更类型的信息。

> **Note**
>
> AMS 目前不 API/CLI 是 AWS 的一部分API/CLI. To access the AMS API/CLI，您可以通过 AMS 控制台下载 AMS 开发工具包。

CT 批准要求

AMS CTs 总是有两个批准条件 AwsApprovalId，CustomerApprovalId这表明RFC是要求AMS还是你或任何人批准执行。

批准条件与执行模式有些相关；有关详细信息，请参阅自动和手动 CTs。

要找出 CT 的批准条件，您可以查看 AMS 变更类型参考或运行GetChangeTypeVersion。两者还将为您提供CT `AutomationStatusId` 或执行模式。

您可以使用 AMS 控制台或使用以下命令进行批准 RFCs ：

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 批准条件

如果 CT 批准条件是	它需要获得批准	并且
AwsApprovalId: Required	AMS 变更类型系统，	无需采取行动。这种情况是自动化的典型情况 CTs。
AwsApprovalId: NotRequiredIfSubmitter	AMS 变更类型系统，没有其他人，如果提交的 RFC 是针对其提交时所针对的账户，	无需采取行动。这种情况是手动操作的典型情况， CTs 因为AMS操作员将始终对其进行审查。
CustomerApprovalId: NotRequired	AMS 变更类型系统，	如果 RFC 通过了语法和参数检查，则会自动获得批准。
CustomerApprovalId: Required	AMS 变更类型系统而你，	系统会向您发送通知，您必须通过回复通知或运行ApproveRfc操作来明确批准 RFC。
CustomerApprovalId: NotRequiredIfSubmitter	如果您提交了 RFC，AMS 将更改类型系统，而没有其他人可用。	如果 RFC 通过了语法和参数检查，则会自动获得批准。
紧急安全事件或补丁	AMS	已通过 auto 批准并实施。

更改类型版本

当对变更类型进行重大更新时，变更类型会被版本控制，版本也会发生变化。

使用 AMS 控制台选择更改类型后，您可以选择打开其他配置区域并选择更改类型版本。您也可以在 API/CLI 命令行中指定更改类型版本。您可能出于各种原因想要这样做，包括：

- 您知道您想要的 “更新” 更改类型的版本必须与您用于创建现在要更新的资源的 “创建变更” 类型的版本相匹配。例如，您可能有一个使用 ELB 创建的 Elastic Load Balancer (ELB) 实例。创建更改类型版本 1。要对其进行更新，请选择 ELB 更新版本 1。
- 您想要使用的更改类型版本中包含的选项与最新的更改类型不同。我们不建议这样做，因为 AMS 更新更改类型主要是出于安全考虑，我们建议您始终选择最新版本。

创建变更类型

创建变更类型 version-to-version与更新变更类型相匹配。也就是说，用于置备资源的更改类型版本必须与您稍后用于修改该资源的更新更改类型的版本相匹配。例如，如果您使用创建 S3 存储桶更改类型为 2.0 的 S3 存储桶，之后又想提交 RFC 来修改该 S3 存储桶，则即使版本 3.0 中存在更新 S3 存储桶更改类型，也必须使用更新 S3 存储桶更改类型版本 2.0。

我们建议记录您在使用创建变更类型置备资源时使用的变更类型 ID 和版本，以备日后您想使用更新更改类型对其进行修改。

更新变更类型

AMS 提供更新更改类型，以更新使用 “创建更改类型” 创建的资源。更新更改类型必须 version-to-version与最初用于置备资源的 “创建” 更改类型相匹配。

我们建议记录您在配置资源时使用的更改类型 ID 和版本，以便于更新。

YouTube 视频：如何使用更新 CTs 来更改 AWS Managed Services (AMS) 账户中的资源？

仅限内部的变更类型

您可以看到仅供内部使用的更改类型。这样您就可以知道 AMS 可以或正在采取哪些行动。如果您想提供仅限内部使用的变更类型，请提交服务请求。

例如，只有内部才有 “管理” | “监控和通知” | “ CloudWatch 警报抑制” | “更新 CT”。AMS 使用它来部署基础设施更新（例如修补），以关闭更新可能错误触发的警报通知。提交此 CT 后，您将在您的 RFC 列表中注意到 CT 的 RFC。部署在 RFC 中的任何仅限内部的 CT 都会显示在您的 RFC 列表中。

更改类型架构

所有变更类型都提供一个 JSON 架构，供您在创建、修改或访问资源时输入内容。架构提供参数及其描述，供您创建更改请求 (RFC)。

成功执行 RFC 会产生执行输出。为了进行配置 RFCs，执行输出包括一个 “stack_id”，它表示中的堆栈 CloudFormation，可以在控制台中搜索。 CloudFormation 执行输出有时包括创建的实例 ID 的输出，

该 ID 可用于在相应的 AWS 控制台中搜索该实例。例如，创建 ELB CT 执行输出包括一个可在中搜索的 “stack_id”， CloudFormation 并输出一个可在亚马逊控制台中搜索 Elastic Load Balancing <stack-xxxx>的 key=elb value=。 EC2

让我们来看看 CT 架构。这是 CodeDeploy 应用程序创建的架构，这是一个相当小的架构。有些架构的Parameter区域非常大。

架构的第一部分向 AMS 提供有关请求的更改类型的信息。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
```

```
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
to
      allow for execution of the change. This will not prolong
execution,
      but the RFC fails if the change is not completed in the
specified time.
      Valid values are 60 up to 360, for long-running
UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
```

该 TimeoutInMinutes 参数允许您指定运行变更类型的边界时间。对于长时间运行 UserData，有效值为 60 到 360。

在“参数”部分中，您可以为正在创建的资源或您请求的操作指定设置。

“其他属性”部分让您知道哪些参数是必需的，哪些是可选的。

```
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

> **Note**
>
> 此架构最多允许 7 个标签；但是，EFS EC2、RDS 和多层创建架构最多允许 50 个标签。

管理变更类型的权限

您可以使用自定义策略来限制哪些更改类型 (CTs) 可供不同的群组或用户使用。

要了解有关执行此操作的更多信息，请参阅 AMS 用户指南中的设置权限部分。

编辑变更类型中的敏感信息

AMS 更改类型架构提供参数属性，`"metadata":"ams:sensitive":"true"`该属性用于包含密码等敏感信息的参数。设置此属性后，所提供的输入将被遮盖。请注意，您无法设置此参数属性；但是，如果您正在与 AMS 合作创建更改类型，并且想要在输入时隐藏某个参数，则可以请求这样做。

使用查询选项查找更改类型

此示例演示如何使用 AMS 控制台查找要提交的 RFC 的相应更改类型。

您可以使用控制台或 API/CLI 来查找更改类型 ID (CT) 或版本。有两种方法，要么是搜索，要么是选择分类。对于这两种选择类型，您可以通过选择 “最常用”、“最近使用” 或 “按字母顺序” 对搜索进行排序。

YouTube 视频：如何使用 AWS Managed Services CLI 创建 RFC，在哪里可以找到 CT 架构？

在 AMS 控制台中，在 RFCs-> 创建 RFC 页面上：

- 选择 “按更改类型浏览”（默认）后，可以：
  - 使用快速创建区域从 AMS 最受欢迎的 AMS 中进行选择 CTs。点击标签，将打开 “运行 RFC” 页面，并自动为您填充主题选项。根据需要完成其余选项，然后单击 “运行” 提交 RFC。
  - 或者，向下滚动到 “所有变更类型” 区域并开始在选项框中键入 CT 名称，您不必输入确切或完整的更改类型名称。您还可以通过输入相关词语按更改类型 ID、分类或执行模式（自动或手动）搜索 CT。

    选择默认卡片视图后，匹配的 CT 卡片会在您键入时出现，选择一张卡片并单击 “创建 RFC”。选择表格视图后，选择相关的 CT，然后单击 “创建 RFC”。两种方法都会打开 “运行 RFC” 页面。
- 或者，要浏览更改类型选择，请单击页面顶部的按类别选择以打开一系列下拉选项框。
- 选择 “类别”、“子类别”、“物料” 和 “工序”。该更改类型的信息框显示在页面底部显示一个面板。
- 准备就绪后，按 Enter，将显示匹配的更改类型列表。
- 从列表中选择更改类型。该更改类型的信息框出现在页面底部。
- 选择正确的更改类型后，选择 “创建 RFC”。

> **Note**
>
> 必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的 “AMS 信息资源” 部分。您可能需要添加身份验证`--profile`选项；例如，`aws amsskms` *`ams-cli-command`* `--profile SAML`。您可能还需要添加该`--region`选项，因为所有 AMS 命令都将使用 us-east-1；例如。`aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> AMS API/CLI（amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

要使用 AMS CM API（参见 ListChangeTypeClassificationSummaries）或 CLI 搜索更改类型，请执行以下操作：

您可以使用筛选器或查询进行搜索。该 ListChangeTypeClassificationSummaries 操作具有Category、SubcategoryItem、和的 “筛选器” 选项Operation，但这些值必须与现有值完全匹配。要在使用 CLI 时获得更灵活的结果，可以使用--query选项。

使用 AMS CM API/CLI 更改类型筛选

属性	有效值	有效/默认条件	备注
ChangeTypeId	任何表示 a 的字符串 ChangeTypeId（例如：ct-abc123xyz7890）	Equals	有关更改类型 IDs，请参阅更改类型参考。 有关变更类型 IDs，请参阅查找变更类型或 CSIO。
类别	任何自由格式的文本	包含	不支持每个字段中的正则表达式。不区分大小写的搜索
子类别			
Item			
操作			

1. 以下是一些商品变更类型分类的示例：

   以下命令列出了所有更改类型类别。

   ```
   aws amscm list-change-type-categories
   ```

以下命令列出了属于指定类别的子类别。

```
aws amscm list-change-type-subcategories --category CATEGORY
```

以下命令列出了属于指定类别和子类别的项目。

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. 以下是一些使用 CLI 查询搜索变更类型的示例：

   以下命令在 CT 分类摘要中搜索项目名称中包含 “S3” 的摘要，并以表格形式创建类别、子类别、项目、操作和更改类型 ID 的输出。

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries         |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. 然后，您可以使用更改类型 ID 获取 CT 架构并检查参数。以下命令将架构输出到名为 creates3Params.schema.json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

   有关使用 CLI 查询的信息，请参阅如何使用--query 选项过滤输出和查询语言参考JMESPath 规范。

4. 获得变更类型 ID 后，我们建议您验证变更类型的版本，以确保它是最新版本。使用以下命令查找指定更改类型的版本：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

要查找AutomationStatus特定更改类型的，请运行以下命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

要查找ExpectedExecutionDurationInMinutes特定更改类型的，请运行以下命令：

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

对 AMS 中的 RFC 错误进行故障排除

可以通过 CloudFormation 文档调查许多 AMS 配置 RFC 故障。参见 AWS 疑难解答 CloudFormation：错误疑难解答

以下各节提供了其他疑难解答建议。

AMS 中的 “管理” RFC 错误

AMS “管理” 类别更改类型 (CTs) 允许您请求访问资源并管理现有资源。本节介绍一些常见问题。

RFC 访问错误

- 确保您在 RFC 中指定的用户名和 FQDN 正确且存在于域中。有关查找您的 FQDN 的帮助，请参阅查找您的 FQ DN。
- 确保您为访问而指定的堆栈 ID 是 EC2相关的堆栈。诸如 ELB 和 Amazon Simple Storage Service (S3) 之类的堆栈不适合访问 RFCs，而是使用您的只读访问权限角色来访问这些堆栈资源。有关查找堆栈 ID 的帮助，请参阅查找堆栈 IDs
- 请确保您提供的堆栈 ID 正确且属于相关账户。

有关其他访问 RFC 故障的帮助，请参阅访问管理。

YouTube 视频：如何正确提出变更申请 (RFC) 以避免被拒绝和失败？

RFC（手动）CT 调度错误

大多数更改类型是 ExecutionMode =Automated，但有些是 ExecutionMode =Manual，这会影响您应如何安排更改以避免 RFC 失败。

如果 RFCs 使用 AMS 控制台创建 R ExecutionMode FC，则必须将其设置为将来至少 24 小时内执行。此注意事项不适用于 AMS API/CLI，但 RFCs 至少提前 8 小时安排手动操作仍然很重要。

AMS 的目标是在四小时内对手动 CT 做出回应，并将尽快回复，但是 RFC 可能需要更长的时间才能真正执行。

RFCs 与手动更新一起使用 CTs

如果您要更新的堆栈类型有 “更新” 更改类型，则 AMS Operations 会拒绝 “管理” | “其他 RFCs ” | “其他” 更新堆栈。

RFC 删除堆栈错误

RFC 删除堆栈失败：如果您使用管理 | 标准堆栈 | 堆栈 | 删除 CT，则将在 CloudFormation 控制台中看到带有 AMS 堆栈名称的堆栈的详细事件。您可以通过将堆栈与 AMS 控制台中的名称进行核对来识别堆栈。 CloudFormation 控制台提供了有关故障原因的更多详细信息。

在删除堆栈之前，应考虑堆栈是如何创建的。如果您使用 AMS CT 创建堆栈，但未添加或编辑堆栈资源，则可以毫无问题地将其删除。但是，在提交针对堆栈的删除堆栈 RFC 之前，最好先从堆栈中移除所有手动添加的资源。例如，如果您使用完整堆栈 CT（HA Two Tier）创建堆栈，则它会包含一个安全组- SG1。如果您随后使用 AMS 创建另一个安全组- SG2，并引用 SG1 已创建的作为完整堆栈一部分的新 SG2 安全组，然后使用删除堆栈 CT 删除该堆栈，则 SG1 不会像引用的那样将其删除 SG2。

> **Important**
>
> 删除堆栈可能会带来意想不到和意想不到的后果。出于这个原因，AMS 倾向于*不*代表客户删除堆栈或堆栈资源。请注意，AMS 只会代表您删除无法使用相应的自动更改类型进行删除的资源（通过提交的管理 | 其他 | 其他 | 更新更改类型）。其它注意事项：
>
> - 如果资源启用了 “删除保护”，则如果您提交 “管理 | 其他 | 其他 | 更新” 更改类型，AMS 可以帮助解除此限制，并且删除保护后，您可以使用自动 CT 删除该资源。
> - 如果堆栈中有多个资源，并且您只想删除堆栈资源的子集，请使用 CloudFormation 更新更改类型（参见载CloudFormation 入堆栈：更新）。您也可以提交 “管理” | “其他” | “其他” | “更新” 变更类型，如果需要，AMS 工程师可以帮助您制作变更集。
> - 如果由于偏差而在使用 CloudFormation 更新 CT 时出现问题，AMS 可以提供帮助，方法是您提交管理 | 其他 | 其他 | 其他 | 更新来解决偏差（在 AWS CloudFormation 服务支持的范围 Management/Custom Stack/Stack From CloudFormation Template/Approve内），并提供一个 ChangeSet 您可以随后使用自动 CT、变更集和更新进行验证和执行的更新。

AMS 维持上述限制，以帮助确保不会出现意外或意外的资源删除。

有关更多信息，请参阅 AWS 疑难解答 CloudFormation：删除堆栈失败。

RFC 更新 DNS 错误

多次 RFCs 更新 DNS 托管区域可能会失败，有些是无缘无故的。同时创建多个 RFCs 用于更新 DNS 托管区域（私有或公共）可能会 RFCs 导致某些区域失败，因为它们正在尝试同时更新同一个堆栈。由于另一个 RFC 已经更新堆栈而无法更新堆栈，AMS 变更管理会拒绝或失败 RFCs 。AMS 建议您一次创建一个 RFC，等待 RFC 成功后再为同一个堆栈筹集一个新的 RFC。

RFC IAM 实体错误

AMS 将许多默认 IAM 角色和配置文件配置到 AMS 账户中，以满足您的需求。但是，您可能需要偶尔请求其他 IAM 资源。

提交 RFCs 请求自定义 IAM 资源的流程遵循手动标准工作流程 RFCs，但批准流程还包括安全审查，以确保适当的安全控制措施到位。因此，该过程通常比其他手册花费更长的时间 RFCs。要缩短这些产品的周期时间 RFCs，请遵循以下准则。

有关我们所说的 IAM 审查的含义以及它如何与我们的技术标准和风险接受流程对应的信息，请参阅了解 RFC 安全评论。

常见的 IAM 资源请求：

- 如果您要求提供与主要云兼容应用程序相关的政策，例如 CloudEndure，请参阅 AMS 预先批准的 IAM CloudEndure 政策：解压WIGs 云端耐久着陆区示例文件并打开 `customer_cloud_endure_policy.json`

  > **Note**
  >
  > 如果您想要更宽松的政策，请与您讨论您的需求， CloudArchitect/CSDM 并在必要时获得 AMS 安全审查和签署，然后再提交实施该政策的 RFC。

- 如果您想修改默认情况下由 AMS 在您的账户中部署的资源，我们建议您索要该资源的修改副本，而不是更改现有资源。
- 如果您正在为人类用户请求权限（而不是向用户授予权限），请将权限附加到某个角色，然后向该用户授予担任该角色的权限。有关执行此操作的详细信息，请参阅临时 AMS 高级控制台访问权限。

- 如果您需要特殊权限来执行临时迁移或工作流程，请在请求中提供这些权限的结束日期。
- 如果您已经与安全团队讨论了请求的主题，请尽可能详细地向您的 CSDM 提供他们批准的证据。

如果 AMS 拒绝 IAM RFC，我们会提供明确的拒绝理由。例如，我们可能会拒绝 IAM 策略创建请求，并解释该策略的哪些内容不合适。在这种情况下，您可以进行已确定的更改并重新提交请求。如果需要进一步明确请求的状态，请提交服务请求或联系您的 CSDM。

以下列表描述了 AMS 在审核您的 IAM 时试图降低的典型风险 RFCs。如果您的 IAM RFC 存在上述任何风险，则可能会导致 RFC 被拒绝。如果您需要例外，AMS 会要求您的安全团队批准。要寻求这样的例外，请与您的 CSDM 进行协调。

> **Note**
>
> AMS 可以出于任何原因拒绝对账户内的 IAM 资源进行任何更改。如对任何 RFC 拒绝有任何疑问，请通过服务请求与 AMS 运营部门联系，或联系您的 CSDM。

- 权限升级，例如允许您修改自己的权限或修改账户内其他资源的权限的权限。示例：
  - `iam:PassRole`与另一个更具特权的角色一起使用。
  - 角色或用户对 attach/detach IAM 策略的权限。
  - 账户中 IAM 策略的修改。
  - 能够在管理基础架构的上下文中进行 API 调用。
- 修改向您提供 AMS 服务所需的资源或应用程序的权限。示例：
  - 修改 AMS 基础设施，例如堡垒、管理主机或 EPS 基础架构。
  - 删除日志管理 AWS Lambda 函数或日志流。
  - 删除或修改默认 CloudTrail 监控应用程序。
  - 目录服务活动目录 (AD) 的修改。
  - 禁用 CloudWatch (CW) 警报。
  - 修改作为 landing zone 一部分部署在账户中的委托人、策略和命名空间。
- 在最佳实践之外部署基础架构，例如允许在危及信息安全的状态下创建基础设施的权限。示例：
  - 创建公有或未加密的 S3 存储桶或公开共享 EBS 卷。
  - 公有 IP 地址的配置。
  - 修改安全组以允许广泛访问。

- 过于宽泛的权限会对应用程序造成影响，例如可能导致数据丢失、完整性丢失、配置不当或基础架构和账户内应用程序服务中断的权限。示例：
  - 禁用或重定向通过 APIs like `ModifyNetworkInterfaceAttribute` 或`UpdateRouteTable`的网络流量。
  - 通过将卷与托管主机分离来禁用托管基础架构。
- 服务权限不在 AMS 服务描述中，也不受 AMS 支持。

  AMS 服务说明中未列出的服务不能用于 AMS 账户。要请求某项功能或服务的支持，请联系您的 CSDM。
- 权限不符合您的既定目标，因为它们要么过于慷慨，要么过于保守，要么应用于错误的资源。示例：
  - 对`s3:PutObject`具有强制性 KMS 加密的 S3 存储桶的权限请求，但没有相关密钥的`KMS:Encrypt`权限。
  - 与账户中不存在的资源相关的权限。
  - IAM， RFCs 其中 RFC 的描述似乎与请求不符。

“部署” RFC 错误

AMS “部署” 类别更改类型 (CTs) 允许您请求将各种 AMS 支持的资源添加到您的账户。

创建资源的大多数 AMS CTs 都是基于 CloudFormation 模板的。作为客户，您可以只读访问所有 AWS 服务 CloudFormation，包括，您可以使用 CloudFormation 控制台根据 CloudFormation 堆栈描述快速识别代表您的堆栈的堆栈。失败的堆栈可能处于 DELETE_COMPLETE 状态。确定 CloudFormation 堆栈后，事件将向您显示创建失败的特定资源及其原因。

使用 CloudFormation 文档进行故障排除

大多数 AMS 配置都 RFCs 使用 CloudFormation 模板，该文档可能有助于进行故障排除。请参阅该 CloudFormation 模板的文档：

- 创建应用程序负载均衡器失败： AWS::ElasticLoadBalancingV2::LoadBalancer （ Application Load Balancer ）
- 创建 Auto Scaling 组： AWS::AutoScaling::AutoScalingGroup （ Auto Scaling 组 ）
- 创建 memcached 缓存： AWS::ElastiCache::CacheCluster （ 缓存集群 ）
- 创建 Redis 缓存： AWS::ElastiCache::CacheCluster （ 缓存集群 ）
- 创建 DNS 托管区域（与创建 DNS 私有/公用 ）： AWS::Route53::HostedZone （ R53 托管区域 ）

- 创建 DNS 记录集（与创建 DNS 私有/公共 DNS 一起使用）：AWS::Route53::RecordSet（资源记录集）
- 创建 EC2 堆栈：AWS::EC2::Instance（弹性计算云）
- 创建弹性文件系统 (EFS): AWS::EFS::FileSystem（弹性文件系统）
- 创建负载均衡器：AWS::ElasticLoadBalancing::LoadBalancer（Elastic Load Balancer）
- 创建 RDS 数据库: AWS::RDS::DBInstance（关系数据库）
- 创建 Amazon S3：AWS::S3::Bucket（简单存储服务）
- 创建队列：AWS::SQS::Queue（简单队列服务）

RFC 创建错误 AMIs

亚马逊机器映像（AMI）是一种包含软件配置（例如，操作系统、应用程序服务器和应用程序）的模板。从 AMI 启动一个实例，该实例是在云中作为虚拟服务器运行的 AMI 的副本。 AMIs 非常有用，是创建 EC2 实例或 Auto Scaling 组所必需的；但是，您必须遵守一些要求：

- 您为其指定的实例`Ec2InstanceId`必须处于停止状态，RFC 才能成功。请勿为此参数使用 Auto Scaling 组 (ASG) 实例，因为 ASG 将终止已停止的实例。
- 要创建 AMS Amazon 系统映像 (AMI)，必须从 AMS 实例开始。在使用该实例创建 AMI 之前，您必须确保它已停止并与其域断开连接，从而对其进行准备。有关详细信息，请参阅使用 Sysprep 创建标准亚马逊系统映像
- 您为新 AMI 指定的名称在账户中必须是唯一的，否则 RFC 将失败。AMI | Creat e 中描述了如何执行此操作，有关更多详细信息，请参阅和 AWS AMI 设计。

> **Note**
>
> 有关为 AMI 创建做准备的其他信息，请参阅 AMI | 创建。

RFCs 正在创建 o EC2s r ASGs 错误

对于带超时 EC2 的 ASG 故障，AMS 建议您确认所使用的 AMI 是否已自定义。如果是，请参阅本指南中包含的 AMI 创建步骤（参见 AMI | Cre ate），以确保正确创建 AMI。创建自定义 AMI 时的一个常见错误是未按照指南中的步骤重命名或调用 Sysprep。

RFCs 创建 RDS 错误

Amazon Relational Database (RDS) 失败的原因可能有很多，因为您在创建 RDS 时可以使用许多不同的引擎，而且每个引擎都有自己的要求和限制。在尝试创建 AMS RDS 堆栈之前，请仔细查看 AWS RDS 参数值，请参阅创建DBInstance。

要了解有关 Amazon RDS 的更多信息，包括大小建议，请参阅亚马逊关系数据库服务文档。

RFCs 创建 Amazon S3 错误

创建 S3 存储桶时的一个常见错误是该存储桶没有使用唯一的名称。如果您提交的 S3 存储桶 Create CT 的名称与之前提交的存储桶名称相同，则该存储桶将失败，因为已经存在与之同名的 S3 存储桶 BucketName。这将在 CloudFormation 控制台中详细介绍，您将在控制台中看到堆栈事件显示存储桶名称已在使用中。

RFC 验证与执行错误

在选定的 RFC 的 AMS 控制台 RFC 详细信息页面上，RFC 失败和相关消息的输出消息有所不同：

- 验证失败的原因仅在 “状态” 字段中可用
- 执行失败的原因可在执行输出和状态字段中找到。

RFC 错误消息

当您在列出的更改类型 (CTs) 中遇到以下错误时，可以使用这些解决方案来帮助您找到问题的根源并进行修复。

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

如果您在参考以下故障排除选项后需要进一步的帮助，请通过 RFC 通信与 AMS 联系或创建服务请求。有关更多详细信息，请参阅 RFC 通信和附件（控制台）和在 AMS 中创建服务请求。

工作负载摄取 (WIGS) 错误

> **Note**
>
> 可以下载适用于 Windows 和 Linux 的验证工具，并直接在您的本地服务器上运行，也可以在 AWS 中的 EC2 实例上运行。这些内容可通过《AMS 高级应用程序开发者指南迁移工作负载：Linux 摄取前验证》和《迁移工作负载：Windows 摄取前验证》中找到。

- 确保目标 AMS 账户中存在 EC2 实例。例如，如果您已将非 AMS 账户的 AMI 共享到 AMS 账户，则必须先在您的 AMS 账户中使用共享 AMI 创建一个 EC2 实例，然后才能提交工作负载摄取 RFC。
- 检查连接到实例的安全组是否允许出口流量。SSM 代理需要能够连接到其公共端点。
- 检查该实例是否具有连接 SSM 代理的正确权限。这些权限附带了`customer-mc-ec2-instance-profile`，你可以在 EC2 控制台中查看：

EC2 实例堆栈停止错误

- 检查实例是否已处于停止或已终止状态。
- 如果 EC2 实例处于联机状态并且您看到`InternalError`错误，请提交服务请求让 AMS 进行调查。
- 请注意，你不能使用更改类型管理 | 高级堆栈组件 | EC2 实例堆栈 | 停止 ct-3mvvt2zkyveqj 来停止 Auto Scaling 组 (ASG) 实例。如果您需要停止 ASG 实例，请提交服务请求。

EC2 实例堆栈创建错误

`InternalError`消息来自 CloudFormation；一个 CREATION_FAILED 状态的原因。您可以按照以下步骤在堆栈事件中找到有关 CloudWatch 堆栈故障的详细信息：

- 在 AWS 管理控制台中，您可以在创建、更新或删除堆栈时查看堆栈事件列表。从该列表中，找到失败事件，然后查看该事件的状态原因。

  状态原因可能包含来自 AWS CloudFormation 或特定服务的错误消息，可以帮助您了解问题。
- 有关查看堆栈事件的更多信息，请参阅在 AWS 管理控制台上查看 AWS CloudFormation 堆栈数据和资源。

EC2 实例卷恢复错误

当 EC2 实例卷恢复失败时，AMS 会创建内部故障排除 RFC。之所以这样做，是因为 EC2 实例卷恢复是灾难恢复 (DR) 的重要组成部分，AMS 会自动为您创建此内部故障排除 RFC。

创建内部疑难解答 RFC 后，会显示一个横幅，为您提供指向 RFC 的链接。此内部故障排除 RFC 可让您更清楚地了解 RFC 故障，与其提交 RFCs 导致相同错误的重试或手动联系 AMS 解决此故障，不如跟踪更改并知道 AMS 正在处理故障。这也降低了他们变更的 time-to-recovery (TTR) 指标，因为 AMS 操作员会主动处理 RFC 故障，而不是等待您的请求。

如何获得有关 RFC 的帮助

您可以联系 AMS 以确定失败的根本原因。AMS 的工作时间为每年 365 天、每周 7 天、每天 24 小时。

AMS 提供了多种途径供您寻求帮助或提出服务请求。

- 要询问信息或建议，或访问 AMS 托管的 IT 服务，或向 AMS 申请其他服务，请使用 AMS 控制台并提交服务请求。有关详细信息，请参阅创建服务请求。有关 AMS 服务请求的一般信息，请参阅服务请求管理。
- 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 控制台并提交事件报告。有关详细信息，请参阅报告事件。有关 AMS 事件管理的一般信息，请参阅事件响应。
- 有关您或您的资源或应用程序如何使用 AMS 的具体问题，或者要升级事件，请通过电子邮件发送以下一项或多封电子邮件：
  1. 首先，如果您对服务请求或事件报告回复不满意，请发送电子邮件至 CSDM：ams-csdm@amazon.com
  2. 接下来，如果需要升级，你可以发送电子邮件给 AMS 运营经理（但你的 CSDM 可能会这样做）：ams-opsmanager@amazon.com
  3. 进一步升级将向 AMS 局长提出：ams-director@amazon.com
  4. 最后，你可以随时联系 AMS 副总裁：ams-vp@amazon.com

AMS 中的直接更改模式

主题

- 直接更改模式入门
- 安全性和合规性

- 直接更改模式下的变更管理
- 使用 “直接更改” 模式创建堆栈
- 直接更改模式用例

AWS Managed Services (AMS) 直接变更模式 (DCM) 通过提供对 AMS Advanced Plus 和高级账户的本机 AWS 访问权限来配置和更新 AWS 资源，从而扩展了 AMS 高级变更管理。使用 DCM，您可以选择使用原生 AWS API（控制台或 CLI/SDK）或 AMS Advanced 变更管理请求进行更改（RFCs），无论哪种情况，AMS 都完全支持资源及其更改，包括监控、补丁、备份、事件响应管理。通过 DCM 配置的资源在 AMS 服务知识管理系统 (SKMS) 中注册，加入 AMS 托管 Active Directory 域（如果适用），并运行 AMS 管理代理。使用现有工具（例如 SDK 和 CD AWS K）开发和部署 AMS CloudFormation 管理的堆栈。 CloudFormation

> **Note**
>
> 直接更改模式不会删除 AMS 变更管理 RFCs。通过 DCM，您可以完全访问 AM RFCs S。

观看 Akash 的视频以了解更多信息 (6:30)

直接更改模式入门

首先检查先决条件，然后在符合条件的 AMS Advanced 账户中提交变更申请 (RFC)。

1. 确认您要在 DCM 中使用的账户是否符合要求：
   - 该账户是 AMS 高级增强版或高级版。
   - 该账户未启用 Service Catalog。我们目前不支持同时登录 DCM 和 Service Catalog 的账号。如果您已加入 Service Catalog 但对 DCM 感兴趣，请与您的云服务交付经理 (CSDM) 讨论您的需求。如果您决定从 Service Catalog 切换到 DCM，请在下面的变更请求中加入询问。有关 AMS 中的服务目录的详细信息，请参阅 AMS 和服务目录。
2. 使用管理 | 托管账户 | 直接更改模式 | 启用更改类型 (ct-3rd4781c2nnhp) 提交变更申请 (RFC)。有关演练示例，请参阅直接更改模式 | 启用。

   处理 CT 后，将在指定账户中配置预定义`AWSManagedServicesUpdateRole`的 IAM 角色`AWSManagedServicesCloudFormationAdminRole`和。
3. 使用您的内部联合流程为需要 DCM 访问权限的用户分配相应的角色。

> **Note**
>
> 您可以指定任意数量的 SAMLIdentity提供商、 AWS 服务和 IAM 实体（角色、用户等）来担任这些角色。您必须至少提供一个：SAMLIdentityProviderARNsIAMEntityARNs、或AWSServicePrincipals。有关更多信息，请咨询贵公司的 IAM 部门或 AMS 云架构师 (CA)。

直接更改模式 IAM 角色和策略

在账户中启用直接更改模式后，将部署以下新的 IAM 实体：

AWSManagedServicesCloudFormationAdminRole：此角色授予访问 CloudFormation 控制台、创建和更新 CloudFormation 堆栈、查看偏差报告以及创建和执行 CloudFormation ChangeSets的权限。此角色的访问权限由您的 SAML 提供商管理。

部署并附加到角色的托管策略AWSManagedServicesCloudFormationAdminRole有：

- AMS 高级多账号 landing zone (MALZ) 应用程序账户
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - 此策略代表授予的权限AWSManagedServicesCloudFormationAdminRole。您和合作伙伴使用此政策授予对账户中现有角色的访问权限，并允许该角色启动和更新账户中的 CloudFormation 堆栈。这可能需要额外的 AMS 服务控制策略 (SCP) 更新，以允许其他 IAM 实体启动 CloudFormation 堆栈。
- AMS 高级单账号 landing zone (SALZ) 账户
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3 次访问 [内联政策]
  - AWS ReadOnlyAccess 政策

AWSManagedServicesUpdateRole：此角色授予对下游 AWS 服务的受限访问权限 APIs。该角色采用托管策略部署，这些策略提供变更和非变更的 API 操作，但通常限制针对某些服务（例如 IAM、KMS、GuardDuty VPC、AMS 基础设施资源和配置等Create/Delete/PUT）的变更操作（例如）。 此角色的访问权限由您的 SAML 提供商管理。

部署并附加到角色的托管策略AWSManagedServicesUpdateRole有：

- AMS 高级多账号 landing zone 应用程序账号
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2而且 RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策
- AMS 高级单账号 landing zone 账号
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2而且 RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策 1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策 2

除此之外，托管策略`AWSManagedServicesUpdateRole`角色还`ViewOnlyAccess`附加了 AWS 托管策略。

安全性和合规性

安全与合规是 AMS Advanced 和您作为我们的客户的共同责任。AMS Advanced Direct Change 模式不会更改此项共同责任。

直接更改模式下的安全性

AMS Advanced 通过规范性的着陆区、变更管理系统和访问管理提供了额外的价值。使用 “直接变更” 模式时，此责任模型不会改变。但是，您应该注意其他风险。

直接更改模式 “更新” 角色（参见直接更改模式 IAM 角色和策略）提供了提升的权限，允许有权访问该角色的实体更改您账户中由 AMS 支持的服务的基础设施资源。权限提升后，会存在不同的风险，具体取决于资源、服务和操作，尤其是在由于疏忽、错误或缺乏对内部流程和控制框架的遵守而导致错误更改的情况下。

根据AMS技术标准，已经确定了以下风险并提出了以下建议。有关 AMS 技术标准的详细信息可通过以下网址获取 AWS Artifact。要进行访问 AWS Artifact，请联系您的 CSDM 获取说明或前往入门。 AWS Artifact

AMS-STD-001：标记

标准	它坏了吗	风险	建议
所有 AMS 拥有的资源都必须具有以下键值对 除上面列出的标签外，所有 AMS 拥有的标签都必须具有类似AMS*或MC*大小写的前缀。upper/lower/mix	是。中断了 CloudFormation、CloudTrail、EFS、OpenSearch、L CloudWatch ogs、SQS、S SM、Tagging api，因为这些服务不支持限制 AMS 命名空间标记的aws:TagsKey 条件。 下表 AMS-STD-003 中给出的标准说明您可以更改环境和 AppId AppName，但不能更改 AMS 拥有的资源。无法通过 IAM 权限实现。	在 AMS 方面，对 AMS 资源进行错误标记可能会对您的资源的报告、警报和修补操作产生不利影响。	必须限制访问权限，才能对 AMS 团队以外的任何人的 AMS 默认标签要求进行任何更改。
不得根据您的更改请求删除 AMS 拥有的堆栈上的任何标签。	是的。 CloudForm ation 不支持限制 AMS 命名空间标签的aws:TagsKey 条件。		
不允许您在基础设施中使用 AMS 标签命名约定，如下表 AMS-STD-002 所述。	是。breaks f CloudWatch or CloudForm ation CloudTrai l、、Amazon Elastic File System (EFS) OpenSearc h、、Logs、A mazon Systems		

标准	它坏了吗	风险	建议
	Queue S EC2 ervice (SQS)、Amazon Systems Manager (SSM)、标记 API；这些服务不支持`aws:TagsKey` 限制 AMS 命名空间标记的条件。		

AMS-STD-002：身份和访问管理 (IAM) Access Management

标准	它坏了吗	风险	建议
4.7 不得允许绕过变更管理流程 (RFC) 的操作，例如启动或停止实例、创建 S3 存储桶或 RDS 实例等。只要在分配的角色范围内执行操作，开发者模式账户和自助服务预置模式服务 (SSP) 就可以获得豁免。	是。自助操作的目的允许您绕过 AMS RFC 系统执行操作。	安全访问模式是 AMS 的核心技术方面，用于控制台或编程访问的 IAM 用户可以规避这种访问控制。AMS 变更管理不监控 IAM 用户的访问权限。访问权限 CloudTrail 仅限登录。	IAM 用户应有时间限制，并根据最低权限向其授予权限。 need-to-know

AMS-STD-003：网络安全

标准	它坏了吗	风险	建议
S2。 EC2 实例上的弹性 IP 只能与正式的风险接受协议或内部团队的有效用例一起使用。	是。自助操作允许您关联和取消关联弹性 IP 地址 (EIP)。	向实例添加弹性 IP 会使其暴露在互联网上。这增加了信息泄露和未经授权活动的风险。	通过安全组阻止任何不必要的流量进入该实例，并验证您的安全组是否与该实例相连，以确保该实例仅

标准	它坏了吗	风险	建议
			在出于业务原因需要时才允许流量。
S14。可以允许属于同一客户的账户之间的 VPC 对等连接和终端节点连接。	是。无法通过 IAM 策略实现。	离开您的 AMS 账户的流量一旦超出账户边界，就不会受到监控。	我们建议仅与您拥有的 AMS 账户建立对等关系。如果您的用例需要这样做，请使用安全组和路由表来限制可以通过相关连接输出的流量范围、资源和类型。
AMS 基础 AMIs 可以在 AMS 管理的账户和非托管账户之间共享，前提是我们可以验证它们归同一个组织所有。 AWS		AMIs 可能包含敏感数据，并且可能会泄露给非预期的帐户。	仅 AMIs 与您的组织拥有的账户共享，或者在组织外部共享之前验证用例和账户信息。

AMS-STD-007：日志记录

标准	它坏了吗	风险	建议
19. 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。	是。由于无法通过 IAM 策略验证客户账户属于同一个组织，因此客户日志可能不安全。	日志可能包含敏感数据，并且可能会泄露给非预期的帐户。	仅与组织管理的账户共享日志，或者在 AWS 组织外部共享之前验证用例和账户信息。我们可以通过多种方式进行验证，请咨询您的云服务交付经理 (CSDM)。
20。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账户，或者将电子邮件域名与客户的公司名称和 PAYER 关联 AWS Organizat			

标准	它坏了吗	风险	建议
ions 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。			

与您的内部授权和身份验证团队合作，相应地控制直接更改模式角色的权限。

直接更改模式下的合规性

直接更改模式与生产和非生产工作负载兼容。您有责任确保遵守任何合规标准（例如 PHI、HIPAA、PCI），并确保直接变更模式的使用符合您的内部控制框架和标准。

直接更改模式下的变更管理

变更管理是 AMS Advanced 用来实施变更请求的流程。变更请求 (RFC) 是由您或 AMS Advanced 通过 AMS Advanced 界面创建的对托管环境进行更改的请求，其中包含特定操作的 AMS 高级更改类型 (CT) ID。有关更多信息，请参阅变更管理。

> **Note**
>
> 直接更改模式不会移除 AMS 变更管理 RFCs，您仍然可以使用 DCM 完全访问 AMS RFCs 。

AMS Direct Change 模式 (DCM) 通过提供对 AMS Advanced Plus 和高级账户的本机 AWS 访问权限来配置和更新 AWS 资源，从而扩展了 AMS 高级变更管理。通过 IAM 角色获得直接更改模式权限的用户可以使用原生 AWS API 访问权限在其 AMS Advanced 账户中配置和更改资源。用户仍然可以使用相同的 IAM 角色 RFCs 使用 AMS 高级变更管理。在这两种情况下，AMS 都完全支持资源及其更改，包括监控、补丁、备份、事件响应管理。在这些账户中没有适当角色的用户必须使用 AMS Advanced 变更管理 RFC 流程进行更改。

变更管理用例

出于安全考虑，AMS Advanced 中的某些更改只能通过变更管理变更申请 (RFC) 流程来完成。`AWSManagedServicesCloudFormationAdminRole`仅限于通过 CloudFormation (CFN) 采取的行动。有关如何通过 DCM 创建堆栈的更多信息，请参阅使用 Direct Change 模式创建堆栈。`AWSManagedServicesUpdateRole`仅限于以下操作。

有关每种变更类型的演练，包括管理 | 托管账户 | 直接更改模式 | 启用 (ct-3rd4781c2nnhp) 变更类型，请参阅 “其他信息” 部分，了解按分类划分的高级更改类型参考变更类型部分的相关变更类型。

服务	操作
AWS Key Management Service (AWS KMS)	更新
AWS Certificate Manager	创建
AWS Identity and Access Management (IAM)	任何
Site-to-Site VPN	任何
AMS 资源调度器	
AWS Backup	创建备份计划
AMS 工作负载接入 () WIGs	任何
AMS 出口过滤（托管帕洛阿尔托）	
AMS 高级 MALZ 账户变更	
Amazon GuardDuty	
AMS 高级堆栈访问权限	任何
亚马逊 Elastic Block Store (EBS) 交易量	删除
亚马逊 Elastic Block Store (EBS) 默认加密	启用默认加密
亚马逊弹性计算云（亚马逊 EC2）	更改主机名
亚马逊机器映像（AMI）	删除、分享
亚马逊 EC2 安全组	任何
AMS 高级 SSP	
AWS 微软 AD 托管	
AMS 高级开发者模式	

服务	操作
Amazon Simple Storage Service（Amazon S3）	创建 S3 存储桶策略
AWS Systems Manager	创建

使用 “直接更改” 模式创建堆栈

为了让 AMS 管理堆栈`AWSManagedServicesCloudFormationAdminRole`，在 CloudFormation 使用中启动堆栈时有两个要求：

- 模板必须包含`AmsStackTransform`。
- 堆栈名称必须以前缀开头，`stack-`后跟一个 17 个字符的字母数字字符串。

> **Note**
>
> 要成功使用`AmsStackTransform`，您必须确认您的堆栈模板包含相应`CAPABILITY_AUTO_EXPAND`功能，以便 CloudFormation (CFN) 创建或更新堆栈。为此，您可以将`CAPABILITY_AUTO_EXPAND`作为创建堆栈请求的一部分传递。如果模板中包含此功能时未确认此功能，则 CFN 会拒绝该请求。`AmsStackTransform`如果您的模板中有转换，CFN 控制台可确保您通过此功能，但是当您通过 CFN 控制台与 CFN 进行交互时，可能会错过此功能。 APIs
>
> 无论何时使用以下 CFN API 调用，都必须通过此功能：
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

使用 DCM 创建或更新堆栈时，将在堆栈上执行 CFN Ingest 和堆栈更新的 CTs 相同验证和增强，有关更多信息，请参阅载CloudFormation 入指南、最佳实践和限制。唯一的例外是，AMS 默认安全组 (SGs) 不会附加到 Auto Scaling 组中的任何独立 EC2 EC2 实例或 Auto Scaling 组 (ASGs) 中的实例。使用独立 EC2 实例或创建 CloudFormation 模板时 ASGs，可以附加默认实例 SGs。

> **Note**
>
> 现在可以使用创建和管理 IAM 角色AWSManagedServicesCloudFormationAdminRole。

AMS 默认 SGs 具有入口和出口规则，允许实例成功启动，并允许稍后由 AMS 操作和您通过 SSH 或 RDP 进行访问。如果您发现 AMS 的默认安全组过于宽松，则可以创建自己的安全组，并 SGs 使用更严格的规则将其附加到您的实例，前提是它仍然允许您和 AMS 操作人员在事件发生期间访问该实例。

AMS 的默认安全组如下：

- SentinelDefaultSecurityGroupPrivateOnly: 可以通过此 SSM 参数在 CFN 模板中进行访问 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: 可以通过此 SSM 参数在 CFN 模板中进行访问 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 转型

在 CloudFormation 模板`Transform`中添加声明。这将添加一个 CloudFormation 宏，用于在启动时验证堆栈并将其注册到 AMS。

JSON 示

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

YAML 示例

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

在更新现有堆栈的模板时，还要添加该`Transform`语句。

JSON 示

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML 示例

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
```

```
      TopicName: !Ref TopicName
```

堆栈名称

堆栈名称必须以前缀开头，stack-后跟一个 17 个字符的字母数字字符串。这是为了保持与在 AMS 堆栈上运行的其他 AMS 系统的兼容性 IDs。

以下是生成兼容堆栈的方法示例 IDs：

Bash：

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python：

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell：

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

直接更改模式用例

以下是直接更改模式的用例：

通过以下方式提供和管理资源 CloudFormation

- 整合 CloudFormation基于现有工具和流程。

持续的资源管理和更新

- 原子变化小，风险低。
- 本来需要通过手动或自动 RFC 进行的更改。
- 需要原生 AWS API 访问权限的工具。
- 如果您处于迁移阶段，则可以使用 DCM 角色。迁移团队利用 DCM 的权限来创建或修改堆栈。

- DCM 角色可以在 CI/CD 管道中用于构建新角色 AMIs、创建 Amazon ECS 任务等。

AMS 高级开发者模式

主题

AWS Managed Services (AMS) 开发者模式使用 AMS 高级增强版和高级版账户中的提升权限在 AMS 高级变更管理流程之外配置和更新 AWS 资源。AMS 高级开发人员模式通过利用 AMS 高级虚拟私有云 (VPC) 中的原生 AWS API 调用来实现这一点，使您能够在托管环境中设计和实施基础设施和应用程序。

使用启用了开发者模式的账户时，将为通过 AMS 高级变更管理流程或使用 AMS Amazon 系统映像 (AMI) 配置的资源提供连续性管理、补丁管理和变更管理。但是，这些 AMS 管理功能不适用于通过本机 AWS APIs配置的资源。

您负责监控在 AMS Advanced 变更管理流程之外配置的基础设施资源。开发者模式与生产和非生产工作负载兼容。有了更高的权限，您就有更多的责任来确保遵守内部控制。

> **Important**
>
> 只有使用 AMS Advanced 变更管理流程创建您使用开发者模式创建的资源才能由 AMS Advanced 管理。

开发者模式是您可以采用的 AMS 高级模式之一。有关更多信息，请参阅 模式概述。

AMS 高级开发者模式入门

了解使用 AMS 高级开发者模式的各种 AMS 高级账户以及如何成功实现开发者模式。

主题

开始使用 AMS 开发者模式之前

在实现开发者模式之前，你应该知道几件事。

AMS Advanced 无法管理在 AMS Advanced 变更管理流程之外通过变更请求创建的 DevMode 账户中的现有堆栈或资源 (RFCs)。但是，当账户处于开启状态时 DevMode，AMS Advanced 将继续使用管理通过 AMS Advanced 变更管理流程配置的 RFCs资源。

您不能先使用 DevMode 账户，然后再将其转换为 AMS Advanced 管理的应用程序账户。

AMS 开发者模式的先决条件

以下是实现开发者模式的先决条件：

- 您必须是 AMS Advanced 客户，并且至少有一个已注册的 AMS Advanced Plus 或高级账户。
- 您使用的任何账户都必须是 AMS Advanced Plus 或高级账户。
- 多账户登录区 (MALZ)：您必须使用`AWSManagedServicesDevelopmentRole`预定义的 AWS Identity and Access Management (IAM) 角色。你申请这个角色。下一节介绍如何获取开发者模式权限。
- 单账户登录区 (SALZ)：您必须使用`customer_developer_role`预定义的 AWS Identity and Access Management (IAM) 角色。你申请这个角色。下一节介绍如何获取开发者模式权限。

如何实现 AMS 高级开发者模式

您可以通过请求为符合条件的 AMS Advanced 账户配置预定义的 IAM 角色来实现开发者模式：

- MALZ：`AWSManagedServicesDevelopmentRole`

- SALZ：customer_developer_role

然后，您将该角色分配给联合网络中的相关用户。

AMS Advanced 建议您确保开发者模式的使用符合您的内部控制框架和标准，因为开发者模式会带来两个变革向量：AMS Advanced 管理的资源的 AMS Advanced 变更管理以及针对您（作为我们的客户）管理的资源的客户管理角色联合。虽然 AMS Advanced 流程仍然符合我们的声明，但可能需要更新客户流程和控制框架。

在您的 AMS 高级账户中实现开发者模式

1. 确认您要在开发者模式下使用的账户符合中列出的要求AMS 开发者模式的先决条件。
2. 使用变更类型 (CT) 管理 | 托管账户 | 开发者模式 | 启用（需要审核）提交变更申请 (RFC)。有关如何使用此 CT 的示例，请参阅开发者模式 | 启用（需要审阅）。

   处理 CT 后，将在请求的账户中配置预定义的 IAM 角色（AWSManagedServicesDevelopmentRole对customer_developer_role于 M ALZ，对于 SALZ）。
3. 使用您的内部联合流程为需要开发者模式访问权限的用户分配相应的角色。

   AMS Advanced 建议您限制访问权限，以防止不必要或未经批准地配置或更改资源。

AMS 高级开发者模式权限

预定义角色（适用AWSManagedServicesDevelopmentRole于 MALZ，customer_developer_role对于 SALZ）授予在 AMS 高级 VPC 中创建应用程序基础设施资源的权限，包括 IAM 角色，同时限制访问由 AMS Advanced 运营的共享服务组件（例如，管理主机、域控制器、趋势科技 EPS、堡垒和不支持的 AWS 服务）。该角色还限制对以下内容的访问 AWS 服务：Amazon GuardDuty、 AWS Organizations AWS Directory Service APIs、和 AMS 高级日志。

虽然该角色允许您创建其他 IAM 角色，但开发人员模式访问权限中包含的相同权限限制也适用于由创建的任何 IAM 角色AWSManagedServicesDevelopmentRole。

开发者模式下的安全性与合规性

安全与合规是 AMS Advanced 和您作为我们的客户的共同责任。AMS Advanced Developer 模式将您在变更管理流程之外配置的资源或通过变更管理配置但使用开发者模式权限更新的资源的共同责任转移给您。有关分担责任的更多信息，请参阅 AWS Managed Services。

注意事项：

- DevMode 允许您和您的授权团队绕过 AMS 安全的核心 deny-by-default原则。必须权衡自助服务、减少等待 AMS 的优点和缺点，任何人都可以在安全团队不知情的情况下执行意想不到的破坏性操作。用于启用开发模式和直接更改模式的自动更改类型已公开，您组织中的任何授权人员都可以运行这些类型 CTs 并启用这些模式。
- 您负责从您的用户群中管理 CT 执行权限。
- AMS 不管理 CT 执行权限

建议

- 保护
  - 客户可以通过权限阻止访问此 CT，请参阅使用 IAM 角色策略声明限制权限
  - 通过实施代理（例如 ITSM 系统）来阻止对此 CT 的访问
  - 利用服务控制策略 (SCPs)，根据需要阻止策略和行为，请参阅 AMS Preventical 和 Detective Control s 库
- 检测
  - 监视你的 RFC 是否正在执行这些内容 CTs （启用开发者模式 ct-1opjmhuddw194 和直接更改模式，启用 ct-3rd4781c2nnhp）并做出相应的响应
  - 查看 and/or 您的账户是否存在 IAM 资源，以确定部署了开发者模式或直接变更模式的账户
- 回应
  - 根据需要在开发者模式下移除账户

开发者模式下的安全性

AMS Advanced 通过规范性的着陆区、变更管理系统和访问管理提供了额外的价值。使用开发者模式时，AMS Advanced 的安全值通过使用与标准 AMS Advanced 账户相同的账户配置来保持 AMS Advanced 的安全值，该账户配置与 AMS Advanced 的基准安全强化网络相同。网络受角色中强制执行的权限边界的保护（`AWSManagedServicesDevelopmentRole`对于 MALZ，`customer_developer_role`对于 SALZ），这限制了用户破坏在设置账户时建立的参数保护。

例如，具有该角色的用户可以访问 Amazon Route 53，但是 AMS 高级内部托管区域受到限制。对创建的 IAM 角色强制执行相同的权限边界`AWSManagedServicesDevelopmentRole`，从而限制用户破坏账户加入 AMS Advanced 时建立的参数保护。`AWSManagedServicesDevelopmentRole`

开发者模式下的合规性

开发者模式与生产和非生产工作负载兼容。您有责任确保遵守任何合规标准（例如 PHI、HIPAA、PCI），并确保开发人员模式的使用符合您的内部控制框架和标准。

开发者模式下的变更管理

变更管理是 AMS Advanced 服务用来实施变更请求的流程。变更请求 (RFC) 是您或 AMS Advanced 通过 AMS Advanced 界面创建的对托管环境进行更改的请求，其中包括特定操作的更改类型 (CT) ID。有关更多信息，请参阅 更改管理模式。

在授予开发者模式权限的 AMS Advanced 账户中，不强制执行变更管理。已获得 IAM 角色的开发者模式权限（`AWSManagedServicesDevelopmentRole`适用于 MALZ、`customer_developer_role` SALZ）的用户可以使用原生 AWS API 访问权限在其 AMS 高级账户中配置和更改资源。在这些账户中没有相应角色的用户必须使用 AMS Advanced 变更管理流程进行更改。

> **Important**
>
> 只有使用 AMS Advanced 变更管理流程创建您使用开发者模式创建的资源才能由 AMS Advanced 管理。对于在 AMS Advanced 变更管理流程之外创建的资源，提交给 AMS Advanced 的更改请求会被 AMS Advanced 拒绝，因为这些请求必须由您处理。

自助配置服务 API 限制

开发者模式支持所有 AMS Advanced 自行配置服务。对自行配置服务的访问受每项服务的相应用户指南部分中概述的限制。如果您的开发者模式角色无法使用自行配置的服务，则可以通过开发者模式更改类型请求更新的角色。

以下服务不提供对服务的完全访问权限 APIs：

自配服务在开发者模式下受到限制

服务	备注
Amazon API Gateway	允许所有网关 APIs 呼叫，但以下情况除外`SetWebACL` 。
Application Auto Scaling	只能注册或取消注册可扩展目标，以及放置或删除扩展策略。

服务	备注
AWS CloudFormation	无法访问或修改名称前缀为的 CloudFormation 堆栈。`mc-`
AWS CloudTrail	无法访问或修改名称前缀为的 CloudTrail 资源。`ams-` and/or `mc-`
Amazon Cognito（用户池）	无法关联软件令牌。 无法创建用户池、用户导入任务、资源服务器或身份提供商。
AWS Directory Service	`Connect`和`WorkSpaces` 服务只需要 Directory Service 执行以下操作。开发者模式权限边界策略拒绝所有其他 Directory Service 操作： • `ds:AuthorizeApplication` • `ds:CreateAlias` • `ds:CreateIdentityPoolDirectory` • `ds:DeleteDirectory` • `ds:DescribeDirectories` • `ds:GetAuthorizedApplication Details` • `ds:ListAuthorizedApplications` • `ds:UnauthorizeApplication` 在单账户 landing zone 账户中，边界策略明确拒绝访问 AMS Advanced 用于维护对启用开发模式的账户的访问权限的 AMS Advanced 托管目录。

服务	备注
Amazon Elastic Compute Cloud	无法访问包含以下字符串 EC2 APIs 的 Amazon：DhcpOptions Gateway、Subnet、VPC、和VPN。 无法访问或修改标签前缀为AMS、、mcManagementHostASG 、 and/or sentinel的 Amazon EC2 资源。
亚马逊 EC2 （报告）	仅授予查看权限（不能修改）。注意：Amazon EC2 Reports 正在更新。“报告” 菜单项将从 Amazon EC2 控制台导航菜单中删除。要在删除后查看您的 Amazon EC2 使用情况报告，请使用 AWS Billing 和成本管理控制台。
AWS Identity and Access Management (IAM)	无法删除现有权限界限，也无法修改 IAM 用户密码策略。 除非您使用正确的 IAM 角色（对于 MALZ，对AWSManagedServicesDevelopmentRole 于 S ALZ），customer_developer_role 否则无法创建或修改 IAM 资源。 无法修改前缀为:ams、、mccustomer_deny_policy 、 and/or sentinel的 IAM 资源。 创建新的 IAM 资源（角色、用户或群组）时，必须附加权限边界（MALZ: AWSManagedServicesDevelopmentRolePermissionsBoundary 、SALZ:ams-app-infra-permissions-boundary ）。
AWS Key Management Service (AWS KMS)	无法访问或修改 AMS 高级管理的 KMS 密钥。
AWS Lambda	无法访问或修改前缀为的 AWS Lambda 函数。AMS

服务	备注
CloudWatch 日志	无法访问名称前缀为:mc、、awslambda、 and/or AMS的 CloudWatch 日志流。
Amazon Relational Database Service (Amazon RDS)	无法访问或修改名称前缀为:mc-的亚马逊关系数据库服务 (Amazon RDSDBs) 数据库 ()。
AWS Resource Groups	只能访问GetList、和Search资源组 API 操作。
Amazon Route 53	无法访问或修改 Route53 AMS 高级维护的资源。
Amazon S3	无法访问名称前缀为:ams-*、、ams或的 Amazon S3 存储桶。ms-a mc-a
AWS Security Token Service	唯一允许的安全令牌服务 API 是DecodeAuthorizationMessage 。
Amazon SNS	无法访问名称前缀为:AMS-Energon-Topic 、或的 SNS 主题。MMS-Topic
AWS Systems Manager 经理 (SSM)	无法修改以ams、mc或为前缀的 SSM 参数。svc 无法SendCommand 对标签前缀为或的 Amazon EC2 实例使用 SSM API。ams mc
AWS 标记	您只能访问前缀为的 AWS 标记 API 操作。Get

服务	备注
AWS Lake Formation	以下 AWS Lake Formation API 操作被拒绝： • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	您只能调用 Elastic Inference API 操作。`elastic-inference:Connect` 此权限包含在`customer_sagemaker_admin_policy` 所附的权限中`customer_sagemaker_admin_role` 。此操作允许您访问 Elastic Inference 加速器。
AWS Shield	无法访问任何此服务 APIs 或控制台。
Amazon Simple Workflow Service	无法访问任何此服务 APIs 或控制台。

在 AMS 开发者模式下配置基础架构

在启用开发者模式的账户中`AWSManagedServicesDevelopmentRole`，没有开发者模式 IAM 角色的用户必须遵循利用 AMS Advanced 的 AMS 高级变更管理流程。 AMIs角色正确（MALZ: **`AWSManagedServicesDevelopmentRole`**、SALZ:`customer_developer_role`）的用户可以使用 AMS Advanced 变更管理系统和 AMS Advanced， AMIs 但不是必需的。

> **Note**
>
> 未通过 AWS AMS 高级工作负载摄取处理或在 AMS 高级账户中创建的 AMI 将不包含 AMS Advanced 所需的配置。

AMS 开发者模式下的 Detective 控件

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM 获取说明或前往 AWS Artifact 入门。

在 AMS 开发者模式下记录、监控和事件管理

对于在 AMS Advanced 变更管理流程之外配置的资源，或者通过变更管理配置然后由使用开发者模式权限的账户更改的资源，不可使用记录、监控和事件管理。

AMS 开发者模式下的事件管理

事件响应时间没有变化。对于在变更管理流程之外配置的资源，或者通过变更管理配置的资源，然后由使用开发者模式权限的账户进行更改，应尽力解决事件。

> **Note**
>
> AMS 服务等级协议 (SLA) 不适用于在 AMS 变更管理系统之外创建或更新的资源（包括更改请求或 RFCs），包括开发人员模式；因此，在开发者模式下更新或创建的资源会自动降级为 P3，AMS 支持是尽力而为。

AMS 开发者模式下的补丁管理

补丁管理不适用于在 AMS Advanced 变更管理流程之外置备的资源，也不可用于通过变更管理配置然后由使用开发者模式权限的账户更改的资源。修补时间：

- 对于重要的安全更新：供应商发布通过变更管理配置然后由使用开发者模式权限的账户更改的资源后 10 个工作日内。
- 重要更新：供应商发布通过变更管理配置的资源，然后由使用开发者模式权限的账户进行更改的资源后 2 个月内。

AMS 开发人员模式下的连续性管理

连续性管理不适用于在 AMS Advanced 变更管理流程之外配置的资源，也不可用于通过变更管理配置然后由使用开发者模式权限的账户更改的资源。

对于在 AMS Advanced 变更管理流程之外配置的资源，或者对于通过变更管理配置然后由使用开发者模式权限的账户更改的资源，环境恢复启动时间可能长达 12 小时。

AMS 开发者模式下的安全和访问管理

防恶意软件保护是指您对在 AMS Advanced 变更管理流程之外配置的资源，或者对通过变更管理配置然后由使用开发者模式权限的账户更改的资源的责任。对未通过 AMS 高级变更管理配置的亚马逊弹性计算云 (Amazon EC2) 实例的访问可能由密钥对控制，而不是提供联合访问权限。

AMS 中的自助服务配置模式

AWS Managed Services (AMS) 自助服务配置 (SSP) 模式提供对 AMS 托管账户中原生 AWS 服务和 API 功能的完全访问权限。您可以通过标准化的、范围缩小的 AWS Identity and Access Management 角色来访问服务。AMS 提供服务请求和事件管理。警报、监控、记录、修补、备份和变更管理是您的责任。在许多情况下，自助服务配置服务 (SSP) 是自我管理或无服务器的，不需要管理某些操作任务，例如修补。在 AMS 护栏定义的环境边界内使用这些服务将使您受益，任何 IAM 更改（包括服务关联角色、服务角色、跨账户角色或策略更新）都需要获得 AMS Operations 的批准，以维护平台的基准安全性。您可以利用 CloudFormation 模板自动部署这些服务，但并非所有 SSP 服务都支持此功能。

> **Important**
>
> 在您的 AWS Managed Services (AMS) 账户中使用 SSP 模式访问和使用 AWS 服务，但限制如上所述。

在您 AWS 服务 的 AMS 账户中，有些无需管理 AMS 即可使用。本节介绍了自助服务配置模式服务（简称 SSP）、如何将它们添加到您的 AMS 账户以及 FAQs 每项服务。

自助配置服务按原样提供，您负责管理这些服务。AMS 不为与这些服务相关的资源提供警报、监控、日志记录或修补。AMS 提供 IAM 角色，使您能够安全地使用 AMS 账户中的服务。AMS SLAs 不适用。

对于您通过自助服务配置的资源，AMS 通过服务请求提供事件管理、侦探控制和护栏、报告、指定资源（云服务交付经理和云架构师）、安全和访问权限以及技术支持。此外，在适用的情况下，您负责在 AMS 变更管理系统之外配置或配置的资源的连续性管理、补丁管理、基础设施监控和变更管理。

AMS 中的 SSP 模式入门

自助配置是您可以使用的多账户着陆区 (MALZ) 的 AMS 模式之一。有关更多信息，请参阅 模式概述。

为了提供自助服务配置功能，AMS 创建了具有权限界限的提升的 IAM 角色，以限制直接 AWS 服务访问的意外更改。这些角色并不能阻止所有更改，您必须遵守内部控制和合规政策，并验证所有 AWS 服务 使用的角色是否符合所需的认证。这是自助配置模式。有关 AWS 合规性要求的详细信息，请参阅AWS 合规性。

要向您的多账户 landing zone Application 账户添加自助配置 AWS 服务，请按照服务的说明使用管理 | 服务 | 自配置服务 | 添加变更类型 (CT)，即需要审阅的 CT 或自动 CT。

> **Note**
>
> 要请求 AMS 提供额外的自助服务配置服务，请提交服务请求。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon API Gateway

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon API Gateway 功能。Amazon API Gateway 是一项完全托管的服务，让开发人员可以轻松地以任何规模创建、发布、维护、监控和保护 APIs 。使用 AWS 管理控制台 可以创建 REST WebSocket APIs ，它可以作为应用程序访问后端服务的数据、业务逻辑或功能的前门，例如在亚马逊弹性计算云 (Amazon EC2) 上运行的工作负载、在上面运行的代码AWS Lambda、任何 Web 应用程序或实时通信应用程序。

API Gateway 可处理接受和处理多达数十万个并发 API 调用所涉及的所有任务，包括流量管理、授权和访问控制、监控以及 API 版本管理。API Gateway 没有最低费用或启动成本。您只需为收到的 API 调用和传出的数据量付费，而且，借助 API Gateway 分层定价模型，您可以随着 API 使用量的扩大而降低成本。要了解更多信息，请参阅 Amazon API Gateway。

常见问题：AMS 中的 API Gateway

问：如何使用我的 AMS 账户申请访问亚马逊 API Gateway？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 API Gateway。此 RFC 为您的账户配置以下 IAM 角色：`customer_apigateway_author_role`和。`customer_apigateway_cloudwatch_role`在您的账户中配置后，您必须在联合解决方案中加入角色。

问：在我的 AMS 账户中使用 Amazon API Gateway 有哪些限制？

- API Gateway 配置仅限于不带前缀AMS-或MC-前缀的资源，以防止对 AMS 基础设施进行任何修改。
- CREATE的权限已禁 VPCLink 用，以防止不受监管地创建弹性负载均衡器。如果 VPCLinks 需要，请参阅 App lication Load Balancer | Creat e。

问：在我的 AMS 账户中使用 Amazon API Gateway 有哪些先决条件或依赖关系？

这取决于你要部署的 API Gateway 的类型。它可以是独立服务，但也可以请求访问现有服务（例如，网络负载均衡器）。

使用 AMS SSP 在你的 AMS 账户中配置 Alexa for Business

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Alexa for Business 功能。Alexa for Business 是一项服务，可让您的组织和员工使用 Alexa 来完成更多工作。有了 Alexa for Business，你可以使用 Alexa 作为智能助手，在会议室、办公桌前，甚至使用已经在家中或旅途中使用的 Alexa 设备提高工作效率。IT 和设施经理可以使用 Alexa for Business 来衡量和提高工作场所现有会议室的利用率。

要了解更多信息，请参阅 Alexa for Business。

AWS Managed Services 中的 Alexa for Business 常见问题解答

问：如何使用我的 AMS 账户申请访问 Alexa for Business？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_alexa_console_role. 还customer_alexa_device_setup_user为 Alexa for Business 提供的设备设置工具创建了 A；然后可以使用此设备设置工具来设置您的设备。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

Alexa for Business 网关使您可以将 Alexa for Business 连接到思科 Webex 和 Poly Group 系列终端，从而使用语音控制会议。网关软件在您的本地硬件上运行，可以安全地将会议指令从 Alexa for Business 代理到您的思科终端。网关需要两对 AWS 凭据才能与 Alexa for Business 通信。我们提供两个访问受限的IAM用户：customer_alexa_gateway_installer_user以及customer_alexa_gateway_execution_user您的Alexa for Business网关，一个用于安装网关，一个用于操作网关；可以通过提交带有部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略（需要审查）更改类型 (ct-3dpd8mdd9jn1r) 的RFC来申请。

> **Note**
>
> 要生成使用情况报告并将其发送到 Amazon S3，请在自配置服务 RFC 中指定 Amazon S3 存储桶名称。

问：在我的 AMS 账户中使用 Alexa for Business 有哪些限制？

没有任何限制。Alexa for Business 的全部功能可通过 Alexa for Business 自行配置服务角色获得。

问：在我的 AMS 账户中使用 Alexa for Business 有哪些先决条件或依赖条件？

- 如果您打算使用 E WPA2 nterprise Wi-Fi 来设置共享设备，请在设备设置工具中指定此网络安全类型，该工具需要使用。 AWS 私有证书颁发机构
- AMS 仅创建以命名空间 “A4B” 开头的密钥。这仅限于此命名空间。

问：Alexa for Business 的哪些功能需要 RFCs单独使用？

要向 Alexa for Business 注册 Alexa 语音服务 (AVS) 设备，请提供对 Alexa 内置设备制造商的访问权限。为此，需要在 Alexa for Business 控制台中创建一个 IAM 角色，该角色可以使用管理 | 其他 | 其他更改类型进行部署。这允许 AVS 设备制造商代表您在 Alexa for Business 上注册和管理设备。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon AppStream 2.0

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon AppStream AppStream 2.0 (2.0) 功能。 AppStream 2.0 允许您将桌面应用程序移至 AWS，而无需重写它们。您可以在 AppStream 2.0 上安装应用程序，设置启动配置，并向用户提供应用程序。 AppStream 2.0 提供了多种虚拟机选项，因此您可以选择最符合应用程序要求的实例类型，并设置自动缩放参数，以便轻松满足最终用户的需求。 AppStream 2.0 使您能够在自己的网络中启动应用程序，这意味着您的应用程序可以与现有 AWS 资源进行交互。

Amazon AppStream 2.0 使您能够使用映像生成器快速轻松地安装、测试和更新应用程序。支持在微软 Windows Server 2012 R2、Windows Server 2016 或 Windows Server 2019 上运行的任何应用程序，你无需进行任何修改。测试完成后，您可以设置应用程序启动配置、默认用户设置，并发布图像以供用户访问。

要了解更多信息，请参阅 AppStream 2.0。

AppStream AWS Managed Services 常见问题中的 2.0

问：如何在 AMS 账户中申请访问 AppStream 2.0？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC，请求访问 AppStream 2.0。此 RFC 为您的账户配置以下 IAM 角色:`customer_appstream_console_role`.

还部署 A `customer_appstream_stream_role` 以流式传输要求用户使用 Active Directory 登录凭据进行身份验证的应用程序。

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：在我的 AMS 账户中使用 AppStream 2.0 有什么限制？

- 以下功能必须由 AMS Support 团队进行配置，并且需要特定 RFCs。有关请求其他功能的说明可在第 4 节中找到。
  - 从接口 VPC 终端节点创建和流式传输。
  - 支持 Amazon S3 终端节点，用于主文件夹和应用程序设置在私有网络上的持久性。
  - 创建并选择将在所有队列流实例上可用的 IAM 角色。
  - 加入 AppStream 2.0 舰队和图像生成器微软 Active Directory 域名。
  - 创建 AppStream 2.0 自定义使用情况报告。
  - 目前不支持自定义品牌。

问：在我的 AMS 账户中使用 AppStream 2.0 有哪些先决条件或依赖关系？

在向板载 AppStream 2.0 提交 RFC 时，请包括用于 AppStream 2.0 使用情况报告的 Amazon S3 存储桶名称。存储桶名称将添加到加`customer-appstream-usagereports-policy`载 AppStream 2.0 时创建的。

问：哪些 AppStream 2.0 功能需要单独使用 RFCs？

- 要为 AppStream 2.0 选择接口 VPC 终端节点，请提交管理 | 其他 | 其他 | 更新更改类型 RFC 以在您的账户中创建 VPC 终端节点。有关为 2.0 创建自定义终端节点的步骤，请参阅 AppStream 2.0 用户指南中的从接口 VPC 终端节点创建和流式传输。 AppStream
- 通过使用 “管理 | 其他 | 其他 | 其他 | 创建更改类型 RFC” 请求 Amazon S3 VPC 终端节点，即可配置对主文件夹和应用程序设置在私有网络上的持久性的支持。RFC 必须包括分别托管主文件夹内容的目标 Amazon S3 存储桶或应用程序设置 Amazon S3 存储桶。此 RFC 将为 AppStream 2.0 提

供其访问 Amazon S3 VPC 终端节点所需的权限。有关为流创建自定义终端节点的步骤，请参阅 AppStream 2.0 用户指南中的将 Amazon S3 VPC 终端节点用于主文件夹和应用程序设置持久性。

- 要创建和选择将在所有队列流实例上可用的 IAM 角色，请提交部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略（需要审查）更改类型 (ct-3dpd8mdd9jn1r) RFC 请求使用所需策略的 IAM 角色。IAM 角色名称应始终以前缀 “customer_appstream” 开头。
- 要将 Amazon AppStream 2.0 舰队和映像生成器加入到 Microsoft Active Directory 中的域中，可以在 Active Directory (AD) 中提交 “管理 | 其他 | 其他 | 其他 | 更新” 更改类型 RFC 以创建服务账户。加入 Microsoft Active Directory 所需的最低权限在授予创建和管理 Active Directory 计算机对象的权限的 AppStream 2.0 文档中定义。
- 要创建自定义 AppStream 2.0 使用情况报告，请提交管理 | 其他 | 其他 | 创建更改类型 RFC，请求以下内容：
  - “AppStreamUsageReports” CFN 堆栈创建
  - 在账户中配置 “customer_appstream_usagereports_role”
  - 此外，请提供以下详细信息：
    - 提供 CRON 表达式来安排 Crawler 运行。默认情况下，每天为世界标准时间 23:00。
    - 用于获取 Athena 查询结果的 Amazon S3 存储桶 ARN。这个存储桶应该有前缀：`aws-athena-query-results`
    - 适用于 AppStream 2.0 的 Amazon S3 存储桶 ARN 使用情况报告日志。

  配置角色后，将该角色加入您的联合解决方案并登录，然后使用使用情况报告角色访问 AWS GlueAWS Glue 和 Athena 以生成自定义报告。有关使用 AppStream 2.0 使用情况报告的详细信息，请参阅 2.0 文档中的创建自定义报告和分析 AppStream AppStream 2.0 使用情况数据。

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 Athena

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 Athena（Athena）功能。Athena 是一项交互式查询服务，可帮助您使用标准 SQL 分析 Amazon S3 中的数据。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。您指向 Amazon S3 中的数据，定义架构，然后开始使用标准 SQL 进行查询。大多数结果会在几秒钟内送达。有了 Athena，无需 extract-transform-load复杂的 (ETL) 任务来准备数据以供分析。这使得任何具有 SQL 技能的人都可以直接快速分析大规模数据集。要了解更多信息，请参阅亚马逊 Athena。

常见问题：AMS 中的 Athena

问：如何使用我的 AMS 账户申请访问亚马逊 Athena？

使用管理 AWS | 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Athena。此 RFC 为您的账户配置以下 IAM 角色:`customer_athena_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Athena 有哪些限制？

没有任何限制。您的 AMS 账户中提供亚马逊 Athena 的全部功能。

问：在我的 AMS 账户中使用 Amazon Athena 的先决条件或依赖条件是什么？

Athena 主要依赖 AWS Glue 该服务，因为它使用使用创建的数据。 catalog/metastore AWS Glue因此， AWS Glue 权限包含在成功的 Athena RFC 中。

该角色`customer_athena_console_role`具有 Amazon S3 存储桶的先决条件。要创建新的存储桶，请使用自动化 CT`ct-1a68ck03fn98r`（部署 | 高级堆栈组件 | S3 存储 | 创建）。当您使用此自动 CT 为 Athena 创建 S3 存储桶时，存储桶名称必须以前缀开头。`athena-query-results-*`

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Bedrock

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Bedrock 功能。Amazon Bedrock 是一项完全托管的服务，可制作来自领先的 AI 初创公司的高性能基础模型 (FMs)，并通过统一的 API AWS 供您使用。您可以从各种根基模型中选择，找到最适合您的用例的模型。Amazon Bedrock 还提供了一系列广泛的功能，可以构建生成式人工智能应用程序，为您提供安全可靠的专属人工智能服务。利用 Amazon Bedrock，您可以轻松试验和评估用例的常用根基模型，使用微调和检索增强生成 (RAG) 等技术，通过自己的数据进行量身定制，并构建使用企业系统和数据来源执行任务的代理。

借助 Amazon Bedrock 的无服务器体验，您可以快速入门，使用自己的数据私下自定义基础模型，并使用 AWS 工具轻松安全地将其集成和部署到您的应用程序中，而无需管理任何基础设施。有关更多信息，请参阅 Amazon Bedrock。

常见问题：AMS 中的 Amazon Bedrock

问：如何使用我的 AMS 账户申请访问 Amazon Bedrock？

要申请访问亚马逊 Bedrock，请使用管理 | AWS 服务 | 自行配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 提交一个 RFC 更改类型。此 RFC 为您的账户配置以下 IAM 角色:`customer_bedrock_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Bedrock 有哪些限制？

- 默认情况下，作为 SSP 角色的一部分，不支持 Amazon Bedrock 知识库，因为它依赖亚马逊无服务器 OpenSearch 服务，AMS 目前不支持该服务。
- 由于依赖亚马逊等不受支持的服务，因此不支持 Bedrock Studio。 DataZone

问：在我的 AMS 账户中使用 Amazon Bedrock 有哪些先决条件或依赖关系？

- 需要 AWS Marketplace 权限的第三方模型订阅必须由默认角色完成（`AWSManagedServicesAdminRole`在 MALZ 和 SALZ `Customer_ReadOnly_Role` 上）。这是因为默认角色包括 AWS Marketplace 权限。
- 如果使用数据加密，则在请求创建控制台角色时必须提供 AWS KMS 密钥 ARN。此外，正在使用的 Amazon S3 存储桶的名称中必须有 “基石”。

使用 AMS SSP CloudSearch 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 CloudSearch 功能。Amazon CloudSearch 是一项 AWS 云端托管服务，您可以经济高效地使用它来设置、管理和扩展您的网站或应用程序的搜索解决方案。Amazon CloudSearch 支持 34 种语言和热门搜索功能，例如突出显示、自动完成和地理空间搜索。要了解更多信息，请参阅 Amazon CloudSearch。

> **Note**
>
> AWS 自 2024 年 7 月 25 日起 CloudSearch，已关闭新买家访问亚马逊的权限。Amazon CloudSearch 现有客户可以继续照常使用该服务。 AWS 继续投资于 Amazon 的安全性、可用性和性能改进 CloudSearch，但我们不打算推出新功能。
> 要了解亚马逊 CloudSearch 和亚马逊 OpenSearch 服务之间的区别，以及如何过渡到 OpenSearch 服务，请联系您的云架构师 (CA) 寻求指导。有关过渡到 OpenSearch 服务的更多信息，请参阅从亚马逊过渡 CloudSearch 到亚马逊 OpenSearch 服务服务。

AWS Managed Services CloudSearch 中的亚马逊常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 CloudSearch ？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 CloudSearch 。此 RFC 为您的账户配置以下 IAM 角

色：customer_csearch_admin_role和。customer_csearch_dev_role在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： CloudSearch 在我的 AMS 账户中使用亚马逊有哪些限制？

您的 AMS 账户中提供 CloudSearch 了 Amazon 的全部功能。Amazon 目前支持所有 AMS 支持的数据库解决方案。 CloudSearch请注意，当前，DynamoDB 是唯一无法建立索引的 AWS 托管数据库解决方案。

问：在我的 AMS 账户 CloudSearch 中使用 Amazon 的先决条件或依赖条件是什么？

Amazon CloudSearch 依靠 Amazon S3 与身份提供商合作来自动分析输入数据并确定表字段。此 RFC 不提供对 Amazon S3 的访问权限，因此必须在服务请求中单独申请。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon CloudWatch Synthetics

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon CloudWatch Synthetics 功能。你可以使用 Amazon S CloudWatch ynthetics 创建 “加那利群岛” 来监控你的终端节点，然后。 APIs

Canarie 是用 Node.js 或 Python 编写的可配置脚本，按计划运行。它们以 Node.js 或 Python 为框架在您的账户中创建 Lambda 函数。金丝雀通过 HTTP 和 HTTPS 两种协议工作。Canaries 会检查您的终端节点的可用性和延迟，并可以存储加载时间数据和 UI 屏幕截图。他们监控您的 REST APIs 和网站内容，并可以检查网络钓鱼、代码注入和跨站脚本是否存在未经授权的更改。 URLs

加那利群岛遵循与客户相同的路线和执行相同的操作，因此即使您的应用程序上没有任何客户流量，您也可以持续验证客户体验。使用金丝雀，您可以早于客户先行发现问题。要了解更多信息，请参阅 Amazon CloudWatch：使用综合监控。

AWS Manage CloudWatch d Services 中的亚马逊 Synthetics 常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 S CloudWatch ynthetics？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66 CloudWatch n899dct) 更改类型提交 RFC，请求访问 Amazon Synthetics。此 RFC 为您的账户配置以下 IAM 角色：“customer_cw_synthetics_console_role” 和 “customer_cw_synthetics_canary_lambda_role”。在您的账户中配置后，您必须在联合解决方案中加入 “customer_cw_synthetics_console_role” 角色。

问：在我的 AMS 账户中使用 Amazon S CloudWatch ynthetics 有哪些限制？

在您的 AMS 账户中使用 Amazon S CloudWatch ynthetics 没有任何限制。禁止在 AMS 提供的服务角色 “customer_cw_synthetics_canary_lambda_role” 之外为加那利群岛创建角色。

问：在我的 AMS 账户中使用 Amazon S CloudWatch ynthetics 有哪些先决条件或依赖条件？

加那利群岛创建并使用默认的 Amazon Synth CloudWatch etics S3 存储桶：cw-syn-results“--” *${accountnumber} ${default-region}*

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Cognito 用户池

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Cognito 用户池功能。Amazon Cognito 用户池提供了一个安全的用户目录，可扩展到数亿用户。作为一项完全托管的服务，Amazon Cognito 用户池的设置无需担心服务器基础设施的架设问题。此服务使您能够管理最终用户池，您可以使用这些用户与内部应用程序集成。此服务为您提供了自定义数据库或网络或移动应用程序最终用户目录的替代方案。同时，Amazon Cognito 用户池提供了目录服务的全套功能，例如密码策略、多因素身份验证、密码恢复和自助注册服务。它还允许该应用程序联合访问其他流行的公共服务，例如OpenID、Facebook、Amazon或Google。

亚马逊 Cognito 分为两个主要产品。亚马逊 Cognito 用户池和亚马逊 Cognito 身份提供商。本节重点介绍 Amazon Cognito 用户池，这些用户池提供对亚马逊 S3 或 DynamoDB 等其他 AWS 服务的访问权限。该服务允许您使用 Amazon Cognito 用户池或第三方身份提供商来提供对服务的访问权限。AWS 它还通过匿名访客访问提供对 AWS 服务的访问。由于 Amazon Cognito 用户池的强大特性，它将 case-by-case作为操作手动服务进行手动管理，以避免账户受到潜在的安全漏洞。要了解更多信息，请参阅 Amazon Cognito 用户池。

AWS Managed Services 常见问题解答中的 Amazon Cognito 用户池

常见问题和答案：

问：如何申请访问我的 AMS 账户中的 Amazon Cognito 用户池？

在 AMS 中实施 Amazon Cognito 用户池分为两个步骤：

1. 提交管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型并请求在您的 AMS 账户中创建 Amazon Cognito 用户池。包括以下信息：
   - AWS 区域。
   - Cognito 用户池的名称。
   - 如果您想使用亚马逊简单电子邮件服务 (Amazon SES) 来发送消息和通知，而不是默认的内部 Cognito 邮件服务，则客户应在账户中提供一个已经过验证的 Amazon SES 服务电子邮件地址。此地址将用于邮件的 “发件人” 和 “回复至” 字段。它们还必须注明激活亚马逊 SES 的地区（us-east-1、eu-west-1 或 us-west-2）。
   - 如果您想使用短信进行一次性密码和验证，则客户应注明。

2. 通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来请求用户访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_cognito_admin_role`和。`customer_cognito_importjob_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。这些角色允许您管理 Amazon Cognito 用户池、管理池中的用户和群组、为用户创建导入任务、修改通知和订阅消息、将应用程序关联到用户池、自行管理向池中添加联合服务以及删除已创建的池。

问：在我的 AMS 账户中使用 Amazon Cognito 用户池有哪些限制？

您将无法创建 Amazon Cognito 用户池。该操作需要创建 IAM 角色才能利用亚马逊 Cognito 使用的服务，例如亚马逊 SES 和亚马逊简单通知服务 (Amazon SNS) Service。

问：在我的 AMS 账户中使用 Amazon Cognito 用户池有哪些先决条件或依赖关系？

如果您想使用 Amazon SES 通过电子邮件向您的用户池发送消息和通知，他们应该已经在账户中激活 Amazon SES 服务，并且已经验证了应在已发送电子邮件的 “发件人” 和 “回复” 字段中使用的电子邮件地址。有关使用 Amazon SES 验证电子邮件地址的更多信息，请参阅在 Amazon S ES 中验证电子邮件地址。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Comprehend

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Comprehend 功能。Amazon Comprehend 是一项自然语言处理 (NLP) 服务，它使用机器学习在文本中查找见解和关系，无需任何机器学习经验。Amazon Comprehend 使用机器学习来帮助您发现非结构化数据中的见解和关系。该服务识别文本的语言；提取关键短语、地点、人物、品牌或事件；了解文本的正面或负面程度；使用分词和部分语音分析文本；并按主题自动整理文本文件集。您还可以使用 Amazon Comprehend 中的 AutoML 功能来构建一组专为您的组织需求量身定制的自定义实体或文本分类模型。要了解更多信息，请参阅亚马逊 Comprehend。

AWS Managed Services 常见问题解答中的亚马逊 Comprehend

问：如何使用我的 AMS 账户申请访问亚马逊 Comprehend？

可以通过提交两个 AMS 服务来申请 Amazon Comprehend 控制台和数据访问角色： RFCs

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_comprehend_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Comprehend 有哪些限制？

通过 Amazon Comprehend 控制台创建新的 IAM 角色功能受到限制。否则，Amazon Comprehend 的全部功能都可以在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Comprehend 有哪些先决条件或依赖关系？

如果亚马逊 S3 存储桶使用密钥加密，则必须使用 Amazon S3 和 AWS Key Management Service (AWS KMS) 才能使用 Amazon Comprehend。 AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Connect

> **Note**
>
> 经过深思熟虑，我们决定从 2026 年 5 月 20 日起终止对 Amazon Connect 语音识别的支持。从 2025 年 5 月 20 日起，Amazon Connect 语音识别将不再接受新客户。作为在 2025 年 5 月 20 日之前注册该服务的账户的现有客户，您可以继续使用 Amazon Connect 语音识别功能。2026 年 5 月 20 日之后，您将无法再使用 Amazon Connect 语音识别码。

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Connect 功能。Amazon Connect 是一个全渠道云联络中心，可帮助公司以更低的成本提供卓越的客户服务。Amazon Connect 为客户和代理提供无缝的语音和聊天体验。这包括一套基于技能的路由工具、强大的实时和历史分析以及 easy-to-use直观的管理工具，所有这些都包含 pay-as-you-go定价。

您可以在 AMS 多账户 landing zone 或单账户着陆区账户中创建虚拟联络中心实例的一个或多个实例。您可以使用现有的 SAML 2.0 身份提供商进行代理访问或使用 Amazon Connect 原生支持进行用户生命周期管理。

此外，您可以从 Amazon Connect 控制台申请每个 Amazon Connect 实例的收费 free/direct 拨号电话号码。您可以使用 easy-to-use图形用户界面创建丰富的联系流程，以实现所需的客户体验和路由。联系流可以利用 AWS Lambda 函数与本地数据存储和 API 集成。你也可以使用 Kinesis Streams 和 Firehose 启用数据流。

通话记录、聊天记录和报告存储在使用 AWS KMS 密钥加密的 Amazon S3 存储桶中。可以将联络流日志保存到 CloudWatch 日志组中。

要了解更多信息，请参阅 Amazon Connect。

AWS Managed Services 常见问题中的 Amazon Connect

问：如何使用我的 AMS 账户申请访问 Amazon Connect？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_connect_console_role`和。`customer_connect_user_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Connect 有哪些限制？

没有任何限制。您的 AMS 账户中提供了 Amazon Connect 的全部功能。

问：在我的 AMS 账户中使用 Amazon Connect 有哪些先决条件或依赖条件？

- 您必须使用标准 AMS 创建 AWS KMS 密钥和 Amazon S3 存储桶 RFCs；Amazon S3 存储桶是存储通话录音和聊天记录所必需的。
- 如果您想与 Active Directory (AD) 集成，则需要 AD 连接器才能在 AMS 托管的 Amazon Connect 实例和您的本地目录服务之间进行集成。可以通过请求 “管理 | 其他 | 其他” RFC 在您的账户中配置 AD Connector。
- 您可以根据您的联系流要求启用以下可选的自行配置服务。
  - AWS Lambda: 您可以使用 Lambda 函数扩展联系流程，以利用现有的本地数据存储或。 APIs您可以使用 Lambda 自行配置的服务来创建 Lambda 函数。
  - Amazon Kinesis D ata Streams：您可以创建数据流以实现向外部应用程序传输数据。您可以流式传输联系人追踪记录或座席事件。
  - Amazon Kinesis D ata Firehose：您可以创建 Data Firehose，将大量联系人追踪记录流式传输到外部应用程序。
  - Amazon Lex：您可以利用 Amazon Lex 聊天机器人创建智能联系流程，利用亚马逊 Alexa 服务，实现丰富的客户体验和自动化。
- 问：如何请求添加拨出或呼入电话的国家/地区列表？

  要添加拨出或呼入电话的国家/地区列表，请向 AMS 提交服务请求。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Data Firehose

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Data Firehose 功能。Firehose 是将流数据可靠地加载到数据湖、数据存储和分析工具的最简单方法。它可以捕获、转换流数据并将其加载到 Amazon S3、Amazon Redshift、Amazon S OpenSearch ervice 和 Splunk 中，从而使用你目前已经在使用的现有商业智能工具和仪表板实现近乎实时的分析。它是一项完全托管的服务，可自动扩展以匹配您的数据吞吐量，并且无需持续管理。它还可以在加载数据之前对其进行批

处理、压缩、转换和加密，从而最大限度地减少目的地使用的存储量并提高安全性。要了解更多信息，请参阅什么是亚马逊数据 Firehose？

AWS Managed Services 常见问题解答中的 Firehose

常见问题和答案：

问：如何通过我的 AMS 账户申请访问亚马逊数据 Firehose？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_kinesis_firehose_user_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Firehose 有什么限制？

没有任何限制。Amazon Data Firehose 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Firehose 的先决条件或依赖条件是什么？

必须为每个交付流请求新的服务相关的 IAM 角色。您还可以使用所需的资源权限（包括 S3 存储桶/KMS 密钥/Lambda Functions/Kinesis 流）更新角色策略，从而为所有直播重复使用单个服务相关角色。

在您提交 RFC 以添加 Firehose 后，AMS 运营工程师将通过服务请求与您联系，请求您想要与 Data Firehose 连接的资源（例如 S3 AWS KMS、Lambda 和 Kinesis Streams）。 ARNs

使用 AMS SSP 在你的 AMS 账户中配置 Amazon DevOps Guru

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon DevOps Guru 功能。Amazon DevOps Guru 是一项完全托管的运营服务，可让开发人员和操作员轻松提高其应用程序的性能和可用性。 DevOpsGuru 可以让你卸下与识别操作问题相关的管理任务，这样你就可以快速实施改进应用程序的建议。 DevOpsGuru 创建了反应式见解，您可以立即使用这些见解来改进您的应用程序。它还可以提供主动见解，帮助您避免将来可能影响应用程序的操作问题。 DevOpsGuru 应用机器学习来分析您的运营数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，您会收到通知。对于每个问题， DevOpsGuru都会提出明智的建议，以解决当前和预测的未来运营问题。

要了解更多信息，请参阅什么是 Amazon DevOps Guru。

AWS Managed Services 常见问题解答中的 Amazon DevOps Guru

问：如何使用我的 AMS 账户申请访问 Amazon DevOps Guru？

要申请访问权限，请提交管理 | AWS 服务 | 自配服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型。此 RFC 为您的账户配置以下 IAM 角色:`customer_devopsguru_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon DevOps Guru 有哪些限制？

没有任何限制。Amazon DevOps Guru 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon DevOps Guru 的先决条件或依赖条件是什么？

没有先决条件。 DevOpsGuru 利用以下 AWS 服务：Amazon Log CloudWatch s、RDS Insights、AWS X-Ray AWS Lambda、和。 AWS CloudTrail

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 DocumentDB（兼容 MongoDB）

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 DocumentDB（兼容 MongoDB）功能。Amazon DocumentDB（兼容 MongoDB）是一种快速、可扩展、高度可用且完全托管的文档数据库服务，支持 MongoDB 工作负载。Amazon DocumentDB 为您提供大规模操作任务关键型 MongoDB 工作负载时所需的性能、可扩展性和可用性。Amazon DocumentDB 通过模拟 MongoDB 客户端期望从 MongoDB 服务器获得的响应来实现 Apache 2.0 开源 MongoDB 3.6 API，允许您在亚马逊 DocumentDB 上使用现有的 MongoDB 驱动程序和工具。在 Amazon DocumentDB 中，存储和计算是分离的，允许两者独立扩展，无论您的数据大小如何，您都可以通过添加多达 15 个低延迟只读副本将读取容量增加到每秒数百万个请求。Amazon DocumentDB 专为 99.99% 的可用性而设计，可在三个 AWS 可用区复制六份数据副本 ()。AZs您可以免费使用 AWS Database Migration Service (DMS)（六个月）将本地或亚马逊弹性计算云 (Amazon) MongoDB 数据库迁移到亚马逊 EC2 DocumentDB，几乎无需停机。要了解更多信息，请参阅亚马逊文档数据库（兼容 MongoDB）。

AWS Managed Services 常见问题解答中的亚马逊 DocumentDB

问：如何使用我的 AMS 账户申请访问亚马逊文档数据库？

可以通过提交两个 AMS RFCs（控制台访问权限和数据访问权限）来请求 Amazon DocumentDB 控制台和数据访问角色：

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊文档数据库。此 RFC 为您的账户配置以下 IAM 角色:`customer_documentdb_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 DocumentDB 有哪些限制？

亚马逊 DocumentDB 需要亚马逊 RDS 特定的权限。由于 AMS 完全管理亚马逊 RDS，因此 Amazon DocumentDB 的 IAM 角色包括对亚马逊 RDS 操作的一些限制。以下限制适用：

- 对`DeleteDBInstance`和的访问`DeleteDBCluster` APIs 已受到限制。要使用这些删除功能 APIs，请提交 RFC，其中包含管理 | 高级堆栈组件 | 身份和访问管理 (IAM) | 更新实体或策略（需要审查）更改类型 (ct-27tuth19k52b4)。
- 您无法在 Amazon RDS 实例中添加或删除标签。
- 您无法将您的亚马逊文档数据库实例设为公有。

问：在我的 AMS 账户中使用亚马逊 DocumentDB 有哪些先决条件或依赖关系？

如果亚马逊 S3 存储桶使用密钥加密， AWS KMS 则必须使用 Amazon S3 和，才能使用亚马逊 DocumentDB。 AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 DynamoDB

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 DynamoDB (DynamoDB) 功能。Amazon DynamoDB 是一个关键值和文档数据库，可在任何规模上提供个位数的毫秒级性能。它是一个完全托管的多区域、多活动数据库，具有内置安全性、备份和恢复功能，以及适用于互联网规模应用程序的内存缓存。要了解更多信息，请参阅Amazon DynamoDB。

Amazon DynamoDB Accelerator (DAX) 是一项直写缓存服务，旨在简化将缓存添加到 DynamoDB 表的过程。DAX 适用于需要高性能读取的应用程序。

AWS Managed Services 中的 DynamoDB 常见问题解答

问：如何使用我的 AMS 账户请求访问 DynamoDB 和 DAX？

使用管理 AWS | 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 DynamoDB 和 DAX。此 RFC 为您的账户配置以下 IAM 角色和策略：

- DynamoDB 角色名称：`customer_dynamodb_role`

  DAX 服务角色名称：`customer_dax_service_role`
- DynamoDB 策略名称：`customer_dynamodb_policy`

  DAX 服务政策：`customer_dax_service_policy`

在您的账户中配置后，您必须在联合解决方案`customer_dynamodb_role`中加载。

问：在我的 AMS 账户中使用 DynamoDB 有哪些限制？

支持所有 DynamoDB 功能，包括 DynamoDB 加速器 (DAX)。

为任何给定表创建警报时，警报名称必须以 “customer*” 为前缀；例如，。`customer-employee-table-high-put-latency`

为 DynamoDB 创建 Amazon SNS 主题时，必须将其命名为：。`dynamodb`

要删除 DynamoDB 创建的 Amazon SNS 主题，请提交 “管理 | 其他 | 其他 | 其他 | 更新更改类型 RFC”。

问：在我的 AMS 账户中使用 DynamoDB 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 DynamoDB 没有任何先决条件或依赖关系。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 弹性容器注册表

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊弹性容器注册表 (Amazon ECR) Container Registry 功能。Amazon Elastic Container Registry 是一个完全托管的 Docker 容器注册表，可让开发人员轻松存储、管理和部署 Docker 容器镜像。Amazon ECR 已与亚马逊弹性容器服务 (Amazon ECS) Service 集成，简化了从开发到生产的工作流程。Amazon ECR 让您无需操作自己的容器存储库，也不必担心底层基础设施的扩展。Amazon ECS 将您的映像托管在高度可用且可扩展的架构中，使您能够可靠地为应用程序部署容器。与 AWS Identity and Access Management (IAM) 集成提供了对每个存储库的资源级控制。使用 Amazon ECR，无需支付任何预付费用或承诺。您只需为存储在存储库中的数据量和传输到 Internet 的数据量付费。

要了解更多信息，请参阅 Amazon 弹性容器注册表。

AWS Managed Services 中的亚马逊弹性容器注册表常见问题解答

问：如何申请访问我的 AMS 账户中的 Amazon ECR？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 ECR。此 RFC 将以下 IAM 角色分别配置到您的账户： `customer_ecr_console_role`、以及`customer_ecr_poweruser_instance_profile`关联的 IAM 策略`customer_ecr_console_policy`和`customer_ecr_poweruser_instance_profile_policy`。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon ECR 有哪些限制？

在您的 AMS 账户中使用 Amazon ECR 时，AMS 命名空间存在限制。容器镜像不得以 “AMS-” 或 “Sentinel-” 为前缀。

问：在我的 AMS 账户中使用 Amazon ECR 有哪些先决条件或依赖条件？

在您的 AMS 账户中使用 Amazon ECR 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 EC2 Image Builder

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 EC2 Image Builder 功能。EC2 Image Builder 是一项完全托管的 AWS 服务，它可以更轻松地自动创建、管理和部署自定义、安全和 up-to-date “黄金” 服务器映像，这些镜像已预先安装并预先配置了软件和设置，以满足特定 IT 标准。

您可以使用 AWS 管理控制台、 AWS CLI 或 APIs 在您的 AWS 账户中创建自定义镜像。当您使用时 AWS 管理控制台，Amazon EC2 Image Builder 向导会指导您完成以下步骤：

- 提供起始构件
- 添加和删除软件
- 自定义设置和脚本
- 运行选定的测试
- 将图像分发到 AWS 区域

您构建的映像是在您的账户中创建的，可以持续配置操作系统补丁。要了解更多信息，请参阅 EC2 Image Builder。

EC2 AWS Managed Services 常见问题中的 Image Builder

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 EC2 Image Builder？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：。`customer_ec2_imagebuilder_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：I EC2 mage Builder 有哪些限制？

AMS 不支持使用服务默认值进行基础设施配置。您可以创建新的基础架构配置或使用现有基础架构配置。

AMS 目前不支持创建容器配方。

问：启用 I EC2 mage Builder 的先决条件或依赖关系是什么？

- EC2 Image Builder 服务相关角色：您无需手动创建服务相关角色。当您在 AWS 管理控制台、CLI 或 AWS AP AWS I 中创建第一个 Image Builder 资源时，Image Builder 会为您创建服务相关角色。
- 用于使用 Image Builder 构建映像和运行测试的实例必须有权访问 Systems Manager 服务。如果 SSM 代理尚不存在，将在源镜像上安装该代理，并在创建镜像之前将其删除。
- AWS IAM：您与实例配置文件关联的 IAM 角色必须有权运行映像中包含的构建和测试组件。必须将以下 IAM 角色策略附加到与实例配置文件关联的 IAM 角色：`EC2InstanceProfileForImageBuilder`和`AmazonSSMManagedInstanceCore`。IAM 角色名称应包含`*imagebuilder*`关键字。
- 如果配置日志记录，在基础设施配置中指定的实例配置文件必须具有目标存储桶 (`arn:aws:s3:::{bucket-name}/*`) 的 `s3:PutObject` 权限。例如：

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- 创建名为 “imagebuilder” 的 SNS 主题，以接收来自 Image Build EC2 er 的任何提醒和通知。

使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon ECS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中通过 AWS Fargate 功能访问 Amazon ECS。 AWS Fargate 是一种可以与 Amazon ECS 配合使用的技术，无需管理服务器或亚马

逊 EC2 实例集群即可运行容器（参见上面的容器 AWS）。使用 AWS Fargate，您无需再预置、配置或扩展虚拟机集群来运行容器。这样一来，您就无需再选择服务器类型、确定扩展集群的时间和优化集群打包。

要了解更多信息，请参阅上的 Amazon ECS AWS Fargate。

AWS Managed Services 常见问题解答中的 Fargate 上的 Amazon ECS

问：如何使用我的 AMS 账户请求访问 Fargate 上的 Amazon ECS？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Fargate 上的 Amazon ECS。此 RFC 将以下 IAM 角色配置到您的账户：`customer_ecs_fargate_console_role`（如果没有提供 ECS 策略与 ECS 策略关联的现有 IAM 角色）`customer_ecs_fargate_events_service_role`、`customer_ecs_task_execution_service` 和`AWSServiceRoleForApplicationAutoScaling_ECSService`。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：使用我的 AMS 账户在 Fargate 上使用 Amazon ECS 有哪些限制？

- Amazon ECS 任务监控和日志记录被视为您的责任，因为容器级别的活动发生在虚拟机管理程序之上，并且日志记录功能受到 Fargate 上的 Amazon ECS 的限制。作为 Fargate 上的 Amazon ECS 用户，我们建议您采取必要步骤启用对您的 Amazon ECS 任务的登录功能。有关更多信息，请参阅为容器启用 awslogs 日志驱动程序。
- 容器级别的安全和恶意软件保护也被视为您的责任。Fargate 上的 Amazon ECS 不包括趋势科技或预先配置的网络安全组件。
- 此服务适用于多账号着陆区和单账号着陆区 AMS 账户。
- 由于创建 Route 53 私有托管区域需要更高的权限，因此默认情况下，自行配置角色限制了 Amazon ECS 服务发现。要在服务上启用服务发现，请提交 “管理” | “其他” | “其他” | “更新” 更改类型。要提供为您的 Amazon ECS 服务启用服务发现所需的信息，请参阅服务发现手册。
- AMS 目前不管理或限制用于在 Amazon ECS Fargate 上部署到容器的映像。您将能够部署来自 Amazon ECR、Docker Hub 或任何其他私有镜像存储库的镜像。因此，我们建议不要部署公共镜像或任何不安全的镜像，因为它们可能会导致账户出现恶意活动。

问：在我的 AMS 账户中在 Fargate 上使用 Amazon ECS 有哪些先决条件或依赖关系？

- 以下是 Amazon ECS 对 Fargate 的依赖关系；但是，使用您的自配置角色启用这些服务无需执行任何其他操作：

- CloudWatch 日志
- CloudWatch 事件
- CloudWatch 警报
- CodeDeploy
- App Mesh
- Cloud Map
- Route 53

- 根据您的使用案例，以下是 Amazon ECS 所依赖的资源，并且在您的账户中使用 Fargate 上的 Amazon ECS 之前可能需要的资源：
  - 要与 Amazon ECS 服务配合使用的安全组。您可以使用部署 | 高级堆栈组件 | 安全组 | 创建 (auto) (ct-3pc215bnwb6p7)，或者，如果您的安全组需要特殊规则，请使用部署 | 高级堆栈组件 | 安全组 | 创建（需要审阅）(ct-1oxx2g2g2d7hc90)。注意：您在 Amazon ECS 上选择的安全组必须专门为 Amazon ECS 服务或集群所在的 Amazon ECS 创建。您可以在 “使用 Amazon ECS 进行设置” 和 “亚马逊弹性容器服务中的安全” 的 “安全组” 部分了解更多信息。
  - 应用程序负载均衡器 (ALB)、网络负载均衡器 (NLB)、用于任务间负载平衡的经典负载均衡器 (ELB)。
  - 的目标群体 ALBs.
  - 用于与 Amazon ECS 集群集成的应用程序网格资源（例如虚拟路由器、虚拟服务、虚拟节点）。
- 目前，在标准 AMS 变更类型之外创建时，AMS 无法自动降低与支持安全组权限相关的风险。我们建议您申请一个用于您的 Fargate 集群的特定安全组，以限制使用未指定用于 Amazon ECS 的安全组的可能性。

使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon EKS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中通过 AWS Fargate 功能访问 Amazon EKS。 AWS Fargate 是一种按需为容器提供大小合适的计算容量的技术（要了解容器，请参阅什么是容器？）。使用 AWS Fargate，您无需再预置、配置或扩展虚拟机组来运行容器。这样一来，您就无需再选择服务器类型、确定扩展节点组的时间和优化集群打包。

亚马逊 Elastic Kubernetes Service（亚马逊 EKS）使用使用 AWS Fargate Kubernetes 提供的上游可扩展模型 AWS 构建的控制器将 Kubernetes 与 Kubernetes 集成。这些控制器作为 Amazon EKS 管理的 Kubernetes 控制平面的一部分运行，负责将原生 Kubernetes pod 调度到 Fargate 上。除了若干转换和验证准入控制器外，Fargate 控制器还包括一个与默认 Kubernetes 调度器一起运行的新调度器。

当您启动满足 Fargate 上的运行条件的 Pod 时，集群中运行的 Fargate 控制器会识别、更新 Pod 并将其安排到 Fargate 上。

要了解更多信息，请参阅AWS Fargate 现已正式上市的 Amazon EKS 和 Amazon EKS 安全最佳实践指南（包括 “建议”，例如 “查看并撤消不必要的匿名访问权限” 等）。

> **Tip**
>
> AMS 有一个变更类型，即部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建 OpenID Connect 提供商 (ct-30ecvfi3tq4k3)，你可以将其与亚马逊 EKS 一起使用。有关示例，请参阅身份和访问管理 (IAM) Management | 创建 OpenID Conn ect 提供商。

AWS Managed Services 常见问题解答 AWS Fargate 中的亚马逊 EKS

问：如何使用我的 AMS 账户申请访问 Fargate 上的 Amazon EKS？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色。

- `customer_eks_fargate_console_role`.

  在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。
- 这些服务角色允许 Fargate 上的 Amazon EKS 代表您拨打其他 AWS 服务：
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

问：在我的 AMS 账户中在 Fargate 上使用 Amazon EKS 有哪些限制？

- AMS 不支持创建托管或自行管理的 EC2 节点组。如果您需要使用 EC2 工作节点，请联系您的 AMS 云服务交付经理 (CSDM) 或云架构师 (CA)。
- AMS 不包括趋势科技或容器映像的预配置网络安全组件。您需要管理自己的图像扫描服务，以便在部署之前检测恶意容器镜像。
- 由于相互依存关系，不支持 EKSCTL。 CloudFormation
- 在创建集群期间，您有权禁用集群控制平面日志记录。有关更多信息，请参阅 Amazon EKS 控制面板日志记录。我们建议您在创建集群时启用所有重要的 API、身份验证和审核日志。

- 在创建集群期间，Amazon EKS 集群的集群终端节点访问权限默认为公用；有关更多信息，请参阅 Amazon EKS 集群终端节点访问控制。我们建议将 Amazon EKS 终端节点设置为私有终端节点。如果需要终端节点才能进行公共访问，则最佳做法是仅针对特定 CIDR 范围将其设置为公用。
- AMS 没有办法强制和限制用于部署到 Amazon EKS Fargate 上的容器中的映像。您可以部署来自 Amazon ECR、Docker Hub 或任何其他私有镜像存储库的镜像。因此，部署可能对账户执行恶意活动的公共镜像存在风险。
- AMS 不支持通过云开发套件 (CDK) 或 CloudFormation Ingest 部署 EKS 集群。
- 您必须使用 ct-3pc215bnwb6p7 部署 | 高级堆栈组件 | 安全组 | 在清单文件中创建和引用创建入口所需的安全组。这是因为该角色`customer-eks-alb-ingress-controller-role`无权创建安全组。

问：在我的 AMS 账户中在 Fargate 上使用 Amazon EKS 有哪些先决条件或依赖关系？

要使用该服务，必须配置以下依赖关系：

- 要针对服务进行身份验证， aws-iam-authenticator必须同时安装 KUBECTL 和；有关更多信息，请参阅管理集群身份验证。
- Kubernetes 依赖一个叫做 “服务账户” 的概念。为了在 EKS 上使用 kubernetes 集群内部的服务账户功能，需要使用管理 | 其他 | 其他 | 更新 RFC，其中包含以下输入：
  - [必填] 亚马逊 EKS 集群名称
  - [必需] 将部署服务账户 (SA) 的 Amazon EKS 集群命名空间。
  - [必填] Amazon EKS 集群 SA 名称。
  - [必填] IAM 策略名称和 permissions/document 待关联。
  - [必需] 正在请求 IAM 角色名称。
  - [可选] OpenID Connect 提供商网址。有关更多信息，请参阅
    - 在集群上为服务账户启用 IAM 角色
    - 为服务账号引入精细的 IAM 角色
- 我们建议配置和监控 Config 规则
  - 公共集群终端节点
  - 已禁用 API 日志记录

  您有责任监控和修正这些 Config 规则。

如果您想部署 ALB 入口控制器，请提交 “管理 | 其他 | 其他更新 RFC”，以配置与 ALB Ing ress Controller Pod 一起使用的必要的 IAM 角色。创建与 ALB Ingress Controller 关联的 IAM 资源需要以下输入（包括您的 RFC 中的这些内容）：

- [必填] 亚马逊 EKS 集群名称
- [可选] OpenID Connect 提供商网址
- [可选] 将部署应用程序负载均衡器 (ALB) 入口控制器服务的 Amazon EKS 集群命名空间。 [默认： kube-system]
- [可选] Amazon EKS 集群服务账户 (SA) 名称。 [默认： aws-load-balancer-controller]

如果要在集群中启用信封密钥加密（我们建议这样做），请在 RFC 的描述字段中提供 IDs 您打算使用的 KMS 密钥以添加服务（管理 | 服务 | 自配置 AWS 服务 | 添加 (ct-1w8z66n899dct)。要了解有关信封加密的更多信息，请参阅 Amazon EKS 使用 AWS KMS 为机密添加信封加密。

使用 AMS SSP 在您的 AMS 账户中配置亚马逊 EMR

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon EMR 功能。亚马逊 EMR 是业界领先的云大数据平台，用于使用 Apache Spark、Apache Hive、Apache Flink、Apache Flink、Apache Hudi 和 P HBase resto 等开源工具处理大量数据。借助 Amazon EMR，您可以以不到传统本地解决方案一半的成本运行 PB 级分析，速度比标准 Apache Spark 快 3 倍以上。对于短期运行的作业，您可以启动和关闭集群，并为使用的实例按秒付费。对于长时间运行的工作负载，您可以创建高度可用的集群，这些集群可以自动扩展以满足需求。

您可以在 AMS 多账户着陆区账户或单账户着陆区账户中创建一个或多个 Amazon EMR 集群实例，以支持临时和永久性 Amazon EMR 集群。您也可以启用 Kerberos 身份验证以启用对本地 Active Directory 域中的用户进行身份验证。

您可以在 Amazon EMR 集群中利用多个数据存储来支持特定于用例的 Hadoop 工具和库。可以使用 OnDemand 或竞价型实例创建 Amazon EMR 集群，并配置自动扩展以管理容量并降低成本。

可以将集群日志文件存档到 Amazon S3 存储桶中以进行日志记录和调试。您还可以访问托管在 Amazon EMR 集群中的网页界面，以支持 hadoop 管理要求或为客户提供笔记本体验。

要了解更多信息，请参阅 Amazon EMR。

AWS Managed Services 常见问题解答中的亚马逊 EMR

问：如何通过我的 AMS 账户申请访问亚马逊 EMR？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

在您的账户中进行配置后，您必须在联合解决方案中加载 customer_emr_console_role。

问：在我的 AMS 账户中使用 Amazon EMR 有哪些限制？

通过 AWS 控制台在 EC2 集群上创建 Amazon EMR 时，我们建议您使用 “创建集群-高级” 选项。必须通过添加带有密钥 “for-use-with-amazon-emr-managed-policies” 且值为 “tru e” 的标签来创建 Amazon EMR 集群。在 “安全” 选项中选择以下配置：

- 为您的集群选择自定义角色：
  - EMR 角色：customer_emr_cluster_service_role
  - EC2 实例配置文件：customer_emr_cluster_instance_profile
  - Auto Scaling 角色：customer_emr_cluster_autoscaling_role
- EC2 安全组：
  - Master: ams-emr-master-security-group
  - 核心和任务： ams-emr-worker-security-group
  - 服务访问权限： ams-emr-serviceaccess-security-group

问：在我的 AMS 账户中使用 Amazon EMR 的先决条件或依赖条件是什么？

AMS 为 Amazon EMR 主节点、工作节点和服务节点创建默认安全组。

要用于 Amazon EMR 集群的启动模板和安全组必须具有标签密钥 “for-use-with-amazon-”，值为 “true emr-managed-policies”。

默认的 Amazon EMR 集群实例配置文件允许访问名称包含 “emr” 的 s3 存储桶和 dynamodb 表等资源。您可以申请其他 IAM 政策，以使用任何其他资源与 Amazon EMR 配合使用。以下资源 ARN 可以使用 customer_emr_cluster_instance_profile 用于亚马逊 EMR 任务：

- arn: aws: dynamodb: *: *: table/*emr*

- arn: aws: kinesis: *: *: stream/*emr*
- arn: aws: sns: *: *: *emr*arn: aws: sqs: *: *: *emr*
- arn: aws: sqs: *: *: *emr*
- arn: aws: sqs: *: *: AWS--* ElasticMapReduce
- arn: aws: sdb: *: *: domain: *emr*
- arn: aws: s3::: *emr*

如果 Amazon EMR 集群需要 kerberos 身份验证：

- 提供用于每个 kerberized Amazon EMR 集群的领域名称和本地 Active Directory IP 地址。
- 基础架构要求：

  多账户登录区 (MALZ)：提交 RFC 以在现有应用程序账户中创建新的托管应用程序账户或新 VPC。

  单账户着陆区 (SALZ)：提交 RFC 以在您的 VPC 中创建新的子网。
- 在预置的 Active Directory 上为集群的领域配置传入信任。
- 提交 RFC 以在托管 AD 中为该领域配置 DNS 区域。
- 领域配置：

  MALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以更新 VPC DHCP 选项设置为使用域名后缀的领域名称。

  SALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以生成新的亚马逊 EMR AMI，使用特定领域作为域名后缀。

要部署 Amazon EMR studio，该角色`customer_emr_cluster_service_role`必须具备亚马逊简单存储服务存储段的先决条件。要创建存储桶，请使用自动化 CT`ct-1a68ck03fn98r`（部署 | 高级堆栈组件 | S3 存储 | 创建）。当您使用此自动 CT 为 Amazon EMR 创建 Amazon S3 存储桶时，存储桶名称必须以前缀开头。`customer-emr-*`而且，您必须在与 Amazon EMR AWS 集群相同的区域中创建存储桶。

使用 AMS SSP EventBridge 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 EventBridge 功能。Amazon EventBridge 是一项无服务器事件总线服务，可以轻松地将您的应用程序与来自各种来源的数据连接起来。 EventBridge 提供来自您自己的应用程序、 Software-as-a-Service (SaaS) 应用程序

和 AWS 服务的实时数据流，并将这些数据路由到目标，例如 AWS Lambda。您可以设置路由规则来确定发送数据的目的地，以便构建能够实时响应所有数据源的应用程序架构。利用 EventBridge ，您可以构建事件驱动的体系结构，这些体系结构是松散耦合的和分布式的。

要了解更多信息，请参阅 Amazon EventBridge。

EventBridge 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 EventBridge 中申请访问权限？

EventBridge 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct)
更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角
色：`customer_eventbridge_role`和。`customer_eventbridge_scheduler_execution_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

执行角色`customer_eventbridge_scheduler_execution_role`是一个 IAM 角色，
EventBridge 日程安排器代替您与其他 AWS 服务 角色进行交互。附加到此角色的权限策略授予 EventBridge 调度程序调用目标的访问权限。

> **Note**
>
> 默认情况下， EventBridge 调度器使用 AWS 自有的密钥 EventBridge 对数据进行加密。要使用客户托管密钥对数据进行加密，请使用管理 | AWS 服务 | 自配置服务 | 添加（需要审核）更改类型 (ct-3qe6io8t6jtny) 提交服务配置的 RFC。 EventBridge

问： EventBridge 在我的 AMS 账户中使用有什么限制？

您必须提交 AMS RFCs 并创建以下资源：用于触发批处理作业的服务角色、SQS 队列 CodeBuild CodePipeline、和 SSM 命令。

问：在我的 AMS 账户 EventBridge 中使用的先决条件或依赖条件是什么？

在使用触发其他 EventBridge资源（例如 Lambda、Amazon SNS、Amazon SNS、Amazon SQS 或亚马逊日志资源）之前，您必须使用部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略（需要审查）更改类型 (ct-3dpd8m AWS dd9jn1r) 申请 EventBridge 服务角色。 AWS Batch CloudWatch 指定在请求您的服务角色时要调用的服务。要了解调用目标所需的权限，请参阅使用基于资源的策略。 EventBridge

EventBridge 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或角色所执行操作 AWS 服务 的记录 EventBridge。 CloudTrail 必须启用并允许其将日志文件存储到 S3 存储桶中。注意：所有 AMS 账户均已 CloudTrail 启用，因此无需执行任何操作。

问：角色 customer_eventbridge_scheduler_execution_role 具有密钥的先决条件（如果用于加密，则为可选）。 AWS Key Management Service 如何在静止/传输时采用 AWS KMS CMKs 数据加密？

默认情况下，S EventBridge cheduler 会加密其存储在 AWS 自有密钥下的事件元数据和消息数据（静态加密）。 EventBridge 调度器还使用传输层安全 (TLS)（传输中的加密）对在 EventBridge 调度程序和其他服务之间传递的数据进行加密。

如果您的特定用例要求您控制和审核在 EventBridge 计划程序上保护您的数据的加密密钥，则可以使用客户托管密钥。

在使用 Ama EventBridge zon 加入许可之前，您必须使用管理 AWS 服务 | | 自行配置服务 | 添加（需要审核）更改类型申请 RFC。 AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Forecast

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Forecast（Forecast）功能。Amazon Forecast 是一项完全托管的服务，它使用机器学习来提供高度准确的预测。

> **Note**
>
> AWS 自 2024 年 7 月 29 日起，已关闭新买家访问 Amazon Forecast 的权限。Amazon Forecast 现有客户可以继续照常使用该服务。 AWS 继续投资于 Amazon Forecast 的安全性、可用性和性能改进，但 AWS 不打算推出新功能。
> 如果你想使用 Amazon Forecast，请联系你的 CSDM，他们可以进一步指导你如何将你的 Amazon Forecast 使用转移到亚马逊 Can vas。 SageMaker

基于亚马逊使用的相同技术，Forecast 使用机器学习将时间序列数据与其他变量相结合以建立预测。Forecast 不需要任何机器学习经验即可开始使用。您只需要提供历史数据，以及您认为可能影响预测的任何其他数据。例如，对特定颜色的衬衫的需求可能会随着季节和商店位置的变化而变化。这种复杂的关系很难单独确定，但是机器学习非常适合识别这种关系。在您提供数据后，Forecast 将自动对其进行检查，确定哪些内容有意义，并生成一个预测模型，该模型能够做出比单独查看时间序列数据高出 50% 的预测准确性。

要了解更多信息，请参阅 Amazon Forecast。

AWS Managed Services 常见问题中的 Amazon Forecast

问：如何使用我的 AMS 账户申请访问 Forecast？

AWS Firewall Manager 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct)
更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_forecast_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Forecast 有哪些限制？

默认 S3 存储桶访问权限仅允许您访问命名模式为 “customer-forecast-*” 的存储桶。如果您对数据存储桶有自己的命名约定，请与您的云架构师 (CA) 讨论存储分区命名和相关访问权限设置。例如：

- 您可以定义您的特定的 Amazon Forecast 服务角色，命名为 “AmazonForecast-ExecutionRole-*”，并关联相应的 S3 存储桶访问权限。在 IAM 控制台中查看服务角色 AmazonForecast-ExecutionRole-Admin和 IAM 策略-customer_forecast_default_s3_access_policy。
- 您可能需要将相关的 S3 存储桶访问权限关联到 IAM 联合角色中。在 IAM 控制台中查看 IAM 政策——customer_forecast_default_s3_access_policy。

问：在我的 AMS 账户中使用 Forecast 的先决条件或依赖条件是什么？

- 在使用 Forecast 之前，必须创建正确的 Amazon S3 存储桶。特别是，默认 S3 存储桶访问权限使用命名模式 “customer-forecast-*”
- 如果要在 S3 存储桶上使用除 “customer-forecast-*” 之外的命名模式，则必须创建一个对存储桶具有 S3 访问权限的新服务角色：
  1. 要创建一个命名为 “AmazonForecast-ExecutionRole-{suffix}” 的新服务角色。
  2. 要创建的新 IAM 策略与 customer_forecast_default_s3_access_policy 类似，并将与新的服务角色和相关的联合管理员角色（例如 “customer_forecast_admin_role”）相关联

问：在使用 Amazon Forecast 时，如何增强数据安全？

- 对于静态数据加密，您可以使用配置客户托管的 CMK AWS KMS 来保护 Amazon S3 服务上的数据存储：
  - 使用配置密钥在存储桶上启用默认加密，并将存储桶策略设置为在放置 AWS KMS 数据时接受数据加密。

  - 启用 Amazon Forecast 服务角色 'AmazonForecast-ExecutionRole-*' 和联盟管理员角色（例如' customer_forecast_admin_role '）作为关键用户。 AWS KMS
- 对于传输中的数据加密，您可以设置 HTTPS 协议，这是根据 Amazon S3 存储桶策略传输对象时所必需的。
- 对访问控制的进一步限制，为Amazon Forecast服务角色 “AmazonForecast-ExecutionRole-*” 和管理员角色（例如 “customer_forecast_admin_role”）的已批准访问启用存储桶策略。

问：使用 Amazon Forecast 时的最佳做法是什么？

- 在 Amazon Forecast 中使用 S3 存储桶时，您应该充分了解自己的数据分类实践并规划相关的数据安全需求。
- 对于 Amazon S3 存储桶配置，我们强烈建议您在 S3 存储桶策略中启用 HTTPS 强制执行。
- 您必须知道管理员角色 “customer_forecast_admin_role” 支持对亚马逊 S3 存储桶进行许可访问（S3 对象Get/Delete/Put），命名为 “customer-forecast-*”。注意：如果您需要对多个团队进行精细的访问控制，请遵循以下做法：
  - 定义您的基于团队的访问权限 IAM 身份（角色/用户），对相关 Amazon S3 存储桶具有最低权限访问权限。
  - team/project 基于创建 AWS KMS CMKs 授予对应的 IAM 身份的适当访问权限。（用户访问权限和 'AmazonForecast-ExecutionRole-{团队/项目}'。
  - 使用创建的设置 S3 存储桶默认加密 AWS KMS CMKs。
  - 在 S3 存储桶策略上使用 HTTPS 协议强制执行 S3 API 流量。
  - 对相关 IAM 身份（用户访问权限和 “AmazonForecast-ExecutionRole-{team/project}”）的已批准访问存储桶强制执行 S3 存储桶配置。
- 如果您想将 “customer_forecast_admin_role” 用于一般用途，请考虑前面列出的保护 S3 存储桶的要点。

问：有关 Amazon Forecast 的合规信息在哪里？

请参阅AWS 服务合规计划。

使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 FSx 功能。Amazon FSx 提供完全托管的第三方文件系统。Amazon FSx 为您提供第三方文件系统的原生兼容性，其功能集适用于基于 Windows 的存储、高性能计算 (HPC)、机器学习和电子设计自动化 (EDA) 等工作负

载。Amazon FSx 可自动执行耗时的管理任务，例如硬件配置、软件配置、修补和备份。Amazon FSx 将文件系统与云原生 AWS 服务集成，使其对更广泛的工作负载更加有用。

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon fo FSx r Lustre。要了解更多信息，请参阅 Amazon FSx。

AWS Managed Services FSx 中的亚马逊常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 FSx ？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 FSx 。此 RFC 为您的账户配置以下 IAM 角色:`customer_fsx_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： FSx 在我的 AMS 账户中使用 Amazon 有哪些限制？

没有任何限制。该服务的全部功能都可用。

问：在我的 AMS 账户 FSx 中使用 Amazon 的先决条件或依赖条件是什么？

没有先决条件。但是，对于多可用区等高级配置，您必须安装和管理 DFS 复制和 DFS 命名空间服务。有关更多信息，请参阅部署多可用区文件系统。

问：如何将我的 Amazon FSx 文件系统与我的多账户 landing zone 托管 AD 集成？

创建亚马逊 FSx 文件系统时，您可以将您的 MALZ 托管 AD 指定为 “AWS 托管的 Microsoft Active Directory”，用于 Windows 身份验证。有关更多信息，请参阅 “将亚马逊 FSx 与微软 Active Dire AWS Directory Service ctory 搭配使用”

您还必须先将托管 AD 共享给应用程序账户。为此，请使用管理 | Directory Service | Directory Service | Directory | 共享目录更改类型 (ct-369odosk0pd9w) 提交 RFC。

问：哪些用户属于 AWS 委派 FSx 管理员组？

只有 IT 文件服务器管理员。该组对所有文件共享都具有完全访问权限。

问：我是否应该使用在配置 FSx系统时创建的默认文件共享（共享）？

不，我们不建议使用已配置的默认文件共享，即共享。它向所有人授予完全访问权限，这违反了最低权限原则。相反，可以创建更小的自定义文件共享，以满足您的业务需求。

问：如何为企业中的特定组织创建自定义文件共享？

有关创建自定义文件共享的说明，请参阅文件共享。使用最低权限原则限制对每个文件共享的访问权限。

使用 AMS SSP 在你的 AMS 账户中 FSx 为亚马逊配置 OpenZFS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托 FSx 管账户中访问亚马逊 OpenZFS 功能。FSx for OpenZFS 是一项完全托管的文件存储服务，无需更改应用程序代码或数据管理方式，即可轻松地将本地 ZFS 或其他基于 Linux 的文件服务器中的数据移动到 AWS。它提供基于开源 OpenZFS 文件系统的高度可靠、可扩展、高性能和功能丰富的文件存储，提供 OpenZFS 文件系统熟悉的特性和功能，同时具有完全托管服务的敏捷性、可扩展性和简单性。 AWS 对于构建云原生应用程序的开发人员，它提供了简单、高性能的存储，并具有丰富的数据处理功能。

FSx openZFS 文件系统可使用行业标准 NFS 协议（v3、v4.0、v4.1、v4.2）从 Linux、Windows 和 macOS 计算实例和容器中广泛访问。OpenZFS 由 AWS Graviton 处理器以及最新的 AWS 磁盘和网络技术（包括 AWS 可扩展的可靠数据报网络和 AWS Nitro 系统）提供支持，可提供高达 100 万个 IOPS，延迟 FSx 为数百微秒。凭借对即时 point-in-time快照和数据克隆等 OpenZFS 功能的全面支持， FSx For OpenZFS 使您可以轻松地将本地文件服务器替换为提供熟悉文件系统功能的 AWS 存储，并且无需进行冗长的资格认证以及更改或重新架构现有应用程序或工具。而且，通过将 OpenZFS 数据管理功能的强大功能与最新 AWS 技术的高性能和成本效益相结合，for OpenZFS 使您能够构建和运行高性能、 FSx 数据密集型应用程序。

作为一项完全托管 FSx 的服务，for OpenZFS 可以轻松启动、运行和扩展完全托管的文件系统 AWS ，取代您在本地运行的文件服务器，同时有助于提供更好的灵活性和更低的成本。使用 f FSx or OpenZFS，您不必再担心设置和配置文件服务器和存储卷、复制数据、安装和修补文件服务器软件、检测和解决硬件故障以及手动执行备份。它还提供了与其他 AWS 服务的丰富集成，例如 AWS Identity and Access Management (IAM)、 AWS Key Management Service (AWS KMS)、Amazon CloudWatch 和 AWS CloudTrail。

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon fo FSx r Lustre。要了解更多信息，请参阅 Amazon FSx。

AWS Man FSx aged Services 常见问题解答中的亚马逊 OpenZFS

问：如何申请在我的 AMS 账户中使用 FSx OpenZFS 的访问权限？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8 FSx z66n899dct) 更改类型提交 RFC，请求访问亚马逊 OpenZFS。此 RFC 为您的账户配置以下 IAM 角色:`customer_fsx_ontap_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 FSx OpenZFS 有哪些限制？

替换 Amazon FSx 弹性网络接口 (ENIs) 上的安全组需要您提交 “管理” | “其他” | “其他” | “更新”， RFCs 因为安全组是 AMS 环境的关键边界。这是唯一的限制。

问：在我的 AMS 账户中使用 FSx OpenZFS 有哪些先决条件或依赖关系？

没有先决条件。但是，您必须已使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊安装。

使用 AMS SSP 在您的 AMS 账户中 FSx 为 NetApp ONTAP 配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管 FSx 账户中访问 Amazon for NetApp ONTAP 功能。Amazon FSx f NetApp or ONTAP 是一项完全托管的服务，它基于广受欢迎的 ONTAP 文件系统提供高度可靠、可扩展、高性能和功能丰富的文件存储。 NetApp它提供了熟悉的特性、性能、功能和 APIs NetApp 文件系统，并具有完全托管的敏捷性、可扩展性和简单性 AWS 服务。

Amazon FSx f NetApp or ONTAP 提供功能丰富、快速且灵活的共享文件存储，可在本地或本地运行的 Linux、Windows 和 macOS 计算实例上广泛访问这些存储空间。 AWS FSx for ONTAP 提供具有亚毫秒延迟的高性能 SSD 存储，您只需单击一下按钮即可快照、克隆和复制文件，从而可以快速轻松地管理数据。它还可以自动将您的数据分层到成本更低的弹性存储，从而无需预置或管理容量，并允许您实现工作负载的 SSD 性能级别，同时只需为一小部分数据支付 SSD 存储费用。它通过完全托管的备份提供高度可用和耐用的存储，并支持跨区域灾难恢复，并支持流行的数据安全和防病毒应用程序，使保护和保护数据变得更加容易。对于在本地使用 NetApp ONTAP 的客户 FSx 来说，for ONTAP 是将基于文件的应用程序从本地迁移、备份或突发到本地的理想解决方案， AWS 无需更改应用程序代码或数据管理方式。

作为一项完全托管的服务，Amazon FSx for NetApp ONTAP 可以轻松地在云中启动和扩展可靠、高性能和安全的共享文件存储。有了 Amazon FSx for NetApp ONTAP，您不必再担心设置和配置文件服务器和存储卷、复制数据、安装和修补文件服务器软件、检测和解决硬件故障、管理故障转移和故障恢复以及手动执行备份。它还提供了与其他 AWS 服务（例如 AWS Identity and Access Management Amazon WorkSpaces 和）的丰富集成 AWS CloudTrail。 AWS Key Management Service

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon fo FSx r Lustre。要了解更多信息，请参阅 Amazon FSx。

AWS M FSx anaged Services 常见问题解答中的亚马逊 NetApp ONTAP 版

问：如何使用我的 AMS 账户申请访问亚马逊 FSx NetApp ONTAP 版？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66 NetApp n899dct) 更改类型提交 RFC，请求访问亚马逊 FSx ONTAP 版。此 RFC 为您的账户配置以下 IAM 角色:`customer_fsx_ontap_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon FSx f NetApp or ONTAP 有哪些限制？

将 Amazon 上的安全组替换 FSx 为 NetApp ONTAP 弹性网络接口 (ENIs) 需要您提交 “管理 | 其他 | 其他 | 其他 | 更新”， RFCs 因为安全组是 AMS 环境的关键边界。这是唯一的限制。

问：在我的 AMS 账户中使用 Amazon FSx for NetApp ONTAP 有哪些先决条件或依赖关系？

没有先决条件。但是，您必须已使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊安装。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Inspector Classic

> **Note**
>
> 终止支持通知：2026年5月20日， AWS 将终止对Amazon Inspector Classic的支持。2026 年 5 月 20 日之后，您将无法再访问亚马逊 Inspector Classic 控制台或亚马逊 Inspector Classic 资源。Amazon Inspector Classic 将不再适用于新账户和在过去六个月内未完成评估的账户。对于所有其他账户，访问权限将在 2026 年 5 月 20 日之前有效，之后您将无法再访问亚马逊 Inspector Classic 控制台或 Amazon Inspector Classic 资源。有关更多信息，请参阅 Amazon Inspector Classic 终止支持。

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Inspector Classic 功能。Amazon Inspector Classic 是一项自动安全评估服务，可帮助提高部署在其上的应用程序的安全性和合规性 AWS。Amazon Inspector Classic 会自动评估应用程序的漏洞、漏洞以及与最佳实践的偏差。执行评估后，Amazon Inspector Classic 会生成一份按严重程度排列优先顺序的安全发现的详细清单。这些发现可以直接查看，也可以作为详细评估报告的一部分进行审查，这些报告可通过 Amazon Inspector Classic 控制台或 API 获得。要了解更多信息，请参阅 Amazon Inspector 经典版。

AWS Managed Services 常见问题中的亚马逊 Inspector

问：如何使用我的 AMS 账户申请访问 Amazon Inspector Classic？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Amazon Inspector Classic。此 RFC 为您的账户`customer_inspector_admin_role`配置 IAM 角

色。该角色包括 AWS托管 AmazonInspectorFullAccess 策略。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Inspector Classic 有哪些限制？

没有任何限制。Amazon Inspector Classic 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Inspector Classic 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon Inspector Classic 没有任何先决条件或依赖关系。

在 AMS 中使用全新 Amazon Inspector

现在，你可以在你的 AMS 账户中使用新的 Amazon Inspector。

对于 Amazon Inspector Classic`AmazonInspectorFullAccess`，必须使用`customer-inspector-admin-role-ssm-inspector-agent-policy`和。但是，SSPS 角色已更新`customer-inspector-admin-role`，现在包括一个新增`policyAmazonInspector2FullAccess`角色。这项新政策允许使用新版本的 Amazon Inspector 的 API 权限。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kendra

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kendra 功能。Amazon Kendra 是一项智能搜索服务，它使用自然语言处理和高级机器学习算法，从您的数据中返回搜索问题的具体答案。与传统的基于关键字的搜索不同，Amazon Kendra 使用其语义和上下文理解功能来确定文档是否与搜索查询相关。Amazon Kendra 会返回问题的具体答案，因此您的体验接近于与人类专家互动。Amazon Kendra 具有高度的可扩展性，能够满足性能需求，与 Amazon S3 和 Amazon Lex 等其他 AWS 服务紧密集成，并提供企业级安全性。要了解更多信息，请参阅 Amazon Kendra;。

AWS Managed Services 常见问题解答中的亚马逊 Kendra

问：如何使用我的 AMS 账户申请访问亚马逊 Kendra？

要申请访问 Amazon Inspector Classic，请使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC。此 RFC 为您的账户`customer_kendra_console_role`配置 IAM 角色。在您的账户中配置后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Kendra 有哪些限制？

没有任何限制。Amazon Kendra 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kendra 的先决条件或依赖条件是什么？

开始使用 Amazon Kendra 没有任何先决条件或依赖关系。但是，根据您的具体用例，您可能需要访问其他 AWS 服务。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kinesis Data Streams

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kinesis Data Streams (KDS) 功能。Amazon Kinesis Data Streams 是一项高度可扩展、耐用的实时数据流服务。KDS 每秒可以持续捕获来自成千上万个来源（例如网站点击流、数据库事件流、财务交易、社交媒体源、IT 日志和位置跟踪事件）的千兆字节数据。收集的数据可在毫秒内获得，以实现实时分析用例，例如实时仪表板、实时异常检测、动态定价等。要了解更多信息，请参阅 Amazon Kinesis Data Stream s。

AWS Managed Services 中的 Kinesis Data Streams 常见问题解答

常见问题和答案：

问：如何通过我的 AMS 账户申请访问亚马逊 Kinesis Data Streams？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求访问亚马逊 Kinesis Data Streams。此 RFC 为您的账户配置以下 IAM 角色:`customer_kinesis_data_streaming_user_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Kinesis Data Streams 有哪些限制？

没有任何限制。Amazon Kinesis Data Streams 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kinesis Data Streams 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon Kinesis Data Streams 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kinesis Video Streams

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kinesis Video Streams (KVS) 功能。Amazon Kinesis Video Streams 可帮助您安全地将视频从联网设备流式传输 AWS 到用于分析、机器学习 (ML)、播放和其他处理的目的。Kinesis Video Streams 可自动配置并弹性扩展从数百万台设备摄取流视频数据所需的所有基础架构。它还可以持久地存储、加密和索引直播中的视频数据，并允许您通过访问数据。 easy-to-use APIsKinesis Video Streams 使您能够播放用于直播和点播观看的视频，并通过与 Amazon Rekognition Video 以及 Apache 和 OpenCV MxNet 等

TensorFlow机器学习框架的库集成，快速构建利用计算机视觉和视频分析的应用程序。要了解更多信息，请参阅 Amazon Kinesis Video Streams。

AWS Managed Services 中的亚马逊 Kinesis Video Streams 常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 Kinesis Video Streams Amazon Kinesis Video Streams？

使用管理 AWS | 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求访问亚马逊 Kinesis Video Streams。此 RFC 为您的账户配置以下 IAM 角色:`customer_kinesis_video_streaming_user_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Kinesis Video Streams 有哪些限制？

没有任何限制。Amazon Kinesis Video Streams 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kinesis Video Streams 有哪些先决条件或依赖关系？

在你的 AMS 账户中使用 Amazon Kinesis Video Streams 没有先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Lex

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Lex 功能。Amazon Lex 是一项使用语音和文本在任何应用程序中构建对话界面的服务。Amazon Lex 提供高级深度学习功能，包括用于将语音转换为文本的自动语音识别 (ASR) 和用于识别文本意图的自然语言理解 (NLU)，使您能够构建具有高度吸引力的用户体验和逼真的对话互动的应用程序。借助 Amazon Lex，任何开发者都可以使用支持 Amazon Alexa 的深度学习技术，使您能够快速轻松地构建复杂的自然语言、对话机器人或聊天机器人。要了解更多信息，请参阅 Amazon Lex。

AWS Managed Services 中的亚马逊 Lex 常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 Amazon Lex？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_lex_author_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Lex 有哪些限制？

为了防止对 AMS 基础设施进行任何修改，Amazon Lex 与 Lambda 的集成仅限于没有 “AMS-” 前缀的 Lambda 函数。

问：在我的 AMS 账户中使用 Amazon Lex 有哪些先决条件或依赖条件？

在您的 AMS 账户中使用 Amazon Lex 没有任何先决条件或依赖关系。

使用 AMS SSP 在您的 AMS 账户中配置亚马逊 MQ

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon MQ 功能。Amazon MQ 是一项适用于 Apache ActiveMQ 的托管消息代理服务，可帮助您在云中设置和操作消息代理。消息代理允许不同的软件系统（通常使用不同的编程语言和不同的平台）来通信和交换信息。Amazon MQ 通过管理流行的开源消息代理 ActiveMQ 的配置、设置和维护来减轻您的运营负担。将您当前的应用程序连接到 Amazon MQ 使用行业标准 APIs 和消息传递协议，包括 JMS、NMS、AMQP、STOMP、MQTT 和。 WebSocket使用标准意味着，在大多数情况下，迁移到 AWS时无需重写任何消息传递代码。要了解更多信息，请参阅什么是 Amazon MQ？

AWS Managed Services 常见问题解答中的亚马逊 MQ

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 MQ？

在您的 AMS 账户中使用亚马逊 MQ 的过程分为两步：

1. 配置亚马逊 MQ 代理。为此，请通过包含亚马逊 MQ Broker 的 RFC 提交 CFN 模板，其中包含部署 | Ingestion | Stack CloudFormation from template | 创建更改类型 (ct-36cn2avfrrj9v)，或者使用管理层 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76) 更改类型提交 RFC，请求配置亚马逊 MQ Broker 已存入您的账户。
2. 访问亚马逊 MQ 控制台。配置亚马逊 MQ Broker 后，使用管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，即可访问亚马逊 MQ 控制台。此 RFC 为您的账户配置以下 IAM 角色:`customer_mq_console_role`.

在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问：在我的 AMS 账户中使用 Amazon MQ 有哪些限制？

Amazon MQ 的全部功能可在您的 AMS 账户中使用；但是，由于需要提升权限，因此无法通过该政策配置亚马逊 MQ Broker。有关如何在您的账户中配置 Amazon MQ 经纪商的详细信息，请参阅上文。

问：在我的 AMS 账户中使用 Amazon MQ 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon MQ 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中为 Apache Flink 配置亚马逊托管服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Apache Flink 的亚马逊托管服务功能。适用于 Apache Flink 的托管服务是分析流数据、获得切实可行的见解以及实时响应业务和客户需求的最简单方法。适用于 Apache Flink 的 Amazon 托管服务降低了构建、管理流应用程序以及与其他 AWS 服务集成的复杂性。SQL 用户可以使用模板和交互式 SQL 编辑器轻松查询流数据或构建整个流应用程序。Java 开发人员可以使用开源 Java 库和 AWS 集成快速构建复杂的流媒体应用程序，以实时转换和分析数据。适用于 Apache Flink 的 Amazon 托管服务负责处理持续运行实时应用程序所需的一切，并自动扩展以匹配传入数据的数量和吞吐量。使用适用于 Apache Flink 的亚马逊托管服务，您只需为流媒体应用程序消耗的资源付费。没有最低费用或安装成本。要了解更多信息，请参阅适用于 A pache Flink 的亚马逊托管服务。

AWS Managed Services 常见问题解答中的 Apache Flink 托管服务

常见问题和答案：

问：如何使用我的 AMS 账户申请访问适用于 Apache Flink 的亚马逊托管服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_kinesis_analytics_application_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用适用于 Apache Flink 的亚马逊托管服务有哪些限制？

- 配置仅限于没有 “AMS-” 或 “MC-” 前缀的资源，以防止对 AMS 基础设施进行任何修改。
- 删除或创建新 Kinesis Data Streams 或 Firehose 的权限已从该政策中删除。我们还有另一项允许这样做的政策。

问：在我的 AMS 账户中使用 Amazon Kinesis Data Streams 有哪些先决条件或依赖关系？

有几个依赖关系：

- 适用于 Apache Flink 的亚马逊托管服务要求在使用适用于 Apache Flink 的托管服务配置应用程序之前，必须先创建 Kinesis Data Streams 或 Firehose。
- 基于资源的策略权限应指明特定的输入数据源。

使用 AMS SSP 在你的 AMS 账户中为 Apache Kafka 配置亚马逊托管流媒体 Kafka

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）功能。适用于 Apache Kafka 的 Amazon Managed Streaming 是一项完全 AWS 托管的流数据服务，可让您轻松构建和运行使用 Apache Kafka 处理流数据的应用程序，而无需成为 Apache Kafka 集群操作专家。Amazon MSK 为您管理 Apache Kafka 集群和 Apache 节点的配置、配置和维护。 ZooKeeper 亚马逊 MSK 还在控制台中显示了 Apache Kafka 的关键性能指标。 AWS

Amazon MSK 为您的 Apache Kafka 集群提供多个级别的安全保护，包括 VPC 网络隔离、用于控制平面 API 授权的 AWS IAM、静态加密、传输中的 TLS 加密、基于 TLS 的证书身份验证、受保护的身份验证。 SASL/SCRAM AWS Secrets Manager要了解更多信息，请参阅 Amazon MSK。

AWS Managed Services 常见问题解答中的亚马逊 MSK

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 MSK？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 策略和角色：

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`
- `customer-msk-admin-role.json`

在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用 Amazon MSK 有哪些限制？

要让 Amazon MSK 将代理日志传送到您配置的目标，请确保将`AmazonMSKFullAccess`策略附加到您的 IAM 角色。因此，完全访问权限已经到位。

问：使用 Amazon MSK 的先决条件或依赖条件是什么？

在创建 MSK 集群之前，您必须拥有一个 VPC 并在该 VPC 内拥有子网。默认情况下，AMS 在创建 AMS VPC 时会将其包括在内。

要了解亚马逊 MSK 的限制，请参阅亚马逊 MSK 限制。

使用 AMS SSP 在您的 AMS 账户中为 Prometheus 配置亚马逊托管服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Prometheus 的亚马逊托管服务 (AMP) 功能。Amazon Managed Service for Prometheus 是一项面向容器指标的无服务器 Prometheus 兼容监控服务，有助于更轻松地实现对容器环境的大规模监控。借助 Amazon Managed Service for Prometheus，您可以使用目前所用的开源 Prometheus 数据模型和查询语言来监控容器化工作负载的性能，还可以享受更高的可扩展性、可用性和安全性，而无需管理底层基础设施。

Amazon Prometheus 托管服务会随着工作负载的扩大和缩小规模而自动扩展操作指标的摄取、存储和查询。它与 AWS 安全服务集成，可以快速、安全地访问数据。有关更多信息，请参阅什么是 Prometheus 的亚马逊托管服务？

AWS Managed Services 常见问题解答中的亚马逊 Prometheus 托管服务

常见问题和答案：

问：如何使用我的 AMS 账户申请访问适用于 Prometheus 的亚马逊 Prometheus 托管服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer-prometheus-console-role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该`customer-prometheus-console-role`角色。

问：在我的 AMS 账户中使用适用于 Prometheus 的亚马逊 Prometheus 托管服务有哪些限制？

支持所有功能。

问：在我的 AMS 账户中使用适用于 Prometheus 的亚马逊 Prometheus 托管服务有哪些先决条件或依赖关系？

开始使用适用于 Prometheus 的亚马逊托管服务没有任何先决条件或依赖关系。但是，根据您的具体用例，您可能需要访问其他 AWS 服务。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Personalize

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Personalize 功能。Amazon Personalize 是一项机器学习服务，可让开发人员轻松为使用其应用程序的客户创建个性化推荐。

机器学习越来越多地用于通过提供个性化的产品和内容推荐、量身定制的搜索结果和有针对性的营销促销来提高客户参与度。但是，由于复杂性，开发制作这些复杂的推荐系统所必需的机器学习能力已超出了当今大多数组织的能力。Amazon Personalize 允许以前没有机器学习经验的开发者使用经过多年在 Amazon.com 上使用而完善的机器学习技术，轻松地在其应用程序中构建复杂的个性化功能。

借助 Amazon Personalize，您可以提供来自应用程序的活动流（点击量、页面浏览量、注册次数、购买次数等）以及您想要推荐的商品（例如文章、产品、视频或音乐）的清单。您也可以选择向 Amazon Personalize 提供来自用户的其他人口统计信息，例如年龄或地理位置。Amazon Personalize 将处理和检查数据，确定有意义的内容，选择正确的算法，并训练和优化针对您的数据定制的个性化模型。Amazon Personalize 分析的所有数据都是保密和安全的，并且仅用于您的定制推荐。您可以通过简单的 API 调用开始提供个性化推荐。您只需按实际用量付费，没有最低费用，也没有预先承诺。

要了解更多信息，请参阅 Amazon Personaliz e。

AWS Managed Services 常见问题解答中的亚马逊个性化

问：如何使用我的 AMS 账户申请访问 Amazon Personalize？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny)
更改类型来请求访问权限，您需要指定哪个 S3 存储桶包含用于个
性化生成推荐的数据。 AWS 此 RFC 为您的账户配置以下 IAM 角
色：`customer_personalize_console_role`和。`customer_personalize_service_role`

- 在您的账户中配置`customer_personalize_console_role`完毕后，您必须在联合解决方案中加入该角色。您也可以将附加`customer_personalize_console_policy`到除之外的其他现有角色`Customer_ReadOnly_Role`。
- 向您的账户提供后，您可以在创建新的数据集组时参考其
  ARN。`customer_personalize_service_role`

此时，AMS Operations 还将在您的账户中部署此服务角
色：`aws_code_pipeline_service_role_policy`。

问：在我的 AMS 账户中使用 Amazon Personalize 有哪些限制？

Amazon Personalize 配置仅限于没有 “ams-” 或 “mc-” 前缀的资源，以防止对 AMS 基础设施进行任何修改。

问：在我的 AMS 账户中使用 Amazon Personalize 有哪些先决条件或依赖条件？

- 如果存储数据的 S3 存储桶已加密，则必须提供 KMS 密钥 ID，这样我们就可以允许 Amazon Personalize 使用的角色解密该存储桶。

  Amazon Personalize 不支持默认 KMS S3 密钥。如果需要使用 KMS，请创建一个自定义密钥，然后打开 RFC，并使用更改类型 KMS Key | Create（需要查看），向其添加以下策略：

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- 必须使用以下存储桶策略创建 S3 存储桶。为此，请提交 RFC，更改类型为 S3 存储 | 创建策略。该政策允许 Amazon Personalize 访问数据；该存储桶将包含供亚马逊个性化使用的数据。

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
```

```
}
```

使用 AMS SSP QuickSight 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 QuickSight 功能。 QuickSight 是一项快速、基于云的商业智能服务，可为组织中的每个人提供见解。作为一项完全托管的服务，QuickSight 您可以轻松创建和发布包含机器学习 (ML) 见解的交互式仪表板。要了解更多信息，请参阅 Amazon QuickSight。

QuickSight 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 QuickSight 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_quicksight_console_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： QuickSight 在我的 AMS 账户中使用有什么限制？

- AWS 由于 IAM 策略依赖关系，您 QuickSight 无法访问上的资源设置。但是，AMS 团队会根据您启用服务的请求为您启用每项资源。
- 此模式不支持个人用户和群组的资源访问权限，因为此功能允许用户更改可能危及 AMS 基础设施的 IAM 权限。
- 由于更改 IAM 对象涉及风险， QuickSight 因此不支持从内部邀请 IAM 身份。
- QuickSight 服务提供两个版本：企业版和标准版。两者都提供了 AMS 支持的单点登录 (SSO) 选项。但是，企业版可以选择 QuickSight 与活动目录 (AD) 集成。 QuickSight 由于 AMS 账户结构与信任要求不兼容，在 AMS 上不支持与 AD 集成。 QuickSight

问：在我的 AMS 账户 QuickSight 中使用的先决条件或依赖条件是什么？

- 当 AMS 收到要添加的 RFC 时 QuickSight，您会收到一份服务请求，要求您提供更多信息；请向他们提供以下信息：
  - QuickSight 账户名（例如，*CustomerName*-quicksight
  - QuickSight 版本（标准版与企业版）

- 启用 QuickSight 服务的 AWS 区域（默认为您的 AMS AWS 区域）。
- QuickSight 账户的通知电子邮件地址。
- （可选）要分析的数据文件所在的 S3 存储桶。
- 连接 IDs 的 VPC 和子网 QuickSight 支持添加 VPC 连接的功能，该功能可在账户内 QuickSight 和资源之间实现私有连接。

AMS 操作员代表您执行注册流程并配置两个 QuickSight 功能：

- 自动发现数据源。
- VPC 连接。

> **Note**
>
> 这些操作需要由 AMS 操作员执行，因为在登录过程中需要提升的 IAM 和 VPC 权限。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Rekognition

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Rekognition 功能。Amazon Rekognition 使用久经考验、高度可扩展的深度学习技术，无需机器学习专业知识即可轻松地将图像和视频分析添加到您的应用程序中。借助 Amazon Rekognition，您可以识别图像和视频中的物体、人物、文本、场景和活动，还可以检测任何不当内容。Amazon Rekognition 还提供高度准确的面部分析和面部搜索功能，您可以使用这些功能来检测、分析和比较人脸，用于各种用户验证、人数统计和公共安全用例。

借助 Amazon Rekognition 自定义标签，您可以识别图像中特定于您的业务需求的对象和场景。例如，您可以构建模型来对装配线上的特定机器零件进行分类或检测不健康的工厂。Amazon Rekognition Custom Labels 为您处理模型开发的繁重工作，因此无需任何机器学习经验。您只需要提供要识别的物体或场景的图像，剩下的交给服务即可。

要了解更多信息，请参阅亚马逊 Rek ognition。

AWS Managed Services 常见问题解答中的亚马逊 Rekognition

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 Rekognition？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_rekognition_console_role & customer_rekognition_service_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Rekognition 有哪些限制？

亚马逊 Rekognition 的全部功能可通过亚马逊 Rekognition 自行配置服务角色获得。

问：在我的 AMS 账户中使用 Amazon Rekognition 有哪些先决条件或依赖关系？

如果您使用为亚马逊 Rekognition Video 流处理器或数据流提供源流视频的 Kinesis Video Streams 作为向 Kinesis Data Streams 写入数据的目标，请在创建 RFC 时向 AMS 提供。`kinesisStreamName`

使用 AMS SSP 在你的 AMS 账户中配置 SageMaker Amazon AI

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 SageMaker Amazon AI 功能。 SageMaker AI 为每位开发人员和数据科学家提供了快速构建、训练和部署机器学习模型的能力。Amazon SageMaker AI 是一项完全托管的服务，涵盖了整个机器学习工作流程，包括标记和准备数据、选择算法、训练模型、调整和优化模型以进行部署、做出预测和采取行动。您的模型能够以更少的工作量和更低的成本更快地投入生产。要了解更多信息，请参阅 Amazon SageMaker AI。

SageMaker AWS Managed Services 中的人工智能常见问题

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 SageMaker AI？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_sagemaker_admin_role`和服务角色`AmazonSageMaker-ExecutionRole-Admin`。在您的账户中配置 SageMaker AI 后，您必须在联合解决方案中加入该`customer_sagemaker_admin_role`角色。您无法直接访问服务角色；SageMaker AI 服务在执行各种操作时使用该角色，如下所述：传递角色。

问：在我的 AMS 账户中使用 SageMaker AI 有哪些限制？

- AMS Amazon A SageMaker I IAM 角色不支持以下用例：
  - SageMaker 目前不支持 AI Studio。
  - SageMaker 不支持 AI Ground Truth 来管理私人员工，因为此功能需要过于宽松地访问 Amazon Cognito 资源。如果需要管理私人员工，则可以申请一个具有 A SageMaker I 和 Amazon Cognito

权限相结合的自定义 IAM 角色。否则，我们建议使用公共劳动力（由 Amazon Mechanical Turk 提供支持）或 AWS Marketplace 服务提供商进行数据标记。

- 创建 VPC 终端节点以支持对 SageMaker AI 服务的 API 调用（aws.sagemaker。 {区域} .notebook，com.amazonaws。 {region} .sagemaker.api & com.amazonaws。 不支持 {region} .sagemaker.runtime），因为权限不能仅限于人工智能相关的服务。 SageMaker 要支持此用例，请提交管理 | 其他 | 其他 RFC 以创建相关的 VPC 终端节点。
- SageMaker 不支持 AI 端点自动缩放，因为 SageMaker AI 需要任何 (“*”) 资源的`DeleteAlarm`权限。要支持端点自动缩放，请提交 “管理 | 其他 | 其他 | 其他 RFC” 来为 SageMaker AI 终端节点设置自动缩放。

问：在我的 AMS 账户中使用 SageMaker AI 的先决条件或依赖条件是什么？

- 以下用例需要在使用前进行特殊配置：
  - 如果要使用 S3 存储桶来存储模型工件和数据，则必须使用部署 | 高级堆栈组件 | S3 存储 | 创建 RFC 请求一个以所需关键字（”、SageMaker “Sagemaker”、“sagemaker” 或 “aws-glue”）命名的 S3 存储桶。
  - 如果要使用弹性文件存储 (EFS)，则必须在同一个子网中配置 EFS 存储，并且必须得到安全组的允许。
  - 如果其他资源需要直接访问 SageMaker AI 服务（笔记本、API、运行时等），则必须通过以下方式请求配置：
    - 提交 RFC 以为终端节点创建安全组（部署 | 高级堆栈组件 | 安全组 | 创建 (auto)）。
    - 提交管理 | 其他 | 其他 | 创建 RFC 以设置相关的 VPC 终端节点。

问：对于**`customer_sagemaker_admin_role`**可以直接访问的资源，支持的命名约定有哪些？（以下内容适用于更新和删除权限；如果您需要其他支持的资源命名约定，请联系 AMS Cloud Architect 进行咨询。）

- 资源：传递`AmazonSageMaker-ExecutionRole-*`角色
  - 权限： SageMaker AI 自行配置的服务角色支持您使用 SageMaker AI 服务角色 (`AmazonSageMaker-ExecutionRole-*`) 和 AWS Glue AWS RoboMaker、和。 AWS Step Functions
- 资源：Secrets Manager 上的 AWS 秘密
  - 权限：使用`AmazonSageMaker-*`前缀描述、创建、获取、更新密钥。
  - 权限：当`SageMaker`资源标签设置为时，描述、获取机密`true`。

- 资源：存储库开启 AWS CodeCommit
  - 权限：创建/删除带AmazonSageMaker-*前缀的仓库。
  - 权限：在带有以下前缀的存储库 Pull/Push 上使用 Git *sagemaker*、*SageMaker*、和。*Sagemaker*
- 资源：Amazon ECR（亚马逊弹性容器注册表）存储库
  - 权限：权限：使用以下资源命名约定时，设置、删除存储库策略和上传容器镜像*sagemaker*。
- 资源：亚马逊 S3 存储桶
  - 权限：当资源具有以下前缀时，获取、放置、删除对象、中止分段上传 S3 对象：*SageMaker*、*Sagemaker*和。*sagemaker* aws-glue
  - 权限：当SageMaker标签设置为时获取 S3 对象true。
- 资源：Amazon CloudWatch 日志组
  - 权限：创建日志组或流、放置日志事件、列出、更新、创建、删除带以下前缀的日志传送：/aws/sagemaker/*。
- 资源：Amazon CloudWatch 指标
  - 权限：使用以下前缀时放入指标数据：AWS/SageMaker、AWS/SageMaker/、aws/SageMaker、aws/SageMaker/、aws/sagemakeraws/sagemaker/、和/aws/sagemaker/.。
- 资源：Amazon CloudWatch 控制面板
  - 权限:使用以下前缀时的 Create/Delete 仪表板:customer_*.
- 资源：Amazon SNS（简单通知服务）主题
  - 权限：使用以下前缀时 Subscribe/Create 的主题：*sagemaker**SageMaker*、和。*Sagemaker*

问：**AmazonSageMakerFullAccess**和有什么区别**customer_sagemaker_admin_role**？

customer_sagemaker_admin_role与customer_sagemaker_admin_policy提供的权限几乎相同，唯一的 AmazonSageMakerFullAccess 不同是：

- 连接 Amazon Cognito 和 AWS Glue 资源的权限。 AWS RoboMaker
- SageMaker AI 端点自动缩放。您必须通过管理 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | 更新实体或策略（需要审查）更改类型 (ct-27tuth19k52b4) 提交 RFC 才能临时或永久提升自动扩展权限，因为自动扩展需要对服务的许可访问权限。 CloudWatch

问：如何在静态数据加密中采用 AWS KMS 客户托管密钥？

您必须确保已在客户托管密钥上正确设置密钥策略，以便相关的 IAM 用户或角色可以使用这些密钥。有关更多信息，请参阅AWS KMS 密钥策略文档。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 简单电子邮件服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊简单电子邮件服务 (Amazon SES) 功能。Amazon Simple Email Service 是一项基于云的电子邮件发送服务，旨在帮助数字营销人员和应用程序开发人员发送营销、通知和交易电子邮件。

您可以使用 SMTP 接口或其中一个接口将 Amazon SES 直接集成 AWS SDKs 到您的现有应用程序中。您还可以将 Amazon SES 的电子邮件发送功能集成到您已经使用的软件中，例如票务系统和电子邮件客户端。

要了解更多信息，请参阅 Amazon 简单电子邮件服务。

AWS Managed Services 中的亚马逊 SES 常见问题解答

问：如何使用我的 AMS 账户申请访问 Amazon SES？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Amazon SES。此 RFC 为您的账户配置以下 IAM 角色:`customer_ses_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon SES 有哪些先决条件或依赖条件？

- 您必须配置 S3 存储桶策略以允许 Amazon SES 向存储桶发布事件。
- 您必须使用默认 (S AWS ES) 或配置 CMK 密钥，以允许 Amazon SES 加密电子邮件并将事件推送到属于该账户的其他服务资源，例如 Amazon S3、Amazon SNS、Lambda 和 Firehose。

问：在我的 AMS 账户中使用 Amazon SES 有哪些限制？

您必须筹集 RFCs 才能创建以下资源：

- PutEvents 有权访问 Kinesis Firehose 直播的 SMTP 用户和 IAM 服务角色。
- 您必须使用 AMS 更改类型创建 S3 存储桶、Firehose 流、SNS 主题等新 AWS 资源，这样您的 Amazon SES 规则和配置集的目标才能使用这些资源。
- SMTP 凭证。要申请新的 SMTP 凭证，请使用更改类型（管理 | 其他 | 其他 | 创建）。AMS 会为您创建凭证并将其添加到 Secrets Manager 中。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 简单工作流程服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊简单工作流服务 (Amazon SWF) Simple Workflow Service 功能。Amazon Simple Workflow Service 可帮助开发人员构建、运行和扩展具有并行或顺序步骤的后台作业。您可以将 Amazon SWF 视为云端完全托管的状态跟踪器和任务协调器。如果您的应用程序的步骤需要超过 500 毫秒才能完成，则需要跟踪处理状态，或者在任务失败时需要恢复或重试，Amazon SWF 可以为您提供帮助。要了解更多信息，请参阅 Amazon 简单工作流程服务。

AWS Managed Services 常见问题解答中的亚马逊 SWF

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 SWF？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_swf_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon SWF 有哪些限制？

Lambda `InvokeFunction` 权限已包含在该服务中，但是，添加到所有 AMS `customer_deny_policy` 客户角色的 AMS 明确拒绝访问 AMS Lambda 函数和 AMS 拥有的资源。要在 Amazon SWF 中标记或取消标记资源，请提交 “管理 | 其他 | 其他更改类型”。

问：在我的 AMS 账户中使用 Amazon SWF 有哪些先决条件或依赖条件？

Amazon SWF 依赖于该 AWS Lambda 服务，因此，该角色提供了调用 Lambda 的权限，并且无需其他权限即可从亚马逊 SWF 调用 Lambda。否则，使用 Amazon SWF 没有任何先决条件。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Textract

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Textract 功能。Amazon Textract 是一项完全托管的机器学习服务，可自动从扫描的文档中提取打印的文本、手写和其他数据，这些数据超出了简单的光学字符识别 (OCR) 范围，可以识别、理解和提取表单和表格中的数据。要了解更多信息，请参阅 Amazon Textract。

AWS Managed Services 常见问题解答中的亚马逊 Textract

常见问题和答案：

问：如何申请在我的 AMS 账户中设置亚马逊 Textract？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_textract_console_role`、`customer_textract_human_review_execution_role` 和 `customer_ec2_textract_instance_profile`。在您的账户中配置该角色后，您必须在联合解决方案 `customer_textract_console_role` 中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Textract 有哪些限制？

在您的 AMS 账户中使用亚马逊 Textract 没有任何限制。

问：在我的 AMS 账户中使用 Amazon Textract 有哪些先决条件或依赖条件？

您必须通过提交 RFC 部署 | 高级堆栈组件 |S3 存储 | 创建 (ct-1a68ck03fn98r) 来请求创建 S3 存储桶。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Transcribe

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Transcribe 功能。Amazon Transcribe 是一项完全托管且持续训练的自动语音识别服务，可自动从音频文件生成带有时间戳的文本脚本。借助 Amazon Transcribe，开发人员可以轻松地为其 speech-to-text应用程序添加功能。计算机几乎不可能搜索和分析音频数据。因此，录制的语音需要先转换为文本，然后才能用于应用程序。从历史上看，客户必须与转录提供商合作，这些提供商要求他们签订昂贵的合同，并且很难集成到他们的技术堆栈中来完成这项任务。这些提供商中有许多使用过时的技术，无法很好地适应不同的场景，例如联络中心常见的低保真电话音频，这会导致准确性差。

Amazon Transcribe 使用一种称为自动语音识别 (ASR) 的深度学习过程来快速准确地将语音转换为文本。Amazon Transcribe 可用于转录客户服务电话、自动添加隐藏式字幕和字幕，以及生成媒体资产的元数据以创建完全可搜索的档案。您可以使用 Amazon Transcribe Medical 为临床文档应用程序添加医疗 speech-to-text功能。要了解更多信息，请参阅 Amazon Transcribe。

AWS Managed Services 中的亚马逊转录常见问题解答

常见问题和答案：

问：如何申请在我的 AMS 账户中设置 Amazon Transcribe？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_transcribe_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Transcribe 有哪些限制？

使用 transcribe 时，您必须使用 “customer-transcribe*” 作为存储桶的前缀，除非 RA 和另有说明。

您无法在 Amazon 转录中创建 IAM 角色。

您不能使用服务托管 S3 存储桶存储默认 SSP 中的输出数据（如果需要，请联系您的账户 CA）。

如果您想使用不属于 AMS 命名空间的客户管理的 KMS 密钥，则必须提交 “风险接受”。

问：在我的 AMS 账户中使用 Amazon Transcribe 有哪些先决条件或依赖条件？

S3 必须有权访问名为 “客户转录*” 的存储桶。如果您的 S3 存储桶使用 KMS 密钥加密，则需要使用 KMS 才能使用 Amazon Transcribe。如果存储桶不需要加密，则可以删除 “KMStranscribeAllow”。

使用 AMS SSP WorkSpaces 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 WorkSpaces 功能。WorkSpaces 允许你为用户配置基于云的虚拟 Microsoft Windows 或 Amazon Linux 桌面，称为 WorkSpaces。 WorkSpaces 无需购买和部署硬件或安装复杂的软件。您可以根据需求的变更，快速添加或删除用户。用户使用 WorkSpaces 支持的设备上的客户端应用程序或者（对于 Windows，则使用 Web 浏览器）进行访问 WorkSpaces，然后使用现有的本地 Active Directory (AD) 凭据登录。

要了解更多信息，请参阅 Amazon WorkSpaces。

WorkSpaces 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 WorkSpaces 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_workspaces_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： WorkSpaces 在我的 AMS 账户中使用有什么限制？

Amazon WorkSpaces 自行配置的服务角色提供了工作空间的全部功能。

问：在我的 AMS 账户 WorkSpaces 中使用的先决条件或依赖条件是什么？

- WorkSpaces 受 AWS 区域限制；因此，AD Connector 必须配置在托管 WorkSpaces 实例的同一 AWS 区域。

客户可以使用以下两种方法之一 WorkSpaces 连接到客户 AD：

1. 使用 AD 连接器代理对本地 Active Directory 服务的身份验证（首选）：

   在将您的 WorkSpaces 实例与本地目录服务集成之前，在您的 AMS 账户中配置 Active Directory (AD) 连接器。AD Connector 充当您的现有 AD 用户（来自您的域）的代理，让他们 WorkSpaces 使用现有本地 AD 凭据进行连接。这是首选，因为 WorkSpaces 它们可以直接加入客户的本地域，该域既充当资源林，又充当用户林，从而增强了客户方面的控制权。

   有关更多信息，请参阅部署 Amazon 的最佳实践 WorkSpaces（场景 1）。

2. 将 AD Connector 与 AWS 微软 AD、共享服务 VPC 以及对本地的单向信任一起使用：

   您还可以先建立从 AMS 管理的 AD 到您的本地 AD 的单向传出信任，从而使用本地目录对用户进行身份验证。 WorkSpaces 将使用 AD Connector 加入 AMS 管理的 AD。 WorkSpaces 然后，访问权限将通过 AMS 托管的 AD 委派给 WorkSpaces 实例，无需与您的本地环境建立双向信任。在这种情况下，用户林将位于客户 AD 中，资源林将位于 AMS 管理的 AD 中（可以通过 RFC 请求对 AMS 管理的 AD 进行更改）。请注意， WorkSpaces VPC 和运行 AMS 托管 AD 的 MALZ 共享服务 VPC 之间的连接是通过 Transit Gateway 建立的。

   有关更多信息，请参阅部署 Amazon 的最佳实践 WorkSpaces（场景 6）。

> **Note**
>
> 可以通过提交 “管理 | 其他 | 其他 | 其他 | 创建更改类型 RFC” 来配置 AD Connector，其中包含先决条件 AD 配置的详细信息；有关更多信息，请参阅创建 AD 连接器。如果使用方法 2 在 AMS 管理的 AD 中创建资源林，请通过运行 AMS 管理的 AD 在 AMS 共享服务账户中提交另一个管理 | 其他 | 其他 | 创建更改类型 RFC。

使用 AMS SSP 在您的 AMS 账户中配置 AMS 代码服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 AMS Code 服务功能。AMS Code 服务是 AWS 代码管理服务的专有捆绑包，详见下文。您可以选择使用 AMS Code 服务在 AMS 中部署所有服务，也可以在 AMS 中单独部署这些服务。

AMS 代码服务包括以下服务：

- AWS CodeCommit：一种完全托管的源代码控制服务，用于托管基于 Git 的安全存储库。它使团队可以在安全且高度可扩展的生态系统中协作处理代码。 CodeCommit 无需操作自己的源代码控制

系统或担心扩展其基础架构。您可以使用 CodeCommit 将源代码中的内容安全地存储到二进制文件中，并且它可与您现有的 Git 工具无缝协作。要了解更多信息，请参阅 AWS CodeCommit。

要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅使用 AMS SSP AWS CodeCommit 在您的 AMS 账户中进行配置。

- AWS CodeBuild：一种完全托管的持续集成服务，用于编译源代码、运行测试和生成随时可以部署的软件包。使用 CodeBuild，您无需预置、管理和扩展自己的构建服务器。 CodeBuild 持续扩展并同时处理多个构建，因此您的构建不会在队列中等待。您可以使用预先打包的构建环境快速开始，也可以创建使用您自己的构建工具的自定义构建环境。使用 CodeBuild，按分钟计费所使用的计算资源。要了解更多信息，请参阅 AWS CodeBuild。

  要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置。
- AWS CodeDeploy：一项完全托管的部署服务，可自动将软件部署到各种计算服务，例如 Amazon EC2 和您的本地服务器。 AWS CodeDeploy 帮助您快速发布新功能，帮助您避免应用程序部署期间的停机，并处理更新应用程序的复杂性。您可以使用 AWS CodeDeploy 自动化软件部署，无需进行容易出错的手动操作。该服务可根据您的部署需求进行扩展。要了解更多信息，请参阅 AWS CodeDeploy。

  要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置。
- AWS CodePipeline：一项完全托管的持续交付服务，可帮助您实现发布管道的自动化，从而实现快速可靠的应用程序和基础设施更新。 CodePipeline 每次发生代码更改时，都会根据您定义的发布模型自动执行发布过程的构建、测试和部署阶段。这让您可以快速而可靠地交付各种功能和更新。您可以轻松地 AWS CodePipeline 与第三方服务集成，例如 GitHub 或与您自己的自定义插件集成。使用 AWS CodePipeline，您只需为实际用量付费。无前期费用，无长期承诺。要了解更多信息，请参阅 AWS CodePipeline。

  要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置。

AWS Managed Services 常见问题解答中的 AMS 代码服务

问：如何使用我的 AMS 账户申请访问 AMS Code 服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_code_suite_console_role`. 在您的账户中配置后，您必须在联合解决方案中加入该角色。此时，AMS Operation

customer_codebuild_service_role s 还将在您的账户中为 CodeDeploy 和aws_code_pipeline_service_role服务部署 CodeBuild、、 CodePipeline 服务角色。customer_codedeploy_service_role如果需要其他 IAM 权限，请提交 AMS 服务请求。customer_codebuild_service_role

> **Note**
>
> 您也可以单独添加这些服务；有关信息，请分别参见使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置、和。

问：在我的 AMS 账户中使用 AMS 代码服务有哪些限制？

- AWS CodeCommit：如果具有创建 SNS 主题的相关权限， CodeCommit 则开启的触发器功能已禁用。直接进行身份验证受到限制；用户应使用 Cre CodeCommit dential Helper 进行身份验证。某些 KMS 命令也受到限制： kms:加密、 kms:解密、 kms:ReEncrypt、 kms:GenereteDataKey kms:GenerateDataKeyWithoutPlaintext、和。 kms: DescribeKey
- CodeBuild：对于 AWS CodeBuild 控制台管理员访问权限，权限在资源级别受到限制；例如，对特定资源的 CloudWatch 操作受到限制，iam:PassRole权限受到控制。
- CodeDeploy：目前仅 CodeDeploy 支持在 Amazon EC2 /本地部署。不支持通过 CodeDeploy ECS 和 Lambda 进行部署。
- CodePipeline: CodePipeline 功能、阶段和提供者仅限于以下内容：
  - 部署阶段：亚马逊 S3 和 AWS CodeDeploy
  - 来源阶段：Amazon S3、 AWS CodeCommit、Bit Bucket 和 GitHub
  - 建造阶段： AWS CodeBuild 还有 Jenkins
  - 批准阶段：亚马逊 SNS
  - 测试阶段： AWS CodeBuild、Jenkins、、Ghost Inspector UI 测试、Micro Focus Loa StormRunner d、Runscope BlazeMeter
  - 调用阶段：Step Functions 和 Lambda

> **Note**
>
> AMS Operations customer_code_pipeline_lambda_policy 在您的账户中部署；它必须与 Lambda 调用阶段的 Lambda 执行角色相关联。提供您想要添加此策略的 Lambda service/execution 角色名称。如果没有自定义 Lambda service/execution 角色，则 AMS

会创建一个名为的新角色customer_code_pipeline_lambda_execution_role，该角色是和的 customer_lambda_basic_execution_role副本。customer_code_pipeline_lambda_policy

问：在我的 AMS 账户中使用 AMS Code 服务的先决条件或依赖条件是什么？

- CodeCommit：如果 S3 存储桶使用 AWS KMS 密钥加密， AWS KMS 则必须使用 AWS CodeCommit S3 和。
- CodeBuild：如果定义的 AWS CodeBuild 服务角色需要其他 IAM 权限，请通过 AMS 服务请求请求这些权限。
- CodeDeploy: 无。
- CodePipeline: 无。 AWS 支持的服务 AWS CodeDeploy—AWS CodeCommit AWS CodeBuild、、— 必须在发布之前或同时启动。 CodePipeline但是，这是由 AMS 工程师完成的。

使用 AMS SSP AWS Amplify 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Amplify 功能。 AWS Amplify 这是一个完整的解决方案，允许前端 Web 和移动开发人员轻松构建、连接和托管全栈应用程序。随着用例的演变，Amplify 可以灵活地利用 AWS 服务的广度。Amplify 提供用于构建全栈 iOS、安卓、Flutter、Web 和 React Native 应用程序的产品。要了解更多信息，请参阅AWS Amplify。

AWS Amplify 在 AWS Managed Services 常见问题中

常见问题和答案：

问： AWS Amplify 如何申请在我的 AMS 账户中进行设置？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_amplify_console_role. 配置到您的账户后，您必须在联合解决方案中加入该角色。

此外，您必须提供风险接受，因为您 AWS Amplify 拥有基础架构变更权限。为此，请与您的云服务交付经理 (CSDM) 合作。

问： AWS Amplify 在我的 AMS 账户中使用有什么限制？

使用 Amplify 时，您必须使用'amplify*'作为存储桶的前缀，除非 RA 和另有说明。

问：在我的 AMS 账户 AWS Amplify 中使用的先决条件或依赖条件是什么？

在您的 AMS 账户 AWS Amplify 中使用没有任何先决条件。

仅限 Malz 环境：Amplify 的默认载入角色是 “customer_amplify_console_role”。要使用自定义角色，请先部署 IAM 实体。然后，再创建一个 RFC，将您的自定义角色添加到应用程序帐户的服务控制策略允许列表中。

使用 AMS SSP 进行配置 AWS AppSync

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS AppSync 功能。 AWS AppSync 允许您创建灵活的 API 来安全地访问、操作和合并来自一个或多个数据源的数据，从而简化应用程序开发。 AWS AppSync 是一项托管服务，它使用 GraphQL 让应用程序可以轻松地准确获取所需的数据。

借 AWS AppSync助，您可以在一系列数据源（例如 NoSQL 数据存储、关系数据库、HTTP APIs 和自定义数据源）上构建可扩展的应用程序，包括那些需要实时更新的应用程序。 AWS Lambda对于移动和 Web 应用程序， AWS AppSync 还可在设备离线时提供本地数据访问权限，并在设备重新联机时提供可自定义冲突解决方案的数据同步。要了解更多信息，请参阅AWS AppSync。

AWS AppSync 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS AppSync ？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角
色：`customer_appsync_service_role`和。`customer_appsync_author_role`在您的账户中配置后，您必须在联合解决方案`customer_appsync_author_role`中加载。

问：使用有哪些限制 AWS AppSync？

- 在客户上 AppSync 创建数据源时，需要指定先前创建的服务角色，不允许创建新角色，因此会返回访问被拒绝的消息
- AppSync 角色配置为限制对包含 “AMS-” 或 “MC-” 前缀的资源的权限，以防止对 AMS 基础设施进行任何修改。

问：使用的先决条件或依赖关系 AWS AppSync是什么？

该服务允许将多个其他服务用作数据源，因此使用这些服务的基本权限包含在服务角色 (`customer_appsync_service_role`) 中，但在使用服务时必须手动选择服务角色。

使用 AMS SSP AWS App Mesh 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS App Mesh 功能。 AWS App Mesh 提供应用程序级联网，使您的服务可以轻松地在多种类型的计算基础设施之间相互通信。App Mesh 标准化了您的服务通信方式，为您提供 end-to-end可视性并确保应用程序的高可用性。

AWS App Mesh 通过为跨多种类型的计算基础设施构建的服务提供一致的可见性和网络流量控制，使服务运行变得更加容易。App Mesh 无需更新应用程序代码，即可更改监控数据的收集方式或服务间流量的路由方式。App Mesh 将每项服务配置为导出监控数据，并在整个应用程序中实现一致的通信控制逻辑。这样可以轻松快速查明错误的确切位置，并在出现故障或需要部署代码更改时自动重新路由网络流量。要了解更多信息，请参阅AWS App Mesh。

AWS App Mesh 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS App Mesh ？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_app_mesh_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用有哪些限制 AWS App Mesh？

的全部功能可在您 AWS App Mesh 的 AMS 账户中使用。

问：使用的先决条件或依赖关系 AWS App Mesh是什么？

您的 AMS 账户 AWS App Mesh 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Audit Manager 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Audit Manager 功能。Audit Manager 可帮助您持续审计 AWS 使用情况，以简化评估风险以及对法规和行业标准的合规性的方式。Audit Manager 可自动收集证据，以便更轻松地评估您的策略、过程和活动是否有效运行。当需要进行审计时，Audit Manager 可以帮助您管理利益相关者对控制措施的审查，并帮助您以更少的手动工作来生成可供审计的报告。要了解更多信息，请参阅 Audit Manager。

AWS Audit Manager 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Audit Manager 的 AMS 账户？

您可以通过提交 AWS 服务 RFC 管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 来申请访问权限。此 RFC 在您的账户中配置以下 IAM 角色:`customer-audit-manager-admin-Role`. 在您的账户中配置后，您必须在联合解决方案中加入该角色。

问：使用有什么限制 AWS Audit Manager？

在您的 AMS 账户 AWS Audit Manager 中使用没有任何限制。提供了 AWS Audit Manager 的全部功能。

问：使用的先决条件或依赖关系 AWS Audit Manager是什么？

1. 您需要向 AMS 提供您 reports/assessments 要存放的 s3 存储桶。
2. 如果您想使用该服务进行加密，则需要向 AMS 提供要使用的 KMS CMK ARN。
3. 如果您想向某个主题发送 SNS 通知，则必须提供该主题的名称或 arn。
4. （可选）如果您想在 Audit Manager 中启用 Organizations 作为多账户登录区域的一部分，并且想要委托管理员帐户，则还有一个额外的先决条件：在 RFC（管理 | AWS 服务 | 兼容服务 | 添加）的描述字段中，提及您要在 Audit Manager 设置中使用委派管理员帐户，并提供以下详细信息：
   - KMS CMK ARN（最初用于设置 Audit Manager）
   - Audit Manager 可以用作此多账户登录区域一部分的委托管理员账户 ID（可以是 MALZ 应用程序账户）

使用 AMS SSP AWS Batch 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Batch 功能。 AWS Batch 使开发人员、科学家和工程师能够轻松高效地运行成千上万的批量计算作业 AWS。 AWS Batch 根据提交的批处理作业的容量和特定资源要求，动态配置计算资源的最佳数量和类型（例如 CPU 或内存优化型实例）。有了它 AWS Batch，您无需安装和管理用于运行作业的批处理计算软件或服务器集群，这样您就可以专注于分析结果和解决问题。要了解更多信息，请参阅AWS Batch。

AWS Batch 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Batch 的 AMS 账户？

1. 要申请访问权限 AWS Batch，请提交 RFC 管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct)。此 RFC 在您的账户中配置了以下 IAM 角色和策略：

IAM 角色：

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

策略：

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. 在您的账户中配置后，您必须在联合解决方案`customer_batch_console_role`中加入该角色。

问：使用有什么限制 AWS Batch？

创建计算环境时，应将 EC2 实例标记为 “customer_batch” 或 “customer_batch”。如果未标记实例，则在任务完成时不会批量终止实例。

问：使用的先决条件或依赖关系 AWS Batch是什么？

您的 AMS 账户 AWS Batch 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Certificate Manager 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Certificate Manager (ACM) 功能。 AWS Certificate Manager 是一项服务，允许您预置、管理和部署用于服务和内部连接资源的公共和私有安全套接字 Layer/Transport 层安全 (SSL/TLS) 证书。 AWS SSL/TLS 证书用于保护网络通信并通过互联网确定网站的身份以及私有网络上的资源。 AWS Certificate Manager 消除了购买、上传和续订 SSL/TLS 证书的耗时手动流程。

借助 AWS Certificate Manager，您可以申请证书，将其部署到集成 ACM 的 AWS 资源（例如弹性负载均衡器、Amazon CloudFront 分配）和 API APIs Gateway 上，然后让我们来 AWS Certificate Manager 处理证书续订。它还使您能够为内部资源创建私有证书，并集中管理证书生命周期。通过预配置的 AWS Certificate Manager 用于集成 ACM 的服务的公有和私有证书是免费的。您只需为为运行应用程序而创建的 AWS 资源付费。使用 AWS 私有证书颁发机构，您按月支付操作费用 AWS 私有 CA 和您颁发的私有证书的费用。要了解更多信息，请参阅 AWS Certificate Manager - AWS 文档。

AWS Managed Services 中的 ACM 常见问题解答

常见问题和答案：

问：如何在 AMS 账户 AWS Certificate Manager 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_acm_create_role`. 您可以使用此角色来创建和管理 ACM 证书。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

即使您尚未添加 IAM 角色，也可以使用以下更改类型创建 AC `customer_acm_create_role` M 证书：

- ACM | 创建公共证书
- ACM | 创建私有证书
- ACM 证书及其他 SANs | 创建

问：使用有哪些限制 AWS Certificate Manager？

您必须向 AMS 提交更改申请 (RFC) 才能删除或修改现有证书，因为这些操作需要完全的管理员访问权限（使用管理 | 其他 | 其他 | 更新更改类型 (ct-0xdawir96cy7k)。 请注意，IAM 策略不能根据标签名称（mc*、ams* 等）排除权限。证书不产生费用，因此删除未使用的证书对时间不敏感。

问：使用 Certificate Manager 的先决条件或依赖条件是什么？

现有的公有 DNS 名称和创建 DNS 别名记录的访问权限，但这些记录无需托管在托管账户中。

使用 AMS SSP AWS 私有证书颁发机构 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS 私有证书颁发机构 功能。私有证书用于识别和保护私有网络上互联资源之间的通信，例如服务器、移动设备和物联网设备和应用程序。 AWS 私有 CA 是一项托管私有 CA 服务，可帮助您轻松安全地管理私有证书的生命周期。

AWS 私有 CA 为您提供高度可用的私有 CA 服务，无需支付运营自己的私有 CA 的前期投资和持续维护成本。 AWS 私有 CA 将 ACM 的证书管理功能扩展到私有证书，使您能够集中创建和管理公有和私有证书。您可以使用 AWS 管理控制台或 ACM API 轻松地为您的 AWS 资源创建和部署私有证书。对于 EC2 实例、容器、物联网设备和本地资源，您可以轻松创建和跟踪私有证书，并使用自己的客户端自动化代码进行部署。对于需要自定义证书生命周期、密钥算法或资源名称的应用程序，您还可以灵活地创建私有证书并自行管理这些证书。要了解更多信息，请参阅AWS 私有 CA。

AWS 私有 CA 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS 私有 CA ？

通过提交 AWS 服务 RFC（管理 | 服务 | 兼容 AWS 服务）来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：。`customer_acm_pca_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用有哪些限制 AWS 私有 CA？

目前， AWS Resource Access Manager (AWS RAM) 不能用于共享您的 AWS 私有 CA 跨账户。

问：使用的先决条件或依赖关系 AWS 私有 CA是什么？

1. 如果您计划创建 CRL，则需要一个 S3 存储桶来存储它。 AWS 私有 CA 自动将 CRL 存入您指定的 Amazon S3 存储桶中，并定期对其进行更新。在设置 CRL 之前，S3 存储桶必须具有以下存储桶策略。要继续处理此请求，请按如下方式使用 ct-0fpjlxa808sh2（管理 | 高级堆栈组件 | S3 存储 | 更新策略）创建 RFC：

- 提供 S3 存储桶名称或 ARN。
- 将以下策略复制到 RFC 上，并`bucket-name`替换为所需的 S3 存储桶名称。

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
```

```
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. 如果上述 S3 存储桶已加密，则服务主体 acm-pca.amazonaws.com 需要解密权限。要继续处理此请求，请按如下方式使用 ct-3ovo7px2vsa6n（管理 | 高级堆栈组件 | KMS 密钥 | 更新）创建 RFC：

- 提供必须更新策略的 KMS 密钥 ARN。
- 将以下策略复制到 RFC 上，并bucket-name替换为所需的 S3 存储桶名称。

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
```

```
    }
}
```

3。 AWS 私有 CA CRLs 不支持 S3 设置 “阻止通过新的访问控制列表 (ACLs) 授予的对存储桶和对象的公开访问权限”。您必须对 S3 账户和存储桶禁用此设置才能允许写入， CRLs 如如何安全地创建和存储 ACM Private CA 的 CRL 中所述。如果您想禁用，请使用 ct-0xdawir96cy7k（管理 | 其他 | 其他 | 更新）创建一个新的 RFC 并附上风险接受书。 AWS 私有 CA 如果您对风险接受有任何疑问，请联系您的云架构师。

使用 AMS SSP AWS CloudEndure 在您的 AMS 账户中进行配置

> **Note**
>
> 成功推出后 AWS Application Migration Service， CloudEndure 迁移服务现已在所有 AWS 地区停用。我们建议客户使用 AWS Application Migration Service 升降和转移到 GovCloud 区域和商业区域的迁移。有关信息，请参阅什么是 AWS Application Migration Service？ 。
> 如果您想使用 AWS Application Migration Service，请联系您的 CA，以便他们为您提供指导。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CloudEndure 功能。AWS CloudEndure 迁移可简化、加快和自动化从物理、虚拟和基于云的基础架构向的大规模迁移。AWS CloudEndure 灾难恢复 (DR) 可防止任何威胁（包括勒索软件和服务器损坏）造成的停机和数据丢失。

AWS CloudEndure 在 AWS Managed Services 常见问题中

问：如何申请访问我 CloudEndure 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 将以下 IAM 用户配置到您的账户:`customer_cloud_endure_user`. 在您的账户中配置访问密钥和密钥后，将在 Secrets Manager 中共享该用户的访问密钥和 AWS 密钥。

这些策略也已配置到账
户：`customer_cloud_endure_policy`和。`customer_cloud_endure_deny_policy`

此外，您必须提供风险承受能力，因为用于应用程序集成的 CloudEndure 灾难恢复解决方案具有基础架构变更权限。为此，请与您的云服务交付经理 (CSDM) 合作。

问： CloudEndure 在我的 AMS 账户中使用有什么限制？

云端忍受复制和转换实例只能在您指定的子网中启动。

问：在我的 AMS 账户 CloudEndure 中使用的先决条件或依赖条件是什么？ 通过 RFC 双向通信共享以下内容：

- 要启动的复制和转换实例的 VPC 子网详细信息。
- 如果 EBS 卷已加密，则为 KMS 密钥亚马逊资源名称 (ARN)。

使用 AMS SSP AWS CloudHSM 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CloudHSM 功能。 AWS CloudHSM 通过在 AWS 云中使用专用的硬件安全模块 (HSM) 实例，帮助您满足企业、合同和监管机构对数据安全的合规性要求。 AWS和 AWS Marketplace 合作伙伴提供了各种解决方案来保护 AWS 平台内的敏感数据，但是对于某些受合同或监管要求约束的管理加密密钥的应用程序和数据，可能需要额外的保护。 AWS CloudHSM 补充现有的数据保护解决方案，并允许您保护其中的加密密钥 HSMs ，这些密钥是按照政府安全密钥管理标准设计和验证的。 AWS CloudHSM 允许您以只有您才能访问的方式安全地生成、存储和管理用于数据加密的加密密钥。要了解更多信息，请参阅AWS CloudHSM。

AWS CloudHSM 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS CloudHSM 的 AMS 账户？

在您的 AMS 账户中使用分为两个步骤：

1. 请求集 AWS CloudHSM 群。为此，请提交 RFC，其中包含管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型。请包括以下详细信息：
   - AWS 区域。
   - 与您提交的 RFC 属于同一账户的 VPC ID/ARN. Provide a VPC ID/VPC ARN。
   - 为集群指定至少两个可用区。
   - 将连接到 HSM 集群的亚马逊 EC2 实例 ID。
2. 访问控制 AWS CloudHSM 台。为此，请使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC。此 RFC 为您的账户配置以下 IAM 角色:`customer_cloudhsm_console_role`.

在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问： AWS CloudHSM 在我的 AMS 账户中使用有什么限制？

访问 AWS CloudHSM 控制台不允许您创建、终止或恢复集群。要做这些事情，请提交 “管理 | 其他 | 其他 | 创建变更类型 (ct-1e1xtak34nx76)” 变更类型。

问：在我的 AMS 账户 AWS CloudHSM 中使用的先决条件或依赖条件是什么？

您必须允许 TCP 流量使用端口 2225 通过 VPC 内的客户端 Amazon EC2 实例，或者要访问 HSM 集群的本地服务器使用 Direct Connect VPN。 AWS CloudHSM 依赖于 Amazon EC2 来提供安全组和网络接口。对于日志监控或审计，HSM 依赖 CloudTrail （ AWS API 操作）和 CloudWatch 日志来处理所有本地 HSM 设备活动。

问：谁将对 AWS CloudHSM 客户端和相关软件库进行更新？

您负责应用库和客户端更新。您需要监视 CloudHSM 版本历史记录页面上的版本，然后使用 C lou d HSM 客户端升级来应用更新。

> **Note**
>
> HSM 设备的软件补丁始终由该 AWS CloudHSM 服务自动应用。

使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeBuild 功能。 AWS CodeBuild 是一项完全托管的持续集成服务，用于编译源代码、运行测试和生成随时可以部署的软件包。使用 CodeBuild，您无需预置、管理和扩展自己的构建服务器。 CodeBuild 持续扩展并同时处理多个构建，因此您的构建不会排队等待。您可以使用预先打包的构建环境快速开始，也可以创建使用您自己的构建工具的自定义构建环境。使用 CodeBuild，按分钟计费所使用的计算资源。要了解更多信息，请参阅AWS CodeBuild。

> **Note**
>
> 要加载 CodeCommit、 CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。 CodeBuild CodeDeploy CodePipeline然后，所有三个角色、`customer_codebuild_service_role`、`customer_codedeploy_service_role`、和`aws_code_pipeline_service_role`都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeBuild 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS CodeBuild 的 AMS 账户？

AWS CodeBuild 在您的 AMS 账户中使用分为两个步骤：

1. 预置构建流程以与 AWS S3 存储桶、Amazon CloudWatch 和日志组进行协调 `CodeBuild Service Role`
2. 请求访问控制 CodeBuild 台

您可以通过管理 | AWS 服务 | 自配服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求在您的 AMS 账户中同时设置两者。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS CodeBuild 在我的 AMS 账户中使用有什么限制？

对于 AWS CodeBuild 控制台管理员的访问权限，权限受资源级别的限制；例如，对特定资源的 CloudWatch 操作受到限制，`iam:PassRole`权限受到控制。

问：在我的 AMS 账户 CodeBuild 中使用的先决条件或依赖条件是什么？

如果定义的 AWS CodeBuild 服务角色需要其他 IAM 权限，请通过 AMS 服务请求进行申请。

使用 AMS SSP AWS CodeCommit 在您的 AMS 账户中进行配置

> **Note**
>
> AWS 自 2024 年 7 月 25 日 AWS CodeCommit起，已关闭新客户访问权限。 AWS CodeCommit 现有客户可以继续照常使用该服务。 AWS 继续投资于安全性、可用性和性能改进 AWS CodeCommit，但我们不打算引入新功能。
> 要将 AWS CodeCommit Git 存储库迁移到其他 Git 提供商，请联系您的云架构师 (CA) 寻求指导。有关迁移 Git 存储库的更多信息，请参阅如何将您的 AWS CodeCommit 存储库迁移到其他 Git 提供商。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeCommit 功能。AWS CodeCommit 是一项完全托管的源代码控制服务，用于托管基于 Git 的安全存储库。它可以帮助

团队在安全且高度可扩展的生态系统中协作处理代码。 CodeCommit 无需操作自己的源代码控制系统或担心扩展其基础架构。您可以使用 CodeCommit 安全地存储从源代码到二进制文件的所有内容，并且它可以与现有 Git 工具无缝协作。要了解更多信息，请参阅AWS CodeCommit。

> **Note**
>
> 要加载 CodeCommit、 CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。 CodeBuild CodeDeploy CodePipeline然后，所有三个角色、`customer_codebuild_service_role`、`customer_codedeploy_service_role`和`aws_code_pipeline_service_role`都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeCommit 在 AWS Managed Services 常见问题中

问：如何申请访问我 CodeCommit 的 AMS 账户？

AWS CodeCommit 可以通过提交两个 AWS 服务 RFCs、控制台访问和数据访问权限来请求控制台和数据访问角色：

- AWS CodeCommit 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_codecommit_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

  数据访问（例如训练和实体列表）要求每个数据源分别 CTs 指定 S3 数据源（必填）、输出存储桶（必填）和 KMS（可选）。只要所有数据源都被授予访问角色，就不会限制创造 AWS CodeCommit 就业机会。要申请数据访问权限，请向管理层 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 提交 RFC。

问： AWS CodeCommit 在我的 AMS 账户中使用有什么限制？

如果具有创建 SNS 主题的相关权限， CodeCommit 则会禁用开启的触发器功能。直接进行身份验证受到限制，用户应使用 Cre CodeCommit dential Helper 进行身份验证。某些 KMS 命令也受到限制：`kms:Encryptkms:Decryptkms:ReEncrypt`、、`kms:GenereteDataKey`、`kms:GenerateDataKe`和`kms:DescribeKey`。

问：在我的 AMS 账户 AWS CodeCommit 中使用的先决条件或依赖条件是什么？

如果使用 KMS 密钥加密 S3 存储桶，则必须使用 AWS CodeCommit S3 和 KMS。

使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeDeploy 功能。 AWS CodeDeploy 是一项完全托管的部署服务，可自动将软件部署到各种计算服务，例如 Amazon EC2 AWS Fargate、 AWS Lambda、和您的本地服务器。 AWS CodeDeploy 帮助您快速发布新功能，帮助您避免应用程序部署期间的停机，并处理更新应用程序的复杂性。您可以使用 AWS CodeDeploy 自动化软件部署，无需进行容易出错的手动操作。该服务可根据您的部署需求进行扩展。要了解更多信息，请参阅AWS CodeDeploy。

> **Note**
>
> 要加载 CodeCommit、 CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。 CodeBuild CodeDeploy CodePipeline然后，所有三个角色、`customer_codebuild_service_role`、`customer_codedeploy_service_role`和`aws_code_pipeline_service_role`都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeDeploy 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 CodeDeploy 中申请访问权限？

CodeDeploy 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_codedeploy_console_role`和。`customer_codedeploy_service_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该`customer_codedeploy_console_role`角色。

问： CodeDeploy 在我的 AMS 账户中使用有什么限制？

目前，我们仅支持计算平台 — Amazon EC2 /on-Premises。 Blue/Green 不支持部署。

问：在我的 AMS 账户 CodeDeploy 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 CodeDeploy 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodePipeline 功能。AWS CodePipeline 是一项完全托管的持续交付服务，可帮助您实现发布管道的自动化，从而实现快速可靠的应用程序和基础架构更新。 CodePipeline 每次发生代码更改时，都会根据您定义的发布模型自动执行发布过程的构建、测试和部署阶段。这让您可以快速而可靠地交付各种功能和更新。您可以轻松地 AWS CodePipeline 与第三方服务集成，例如 GitHub 或与您自己的自定义插件集成。使用 AWS CodePipeline，您只需为实际用量付费。无前期费用，无长期承诺。要了解更多信息，请参阅AWS CodePipeline。

> **Note**
>
> 要加载 CodeCommit、 CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。 CodeBuild CodeDeploy CodePipeline然后，所有三个角色、`customer_codebuild_service_role`、`customer_codedeploy_service_role`、和`aws_code_pipeline_service_role`都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。
> CodePipeline 在 AMS 中，不支持源阶段的 “Amazon Ev CloudWatch ents”，因为它需要更高的权限才能创建服务角色和策略，从而绕过最低权限模型和 AMS 变更管理流程。

CodePipeline 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 CodePipeline 中申请访问权限？

CodePipeline 通过在相关账户`customer_code_pipeline_console_role`中提交服务请求来请求访问权限。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

此时，AMS Operations 还将在您的账户中部署此服务角色：`aws_code_pipeline_service_role_policy`。

问： CodePipeline 在我的 AMS 账户中使用有什么限制？

是的。 CodePipeline 功能、阶段和提供者仅限于以下内容：

1. 部署阶段：仅限于 Amazon S3，以及 AWS CodeDeploy
2. 来源阶段：仅限于 Amazon S3 AWS CodeCommit、 BitBucket、和 GitHub
3. 建造阶段：仅限于 AWS CodeBuild，而且 Jenkins

4. 批准阶段：仅限于亚马逊 SNS
5. 测试阶段：仅限于 Jenkins AWS CodeBuild、、Ghost Inspector 用户界面测试、Micro Focus StormRunner 加载和 Runscope API 监控 BlazeMeter
6. 调用阶段：仅限于 Step Functions 和 Lambda

> **Note**
>
> AMS 操作将在您的账户`customer_code_pipeline_lambda_policy`中部署；它必须与 Lambda 调用阶段的 Lambda 执行角色相关联。请提供您想要添加此策略的 Lambda service/execution 角色名称。如果没有自定义 Lambda service/execution 角色，AMS 将创建一个名为的新角色`customer_code_pipeline_lambda_execution_role`，该角色将作为副`customer_lambda_basic_execution_role`本。`customer_code_pipeline_lambda_pol`

问：在我的 AMS 账户 CodePipeline 中使用的先决条件或依赖条件是什么？

AWS 支持的服务 AWS CodeCommit AWS CodeDeploy 必须在发布之前或同时启动 CodePipeline。AWS CodeBuild

使用 AMS SSP AWS Compute Optimizer 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Compute Optimizer 功能。 AWS Compute Optimizer 使用机器学习来分析历史利用率指标，为您的工作负载推荐最佳 AWS 计算资源，从而降低成本并提高性能。过度配置计算（Amazon EC2 和 ASGs）可能会导致不必要的基础设施成本，而计算配置不足会导致应用程序性能不佳。Compute Optimizer 可帮助您根据使用率数据选择最佳的亚马逊 EC2 实例类型，包括属于 Amazon A EC2 uto Scaling 组的实例类型。要了解更多信息，请参阅AWS Compute Optimizer。

AWS 托管服务中的 Compute Optimizer 常见问题解答

问：如何使用我的 AMS 账户申请访问 Compute Optimizer？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_compute_optimizer_readonly_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Compute Optimizer 有哪些限制？

没有任何限制。的全部功能可在您 AWS Compute Optimizer 的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Compute Optimizer 有哪些先决条件或依赖关系？

- 您必须提交 RFC（管理 | 其他 | 其他 | 更新），授权 AMS Ops 在账户中启用该服务。在部署期间，将创建一个服务关联角色 (SLR)，以允许收集指标和生成报告。单反相机标有“AWSServiceRoleForComputeOptimizer”。有关更多信息，请参阅使用服务相关角色 AWS Compute Optimizer
- CloudWatch 必须为以下指标启用指标：
  - CPU 利用率：实例上正在使用的已分配的 Amazon EC2 计算单元的百分比。该指标确定了在选定实例上运行应用程序所需的处理能力。
  - 内存利用率：在采样期间以某种方式使用的内存量。该指标用于确定在选定实例上运行应用程序所需的内存。仅针对安装了统一 CloudWatch 代理的资源分析内存利用率。有关更多信息，请参阅使用 CloudWatch 代理启用内存利用率（第 10 页）。
  - 网络输入：实例在所有网络接口上接收的字节数。该指标用于识别单个实例的传入网络流量。
  - 网络输出：实例在所有网络接口上发送的字节数。该指标用于识别来自单个实例的传出网络流量。
  - 本地磁盘 input/output (I/O)：本地磁盘的 input/output 操作次数。该指标用于识别实例根卷的性能

使用 AMS SSP AWS DataSync 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS DataSync 功能。 AWS DataSync 在本地存储和亚马逊 S3、Amazon Elastic File System（亚马逊弹性文件系统）或亚马逊之间在线移动大量数据 FSx。与数据传输相关的手动任务可能会减慢迁移速度并给 IT 运营带来负担。DataSync 消除或自动处理其中的许多任务，包括编写拷贝作业脚本、安排和监控传输、验证数据以及优化网络利用率。 DataSync 软件代理连接到您的网络文件系统 (NFS) 和服务器消息块 (SMB) 存储，因此您无需修改应用程序。 DataSync 可以通过 Internet 或 AWS Direct Connect 链接传输数百 TB 和数百万个文件，速度比开源工具快 10 倍。您可以使用将活动数据集或存档迁移 DataSync 到云端 AWS，将数据传输到云端以便及时进行分析和处理，或者将数据复制到云端以 AWS 实现业务连续性。

要了解更多信息，请参阅AWS DataSync。

DataSync 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 DataSync 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_datasync_console_role`.

在您的账户中配置后，您必须在联合解决方案中加入角色。

用于流式传输任务 CloudWatch 日志的日志组是 “/aws/datasync”。

问： DataSync 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS DataSync 的 AMS 账户中使用。

问：在我的 AMS 账户 DataSync 中使用的先决条件或依赖条件是什么？

- 与将使用 DataSync 服务角色`customer_datasync_service_role`执行的 DataSync 任务关联的所有 S3 存储桶都需要 Amazon S3 ARNs （ Amazon 资源名称 ）。
- 在使用 VPC 终端节点之前，必须使用管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型的 RFC 请求 DataSync 代理的 VPC 终端节点和安全组。
- AWS DataSync 代理作为设备在 AMS 中运行。该服务已对 AWS DataSync 代理进行修补和更新；有关详细信息，请参阅AWS DataSync 常见问题解答。
- 要启动 AWS DataSync 代理，请提交带有管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型的 RFC，请求部署代理。提供 AWS DataSync Amazon EC2 AMI ID、实例类型、子网、安全组；并引用现有的 Amazon EC2 密钥对或请求创建新的密钥对。

> **Note**
>
> AMS 代表客户手动配置 AWS DataSync 代理，并且不需要在 Amazon AWS DataSync AMI 上进行 WIGS 摄取流程。 EC2

使用 AMS SSP AWS Device Farm 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Device Farm 功能。 AWS Device Farm 是一项应用程序测试服务，可让您通过在各种桌面浏览器和真实移动设备上测试 Web 和移动应用程序来提高其质量，而无需预置和管理任何测试基础架构。该服务使您能够在多个桌面浏览器或真实设备上同时运行测试，以加快测试套件的执行速度，并生成视频和日志以帮助您快速识别应用程序存在的问题。

要了解更多信息，请参阅AWS Device Farm。

AWS Device Farm 在 AWS Managed Services 常见问题中

问：如何申请访问我 AWS Device Farm 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_devicefarm_role`.

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问： AWS Device Farm 在我的 AMS 账户中使用有什么限制？

除了在 “名称” 标签中使用 AMS 命名空间外，还提供对该 AWS Device Farm 服务的完全访问权限。

问：在我的 AMS 账户 AWS Device Farm 中使用的先决条件或依赖条件是什么？

无。

使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elastic Disaster Recovery 功能。 AWS Elastic Disaster Recovery 使用经济实惠的存储、最少的计算和恢复，快速、可靠地 point-in-time恢复本地和基于云的应用程序，最大限度地减少停机时间和数据丢失。当您使用 AWS Elastic Disaster Recovery 复制在支持的操作系统上运行的本地应用程序或基于云的应用程序时，可以提高 IT 弹性。使用 AWS 管理控制台 来配置复制和启动设置、监控数据复制以及启动用于演练或恢复的实例。

要了解更多信息，请参阅AWS Elastic Disaster Recovery。

AWS Elastic Disaster Recovery 在 AWS Managed Services 常见问题中

问：如何申请访问我 AWS Elastic Disaster Recovery 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_drs_console_role`.

在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS Elastic Disaster Recovery 在我的 AMS 账户中使用有什么限制？

在您的 AMS 账户 AWS Elastic Disaster Recovery 中使用没有任何限制。

问：在我的 AMS 账户 AWS Elastic Disaster Recovery 中使用的先决条件或依赖条件是什么？

- 访问控制台角色后，您必须初始化 Elastic 灾难恢复服务，以便在账户中创建所需的 IAM 角色。

  - 您必须提交更改类型管理 | 应用程序 | IAM 实例配置文件 | 创建（需要审查）更改类型 ct-0ixp4ch2tiu04 RFC 才能创建实例配置文件的克隆并附加策略。`customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy`您必须指定要将新策略附加到哪些计算机。
  - 如果实例未使用默认实例配置文件，则 AMS `AWSElasticDisasterRecoveryEc2InstancePolicy` 可以通过自动化进行连接。
- 您必须使用客户拥有的 KMS 密钥进行跨账户恢复。必须按照策略更新源账户的 KMS 密钥以允许目标账户访问。有关更多信息，请参阅与目标账户共享 EBS 加密密钥。
- 如果您不想切换角色进行查看，则必须更新 KMS 密钥策略以允许允许`customer_drs_console_role`查看策略。
- 对于跨账户、跨区域灾难恢复，AMS 必须将源账户和目标账户设置为可信账户，并通过部署故障恢复和大小合适的角色AWS。 CloudFormation

使用 AMS SSP AWS Elemental MediaConvert 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaConvert 功能。 AWS Elemental MediaConvert 是一种基于文件的视频转码服务，具有广播级功能。它使您能够创建 video-on-demand（VOD）内容，用于大规模广播和多屏传送。该服务将高级视频和音频功能与简单的 Web 服务界面和 pay-as-you-go定价相结合。借 AWS Elemental MediaConvert助，您可以专注于提供引人入胜的媒体体验，而不必担心构建和运营自己的视频处理基础设施的复杂性。

要了解更多信息，请参阅AWS Elemental MediaConvert。

MediaConvert 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaConvert 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_mediaconvert_author_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

将提供第二个角色`customer_MediaConvert_Default_Role`，该角色用于从源 S3 存储桶读取数据并将输出写入目标 S3 存储桶，还用于在需要数字版权管理 (DRM) 时调用 API 网关。 MediaConvert

问： MediaConvert 在我的 AMS 账户中使用有什么限制？

在 AMS MediaConvert 中使用没有任何限制。

问：在我的 AMS 账户 MediaConvert 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaConvert 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaLive 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaLive 功能。 AWS Elemental MediaLive 是一项广播级的直播视频处理服务。它使您能够创建高质量的视频流，以传送到广播电视和联网的多屏设备，例如联网设备、平板电脑 TVs、智能手机和机顶盒。该服务的工作原理是对您的直播视频流进行实时编码，获取较大的实时视频源，然后将其压缩成较小的版本以分发给您的观众。借助高级广播功能 AWS Elemental MediaLive、高可用性和定价，您可以轻松地为直播活动和全天候频道设置直播。 pay-as-you-go AWS Elemental MediaLive 让您可以专注于为观众创造引人入胜的实时视频体验，而无需复杂地构建和运营广播级视频处理基础架构。

要了解更多信息，请参阅AWS Elemental MediaLive。

MediaLive 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaLive 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_medialive_author_role`.

作为本 RFC 的一部分，第二个角色将部署到您的账户；
该`customer_medialive_service_role`角色可以分配给您的媒体直播频道和输入，以便与其他服务（例如 Amazon S3 和 CloudWatch 日志）进行交互。 MediaStore

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问： MediaLive 在我的 AMS 账户中使用有什么限制？

在 AMS MediaLive 中使用没有任何限制。

问：在我的 AMS 账户 MediaLive 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaLive 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaPackage 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaPackage 功能。 AWS Elemental MediaPackage 可靠地准备和保护您的视频，以便通过互联网传输。通过单个

视频输入， AWS Elemental MediaPackage 创建格式化为可在联网手机 TVs、计算机、平板电脑和游戏机上播放的视频流。它可以轻松地为观众实现流行的视频功能（重播、暂停、倒带等），就像上面常见的功能一样。 DVRs AWS Elemental MediaPackage 还可以使用数字版权管理 (DRM) 保护您的内容。 AWS Elemental MediaPackage 根据加载量自动缩放，因此您的观众将始终获得出色的体验，而不必事先准确预测所需的容量。

要了解更多信息，请参阅AWS Elemental MediaPackage。

MediaPackage 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 AWS Elemental MediaPackage 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_mediapackage_author_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

将提供第二个角色`customer_mediapackage_service_role`，可以将其分配给您的媒体直播频道和输入，以便与其他服务（例如 S3 和 Secrets Manager）进行交互。

问： MediaPackage 在我的 AMS 账户中使用有什么限制？

在 AMS MediaPackage 中使用没有任何限制。

问：在我的 AMS 账户 MediaPackage 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaPackage 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaStore 在您的 AMS 账户中进行配置

> **Note**
>
> 经过仔细考虑，决定停产 MediaStore， AWS 自2025年11月13日起生效。如果您是的活跃客户 MediaStore，则可以照常使用 MediaStore ，直到 2025 年 11 月 13 日该服务的支持将终止。在此日期之后，您将无法再使用本服务提供的 MediaStore 任何功能。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaStore 功能。 AWS Elemental MediaStore 是一项针对媒体进行了优化的 AWS 存储服务。它为您提供交付直播视频内容所需的性能、一致性和低延迟。 AWS Elemental MediaStore 在您的视频工作流程中充当原始

存储。其高性能功能可满足最苛刻的媒体交付工作负载的需求，再加上长期且经济实惠的存储。要了解更多信息，请参阅AWS Elemental MediaStore。

MediaStore 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaStore 的 AMS 账户？

MediaStore 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_mediastore_author_role`. 作为本 RFC 的一部分，将在您的账户中部署第二个角色：`MediaStoreAccessLogs`角色，如果您选择启用该功能 CloudWatch，则 MediaStore 服务使用该角色来登录活动。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

此时，AMS 运营部门还将在您的账户中部署此服务角色：`aws_code_pipeline_service_role_policy`。

问： MediaStore 在我的 AMS 账户中使用有什么限制？

在 AMS MediaStore 中使用没有任何限制。

问：在我的 AMS 账户 MediaStore 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaStore 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaTailor 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaTailor 功能。 AWS Elemental MediaTailor 允许视频提供商在不牺牲广播 quality-of-service级别的情况下将单独定向的广告插入到其视频流中。这样 AWS Elemental MediaTailor，您的直播或点播视频的观众都会收到一个将您的内容与针对他们的个性化广告相结合的直播。但是，与其他个性化广告解决方案不同，AWS Elemental MediaTailor 您的整个视频流（视频和广告）都以广播级的视频质量投放，以改善观众的体验。 AWS Elemental MediaTailor 提供基于客户端和服务器端广告投放指标的自动报告，以准确衡量广告展示次数和观众行为。您可以轻松地通过意想不到的高需求观看活动获利，而无需支付任何前期费用。 AWS Elemental MediaTailor它还可以提高广告投放率，帮助您从每个视频中获得更多收益，并且可以与更多种类的内容交付网络、广告决策服务器和客户端设备配合使用。

要了解更多信息，请参阅AWS Elemental MediaTailor。

MediaTailor 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaTailor 的 AMS 账户？

MediaTailor 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer-mediatailor-role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： MediaTailor 在我的 AMS 账户中使用有什么限制？

在 AMS MediaTailor 中使用没有任何限制。

问：在我的 AMS 账户 MediaTailor 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaTailor 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Global Accelerator 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问全球加速器功能。Global Accelerator 是一项网络层服务，您可以在其中创建加速器以提高全球受众使用的互联网应用程序的可用性和性能。要了解更多信息，请参阅全球加速器。

AWS Managed Services 中的全球加速器常见问题解答

常见问题和答案：

问：如何申请在我的 AMS 账户中设置全球加速器？

通过提交 AWS 服务 RFC（管理 | 服务 | 自配 AWS 服务）来请求访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：。`customer_global_accelerator_console_role`在您的账户中配置控制台角色后，您必须在联合解决方案中加入控制台角色。

问：在我的 AMS 账户中使用全球加速器有哪些限制？

Global Accelerator 是一项全球服务，支持 AWS 区域表中列出的多个AWS 区域的终端节点。

问：在我的 AMS 账户中使用全球加速器的先决条件或依赖条件是什么？

使用全球加速器设置加速器时，可以将静态 IP 地址关联到一个或多个 AWS 区域的区域终端节点。对于标准加速器，终端节点是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。对于自定义路由加速器，终端节点是具有一个或多个 EC2 实例的虚拟私有云 (VPC) 子网。

使用 AMS SSP AWS Glue 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Glue 功能。 AWS Glue 是一项完全托管的提取、转换和加载 (ETL) 服务，可帮助您准备和加载数据以进行分析。只需在中单

击几下即可创建和运行 ETL 作业。 AWS 管理控制台您指 AWS Glue 向存储在上的数据 AWS， AWS Glue 发现您的数据并将关联的元数据（例如表定义和架构）存储在中 AWS Glue Data Catalog。对您的数据进行编目后，即可立即搜索和查询，并可用于ETL操作。要了解更多信息，请参阅AWS Glue。

AWS Glue 在 AWS Managed Services 常见问题中

常见问题和答案：

问： AWS Glue 如何申请在我的 AMS 账户中进行设置？

AWS Glue 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：

- `customer_glue_console_role`
- `customer_glue_service_role`

前面的角色包括以下附加策略：

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

在您的账户中配置角色后，您必须将其加入您的联合解决方案中。

要访问爬虫、作业和开发终端节点（特定用例所需的角色），请使用部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略 (ct-3dpd8mdd9jn1r) 提交 RFC。

问： AWS Glue 在我的 AMS 账户中使用有什么限制？

没有任何限制。的全部功能可在您 AWS Glue 的 AMS 账户中使用。要获得可以创作和测试 ETL 脚本的交互式环境，请使用 AWS Glue Studio 上的笔记本。 AWS Glue Interactive Sessions 和 Job Notebook 是无服务器功能，你可以在中 AWS Glue 使用这些功能，也可以利用 AWS Glue 服务角色。AWS Glue

AWS Glue 2.0 之前版本： AWS Glue 笔记本是一种非托管资源，可在账户中启动 Amazon EC2 实例。最佳做法是启动您自己的 Amazon EC2 实例并安装支持笔记本环境和开发所需的软件。有关更多信息，请参阅教程：设置本地 Apache Zeppelin 笔记本来测试和调试 ETL 脚本以及使用开发端点开发脚本。

问：在我的 AMS 账户 AWS Glue 中使用的先决条件或依赖条件是什么？

AWS Glue 依赖于 Amazon S3 CloudWatch、和 CloudWatch 日志。传递依赖关系因数据源和可能与之交互的其他 AWS Glue 服务功能而异（例如：Amazon Redshift、Amazon RDS、Athena）。

使用 AMS SSP AWS Lake Formation 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Lake Formation 功能。AWS Lake Formation 是一项服务，可让您在几天之内轻松设置安全的数据湖。数据湖是一种集中的、策管的、安全存储库，用于存储所有数据，包括原始形式和准备进行分析的形式。数据湖能够打破数据孤岛，将不同类型的分析结合起来，获得信息并指导更好的业务决策。

使用 Lake Formation 创建数据湖很简单，以及要应用的数据访问和安全策略。然后，Lake Formation 可帮助您从数据库和对象存储收集和编目数据，将数据移动到新的 Amazon S3 数据湖，使用机器学习算法清理和分类数据，安全访问敏感数据。您的用户可以访问集中式数据目录（有关详细信息，请参阅AWS Glue 常见问题解答），该目录描述了可用数据集及其适当用法。然后，您的用户将这些数据集与他们选择的分析和机器学习服务结合起来，例如亚马逊 Redshift、Amazon At hena 和（测试版）适用于 Apache Spark 的 A ma zon EMR。Lake Formation 建立在中提供的功能之上AWS Glue。

要了解更多信息，请参阅AWS Lake Formation。

AWS 托管服务中的 Lake Formation 常见问题解答

问：如何申请访问我 AWS Lake Formation 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_lakeformation_data_analyst_role`. 在您的账户中配置角色后，您必须在联合解决方案中加入角色。

此外，以下两个角色是可选的：

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

要获得管理员权限，您可以选择将该角色`customer_lakeformation_admin_role`作为相同 SSP 更改类型（ct-3qe6io8t6jtny）的一部分加入。

如果要在 AWS Lake Formation 控制台中创建蓝图，则需要提交管理 | 其他 | 其他 RFC (ct-1e1xtak34nx76) 来部署。`customer_lakeformation_workflow_role`在 RFC 中，如果创建蓝图时存储桶是源，则必须提供 S3 存储桶名称。如果蓝图类型为 AWS CloudTrail Classic Load Balancer 日志或应用程序负载均衡器日志，则 S3 存储桶适用。

问： AWS Lake Formation 在我的 AMS 账户中使用有什么限制？

Lake Formation 的全部功能已在 AMS 中提供。

问：在我的 AMS 账户 AWS Lake Formation 中使用的先决条件或依赖条件是什么？

Lake Formation 与该 AWS Glue 服务集成，因此 AWS Glue 用户只能访问他们拥有 Lake Formation 权限的数据库和表。此外， AWS Athena 和 Amazon Redshift 用户只能查询他们拥有 Lake Formation 权限 AWS Glue 的数据库和表。

使用 AMS SSP AWS Lambda 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Lambda 功能。 AWS Lambda 允许您在不预置或管理服务器的情况下运行代码。您只需为所消耗的计算时间付费，当您的代码未运行时不收取任何费用。借助 Lambda，您几乎可以为任何类型的应用程序或后端服务运行代码，所有这些都无需任何管理。上传您的代码，Lambda 会处理运行和扩展代码所需的一切，使其具有高可用性。您可以将代码设置为从其他 AWS 服务自动触发，或者直接从任何 Web 或移动应用程序调用。要了解更多信息，请参阅AWS Lambda。

AWS Managed Services 中的 Lambda 常见问题解答

问：如何在 AMS 账户 AWS Lambda 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_lambda_admin_role`和。`customer_lambda_basic_execution_role`在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问： AWS Lambda 在我的 AMS 账户中使用有什么限制？

- Lambda 函数旨在由事件源调用。有关可用作 Lambda 事件源的服务列表，请参阅与其他服务 AWS Lambda 一起使用。目前，并非所有这些服务都在 AMS 账户中可用。如果您需要的服务不可用，请与您的 AMS CSDM 合作提交例外申请。
- 默认情况下，AMS 为您提供包含`AWSLambdaBasicExecutionRole`和`AWSXrayWriteOnlyAccess`权限的基本 Lambda 初始角色；有关信息，请参阅AWS Lambda 初始角色。如果您需要其他权限，例如能够在您的 AMS VPC 中配置 Lambda 函数，请使用管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型提交 RFC。

问：在我的 AMS 账户 AWS Lambda 中使用的先决条件或依赖条件是什么？

开始时没有先决条件或依赖关系 AWS Lambda；但是，根据您的具体用例，您可能需要访问其他 AWS 服务才能创建事件源，或者您的函数需要额外的权限才能执行各种操作。如果需要其他权限，请使用管理 | AWS 服务 | 自配置服务 | 添加（需要审核）更改类型 (ct-3qe6io8t6jtny) 提交 RFC。

问：要在我的任何账户中运行 Lambda 函数，我需要做什么？

要在核心账户中部署 Lambda 函数，请使用以下指南：

- 确保已加载 SSP f AWS Lambda or。
- 只要您的 AMS 资源受到保护且合规，AMS 职责下没有禁止这种部署的具体限制。
- 如果您希望 AMS 创建 Lambda 函数，则必须首先使用所提供的 SSP 角色。 AWS Lambda然后，如果您仍希望 AMS 协助部署或支持该功能，请联系您的 CA 并启动超出范围 (OOS) 流程。

使用 AMS SSP AWS License Manager 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS License Manager 功能。AWS License Manager 与 AWS 服务集成，通过单 AWS 一账户简化多个 AWS 账户、IT 目录和本地许可证的管理。 AWS License Manager 允许管理员创建模拟其许可协议条款的自定义许可规则，然后在 Amazon 实例启动时强制执行这些规则 EC2 。中的规则 AWS License Manager 使您能够通过实际阻止实例启动或将违规行为通知管理员来限制许可违规行为。要了解更多信息，请参阅AWS License Manager。

AWS Managed Services 中的许可证管理器常见问题解答

常见问题和答案：

问： AWS License Manager 如何申请在我的 AMS 账户中进行设置？

AWS License Manager 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_license_manager_role`. 在您的账户中配置 License Manager IAM 角色后，您必须在联合身份验证解决方案中加入该角色。

问： AWS License Manager 在我的 AMS 账户中使用有什么限制？

您可以将规则与 AMIs 您自己的 AWS License Manager 规则相关联（在 “我拥有” 下筛选）。如果您选择强制与 AMI 建立限制关联（例如：只能支持此 AMI 的 100 个 vCPU）并耗尽限制，则未来使用该 AMI 的启动将被阻止，并返回一条错误消息，指出 “没有可用许可证”。这是本服务的预期行为（不允许许可证耗尽）。如果您已用尽限制，但需要再次启动 AMI，则必须修改中配置的规则 AWS License Manager。

问：在我的 AMS 账户 AWS License Manager 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS License Manager 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Migration Hub 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Migration Hub 功能。AWS Migration Hub 提供了一个位置，您可以在其中跟踪跨多个解决方案 AWS 和合作伙伴解决方案的应用程序迁移进度。使用 Migration Hub，您可以选择最适合自己需求的迁移工具 AWS 和合作伙伴，同时可以查看整个应用程序组合的迁移状态。Migration Hub 还提供各个应用程序的关键指标和进度，无论使用何种工具进行迁移。这使您可以快速获取所有迁移的进度更新，轻松识别和解决任何问题，并减少在迁移项目上花费的总体时间和精力。要了解更多信息，请参阅AWS Migration Hub。

AWS Managed Services 中的迁移中心常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 Migration Hub？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Migration Hub。此 RFC 为您的账户配置以下 IAM 角色:`customer_migrationhub_author_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：Migration Hub 有哪些限制？

无。

问：启用 Migration Hub 的先决条件是什么？

在您的 AMS 账户中开始使用 Migration Hub 不需要任何先决条件。但是，在管理服务期间，可能需要在 Migration Hub 之外的权限，例如向 Amazon S3 写入上传服务器信息的权限。

使用 AMS SSP AWS Outposts 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Outposts 功能。 AWS Outposts 是一项完全托管的服务，可将 AWS 基础架构 APIs、 AWS 服务和工具扩展到几乎任何数据中心、托管空间或本地设施，以提供一致的混合体验。 AWS Outposts 适用于需要低延迟访问本地系统、本地数据处理或本地数据存储的工作负载。要了解更多信息，请参阅AWS Outposts。

AWS Outposts 在 AWS Managed Services 常见问题中

常见问题和答案：

问： AWS Outposts 如何申请在我的 AMS 账户中进行设置？

AWS Outposts 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_outposts_role`. 在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问： AWS Outposts 在我的 AMS 账户中使用有什么限制？

在您的 AMS 账户 AWS Outposts 中使用没有任何限制。

问：在我的 AMS 账户 AWS Outposts 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Outposts 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Resilience Hub 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Resilience Hub 功能。AWS Resilience Hub 帮助您主动准备并保护 AWS 应用程序免受中断。Resilience Hub 提供弹性评估和验证，可集成到您的软件开发生命周期中，以发现弹性弱点。Resilience Hub 可帮助您估算您的应用程序能否满足恢复时间目标 (RTO) 和恢复点目标 (RPO) 目标，并在问题发布到生产环境之前帮助解决问题。将 AWS 应用程序部署到生产环境后，您可以使用 Resilience Hub 继续跟踪应用程序的弹性状况。如果发生中断，Resilition Hub 会向操作员发送通知，要求其启动相关的恢复流程。

AWS Resilience Hub 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Resilience Hub 中申请访问权限？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问弹性中心。此 RFC 为您的账户配置以下 IAM 角色和策略：

IAM 角色

- `customer_resiliencehub_console_role`
- `customer_resiliencehub_service_role`

策略

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

在您的账户中配置该角色后，您必须在联合解决方案`customer_resiliencehub_console_role`中加入该角色。

问： AWS Resilience Hub 在我的 AMS 账户中使用有什么限制？

没有任何限制。Resilience Hub 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Resilience Hub 中使用的先决条件或依赖条件是什么？

在您的 AMS 账户中使用 Resilience Hub 没有任何先决条件或依赖关系。

使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Secrets Manager 功能。AWS Secrets Manager 帮助您保护访问应用程序、服务和 IT 资源所需的机密。该服务使您能够在数据库凭证、API 密钥和其他密钥的整个生命周期中轻松轮换、管理和检索它们。用户和应用程序通过调用 Secrets Manager 来检索机密 APIs，无需以纯文本格式对敏感信息进行硬编码。Secrets Manager 使用 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的内置集成提供密钥轮换。此外，该服务还可扩展到其他类型的机密，包括 API 密钥和 OAuth 令牌。要了解更多信息，请参阅AWS Secrets Manager。

> **Note**
>
> 默认情况下，AMS 操作员可以访问使用账户默认密 AWS KMS 钥 (CMK) 加密的机密。 AWS Secrets Manager 如果您希望 AMS Operations 无法访问您的机密，请使用自定义 CMK，其中包含一个 AWS Key Management Service (AWS KMS) 密钥策略，该策略定义了与存储在密钥中的数据相应的权限。

AWS 托管服务中的 Secrets Manager 常见问题解答

问：如何申请访问我 AWS Secrets Manager 的 AMS 账户？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC，请求访问 Secrets Manager。此 RFC 为您的账户配置以下 IAM 角色：`customer_secrets_manager_console_role`和。`customer-rotate-secrets-lambda-role`用作管理员角色来配置和管理密钥，并用作轮换密钥`customer-rotate-secrets-lambda-role`的 Lambda 函数的 Lambda 执行角色。`customer_secrets_manager_console_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该`customer_secrets_manager_console_role`角色。

问： AWS Secrets Manager 在我的 AMS 账户中使用有什么限制？

的全部功能均可在您 AWS Secrets Manager 的 AMS 账户中使用，同时还提供自动轮换密钥的功能。但是，请注意，不支持使用 “创建新的 Lambda 函数来执行轮换” 来设置轮换，因为它需要更高的权限才能创建 CloudFormation 堆栈（ IAM 角色和 Lambda 函数创建），从而绕过变更管理流程。AMS Advanced 仅支持 “使用现有 Lambda 函数执行轮换”，在这种模式下，您可以使用 Lambda SSP 管理员角色管理您的 Lambda 函数以轮换密钥。 AWS AMS Advanced 不会创建或管理 Lambda 来轮换密钥。

问：在我的 AMS 账户 AWS Secrets Manager 中使用的先决条件或依赖条件是什么？

以下命名空间保留给 AMS 使用，不能作为直接访问的一部分使用： AWS Secrets Manager

- arn: aws: secretsmanager: *: *: secret: ams-shared/*
- arn: aws: secretsmanager: *: *: secret: customershared/*
- arn: aws: secretsmanager: *: *: secret: ams/*

使用 Secrets Manager (AMS SSP) 共享密钥

以 RFC、服务请求或事件报告的纯文本形式与 AMS 共享机密会导致信息泄露事件，AMS 会从案例中删除这些信息，并要求您重新生成密钥。

你可以在这个命名空间下使用 AWS Secrets Manager(Secrets Manager) `customer-shared`。

使用 Secrets Manager 共享密钥常见问题解答

问：必须使用 Secrets Manager 共享哪种类型的机密？

一些示例包括用于创建 VPN 的预共享密钥、身份验证密钥（ IAM、SSH ）、许可证密钥和密码等机密密钥。

问：如何使用 Secrets Manager 与 AMS 共享密钥？

1. 使用您的联合访问权限和相应的角色登录 AWS 管理控制台：

   对于 SALZ 来说，`Customer_ReadOnly_Role`

   对于 MALZ 来说，`AWSManagedServicesChangeManagementRole`。
2. 导航到AWS Secrets Manager 控制台，然后单击 “存储新密钥”。
3. 选择其他密钥类型。

4. 以纯文本形式输入密钥值并使用默认 KMS 加密。单击下一步。
5. 输入密钥名称和描述，名称始终以 customers hared/开头。例如，客户共享 /mykey2022。单击下一步。
6. 禁用自动轮换，单击 “下一步”。
7. 查看并单击 “存储” 以保存密钥。
8. 通过服务请求、RFC 或事件报告回复我们并提供机密名称，以便我们识别和检索机密。

问：使用 Secrets Manager 共享密钥需要什么权限？

SALZ：查找`customer_secrets_manager_shared_policy`托管 IAM 策略并验证策略文档是否与以下创建步骤中附加的策略文档相同。确认该策略已附加到以下 IAM 角色：`Customer_ReadOnly_Role`。

MALZ：验证`AMSSecretsManagerSharedPolicy`，是否已附加到允许您在`ams-shared`命名空间中`GetSecretValue`执行操作的`AWSManagedServicesChangeManagementRole`角色。

示例：

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> 当您添加为自助服务配置服务时 AWS Secrets Manager ，将授予必要的权限。

使用 AMS SSP AWS Security Hub CSPM 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Security Hub CSPM 功能。 AWS Security Hub CSPM 让您全面了解自己的安全状态以及您对安全行业标准 AWS 和最佳实践的遵守情况。Security Hub 集中处理来自 AWS 账户、服务和支持的第三方合作伙伴的安全和合规调查

结果并确定其优先级，以帮助您分析安全趋势并确定优先级最高的安全问题。要了解更多信息，请参阅AWS Security Hub CSPM。

AWS 托管服务中的 Security Hub 常见问题解答

问：如何申请访问我 AWS Security Hub CSPM 的 AMS 账户？

通过管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请 Security Hub 的访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_securityhub_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Security Hub 有哪些限制？

存档功能已被视为潜在的安全和操作风险，并且作为自配置服务安全角色的一部分受到限制。

问：在我的 AMS 账户 AWS Security Hub CSPM 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Security Hub CSPM 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AppRegistry 功能。AppRegistry 支持从中心位置进行应用程序搜索、报告和管理操作。构建者很少在单个 AWS 账户中创建应用程序。它们通常按生命周期阶段（例如开发、测试和生产）来分隔应用程序资源。 AppRegistry 允许您对您定义的 AWS 账户中的所有资源集进行分组和查看。

使用 AppRegistry，您可以存储您的 AWS 应用程序、与您的应用程序关联的资源集合以及应用程序属性组。要了解更多信息，请参阅什么是 AppRegistry。

常见问题： AWS Service Catalog AppRegistry 在 AMS 中

问：如何申请访问我 AWS Service Catalog AppRegistry 的 AMS 账户？

AppRegistry 通过使用管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer-appregistry-console-role`. 在您的账户中配置后，您必须在联合解决方案中加入该角色。

问： AWS Service Catalog AppRegistry 在我的 AMS 账户中使用有什么限制？

除了在`'Name'`标签中使用 AMS 命名空间外，还提供对该 AppRegistry 服务的完全访问权限。

问：在我的 AMS 账户 AWS Service Catalog AppRegistry 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AppRegistry 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Shield Advanced 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Shield Advanced 功能。AWS Shield Advanced 是一项托管的分布式拒绝服务 (DDoS) 保护服务，可保护正在运行的应用程序 AWS。Shield Advanced 提供不间断检测和自动内联缓解措施，可最大限度地减少应用程序停机时间和延迟，因此无需与 Su AWS pport 合作即可从 S 保护中受益。 DDo有两个等级 AWS Shield ——标准和高级；AMS 提供 Shield Advanced。要了解更多信息，请参阅 Shield Advanced。

所有 AWS 客户均可享受自动保护 AWS Shield Standard，无需支付额外费用。 AWS Shield Standard 抵御针对您的网站或应用程序的最常见、最常发生的网络和传输层 DDo S 攻击。当您 AWS Shield Standard 与 Amazon CloudFront 和 Amazon Route 53 配合使用时，您将获得针对所有已知基础设施（第 3 层和第 4 层）攻击的全面可用性保护。

要获得更高级别的保护，抵御针对在亚马逊弹性计算云 (Amazon EC2)、Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator、亚马逊和亚马逊 Route 53 资源上运行的应用程序的攻击，您可以订阅。 AWS Shield Advanced

除了随 AWS Shield Standard附的网络和传输层保护外，还 AWS Shield Advanced 提供了针对大型复杂的 DDo S 攻击的额外检测和缓解措施、近乎实时的攻击可见性以及与 AWS WAF Web 应用程序防火墙的集成。 AWS Shield Advanced 还允许你全天候访问 AWS Shield 响应小组 (SRT)，并防止亚马逊弹性计算云 (亚马逊)、弹性负载平衡（弹性负载平衡 EC2）、亚马逊和亚马 CloudFront逊 Route 53 费用中与 DDo S 相关的峰值。 AWS Global Accelerator

AWS Managed Services 常见问题解答中的 Shield Ad

问：如何在我的 AMS 账户中申请访问 Shield Advanced？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Shield Advanced。此 RFC 为您的账户配置以下 IAM 角色：`customer_shield_role`和。`aws_drt_shield_role`在您的账户中配置角色后，您必须在联合解决方案中加入角色。

将角色部署到您的账户后，您可以使用在`customer_shield_role`您的账户 AWS Shield Advanced 中确认订阅。

> **Note**
>
> 请注意，使用需要支付月费和一年的使用期限 AWS Shield Advanced。此外， AWS Shield Advanced 在 AMS 中使用会授权 AMS 升级到 AWS Shield (SRT)，后者可以在分布式拒绝服

务 (S AWS WAF) 事件升级期间更改您的 Web 应用程序防火墙 (DDo) 规则。这些变更将与AMS协调进行。

问：在我的 AMS 账户中使用 Shield Advanced 有哪些限制？

尽管不是限制，但你应该明白，使用 Shield Advanced 会部署`aws_drt_shield_role`，这允许 AWS Shield 队伍 (SRT) 在 S 事件升级 DDo期间对 AMS 账户内的 AWS WAF 规则进行紧急更改。AMS 建议这样做是为了最快地修复 DDo S 攻击，并且会在 AMS 升级到 SRT 之后发生。

问：在我的 AMS 账户中使用 Shield Advanced 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Shield Advanced 没有任何先决条件或依赖关系。

使用 AMS SSP AWS Snowball Edge 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Snowball Edge 功能。Snowball Edge 是一种 PB 级的数据传输解决方案，它使用专为安全设计的设备将大量数据传输到云端和从云端传出。 AWS Snowball Edge 解决了大规模数据传输的常见挑战，包括高昂的网络成本、较长的传输时间和安全问题。您可以使用 Snowball Edge 迁移分析数据、基因组学数据、视频库、图像存储库、备份，并存档部分数据中心关闭、磁带更换或应用程序迁移项目。使用 Snowball Edge 传输数据既简单、快速、更安全，而且只需通过高速互联网传输数据的成本的五分之一。

使用 Snowball Edge，您无需编写任何代码或购买任何硬件即可传输数据。首先使用 AWS 管理控制台为 Snowball 创建导入任务，Snowball 设备将自动发送给您。设备到达后，将设备连接到您的本地网络，下载并运行 Snowball Client (“客户端”) 以建立连接，然后使用客户端选择要传输到设备的文件目录。然后，客户端会加密文件并将其高速传输到设备。转移完成并准备退回设备后，电子墨水的运输标签会自动更新，您可以通过亚马逊简单通知服务 (Amazon SNS) Simple Notification Service、短信或直接在控制台中跟踪任务状态。要了解更多信息，请参阅AWS Snowball Edge。

AWS Managed Services 常见问题中的 Snowball Edge

常见问题和答案：

问：如何申请访问我 AWS Snowball Edge 的 AMS 账户？

在 AMS 中实施 Snowball Edge 分为两个步骤：

1. 提交管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型，然后为你的 AMS 账户申请 Snowball Edge 的服务角色。

2. 通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来请求用户访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_snowball_console_role`、`customer_snowball_export_role` 和 `customer_snowball_import_role`。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS Snowball Edge 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Snowball Edge 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Snowball Edge 中使用的先决条件或依赖条件是什么？

您必须拥有如上所述的服务角色帐户。

使用 AMS SSP AWS Step Functions 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Step Functions 功能。AWS Step Functions 是一项 Web 服务，使您能够使用可视化工作流来协调分布式应用程序和微服务的组件。您可通过能执行离散函数（或称为任务）的各单独组件构建应用程序，这样您能够快速扩展和更改应用程序。Step Functions 提供了一种可靠的方法来协调组件并逐步执行应用程序的函数。Step Functions 提供了一个图形控制台，可将应用程序的组件可视化为一系列步骤。它会自动触发和跟踪每个步骤，并在出现错误时重试，因此您的应用程序每次都能按预期按顺序运行。Step Functions 会记录每个步骤的状态，这样在出现错误时，您就能够迅速诊断并调试问题。要了解更多信息，请参阅AWS Step Functions。

AWS 托管服务常见问题解答中的 Step Functions

常见问题和答案：

问：如何在 AMS 账户 AWS Step Functions 中申请访问权限？

AWS Step Functions 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_step_functions_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS Step Functions 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Step Functions 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Step Functions 中使用的先决条件或依赖条件是什么？

在运行时，Step Functions 使用的角色必须有权访问步进函数所使用的服务。例如，步进函数可能依赖于 Lambda 函数。创作步骤函数的人很可能同时创建 Lambda 函数，并且还必须请求访问该服务。

使用 AMS SSP 在您的 AMS 账户中配置 AWS Systems Manager 参数存储

使用 AMS 自助配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Systems Manager 参数存储功能。 AWS Systems Manager Parameter Store 为配置数据管理和密钥管理提供安全的分层存储。也可以将密码、数据库字符串和许可证代码等数据存储为参数值。可以将值存储为纯文本或加密数据。然后，可以使用创建参数时指定的唯一名称来引用对应值。Parameter Store 具有高度的可扩展性、可用性和耐用性，由 AWS 云端提供支持。要了解更多信息，请参阅AWS Systems Manager 参数存储。

> **Note**
>
> 如果您想要一个具有生命周期管理功能的专用密钥存储库，请使用使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置而不是参数存储。Secrets Manager 允许您自动轮换密钥，从而帮助您满足安全和合规要求。Secrets Manager 在 Amazon RDS 上为 MySQL、PostgreSQL 和 Amazon Aurora 提供了内置集成，可通过自定义 Lambda 函数将其扩展到其他类型的机密。

AWS Systems Manager AWS Managed Services 中的参数存储常见问题

常见问题和答案：

问：如何在我的 AMS 账户中请求访问 Systems Manager 参数存储区？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请对 AWS Systems Manager 参数存储的访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_systemsmanager_parameterstore_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 P AWS Systems Manager arameter Store 有哪些限制？

您需要使用 AWS 托管密钥；创建自定义 KMS 密钥的访问权限受到限制。但是，如果需要自定义密钥，请提交 RFC 以使用此 IAM 角色的部署 | 高级堆栈组件 | KMS 密钥 | 创建更改类型 (ct-1d84keiri1jhg) 作为和参数的值来创建客户管理的密钥 (CMK)。`customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions` `IAMPrincipalsRequiringEncryptPermissionsPrincipal`创建 KMS 密钥后，您可以使用它创建安全字符串。

问：在我的 AMS 账户中使用 P AWS Systems Manager arameter Store 有哪些先决条件或依赖关系？

没有先决条件；但是，SSM Parameter Store 依赖 KMS 来创建安全字符串，因此您可以加密和解密存储在参数存储中的值。

使用 AMS SSP 在您的 AMS AWS Systems Manager 账户中配置自动化

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 AWS Systems Manager 自动化功能。 AWS Systems Manager 自动化使用运行手册、操作和服务配额简化了 Amazon Elastic Compute Cloud 实例和其他 AWS 资源的常见维护和部署任务。它使您能够大规模构建、执行和监控自动化。Systems Manager Automation 是一种系统管理器文档，它定义了系统管理器对您的托管实例执行的操作。一本运行手册，用于执行常见的维护和部署任务，例如在托管实例中运行命令或自动化脚本。Systems Manager 包括一些功能，可帮助您使用亚马逊弹性计算云标签定位大量实例，以及帮助您根据定义的限制推出更改的速度控制。运行手册是使用 JavaScript 对象表示法 (JSON) 或 YAML 编写的。但是，通过使用 Systems Manager 自动化中的文档生成器，您可以创建运行手册，而无需使用本机 JSON 或 YAML 创作。或者，您可以使用 Systems Manager 提供的运行手册，其中包含适合您需求的预定义步骤。要了解更多信息，请参阅 AWS Systems Manager 文档中的使用运行手册。

> **Note**
>
> 尽管 Systems Manager Automation 支持 20 种可在运行手册中使用的操作类型，但在创作要在 AMS 高级账户中使用的运行手册时，您可以使用的操作数量有限。同样，系统管理器提供的运行手册数量有限，既可以直接使用，也可以从自己的运行手册中使用。有关详细信息，请参阅以下常见问题解答中的限制。

AWS Systems Manager AWS Managed Services 中的自动化常见问题解答

常见问题和答案：

问：如何通过我的 AMS 账户申请访问 Systems Manager Automation？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请 AWS Systems Manager 自动化的访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_systemsmanager_automation_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 AWS Systems Manager 自动化有什么限制？

你需要编写运行手册，只有在托管实例中运行命令 and/or 脚本时，Systems Manager 支持的操作有限。下文概述了可供您执行的操作以及任何限制。

AWS Systems Manager 自动化限制

操作	说明	限制
aws：assertAwsResource财产 —	断言 AWS 资源状态或事件状态	仅限 EC2 实例
aw: aws: branch —	运行条件自动化步骤	没有限制
AWS: 创建标签 —	为 AWS 资源创建标签	仅适用于您撰写的 SSM 自动化运行手册
AWS: 执行自动化 —	运行另一个自动化	只有您撰写的自动化运行手册
aws: 执行脚本 —	运行脚本	唯一不对任何服务进行任何 API 调用的脚本
aws: 暂停 —	暂停自动化	没有限制
aws: runCommand	在托管实例上运行命令	仅使用系统管理器提供的文档 — AWS RunShellScript 和 AWS-RunPowerShellScript
aws: sleep —	延迟自动化	没有限制
aws: waitForAws ResourceProperty —	等待 AWS 资源属性	仅限 EC2 实例

您也可以选择使用 Systems Manager 控制台中的 “运行命令” 功能直接RunPowerShellScript 使用 Systems Manager 提供的运行手册 AWS RunShellScript 和 AWS 运行手册运行命令或脚本。您还可以将这些运行手册嵌套在运行手册中，以满足额外的 and/or 后期验证或任何复杂的自动化逻辑。

该角色遵循最低权限原则，仅提供创作、执行和检索旨在在托管实例中执行命令 and/or 脚本的 runbook 的执行详细信息所需的权限。它不为 AWS Systems Manager 服务提供的任何其他功能提供权限。虽然该功能允许您编写自动化运行手册，但不能将运行手册的执行定向 AMS 拥有的资源。

问：在我的 AMS 账户中使用 AWS Systems Manager 自动化的先决条件或依赖条件是什么？

没有先决条件；但是，在编写运行手册时，必须确保 and/or 遵守内部流程合规性控制。我们还建议在根据生产资源执行运行手册之前，对其进行全面测试。

问：Systems Manager 策略**customer_systemsmanager_automation_policy**能否附加到其他 IAM 角色？

不可以，与其他启用自行配置的服务不同，此策略只能分配给已配置的默认角色。`customer_systemsmanager_automation_console_role`

与其他 SSP 角色的策略不同，此 SSM SSP 策略不能与其他自定义 IAM 角色共享，因为此 AMS 服务仅用于在托管实例中运行命令或自动化脚本。如果允许将这些权限附加到其他自定义 IAM 角色（可能具有其他服务的权限），则允许的操作范围可能会扩展到托管服务，并可能降低您账户的安全状况。

要根据我们的 AMS 技术标准评估任何变更请求 (RFCs)，请与您各自的云架构师或服务交付经理合作，请参阅 RFC 安全审查。

> **Note**
>
> AWS Systems Manager 允许您使用与您的帐户共享的运行手册。我们建议您在使用共享运行手册时谨慎行事并进行尽职调查，并确保在执行运行手册之前查看内容以了解 command/scripts 其运行情况。有关详细信息，请参阅共享 SSM 文档的最佳实践。

使用 AMS SSP AWS Transfer Family 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Transfer Family（Transfer Family）功能。 AWS Transfer Family 是一项完全托管的 AWS 服务，允许您通过安全文件传输协议 (SFTP) 将文件传输到亚马逊简单存储服务 (Amazon S3) Simple S3 Service 存储和传出亚马逊简单存储服务 (Amazon S3) 存储。SFTP 也称为安全外壳 (SSH) 文件传输协议。SFTP 用于不同行业的数据交换工作流程，例如金融服务、医疗保健、广告和零售等。

使用 AWS SFTP，您 AWS 无需运行任何服务器基础架构即可访问 SFTP 服务器。您可以使用此服务将基于 SFTP 的工作流程迁移到， AWS 同时保持最终用户的客户端和配置不变。首先将您的主机名与 SFTP 服务器端点相关联，然后添加您的用户并为其配置适当的访问级别。完成后，将直接从您的 AWS SFTP 服务器端点处理用户的传输请求。要了解更多信息 AWS Transfer for SFTP，另请参阅创建支持 SFTP 的服务器。

AWS Transfer for SFTP 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Transfer for SFTP 的 AMS 账户？

AWS Transfer for SFTP 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色和策略：

- `customer_transfer_author_role`。 此角色旨在让您通过控制台管理 SFTP 服务。
- `customer_transfer_sftp_server_logging_role`。 此角色旨在附加到 SFTP 服务器上。它允许 SFTP 服务器提取日志。 CloudWatch
- `customer_transfer_sftp_user_role`。 此角色旨在附加到 SFTP 用户身上。它允许 SFTP 用户与 S3 存储桶进行交互。
- `policy customer_transfer_scope_down_policy`。 此策略是一项范围缩小策略，可应用于 SFTP 用户，将他们对 S3 存储桶的访问权限限制为其主文件夹。
- `customer_transfer_sftp_efs_user_role`。 此角色旨在附加到 SFTP 用户身上。它允许 SFTP 用户与 EFS 文件系统进行交互。

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问： AWS Transfer for SFTP 在我的 AMS 账户中使用有什么限制？

AWS SFTP 配置的传输仅限于没有 “AMS-” 或 “MC-” 前缀的资源，以防止对 AMS 基础设施进行任何修改。

问：在我的 AMS 账户 AWS Transfer for SFTP 中使用的先决条件或依赖条件是什么？

- 在创建服务器和用户之前，您必须拥有名称包含关键字 “transf AWS Transfer for SFTP er” 的 Amazon S3 存储桶。
- 要使用 “客户识别提供商”，您必须部署 API Gateway、Lambda 函数和您的用户存储库（AD、Secrets Manager 等）。有关更多信息，请参阅启用密码身份验证以 AWS Transfer for SFTP 使用 AWS Secrets Manager和使用身份提供商。

使用 AMS SSP AWS Transit Gateway 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Transit Gateway 功能。AWS Transit Gateway 是一项服务，可让您将 Amazon Virtual Private Cloud (VPCs) 和本地网络连接到单个网关。随着运行的工作负载数量的增加 AWS，您需要能够跨多个账户和 Amazon 扩展您的网络， VPCs 以跟上增长的步伐。如今，您可以使用对等互连连接成对的A VPCs mazon。但是，如果无法集中管理 point-to-point连接策略 VPCs，则管理许多 Amazon 的连接可能在运营上成本高昂且繁

琐。要实现本地连接，您需要将 AWS VPN 连接到每个 Amazon VPC。此解决方案的构建可能非常耗时，而且在数量 VPCs 增加到数百个时也难以管理。要了解更多信息，请参阅AWS Transit Gateway。

AWS Transit Gateway 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Transit Gateway 中申请访问权限？

AWS Transit Gateway 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_tgw_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS Transit Gateway 在我的 AMS 账户中使用有什么限制？

除了 Trans AWS Transit Gateway it Gateway 路由的路线表修改外，您的 AMS 单账户着陆区账户中提供了的全部功能。通过提交管理 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76) 来请求更改路由表。

> **Note**
>
> 此服务仅支持单账户着陆区 (SALZ)，不支持多账户着陆区 (MALZ)。

问：在我的 AMS 账户 AWS Transit Gateway 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Transit Gateway 中没有必备条件或依赖项可供使用。

使用 AMS SSP 在您的 AMS 账户中配置 AWS WAF -Web 应用程序防火墙

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS WAF 功能。 AWS WAF 是一种 Web 应用程序防火墙 (AWS WAF)，可帮助保护您的 Web 应用程序免受常见 Web 漏洞的侵害，这些漏洞可能会影响应用程序可用性、危及安全性或消耗过多资源。 AWS WAF 通过定义可自定义的 Web 安全规则，您可以控制允许或阻止哪些流量进入您的 Web 应用程序。您可以使用 AWS WAF 创建阻止常见攻击模式（例如 SQL 注入或跨站点脚本）的自定义规则；以及专为您的特定应用程序设计的规则。

要了解更多信息，请参阅 AWS WAF -Web 应用程序防火墙。

AMS 不支持监控（CloudWatch 警报/事件/彩信提醒）。 AWS WAF由于的性质 AWS WAF，您必须为应用程序创建自定义规则；如果没有应用程序的上下文，AMS 无法为您量化和创建警报。要了解更多信息，请参阅 AWS WAF -Web 应用程序防火墙。

AWS WAF 在 AWS Managed Services 常见问题中

常见问题和答案：

问： AWS WAF 如何申请在我的 AMS 账户中进行设置？

AWS WAF 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_waf_role`. 在您的账户中配置 I AWS WAF AM 角色后，您必须在联合身份验证解决方案中加入该角色。

问：使用有什么限制 AWS WAF？

配置权限后，您将拥有的全部功能。 AWS WAF

问：使用的先决条件或依赖关系 AWS WAF是什么？

您的 AMS 账户 AWS WAF 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Well-Architected Tool 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Well-Architected Tool 功能。 AWS Well-Architected Tool 可帮助您查看工作负载的状态，并将其与最新的 AWS 架构最佳实践进行比较。该工具基于Well-Architect AWS ed Framework，旨在帮助云架构师构建安全、高性能、弹性和高效的应用基础架构。该框架为您评估架构提供了一种一致的方法，已在 AWS 解决方案架构团队进行的数万次工作负载审查中使用，并提供了指导以帮助实施可随着时间的推移随应用程序需求而扩展的设计。要了解更多信息，请参阅AWS Well-Architected Tool。

AWS WA Tool 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Well-Architected Tool 中申请访问权限？

AWS Well-Architected Tool 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_well_architected_tool_console_admin_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问： AWS Well-Architected Tool 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Well-Architected Tool 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Well-Architected Tool 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Well-Architected Tool 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS X-Ray 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS X-Ray (X-Ray) 功能。AWS X-Ray 帮助开发人员分析和调试生产型分布式应用程序，例如使用微服务架构构建的应用程序。借助 X-Ray，您可以了解您的应用程序及其底层服务的性能，从而识别和排除性能问题和错误的根本原因。X-Ray 提供请求在应用程序中传输时的 end-to-end视图，并显示应用程序底层组件的地图。您可以使用 X-Ray 分析开发和生产中的应用程序，从简单的三层应用程序到由数千个服务组成的复杂微服务应用程序。要了解更多信息，请参阅AWS X-Ray。

AWS 托管服务中的 X-Ray 常见问题解答

常见问题和答案：

问：如何申请访问我 AWS X-Ray 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_xray_console_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。此外，您必须拥有将数据从您的 Amazon EC2 实例推送`customer_xray_daemon_write_instance_profile`到 X-Ray 的权限。此实例配置文件是在您收到时创建的`customer_xray_console_role`。

您可以向 AMS Operations 提交服务请求以将其分配给现有实例配置文件，也可以使用 AMS Operations 为您启用 X-Ray 时创建的实例配置文件。`customer_xray_daemon_write_policy`

问： AWS X-Ray 在我的 AMS 账户中使用有什么限制？

除了使用 KM AWS X-Ray S 密钥（KMS 密 AWS 钥）进行加密外，您的 AMS 账户中还提供的所有功能。 AWS X-Ray 默认情况下会加密所有跟踪数据。默认情况下，X-Ray 对静态跟踪和相关数据进行加密。如果您需要使用密钥加密静态数据，则可以选择由托管的 KMS 密钥 (aws/xray) 或 KMS 客户AWS管理的密钥。对于用于 X-Ray 加密的 KMS 客户管理密钥，请提交管理 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76)。

问：在我的 AMS 账户 AWS X-Ray 中使用的先决条件或依赖条件是什么？

AWS X-Ray 依赖于 Amazon S3 和 CloudWatch 日志，它们已在 AMS 账户中实现。 CloudWatch 传递依赖关系因数据源和功能可能与之交互的其他 AWS 服务 AWS X-Ray （例如 Amazon Redshift、Amazon RDS、Athena）而异。

使用 AMS SSP Import/Export 在您的 AMS 账户中配置虚拟机

使用 AMS 自助配置 (SSP) 模式 Import/Exportcapabilities 直接在您的 AMS 托管账户中访问虚拟机。通过虚拟机， Import/Export 您可以轻松地将虚拟机映像从现有环境导入到 Amazon EC2 实例，然后将其导出回本地环境。该产品允许您将虚拟机 EC2 作为 ready-to-use实例引入 Amazon，从而利用您为满足 IT 安全、配置管理和合规要求而构建的虚拟机的现有投资。您还可以将导入的实例导回本地虚拟化基础架构，从而可以在 IT 基础架构中部署工作负载。要了解更多信息，请参阅虚拟机导入/导出。

AWS Managed Services Import/Export 中的虚拟机常见问题

常见问题和答案：

问：如何使用我的 AMS 账户申请虚拟机的 Import/Export 访问权限？

Import/Export 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来请求访问虚拟机。此 RFC 为您的账户提供以下 IAM 政策:`customer_vmimport_policy`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

服务需要一个额外的角色，即虚拟机 Import/Export 服务角色，才能在您的账户中执行操作。

问： Import/Export 在我的 AMS 账户中使用 VM 有哪些限制？

- AMS VM Import/Export 中均提供导入自定义机器映像和数据量的功能。但是，对 S3 的权限范围已缩小，将操作限制`customer-vmimport-*`在与名称相匹配的存储桶上，从而限制对账户内信息的访问。
- AMS 虚拟机导入/导出支持图像和快照导入。但是，由于安全措施，实例导入和实例导出功能不可用。
- 此外，为了降低导出受限和敏感数据的风险，导出功能已被禁用。

问：在我的 AMS 账户 Import/Export 中使用 VM 有哪些先决条件或依赖关系？

- 您必须提供支持的磁盘映像才能导入到 AWS 环境中。有关信息，请参阅虚拟机 Import/Export 要求。
- Import/Export 无法通过 AWS 控制台访问虚拟机。您必须通过 AWS CLI AWS Tools for PowerShell、或访问此服务 AWS SDKs。或者，您可以通过提交更改类型 ct-117rmp64d5mvb：部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | 创建实例配置文件来请求实例配置文件。EC2 此实例配置文件允许工具从实例执行命令。

客户管理模式

AWS Managed Services (AMS) 客户管理模式提供了一种灵活且可以根据您的要求进行调整的管理模型。这可以被视为 AMS 无法为您运行的服务和应用程序的备用选项。AMS 不运营托管在此模式下创建的账户中的基础设施。但是，您可以在此模式下利用集中式多账户管理。在此模式下，可以利用以下多账户登录区域功能：

- 自动账户部署
- 通过网络账户中的 Transit Gateway 进行连接
- AMS Config 规则库
- 将日志副本存储在登录账户中
- 将客户管理的 Guard Duty 警报汇总到安全账户
- 整合账单
- 启用自定义服务控制策略。

例如：如果您想在 Ubuntu Pro 上运行工作负载，而该操作系统不是 AMS 管理的操作系统，则可以使用客户管理的账户来托管。您还可以通过客户托管账户整合工作负载，以利用通过在 AWS 组织之间共享而获得的预留 Instances/Sharing 计划的批量折扣。

开始使用客户管理模式

AMS 客户管理模式可通过特殊的多账户 landing zone 应用程序账户获得。

有关详细信息，包括如何创建客户托管应用程序帐户，请参阅客户管理的应用程序帐户。

AMS 和 AWS Service Catalog

AWS Managed Services (AMS) 中的 Service Catalog 允许组织创建和管理 AWS 信息技术 (IT) 服务的目录，并允许 IT 管理员创建、管理和向其账户中的最终用户分发经批准的产品目录，然后他们可以在个性化的服务门户中访问所需的产品。管理员可以控制哪些用户有权访问每种产品，以强制遵守组织业务政策。管理员还可以设置角色，这样最终用户只需要访问 Service Catalog 的 IAM 访问权限即可部署已批准的资源。Service Catalog 使您的组织能够从更高的灵活性和更低的成本中受益，因为最终用户只能从您控制的目录中查找和发布他们需要的产品。

Service Catalog 为您提供 AMS 变更申请 (RFC) 流程的替代方案，用于在您的 AMS 托管账户中配置和更新资源。AMS 为通过 Service Catalog 配置的所有基础设施资源管理大规模运行 AWS 所需的所

有基础设施运营任务，包括安全、合规、配置、可用性、补丁、监控、警报、报告、事件响应和成本优化。在您的 AMS 托管账户中使用 Service Catalog 可为您提供一种集中管理常用部署的 IT 服务的机制，并帮助您实现一致的治理，同时使用户能够快速将他们需要的经批准的 IT 服务部署到其托管环境中。

Service Catalog 入门

要开始使用 AMS 中的 Service Catalog，请通过 AMS 控制台提交服务请求以请求访问服务目录。提交请求后，将向您的账户部署三个 IAM 角色以及一个包含调用 AMS 的 CloudFormation 宏的 AMS 托管堆栈`Transform`（如前所述），以便我们可以在系统中注册产品，并对通过 Service Catalog 配置的基础设施执行操作。部署的三个 IAM 角色包括 IT 管理员以服务目录管理员的身份管理产品的角色；一个供应用程序所有者和最终用户配置、启动和管理产品的角色；以及一个用作启动约束的角色，用于定义 Service Catalog 在启动或更新产品时将使用的权限。

开始之前 AMS 中的 Service Catalog

Service Catalog 是否会取代现有的 AMS 变更申请 (RFC) 流程？

> 在启用了 Service Catalog 的账户中，它将充当变更管理系统，您可以在其中通过预定义的产品目录在 AMS 账户中配置和更新 IT 服务；AMS 将提供默认 portfolio/product 目录，您的 IT 管理员可以创建和配置自己的目录。Service Catalog 只会确认通过 Service Catalog 置备的堆栈。同样，通过 Service Catalog 提供的服务也无法通过 AMS RFC 流程进行修改，因为在 Service Catalog 之外的修改会使堆栈偏离经批准的产品配置。

我能否在 AMS 控制台中查看通过服务目录配置的堆栈？

> 是。您可以在 AMS 控制台中查看通过服务目录配置的所有堆栈。通过服务目录配置的堆栈可通过 “SC-” 的堆栈 ID 轻松识别。尽管可以在 AMS 控制台中查看堆栈，但您将无法通过 AMS RFC 流程进行更新。对 AMS 变更管理系统 (RFCs) 的访问仅限于访问请求、补丁编排和备份 RFCs 。

如果我通过 Service Catalog 配置 and/or 更新堆栈，AMS 控制台中是否会有相应的 RFC？

> AMS 控制台中唯一会显示的 RFC 是在最初配置堆栈时向 AMS 注册堆栈的 RFC。此 RFC 由 AMS 验证流程自动归档，该流程是在通过 Service Catalog 启动堆栈时触发的。所有其他配置和更改都直接在 Service Catalog 中进行跟踪，也可以在服务目录控制台中查看。此外，您还可以使用 Service Catalog 中的预配置产品计划功能来查看在置备或更新产品之前将对资源所做的更改列表。

在我的 AMS 托管账户中配置产品时，我需要做任何具体的事情吗？

> 是。在 AMS 账户中配置的所有 Service Catalog 产品都必须在定义该产品的 CFN 模板中包含以下 JSON 行：

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

在您的 AMS 托管账户中配置资源之前，这段 CloudFormation 代码会触发所需的 AMS 验证。您有责任将此行代码作为产品定义的一部分。如果不包括在内，则配置将失败并显示以下错误消息：“无法创建产品。此账户由 AMS 管理。AMS 账户中的所有商品的模板中都必须有 AMS `Transform` 代码。”

在发布时，是否有任何不 and/or 限于 AMS 客户的 Service Catalog 功能？

是的，以下 SC 功能在首次发布时不适用于 AMS 客户：

- 通过 Service Catalog 创建账户
- 能够通过 Service Catalog 在 AMS 管理的账户中启动所有 AWS 服务。AWS 服务的可用性仅限于 AMS 支持的服务（托管和自行配置）。有关 AMS 支持的服务的更多信息，请参阅 AMS 服务说明。
- Service Catalog IT 服务管理器 (ITSM) 连接器无法与 AMS 事件报告和服务请求进行通信。
- 无需修改即可利用 Service Catalog 快速入门和参考架构。请记住，AMS 账户的 Service Catalog 产品必须包含以下一行 JSON 代码：

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  在 CNF 模板中。请注意，此行不是典型的 AWS CloudFormation 模板的一部分，必须明确添加。
- AMS 目前不支持 Terraform 来配置 Service Catalog 产品。
- AMS 不支持 AWS CFN 堆栈集。
- 您无法创建自定义 IAM 角色。
- 服务操作仅限于：
  - AWS-RebootRdsInstance
  - AWS EC2 重启实例
  - AWS 启动实例 EC2
  - AWS-StartRdsInstance
  - AWS-stop 实例 EC2
  - AWS-StopRdsInstance
  - AWS-CreateImage

- AWS-CreateRdsSnapshot
- AWS-CreateSnapshot

> **Note**
>
> 创建服务操作时，您可以将执行角色配置为最终用户的权限、启动角色或您选择的自定义 IAM 角色。所选执行角色必须具有足够的权限才能执行服务操作，并且必须具有允许 Service Catalog 代入 TrustPolicy 该服务操作的权限，否则该服务操作将在执行时失败。我们建议使用具有正确权限和信任策略的，可用作服务操作。 AWSManaged ServicesServiceCatalogLaunchRole

我还需要使用 AMS RFC 系统做什么？

正式上市 (GA) 后，您仍需要使用 RFCS 来运行以下操作：

- 配置补丁编排器
- 配置备份策略
- 请求实例访问权限
- 创建和分配不符合 AMS 准则的安全组。
- 执行工作负载摄取 (WIGS)
- 创建 IAM 角色

我能否使用 Service Catalog CLI 访问我的 AMS 托管账户中的服务目录？

是的，Service Catalog APIs 可用并通过 CLI 启用。从 Service Catalog 对象的管理到配置和终止这些构件的操作都可用。有关更多信息，请参阅 AWS Service Catalog 资源，或下载最新的 AWS 开发工具包或 CLI。

谁创建、管理和分发客户的批准产品目录？

客户的目录管理员 and/or IT 管理员或分配的资源负责管理您的 Service Catalog 目录和批准的产品。

我可以使用 AMS AMIs 吗？

2020 年 3 月之后 AMIs 销售的 AMS 可以通过 AWS Service Catalog 进行部署。

如何使用 Service Catalog 迁移到 AMS？

要使用 Service Catalog 将工作负载迁移到 AMS，首先要按照工作负载摄WIGs取 () 流程在 AMS 中创建 AMI。您可以使用 WIGS 生成的 AMI 在 Service Catalog 中创建产品。AWS Service Catalog-入门中详细介绍了如何执行此操作。

AMS 多账号 landing zone (MALZ) 入门

MALZ 网络架构

关于多账号 landing zone 网络架构

在开始登录 AWS Managed Services (AMS) 多账户着陆区 (MALZ) 之前，请务必了解 AMS 代表您创建的基准架构或着陆区、其组件和功能。

AMS multi-account landing zone 是一种多账户架构，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。

> **Note**
>
> 有关成本估算，请参阅 AMS 多账户 landing zone 环境基本组件。

主题

- 服务区域
- 组织部门
- 服务控制策略和 AWS 组织

下图概述了账户结构以及如何将基础设施划分到每个账户中：

服务区域

由于 Active Directory 和 Transit Gateway 当前的跨区域限制，AMS 多账户着陆区内的所有资源都部署在您选择的单个 AWS 区域内。

组织部门

典型的 AMS 多账户登陆区由四个顶级组织单位 (OUs) 组成：

- 核心组织单位 (OU)（用于将账户组合在一起，作为一个单元进行管理）
- 应用程序 OU

- 客户管理的 OU
- 加速 OU

AMS 管理的多账户 landing zone 还允许您创建 OUs 用于分组和组织 AWS 账户的自定义账户，并将自定义账户 SCPs 与之关联；有关执行此操作的示例，请分别参阅管理账户 | 创建自定义账户 OUs和管理账户 | 创建自定义 SCP（需要审核）。AMS 提供了四个现有账户，可以在这些账户 OUs 下申请新的 OUs 和账户：加速、应用程序 > 托管、应用程序 > 开发和客户管理。

- 加速 OU：

  这是 AMS 多账户着陆区 (MALZ) 中的顶级组织单位。此 OU 下的账户由 AMS 提供 RFC（部署 | 托管着陆区 | 管理账户 | 创建加速账户，更改类型 ID：ct-2p93tyd5angmi）。在这些加速应用程序帐户中，您可以受益于加速运营服务，例如监控和警报、事件管理、安全管理和备份管理。有关更多详细信息，请参阅 AMS 加速账户。

- 应用程序 > 托管 OU：

  在应用程序 OU 的这个子组织单元中，账户完全由 AMS 管理，包括所有操作任务。运营任务包括服务请求管理、事件管理、安全管理、连续性管理、补丁管理、成本优化、监控和事件管理。这些任务是为了管理您的基础架构而执行的。在达到 AWS 组织的最大嵌套 OUs 限制之前， OUs 可以根据需要创建多个子项目。有关详细信息，请参阅 AWS Organizations 的配额。

- 应用程序 > 开发 OU:

  在 AMS 管理的 landing zone 中应用程序 OU 的子组织单位下，账户是开发者模式账户，可为您提供在 AMS 变更管理流程之外配置和更新 AWS 资源的高级权限。此 OU 还支持根据需要创建新的子项 OU。

- 客户管理的 OU：

  这是 AMS 多账号 landing zone 中的顶级 OU。此 OU 下的账户由 AMS 提供 RFC。在这些账户中，工作负载和 AWS 资源的操作由您负责。此 OU 还支持根据需要创建新的子项 OU。

作为最佳实践，我们建议根据其功能 OUs 和政策对这些账户和自定义请求的子账号OUs 进行分组。

服务控制策略和 AWS 组织

AWS 为 AWS 组织中的权限管理提供服务控制策略 (SCPs)。 SCPs 用于为用户在哪些操作中可以执行的操作定义额外的护栏。 OUs默认情况下，AMS 提供一组 SCPs 部署在管理账户中的账户，这些账户在不同的默认 OU 级别提供保护。如需了解 SCP 限制，请联系您的 CSDM。

您也可以创建自定义 SCPs 并将它们附加到特定的 OUs。可以使用变更类型 ct-33ste5yc7hprs 向您的管理账户申请它们。然后，AMS 会审核所 SCPs 请求的自定义，然后再将其应用于目标 OUs。有关示例，请参阅管理账户 | 创建自定义账户 OUs和管理账户 | 创建自定义 SCP（需要审阅）。

选择单个 MALZ 或多个 MALZs

下表提供了在单个多账户着陆区 (MALZ) 与多个多账户着陆区（例如，两个多账户着陆区-Prod 和 non-Prod）之间做出决定时的一些高级注意事项。通常，选择取决于个人需求、法律要求和运营实践。

单个多账户着陆区与多个多账户着陆区

实体	单个 AMS 着陆区	多个（两个或更多）着陆区
基础成本	较低，经过优化，每月约为3,000美元。	更高，每个环境的额外成本约为 3,000 美元。
计费	单一账单，由于单一账单/管理账户。	每个多账号 landing zone 均需单独计费。目前，AWS Org 不支持使用单一账单的多管理账户。
现有预留实例的可移植性 () RIs	低。AWS RIs 目前无法在多个账单账户之间进行转换。你可以将现有资源重新 RIs 用于多账户 landing zone。	更低。您将重新调整用途并在 RIs 所有多账号 landing zone 上进行分发。
产品分层折扣	高。参见批量折扣。	低。参见批量折扣。
初始设置开销（按 project/migration 时间表计算）	低。Active Directory、联网和单点登录 (SSO) 集成仅限一次。	高。您将为每个着陆区执行 Active Directory、网络集成和 SSO 集成。这可能会导致任何迁移项目出现延迟。
常用服务可配置性	不费吹灰之力。您可以配置 DNS、备份、监控、日志记录等 common/shared 服务。	付出高昂的努力。需要进行额外的规划，以解决公共基础设施或服务的发展方向。在每个着陆区（landing zoneTGWs）中穿越多个公交网关 () 的流量可能会导致额外费用。
可扩展性	中等。AMS 目前的实际限制为每个多账号着陆区 150 个账户。在同一个账户中运行应用程序的多个团队或供应商	高。能够利用多个多账户 landing zone 来分配账户，同时实现账户或应用程序

实体	单个 AMS 着陆区	多个（两个或更多）着陆区
	可以访问不同团队拥有的堆栈。可以通过控制 ServiceNow 层对特定应用程序堆栈的访问来缓解这种限制（通过集成 AMS Conn ServiceNow ector 应用程序并使用标签）。询问 AMS 技术交付经理 (TDMs) 或云架构师 (CAs) 如何实现这一点。	的隔离级别。管理大量账户可能会导致运营或成本开销。
运营风险	（视情况而定）低。操作整合和准备就绪仅一次。流程漂移的可能性更小。	（视情况而定）低。多种整合和运营活动。在此期间，在多个着陆区漂移可能会导致操作风险。
多 AWS 区域	单个 AWS 区域。AMS 多账户 landing zone 仅限于单个 AWS 区域。要跨越多个 AWS 区域，请使用多个多账户 landing zone。	多 AWS 区域。借助多个多账户着陆区，您可以将每个 MALZ 部署在一个区域中，并使用公交网关 (TGW) 对等互连将它们互连。
账户迁移或可移植性	是。在同一 AWS 组织内将账户从一个 OU 转移到另一个 OU 是可能的。	不是。 AMS 不支持跨着陆区（即 AWS Organizations）迁移账户。工作负载可以通过传输网关 (TGW) 或 VPC 对等互连跨着陆区域传输。
变更管理	中等。对 TGW、Active Directory (AD) 或出站（出口）等常见组件进行破坏性更改可能会影响多账户着陆区中的所有工作负载。但是，对 AMS 管理的组件所做的更改需要在内部进行测试，并以滚动更新形式推送。	低。对 TGW、AD 或出站（出口）等常见组件进行破坏性更改只能影响该特定多账户 landing zone 中的工作负载。
数据和访问控制	（视情况而定）如果您想连接不同的本地 ADs 和网络来处理生产和非生产工作负载，则控制不足。SAML 联合、TGW 域和安全组 (SGs) 也可以帮助实现所需的控制。	（视情况而定）如果您想连接不同的本地 ADs 和网络以处理生产和非生产工作负载，则可以进行高度控制。使用单独的着陆区以满足严格的合规要求。

实体	单个 AMS 着陆区	多个（两个或更多）着陆区
合规与安全	（视情况而定）如果有严格的合规要求将材料和非物质工作负荷完全分开，则为低。AMS 标准的预防和侦查控制措施已到位。	（视情况而定）High as multi-account landing zone可以通过将材料和非物质工作量完全隔离来帮助实现严格的合规要求。AMS 标准的预防和侦查控制措施已到位。

建议：如果没有严格的合规或多区域需求，从单个 AMS 多账户 landing zone 开始，就可以在成本、安全、卓越运营和迁移复杂性之间取得良好的平衡。如果遇到任何账户或业务限制，你可以随时设置额外的 landing zone。

单个多账户着陆区与多个多账户着陆区 FAQs

选择设置单个多账户着陆区或多个多账户着陆区时的一些常见问题：

问题 1：如果遇到任何账户限制或业务限制，我能否从单个多账户着陆区开始，然后转移到多个多账户着陆区？

答：是的。您可以选择在任何给定时间设置另一个多账号着陆区：

- 需要设置新的账单付款人账户（目前 AWS 不支持单个 AWS 组织中的多付款人账户）。
- 填写多账户 landing zone 问卷后，多账户 Landing Zone 基础建设最多需要 2 周的交货时间。
- 每个多账户 landing zone 意味着每月增加约 3K 美元的运营成本。
- 新的 MALZ 需要集成 N/W、AD、DNS 和 SSO。
- 需要为新的多账户 landing zone 设置任何预留实例 (RIs)、成本节省计划（RIs 不可转让）。
- AMS 多账户着陆区不支持跨多账户着陆区账户迁移账户；例如，跨AWS Orgs。但是，使用标准迁移方法可以将应用程序从一个帐户转移到另一个帐户。

问题 2：AMS 对 MALZ updates/changes 的 underlying/shared 基础设施和量化客户风险的方法是什么？ 请详细说明流程中包含哪些保证。客户如何放心 MALZ updates/changes 不会影响客户？ 客户需要采取任何措施来防止中断吗？

答：AMS 采用严格的变更方法，使用内部工具，使我们能够定义、审查、安排和执行对客户环境的更改。

发布更新的过程强制执行代码审查、集成测试、在 gamma 和 beta 环境中部署，以及在 beta 和 gamma 环境中进行额外的烘焙时间和测试，然后再发布给客户环境。所有版本都包含回滚程序，并受到发布团队以及创建和请求变更的团队的密切监控。版本的范围仅限于 AMS 拥有和提供的堆栈。平均而言，我们每周至少执行一个版本。

此外：

- AMS 服务等级协议适用。根据AMS服务描述，在共享基础设施维护活动后提出的任何事件都将遵守相应的服务等级协议，以获得解决方案或积分。
- 客户无需采取特殊的预防措施来防止公共基础设施中断。客户对 AWS Org 或核心 OU 账户拥有只读权限，因此客户无法对 MALZ 核心环境进行任何破坏性更改。客户对核心基础设施的所有请求都需要 AMS 的审查和批准。
- SCPs/Roles 在应用程序 OU 级别传播更改之前，客户可以测试某些组织级别的更改，例如在个人非生产账户级别进行更改。AMS路线图上允许使用多个应用程序 OUs（2020年第二季度），这将进一步降低进行某些ORG级别更改的风险。MALZ 团队已经为 “构建模式” 账户发布了单独的 OU，以确保明确区分客户所有权和单独的控制措施。
- 其中大多数变更使AMS能够以有效和高效的方式操作工作负载，并且不一定会影响客户的工作量。如果 AMS 认为共享基础设施变更会对客户的工作负载产生影响，那么他们就会与客户的变更窗口保持一致。

高级建议，如果出现以下情况，则从多个多账户着陆区域开始：

- 它是否可以帮助您实现任何特定的合规性。
- 如果您需要使用多区域。
- 如果您的本地 ADs 和网络 Prod/Material 与非工作负载不同Prod/Non-Material workloads, to clearly segregate b/w。

多账号着陆区账号

主题

- 管理账户
- 社交账号
- 共享服务账户
- 日志存档账户
- 安全账户

- 应用程序账户类型
- AMS 工具账户（迁移工作负载）

管理账户

管理账户是您开始使用 AMS 时的初始 AWS 账户。它使用 AWS Organizations 作为管理账户（也称为支付所有成员账户费用的付款人账户），这使该账户能够创建成员账户并对其进行财务管理。它包含 AWS landing zone (ALZ) 框架、账户配置堆栈集、AWS 组织服务控制策略 (SCPs) 等。

有关使用管理账户的更多信息，请参阅管理账户的最佳实践。

下图简要概述了管理账户中包含的资源。

管理账户中的资源

除上述标准服务外，在入职期间不会在管理账户中创建额外的 AWS 资源。在加入 AMS 期间，需要输入以下内容：

- 管理账户 ID：最初由您创建的 AWS 账户 ID。
- 核心账户电子邮件：提供要与每个核心账户关联的电子邮件：网络、共享服务、日志和安全账户。
- 服务区域：提供您的 AMS landing zone 的所有资源都将部署到的 AWS 区域。

社交账号

Networking 账户充当 AMS 多账户 landing zone 账户、本地网络和传出 Internet 的出口流量之间进行网络路由的中心枢纽。此外，该账户还包含公共 DMZ 堡垒，这些堡垒是 AMS 工程师访问 AMS 环境中主机的入口点。有关详细信息，请参阅以下网络帐户的高级示意图。

网络账户架构

下图描绘了 AMS 多账户 landing zone 环境，显示了账户间的网络流量，并且是高可用性设置的示例。

AMS 根据我们的标准模板和您在入职期间提供的选择选项为您配置网络的各个方面。标准的 AWS 网络设计适用于您的 AWS 账户，然后为您创建一个 VPC，并通过 VPN 或 Direct Connect 连接到

AMS。有关 Direct Connect 的更多信息，请参阅 AWS Direct Connect。标准 VPCs 包括 DMZ、共享服务和应用程序子网。在入职过程中， VPCs 可能会要求并创建其他内容以满足您的需求（例如，客户部门、合作伙伴）。入门后，您将获得一张网络图：一份环境文档，说明您的网络是如何设置的。

> **Note**
>
> 有关所有活动服务的默认服务限制和限制的信息，请参阅 AWS 服务限制文档。

我们的网络设计围绕 Amazon 的 “最低权限原则” 构建。为了实现这一目标，除了来自可信网络的流量外，我们会通过 DMZ 路由所有流量（入口和出口）。唯一可信的网络是通过使用 VPN 和 AWS Direct Connect (DX) 在您的本地环境和 VP and/or C 之间配置的网络。通过使用堡垒实例授予访问权限，从而防止直接访问任何生产资源。您的所有应用程序和资源都位于可通过公共负载均衡器访问的私有子网中。公共出口流量通过出口 VPC（在网络账户中）中的 NAT 网关流向 Internet Gateway，然后流向互联网。或者，流量可以通过您的 VPN 或 Direct Connect 流向您的本地环境。

与 AMS 多账户 landing zone 环境的专用网络连接

AWS 通过虚拟专用网络 (VPN) 连接或使用 AWS Direct Connect 的专用线路提供私有连接。在您的多账户环境中，私有连接是使用下述方法之一设置的：

- 使用 Transit Gateway 实现集中边缘
- 将 Direct Connect (DX) and/or VPN 连接到账户虚拟私有云 () VPCs

使用公交网关实现集中边缘连接

AWS Transit Gateway 是一项服务，可让您 VPCs 和您的本地网络连接到单个网关。Transit Gateway (TGW) 可用于整合您现有的边缘连接并通过单个 ingress/egress 点进行路由。Transit 网关是在您的 AMS 多账户环境的网络账户中创建的。有关公交网关的更多详细信息，请参阅 AWS Transit Gateway。

AWS Direct Connect (DX) 网关用于通过中转虚拟接口将您的 DX 连接连接到 VPCs 或 VPNs 连接到您的传输网关。将 Direct Connect 网关与中转网关关联。然后，为您与 Direct Connect 网关的 AWS Direct Connect 连接创建一个传输虚拟接口。有关 DX 虚拟接口的信息，请参阅 AWS Direct Connect 虚拟接口。

此配置提供以下好处。您可以：

- 管理同一 AWS 区域中的多个 VPCs 或 VPNs 多个连接的单个连接。

- 将前缀从本地发布到 AWS，从 AWS 发布到本地。

> **Note**
>
> 有关在 AWS 服务中使用 DX 的信息，请参阅弹性工具包部分 Classic。有关更多信息，请参阅 T ransit Gateway 关联。

为了提高连接的弹性，我们建议您将来自不同的 AWS Direct Connect 位置的至少两个传输虚拟接口连接到 Direct Connect 网关。有关更多信息，请参阅 AWS Direct Connect 弹性建议。

将 DX 或 VPN 连接到账户 VPCs

使用此选项，您的 VPCs AMS 多账户着陆区环境将直接连接到 Direct Connect 或 VPN。流量直接从流向 Direct Connect 或 VPN，无需通过传输网关。 VPCs

社交账户中的资源

如网络账户图所示，以下组件是在该账户中创建的，需要您输入。

网络账户包含两个 VPCs：出口 VPC 和隔离区 VPC（也称为外围 VPC）。

AWS 网络管理器

AWS Network Manager 是一项服务，可让您可视化您的传输网关 (TGW) 网络，而无需向 AMS 支付额外费用。它提供对 AWS 资源和本地网络的集中式网络监控，在拓扑图和地理地图中提供其专用网络的单一全局视图，以及利用率指标，例如字节in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down连接状态。有关信息，请参阅AWS Network Manager。

使用以下角色之一访问此资源：

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

出口 VPC

出口 VPC 主要用于向 Internet 的出口流量，由位于最多三个可用区的 public/private 子网组成（ ）。AZs网络地址转换 (NAT) 网关在公有子网中配置，传输网关 (TGW) VPC 附件在私有子网中创

建。来自所有网络的出站或出站互联网流量通过 TGW 通过私有子网进入，然后通过 VPC 路由表路由到 NAT。

对于在公有子网中 VPCs 包含面向公众的应用程序的用户，源自 Internet 的流量包含在该 VPC 中。返回流量不会路由到 TGW 或出口 VPC，而是通过 VPC 中的互联网网关 (IGW) 路由回来。

> **Note**
>
> 网络 VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.16.0/24。这是您的 VPC 的主要 CIDR 块。
> AMS 多账户 landing zone 团队建议范围为 24（具有更多 IP 地址），以便在将来部署其他资源/设备时提供一些缓冲。

托管的帕洛阿尔托出口防火墙

AMS 提供托管 Palo Alto 出口防火墙解决方案，该解决方案支持对多账户着陆区环境中的所有网络（不包括面向公众的服务）中的所有网络进行互联网绑定出站流量过滤。该解决方案将业界领先的防火墙技术（Palo Alto VM-300）与AMS的基础设施管理功能相结合，可在合规的操作环境中部署、监控、管理、扩展和恢复基础架构。包括Palo Alto Networks在内的第三方无法访问防火墙；它们完全由AMS工程师管理。

交通管制

托管出站防火墙解决方案管理一个域允许列表，该列表由 AMS 必需的域组成，用于备份和补丁等服务，以及您定义的域。当出站 Internet 流量路由到防火墙时，将打开会话，评估流量，如果流量与允许的域相匹配，则将流量转发到目的地。

架构

托管出口防火墙解决方案遵循高可用性模式，即根据可用区域的数量部署两到三个防火墙（ ）。AZs该解决方案利用了默认出口 VPC 中的部分 IP 空间，但还预配置 VPC 扩展 (/24)，用于管理防火墙所需的额外资源。

网络流

总体而言，公共出口流量路由保持不变，但流量从出口 VPC 路由到 Internet 的方式除外：

1. 发往互联网的出口流量通过 VPC 路由表发送到 Transit Gateway (TGW)
2. TGW 通过 TGW 路由表将流量路由到出口 VPC
3. VPC 通过私有子网路由表将流量路由到互联网
   a. 在默认的多账户着陆区环境中，互联网流量直接发送到网络地址转换 (NAT) 网关。托管防火墙解决方案重新配置私有子网路由表，改为将默认路由 (0.0.0.0/0) 指向防火墙接口。

防火墙本身包含三个接口：

1. 可信接口：用于接收待处理的流量的私有接口。
2. 不可信接口：用于向互联网发送流量的公共接口。由于防火墙执行 NAT，因此外部服务器接受来自这些公有 IP 地址的请求。
3. 管理接口：用于防火墙 API、更新、控制台等的私有接口。

在所有路由中，流量都保持在同一个可用区 (AZ) 内，以减少跨可用区的流量。只有在发生故障转移 AZs 时，流量才会交叉。

修改允许名单

入职后，将创建一个名为的默认允许列表，其中包含 AMS 所需的公共端点以及用于修补 Windows 和 Lin `ams-allowlist` ux 主机的公共端点。操作完成后，您可以在 AMS 控制台的 “管理 | 托管防火墙 | 出站（Palo Alto）” 类别下创建 RFC，以创建或删除允许列表或修改域。请注意，这是`ams-allowlist`无法修改的。RFC 是完全自动化处理的（它们不是手动的）。

自定义安全策略

安全策略根据流量属性（例如源和目标安全区域、源和目标 IP 地址以及服务）来确定是阻止还是允许会话。全自动支持自定义安全策略 RFCs。 CTs 创建或删除安全策略可以在管理 | 托管防火墙 | 出站（帕洛阿尔托）类别下找到，编辑现有安全策略的 CT 可以在部署 | 托管防火墙 | 出站（帕洛阿尔托）类别下找到。您将能够创建新的安全策略、修改安全策略或删除安全策略。

> **Note**
>
> `ams-allowlist`无法修改默认安全策略

CloudWatch PA 出口仪表板

在中可以找到两个仪表板 CloudWatch 来提供帕洛阿尔托（宾夕法尼亚州）的汇总视图。AMS-MF-PA-egress-config-Das hboard 提供了 PA 配置概述、许可名单链接以及包括其属性在内的所有安全策略的列表。可以自定义 AMS-MF-PA-egress-Dashboard 以过滤流量日志。例如，要为安全策略创建控制面板，您可以使用以下筛选器创建 RFC：

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
 as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
 @dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,
 @x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,
 @source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,
 @bytes_sent, @bytes_recieved, @packets, @x36, @x37, @category, @x39, @x40, @x41,
 @source_country, @destination_country, @x44, @packets_sent, @packets_recieved,
 @session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
 @destination_ip, @source_port, @destination_port, @session_id, @from_zone,
 @to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
 @source_country, @destination_country
```

故障转移模型

防火墙解决方案包括两三台帕洛阿尔托 (PA) 主机（每个可用区一台）。健康检查加那利群岛按固定时间表运行，以评估宿主的健康状况。如果主机被识别为运行状况不佳，则会通知 AMS，并通过更改路由表将该 AZ 的流量自动转移到另一可用区中的健康主机。由于运行状况检查工作流程持续运行，因此如果主机由于暂时性问题或手动修复而恢复正常，则流量将转移回主机的正确可用区。

扩展

AMS 监控防火墙的吞吐量和扩展限制。当吞吐量限制超过较低的水位线阈值（CPU/网络）时，AMS 会收到警报。低水机阈值表示资源已接近饱和，达到了 AMS 将随着时间的推移评估指标并伸出援手提出扩展解决方案的地步。

备份与还原

备份是在初始启动期间、任何配置更改后按固定时间间隔创建的。初始启动备份是以每台主机为单位创建的，但是调用备份工作流程时，将在所有防火墙主机上进行配置更改和定期间隔备份。AMS 工程师可以在这些窗口之外创建其他备份，或者根据要求提供备份详细信息。

如果需要，AMS 工程师可以恢复配置备份。如果需要恢复，则将在所有主机上进行恢复，以使主机之间的配置保持同步。

当主机需要完全回收实例时，也可以进行恢复。配置新 EC2 实例时，会自动恢复最新的备份。通常，主机不会定期回收，而是预留用于严重故障或必需的 AMI 交换。主机回收是手动启动的，并且在进行回收之前会通知您。

除了防火墙配置备份外，您的特定允许列表规则会单独备份。修改您定义的允许列表规则后，系统会自动创建备份。如果需要，可以由 AMS 工程师恢复允许名单备份。

更新

AMS 托管防火墙解决方案需要随着时间的推移进行各种更新，以增加系统的改进、其他功能或对防火墙操作系统 (OS) 或软件的更新。

大多数更改不会影响运行环境，例如更新自动化基础架构，但其他更改（例如防火墙实例轮换或操作系统更新）可能会导致中断。在评估更新可能导致的服务中断时，AMS 将与您协调以适应维护时段。

操作员访问权限

AMS 操作员使用其 ActiveDirectory 凭据登录帕洛阿尔托设备执行操作（例如，修补、响应事件等）。该解决方案保留了标准的 AMS 操作员身份验证和配置更改日志，以跟踪在 Palo Alto 主机上执行的操作。

默认日志

默认情况下，防火墙生成的日志存储在每个防火墙的本地存储中。随着时间的推移，将根据存储利用率删除本地日志。AMS 解决方案可将日志从计算机实时传送到 CloudWatch 日志；有关更多信息，请参阅CloudWatch 日志集成。

如果需要，AMS 工程师仍然可以直接从计算机上查询和导出日志。此外，还可以将日志发送到客户拥有的 Panorama；有关更多信息，请参阅Panorama 集成。

该解决方案收集的日志如下：

RFC 状态码

日志类型	说明
流量	显示每个会话开始和结束的条目。每个条目都包括日期和时间、源和目标区域、地址和端口、应用程序名称、应用于流的安全规则名称、规则操作（允许、拒绝或丢弃）、入口和出口接口、字节数以及会话结束原因。

日志类型	说明
	“类型” 列指示该条目是针对会话的开始还是结束，或者会话是被拒绝还是被删除。“丢弃” 表示阻止流量的安全规则指定了 “任何” 应用程序，而 “拒绝” 表示该规则标识了特定的应用程序。 如果在识别应用程序之前丢弃了流量，例如规则丢弃了特定服务的所有流量，则该应用程序将显示为 “不适用”。
威胁	显示防火墙生成的每个安全警报的条目。每个条目都包括日期和时间、威胁名称或 URL、源和目标区域、地址和端口、应用程序名称以及警报操作（允许或阻止）和严重性。 类型列表示威胁的类型，例如 “病毒” 或 “间谍软件”；“名称” 列是威胁描述或 URL；“类别” 列是威胁类别（例如 “键盘记录器”）或 URL 类别。
网址过滤	显示 URL 过滤器的日志，这些过滤器控制对网站的访问以及用户是否可以向网站提交凭据。
配置	显示每项配置更改的条目。每个条目都包括日期和时间、管理员用户名、进行更改的 IP 地址、客户机类型（Web 界面或 CLI）、命令运行的类型、命令成功还是失败、配置路径以及更改前后的值。
系统	显示每个系统事件的条目。每个条目都包括日期和时间、事件严重性以及事件描述。
警报	警报日志记录有关系统生成的警报的详细信息。此日志中的信息也会在警报中报告。请参阅 “定义警报设置”。
身份验证	显示有关最终用户尝试访问由身份验证策略规则控制访问权限的网络资源时发生的身份验证事件的信息。用户可以使用这些信息来帮助解决访问问题，并根据需要调整用户身份验证策略。结合关联对象，用户还可以使用身份验证日志来识别用户网络上的可疑活动，例如暴力攻击。 或者，用户可以将身份验证规则配置为记录身份验证超时。这些超时与用户只需要对资源进行一次身份验证但可以重复访问该资源的时间段有关。查看有关超时的信息可以帮助用户决定是否以及如何调整超时。

日志类型	说明
统一	在单个视图中显示最新的流量、威胁、URL 过滤、 WildFire 提交和数据筛选日志条目。集体日志视图使用户能够一起调查和筛选这些不同类型的日志（而不是单独搜索每个日志集）。或者，用户可以选择要显示的日志类型：单击筛选字段左侧的箭头，然后选择流量、威胁、网址、数据、w and/or ildfire，以仅显示选定的日志类型。

活动管理

AMS 持续监控防火墙的容量、运行状况和可用性。防火墙生成的指标以及 AWS/AMS 生成的指标用于创建警报，AMS 运营工程师将收到这些警报，他们将调查并解决问题。当前警报涵盖以下情况：

事件警报：

- 防火墙数据平面 CPU 利用率
  - CPU 利用率-数据平面 CPU（处理流量）
- 防火墙数据平面数据包利用率高于 80%
  - 数据包利用率-数据平面（处理流量）
- 防火墙数据平面会话利用率
- 防火墙数据平面会话处于活动状态
- 聚合防火墙 CPU 利用率
  - 所有的 CPU 利用率 CPUs
- 按可用区进行故障转移
  - 可用区发生故障转移时发出警报
- 不健康的 Syslog 主机
  - Syslog 主机未通过运行状况检查

管理警报：

- Health Check 监控器故障警报
  - 当运行状况检查工作流程意外失败时
  - 这适用于工作流程本身，而不是防火墙运行状况检查失败的情况
- 密码轮换失败警报

- 当密码轮换失败时
- API/服务用户密码每 90 天轮换一次

指标

所有指标都被捕获并存储 CloudWatch 在网络账户中。可以通过获得网络帐户的控制台访问权限并导航到控制 CloudWatch 台来查看这些内容。可以在指标选项卡下查看单个指标，也可以通过导航到 “控制面板” 选项卡并选择 AMS-MF-PA-egress-Dashboard 来查看所选指标的单窗格仪表板视图和汇总指标。

自定义指标：

- 运行状况检查
  - 命名空间: AMS/MF/PA/Egress
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- 已生成防火墙
  - 命名空间：AMS/MF/PA/Egress/<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - 平底锅 GPGateway UtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch 日志集成

CloudWatch 日志集成可将日志从防火墙转发到 CloudWatch 日志中，从而降低由于本地存储利用率而丢失日志的风险。日志会在防火墙生成时实时填充，并且可以通过控制台或 API 按需查看。

可以为日志分析构建复杂查询，也可以使用 CloudWatch Insights 导出到 CSV。此外，自定义 AMS Managed Firewall CloudWatch 控制面板还将显示特定流量日志查询的快速视图以及一段时间内流量和策略命中率的图表可视化。利用 CloudWatch 日志还可以实现与其他 AWS 服务（例如 AWS Kinesis）的本机集成。

> **Note**
>
> PA 日志无法直接转发到现有的本地或第三方 Syslog 收集器。AMS 托管防火墙解决方案可将日志从 PA 计算机实时传输到 AWS CloudWatch 日志。您可以使用 CloudWatch Logs Insight 功能来运行临时查询。此外，日志可以发送到您的帕洛阿尔托的Panorama管理解决方案。CloudWatch 也可以使用 CloudWatch 订阅过滤器将日志转发到其他目的地。在下一节中了解有关 Panorama 的更多信息。要了解有关 Splunk 的更多信息，请参阅与 Splunk 集成。

Panorama 集成

AMS 托管防火墙可以选择与您现有的 Panorama 集成。这使您可以从 Panorama 查看防火墙配置或将日志从防火墙转发到 Panorama。Panorama 与 AMS 托管防火墙的集成是只读的，不允许从 Panorama 更改防火墙的配置。Panorama 完全由您管理和配置，AMS 仅负责配置与其通信的防火墙。

许可

AMS 托管防火墙的价格取决于所使用的许可证类型、每小时许可证或自带许可证 (BYOL)，以及设备运行的实例大小。您需要通过 AWS Marketplace 订购您喜欢的帕洛阿尔托防火墙的实例大小和许可证。

- Marketplace 许可：接受 MALZ 网络账户中虚拟机系列下一代防火墙捆绑包 1 的条款和条件。
- BYOL 许可证：接受 MALZ 网络账户中虚拟机系列下一代防火墙 (BYOL) 的条款和条件，并将购买许可证后获得的 “BYOL 身份验证码” 共享给 AMS。

限制

目前，AMS 支持 VM-300 系列或 VM-500 系列防火墙。可以在此处找到配置：AWS EC2 实例上的 VM 系列模型，

> **Note**
>
> AMS 解决方案在 Active-Active 模式下运行，因为其可用区中的每个 PA 实例都会处理其相应可用区的出口流量。因此，如果有两个 PA 实例 AZs，则每个 PA 实例可处理高达 5 Gbps 的出口流量，并有效地在两个实例之间提供 10 Gbps 的总吞吐量。 AZs每个可用区中的所有限制也是如此。如果 AMS 运行状况检查失败，我们会将流量从 PA 不佳的可用区转移到另一个可用区，在实例替换期间，容量将减少到剩余 AZs 限制。

AMS 目前不支持 AWS Marketplace 上提供的其他 Palo Alto 捆绑包；例如，您不能索取 “VM 系列下一代防火墙捆绑包 2”。请注意，使用 Palo Alto 的 AMS 托管防火墙解决方案目前仅提供出口流量过滤服务，因此使用高级 VM 系列捆绑包不会提供任何其他功能或优势。

入职要求

- 您必须在 AWS Marketplace 中查看并接受帕洛阿尔托推出的虚拟机系列下一代防火墙的条款和条件。
- 您必须根据您的预期工作负载确认要使用的实例大小。
- 您必须提供与多账户着陆区环境或本地网络不冲突的 /24 CIDR 区块。它必须与出口 VPC 属于同一类别（解决方案为出口 VPC 预配置 /24 VPC 扩展）。

定价

AMS 托管防火墙基础架构成本分为三个主要驱动因素：托管 Palo Alto 防火墙的 EC2 实例、软件许可证 Palo Alto VM 系列许可证和集成。 CloudWatch

以下定价基于 VM-300 系列防火墙。

- EC2 实例：Palo Alto 防火墙在 2-3 个 EC2 实例的高可用性模型中运行，其中实例基于预期的工作负载。实例的成本取决于地区和数量 AZs
  - 例如 us-east-1、m5.xlarge、3 AZs
    - 0.192 * 24 * 30 * 3 = 414.72 美元
  - https://aws.amazon.com/ec2/定价/按需定价/
- 帕洛阿尔托许可证：Palo Alto VM-300 下一代防火墙的软件许可成本取决于可用区的数量和实例类型。
  - 例如 us-east-1、m5.xlarge、3 AZs
    - 0.87 * 24 * 30 * 3 = 1879.20 美元
    - https://aws.amazon.com/marketplace/pp/b083m7jpkb？ ref_=srh_res_product_title #pdp-pricing
- CloudWatch 日志集成： CloudWatch 日志集成使用 SysLog 服务器 (EC2 -t3.medium)、NLB 和日志。 CloudWatch 服务器的成本取决于区域和数量 AZs， NLB/CloudWatch 日志的成本因流量利用率而异。
  - 例如 us-east-1、t3.medium、3AZ

  - 0.0416 * 24 * 30 * 3 = 89.86 美元
- https://aws.amazon.com/ec2/定价/按需定价/
- https://aws.amazon.com/cloudwatch/定价/

周长 (DMZ) VPC

外围或 DMZ、VPC 包含 AMS 运营工程师访问 AMS 网络所需的必要资源。它包含跨越 2-3 个的公共子网 AZs，在 Auto Scaling 组 (ASG) 中包含 SSH 堡垒主机，AMS 运营工程师可以登录或通过隧道通过。附加到隔离区堡垒的安全组包含来自亚马逊公司网络的端口 22 入站规则。

DMZ VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.16.0/24。这是您的 VPC 的主要 CIDR 块。

> **Note**
>
> AMS 团队建议将范围设为 24（具有更多 IP 地址），以便在将来部署其他资源（例如防火墙）时提供一些缓冲。

AWS Transit Gateway

AWS Transit Gateway (TGW) 是一项服务，可让您将亚马逊虚拟私有云 (VPCs) 和本地网络连接到单个网关。传输网关是处理 AMS 账户网络和外部网络之间路由的网络主干。 有关 Transit Gateway 的信息，请参阅 AWS Transit Gateway。

提供以下输入以创建此资源：

- Transit Gateway ASN 编号 *：为您的公交网关提供私有自治系统编号 (ASN)。这应该是边界网关协议 (BGP) 会话的 AWS 端的 ASN。16 位的范围为 64512 到 65534。 ASNs

共享服务账户

共享服务账户是大多数 AMS 数据平面服务的中心枢纽。该账户包含访问管理 (AD)、端点安全管理 (趋势科技) 所需的基础架构和资源，还包含客户堡垒 (SSH/RDP)。 下图显示了共享服务帐户中包含的资源的高级概述。

共享服务 VPC 由三个可用区中的 AD 子网、EPS 子网和客户堡垒子网组成（AZs）。下面列出了在共享服务 VPC 中创建的资源，需要您输入。

- 共享服务 VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.1.0/24。这是您的 VPC 的主要 CIDR 块。

  > **Note**
  >
  > AMS 团队建议的射程为 /23。

- A@@ ctive Directory 详情：Microsoft Active Directory (AD) 用于 user/resource 管理、身份验证/授权和所有 AMS 多账户登录区域账户的 DNS。AMS AD 还配置了对您的 Active Directory 的单向信任，以进行基于信任的身份验证。 创建 AD 需要以下输入：
  - 域名完全限定域名 (FQDN)：AWS 托管的 Microsoft AD 目录的完全限定域名。该域不应是现有域或网络中现有域的子域。
  - 域 NetBIOS 名称：如果您未指定 NetBIOS 名称，AMS 会将该名称默认为您的目录 DNS 的第一部分。例如，corp 代表目录 DNS corp.example.com。

- 趋势科技-端点保护安全 (EPS)：趋势科技端点保护 (EPS) 是 AMS 中用于操作系统安全的主要组件。该系统由趋势科技服务器深度安全防护系统管理中心 (DSM)、 EC2 EC2 实例、中继实例以及存在于所有数据平面和客户 EC2 实例中的代理组成。

  您必须使用共享服务帐户，并订阅趋势科技服务器深度安全防护系统 (BYOL) AMI 或趋势科技趋势科技服务器深度安全防护系统 (Marketplace)。`EPSMarketplaceSubscriptionRole`

  创建 EPS 需要以下默认输入（如果您想更改默认值）：
  - 中继实例类型：默认值-m5.large
  - DSM 实例类型：默认值-m5.xlarge
  - 数据库实例大小：默认值-200 GB
  - RDS 实例类型：默认值——db.m5.large

- 客户堡垒：共享服务账户中为您提供 SSH 或 RDP 堡垒（或两者兼而有之），用于访问您的 AMS 环境中的其他主机。为了以用户身份访问 AMS 网络（SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN 到传输网关 (TGW)，然后路由到共享服务 VPC。一旦您能够访问堡垒，就可以跳转到 AMS 环境中的其他主机，前提是访问请求已获得批准。
  - SSH 堡垒需要以下输入。
    - SSH 堡垒所需实例容量：默认值-2。

- SSH 堡垒最大实例数：默认值-4。
- SSH 堡垒最低实例数：默认值 -2。
- SSH 堡垒实例类型：默认值-m5.large（可以更改以节省成本；例如 t3.medium）。
- SSH 堡垒入口 CIDRs：您网络中的用户从中访问 SSH 堡垒的 IP 地址范围。

- Windows RDP 堡垒需要以下输入。
  - RDP 堡垒实例类型：默认值-t3.medium。
  - RDP Bastion 所需的最小会话数：默认值-2。
  - RDP 最大会话数：默认值 -10。
  - RDP 堡垒配置类型：您可以选择以下配置之一
    - SecureStandard = 一个用户收到一个堡垒，只有一个用户可以连接到堡垒。
    - SecureHA = 用户在两个不同的可用区收到两个堡垒可供连接，并且只有一个用户可以连接到堡垒。
    - SharedStandard = 一个用户收到一个要连接的堡垒，两个用户可以同时连接到同一个堡垒。
    - SharedHA = 用户在两个不同的 AZ 中收到两个堡垒可供连接，两个用户可以同时连接到同一个堡垒。
  - 客户 RDP 入口 CIDRs：您网络中的用户将从中访问 RDP 堡垒的 IP 地址范围。

共享服务更新：多账户登录区

AMS 每月向托管账户发布数据平面版本，恕不另行通知。

AMS 使用核心 OU 在您的多账户着陆区提供共享服务，例如访问、联网、EPS、日志存储、警报聚合。AMS 负责解决这些共享服务的漏洞、修补和部署。AMS 会定期更新用于提供这些共享服务的资源，以便用户可以访问最新功能和安全更新。更新通常每月进行一次。这些更新中包含的资源有：

- 属于核心 OU 的账户。

  管理账户、共享服务账户、网络账户、安全账户和日志存档账户拥有用于 RDP 和 SSH 堡垒、代理、管理主机和端点安全 (EPS) 的资源，这些资源通常每月更新一次。AMS 使用不可变 EC2 部署作为共享服务基础设施的一部分。
- AMIs 包含最新更新的新 AMS。

> **Note**
>
> AMS 操作员在执行数据平面更改时使用内部警报抑制更改类型 (CT)，并且该 CT 的 RFC 会显示在您的 RFC 列表中。这是因为，在部署数据平面版本时，各种基础架构可能会关闭、重新启动、离线，或者部署可能会出现 CPU 峰值或其他影响，从而触发在数据平面部署期间无关的警报。部署完成后，将验证所有基础设施是否正常运行，并重新启用警报。

日志存档账户

日志存档账户是在 AMS 多账户 landing zone 环境中存档日志的中心中心。账户中有一个 S3 存储桶，其中包含每个 AMS 多账户着陆区环境账户的 AWS CloudTrail 和 AWS Config 日志文件的副本。您可以将此账户用于与 AWS Firehose 或 Splunk 等相关的集中式日志解决方案。AMS 仅限少数用户访问此账户；仅限审计师和安全团队进行与账户活动相关的合规和取证调查。

安全账户

安全账户是住房保障相关操作的中心枢纽，也是向AMS控制飞机服务发送通知和警报的主要点。此外，安全账户还存放了 Amazon Guard Duty 管理账户和 AWS Config 聚合器。

应用程序账户类型

应用程序账户是您用来托管工作负载的 AMS 管理的 landing zone 架构中的 AWS 账户。AMS 提供三种类型的应用程序账户：

- AMS 管理的应用程序账户
- AMS 加速账户
- 客户托管应用程序账户

根据应用程序账户类型，AWS Organizations OUs 中的应用程序账户按不同的分组方式：

- root OU：
  1. 应用程序 OU
     - 托管 OU：AMS 管理的账户
     - 开发 OU：启用开发者模式的 AMS 管理的账户
  2. 加速 OU：AMS 加速应用程序账户

3. 客户管理的 OU：客户管理的应用程序帐户

应用程序账户通过管理账户提交的 RFC 进行配置：

- 使用 VPC 创建应用程序账户 ct-1zdas mc2ewzrs
- 创建加速账户 ct-2p93tyd5angmi
- 创建客户管理的应用程序账户 ct-3pwbixz27n3tn

AMS 管理的应用程序账户

完全由 AMS 管理的应用程序帐户称为 AMS 管理的应用程序帐户，其中部分或全部操作任务，例如服务请求管理、事件管理、安全管理、连续性管理（备份）、补丁管理、成本优化或基础设施的监控和事件管理，由 AMS 执行。

AMS 执行的任务数量取决于您选择的变更管理模式。AMS 管理的账户支持不同的变更管理模式：

- RFC 模式
- AMS 中的直接更改模式
- AMS 和 AWS Service Catalog
- AMS 高级开发者模式
- AMS 中的自助服务配置模式

有关变更管理和不同模式的更多信息，请参阅更改管理模式。

有些 AWS 服务可以在您的 AMS 托管账户中使用，而无需管理 AMS。自助服务配置部分介绍了这些 AWS 服务的列表以及如何将其添加到您的 AMS 账户。

AMS 加速账户

AMS Accelerate 是 AMS 运营计划，可以运行支持工作负载的 AWS 基础设施。您可以从 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 AWS 的使用方式。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。您将使用首选的访问和变更机制，而 AMS 将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。

> **Note**
>
> AMS Advanced 中的 AMS Accelerate 账户没有 AMS 变更管理 (RFCs) 或 AMS 高级控制台。相反，他们有 AMS Accelerate 控制台和功能。

加速账户只能通过您的 AMS 多账户 landing zone 管理账户进行配置。加速提供不同的运营能力。要了解更多信息，请参阅加速服务说明。

- 您将继续享受多账户着陆区 (MALZ) 核心账户的某些功能，例如集中记录、单一账单、安全账户中的 Config Aggregator 和。 SCPs
- AMS Accelerate 不提供某些 AMS 高级服务，例如 EPS、访问管理、变更管理和配置。我们建议您按照以下步骤获取访问权限并配置传输网关 (TGW)。

有关加速的更多详细信息，请参阅什么是加速。

创建您的加速账户

要创建加速账户，请按照此处列出的步骤创建加速账户。

访问您的加速账户

在您的多账户 landing zone (MALZ) 账户中配置 Accelerate 账户后`AccelerateDefaultAdminRole`，账户中将有一个具有管理访问权限的角色供您代入。

要访问新的加速账户，请执行以下操作：

1. 使用该角色登录管理账户的 IAM 控制台。`CustomerDefaultAssumeRole`
2. 在 IAM 控制台的导航栏上，选择您的用户名。
3. 选择切换角色。如果这是您首次选择该选项，则会显示一个包含更多信息的页面。在阅读该信息后，请选择切换角色。如果清除您的浏览器 Cookie，则此页面会重新再出现。
4. 在“切换角色”页面上，键入加速账户 ID 和要代入的角色名称：`AccelerateDefaultAdminRole`。

现在您可以访问了，可以创建新的 IAM 角色来继续访问您的环境。如果您想将 SAML 联合身份验证用于您的加速账户，请参阅启用 SAML 2.0 联合用户访问 AWS 管理控制台。

将你的加速账户与 Transit Gateway 关联起来

AMS 不管理加速账户的网络设置。您可以选择使用 AWS APIs（参见网络解决方案）管理自己的网络，也可以使用 AMS MALZ 中部署的现有 Transit Gateway (TGW) 连接到由 AMS 管理的 MALZ 网络。

> **Note**
>
> 只有当加速账户位于同一 AWS 区域时，您才能将 VPC 关联到 TGW。有关更多信息，请参阅公交网关。

要将你的 Accelerate 账户添加到 Transit Gateway，请使用部署 | 托管着陆区 | 网络账户 | 添加静态路线 (ct-3r2ckznmt0a59) 更改类型申请新路线，包括以下信息：

- Blackhol e：True 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 false。
- DestinationCidrBlock：用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：10.0.2.0/24。
- TransitGatewayAttachmentId：将用作路由表目标的 TGW 附件 ID。如果 Blackhol e 为假，则此参数为必填项，否则将此参数留空。示例：tgw-attach-04eb40d1e14ec7272。
- TransitGatewayRouteTableId: TGW 路由表的 ID。示例：tgw-rtb-06ddc751c0c881c。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的 MALZ 网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望这个 Accerate VPC 与什么通信。
3. 提交部署 | 托管着陆区 | 网络账户 | 添加静态路由 (ct-3r2ckznmt0a59) 更改类型，包括以下信息：
   - Blackhol e：True 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 false。
   - DestinationCidrBlock：用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：10.0.2.0/24。
   - TransitGatewayAttachmentId：将用作路由表目标的 TGW 附件 ID。如果 Blackhol e 为假，则此参数为必填项，否则将此参数留空。示例：tgw-attach-04eb40d1e14ec7272。
   - TransitGatewayRouteTableId: TGW 路由表的 ID。示例：tgw-rtb-06ddc751c0c881c。

将新的加速账户 VPC 连接到 AMS 多账户着陆区网络（创建 TGW VPC 附件）：

1. 在您的多账户 landing zone 网络账户中，打开 Amazon VPC 控制台。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。记录您看到的公交网关的 TGW ID。
3. 在您的加速账户中，打开亚马逊 VPC 控制台。
4. 在导航窗格中，选择 T ransit Gateway 附件 > 创建 Transit Gateway 附件。做出以下选择：
   - 对于 T ransit Gatew ay ID，请选择您在步骤 2 中记录的公交网关 ID。
   - 对于 Attachment type (连接类型)，选择 VPC。
   - 在 VPC Attachment (VPC 挂载) 下，（可选）为 Attachment name tag (挂载名称标签) 键入名称。
   - 选择是否启用 DNS Support and S u IPv6 ppor t。
   - 对于 VPC ID，选择要附加到中转网关的 VPC。此 VPC 必须至少有一个子网与其关联。
   - 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。
5. 选择 Create attachment (创建挂载)。记录新创建的 TGW 附件的 ID。

将 TGW 附件关联到路由表：

1. 决定您要将 VPC 与哪个 TGW 路由表关联。我们建议 VPCs 使用部署 | 托管着陆区 | 网络账户 | 创建公交网关路由表 (ct-3dscwaeyi6cup) 更改类型为 Accelerate 账户创建新的应用程序路由表。
2. 在网络账户上提交管理 | 托管着陆区 | 网络账户 | 关联 TGW 附件 (ct-3nmhh0qr338q6) RFC，将 VPC 或 TGW 附件关联到你选择的路由表。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的多账户 landing zone 网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望这个 Accerate 账户 VPC 与什么通信。
3. 提交部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由 (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

将您的 VPC 路由表配置为指向 AMS 多账户 landing zone 公交网关：

1. 与您的解决方案架构师一起决定要向 AMS 多账户着陆区公交网关发送哪些流量。

2. 提交部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由 (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

客户托管应用程序账户

您可以创建 AMS 无法以标准方式管理的账户。这些账户被称为客户管理账户，它们使您可以完全控制账户内的基础设施，同时享受由 AMS 管理的集中式架构的好处。

客户托管账户无权访问 AMS 控制台或我们提供的任何服务（补丁、备份等）。

客户管理账户只能通过您的 AMS 多账户 landing zone 管理账户进行配置。

不同的 AMS 模式对应用程序账户的使用方式不同；要了解有关这些模式的更多信息，请参阅 AWS Managed Services 模式。

要创建您的客户托管应用程序帐户，请参阅管理账户 | 创建客户管理的应用程序帐户。

要删除客户管理的应用程序帐户，请使用管理帐户 | Offboard 应用程序帐户。（确认离职 CT 不适用于客户管理的应用程序账户。）

访问您的客户管理账户

在多账户 landing zone 中配置客户管理账户 (CMA) 后，账户中将有一个管理员角色 (MALZ)`CustomerDefaultAdminRole`，供您通过 SAML 联合代入来配置账户。

要访问 CMA，请执行以下操作：

1. 使用该角色登录管理账户的 IAM 控制台。CustomerDefaultAssumeRole
2. 在 IAM 控制台的导航栏上，选择您的用户名。
3. 选择切换角色。如果这是您首次选择该选项，则会显示一个包含更多信息的页面。在阅读该信息后，请选择切换角色。如果清除您的浏览器 Cookie，则此页面会重新再出现。
4. 在“切换角色”页面上，键入客户管理的账户 ID 和要担任的角色的名称：CustomerDefaultAdminRole。

现在您可以访问了，可以创建新的 IAM 角色来继续访问您的环境。如果您想将 SAML 联合身份验证用于您的 CMA 账户，请参阅启用 SAML 2.0 联合用户访问 AWS 管理控制台。

将 CMA 与 Transit Gateway 连接起来

AMS 不管理客户管理账户 (CMAs) 的网络设置。您可以选择使用 AWS APIs （参见联网解决方案）管理自己的网络，也可以使用 AMS MALZ 中部署的现有 Transit Gateway (TGW) 连接到由 AMS 管理的多账户着陆区网络。

> **Note**
>
> 只有当 CMA 位于同一 AWS 区域时，您才能将 VPC 连接到 TGW。有关更多信息，请参阅公交网关。

要将你的 CMA 添加到 Transit Gateway，请使用网络账户申请一条新路线 | 添加静态路由 (ct-3r2ckznm t0a59) 更改类型并包含以下信息：

- Blackhol e：True 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 false。
- DestinationCidrBlock：用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：`10.0.2.0/24`。
- TransitGatewayAttachmentId：将用作路由表目标的 TGW 附件 ID。如果 Blackhol e 为假，则此参数为必填项，否则将此参数留空。示例：`tgw-attach-04eb40d1e14ec7272`。
- TransitGatewayRouteTableId: TGW 路由表的 ID。示例：`tgw-rtb-06ddc751c0c0c881c`。

将新的客户管理的 VPC 连接到 AMS 多账户着陆区域网络（创建 TGW VPC 附件）：

1. 在您的多账户 landing zone 网络账户中，打开 Amazon VPC 控制台。
2. 在导航窗格中，选择传输网关。记录您看到的公交网关的 TGW ID。
3. 在您的客户管理账户中，打开 Amazon VPC 控制台。
4. 在导航窗格中，选择 T ransit Gateway 附件 > 创建 Transit Gateway 附件。做出以下选择：
    a. 对于 T ransit Gatew ay ID，请选择您在步骤 2 中记录的公交网关 ID。
    b. 对于 Attachment type (连接类型)，选择 VPC。
    c. 在 VPC Attachment (VPC 挂载) 下，（可选）为 Attachment name tag (挂载名称标签) 键入名称。
    d. 选择是否启用 DNS Support and S u IPv6 ppor t。
    e. 对于 VPC ID，选择要附加到中转网关的 VPC。此 VPC 必须至少有一个子网与其关联。

f. 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。

5. 选择 Create attachment (创建挂载)。记录新创建的 TGW 附件的 ID。

将 TGW 附件关联到路由表：

决定您要将 VPC 与哪个 TGW 路由表关联。我们建议提交部署 | 托管 VPCs 着陆区 | 网络账户 | 创建公交网关路由表 (ct-3dscwaeyi6cup) RFC，为客户管理创建新的应用程序路由表。要将 VPC 或 TGW 附件关联到您选择的路由表，请在网络账户上提交部署 | 托管着陆区 | 网络账户 | 关联 TGW 附件 (ct-3nmhh0qr338q6) RFC。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的多账户着陆区网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望此客户托管的 VPC 与什么通信。提交部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由 (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

> **Note**
>
> 此 CT（ct-3r2ckznmt0a59）不允许向核心路由表添加静态路由 EgressRouteDomain；如果你的 CMA 需要允许出口流量，请使用 ct-0xdawir96cy7k 提交管理 | 其他 | 其他 (MOO) RFC。

将您的 VPC 路由表配置为指向 AMS 多账户着陆区中转网关：

与您的解决方案架构师一起决定要向 AMS 多账户着陆区公交网关发送哪些流量。更新您的 VPC 路由表以将流量发送到之前创建的 TGW 附件

获取有关客户管理账户的运营帮助

AMS 可以通过将客户托管账户注册到 AMS Accelerate 来帮助您操作在客户管理账户中部署的工作负载。借助 AMS Accelerate，您可以从监控和警报、事件管理、安全管理和备份管理等运营服务中受益，而无需进行新的迁移、停机或更改使用 AWS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。使用 AMS Accelerate，您可以继续以本地方式或首选工具使用、配置和部署所有 AWS 服务；就像使用 AMS 高级客户管理账户一样。您使用首选的访问和变更机制，而 AMS 则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。要了解更多信息，请参阅加速服务说明。

要将您的客户管理账户注册到 Accelerate，请联系您的 CSDM 并按照 AMS Accelerate 入门中的步骤进行操作。

> **Note**
>
> AMS Advanced 中的 AMS Accelerate 账户没有 AMS 变更管理（变更请求或 RFCs）或 AMS 高级控制台。相反，他们有 AMS Accelerate 控制台和功能。

AMS 工具账户（迁移工作负载）

您的多账户着陆区工具账户（使用 VPC）有助于加快迁移工作，提高您的安全地位，降低成本和复杂性，并标准化您的使用模式。

工具账户提供以下内容：

- 为系统集成商在生产工作负载之外访问复制实例提供了明确的边界。
- 允许您创建一个隔离的密室，以检查工作负载中是否存在恶意软件或未知的网络路由，然后再将其存入具有其他工作负载的帐户。
- 作为定义的帐户设置，它可以更快地为工作负载迁移做好准备和准备。
- 隔离的网络路由到来自本地-> 工具账户- CloudEndure > AMS 摄取的图像的安全流量。提取图像后，您可以通过 AMS 管理 | 高级堆栈组件 | AMI | 共享 (ct-1eiczxw8ihc18) RFC 将图像共享到目标账户。

高级架构图：

使用部署 | 托管着陆区 | 管理账户 | 创建工具账户（使用 VPC）更改类型 (ct-2j7q1hgf26x5c)，在多账户着陆区环境中快速部署工具账户并实例化工作负载摄取流程。参见管理账户，工具账户：创建（使用 VPC）。

> **Note**
>
> 我们建议有两个可用区 (AZs)，因为这是一个迁移中心。

默认情况下，AMS 在每个账户中创建以下两个安全组 (SGs)。确认这两个 SGs 都存在。如果他们不在场，请向 AMS 团队提交新的服务申请，请求他们。

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

确保在私有子网中创建 CloudEndure 复制实例，那里有返回本地的路由。您可以通过确保私有子网的路由表中包含返回 TGW 的默认路由来确认这一点。但是，执行 CloudEndure 计算机切换操作应进入 “隔离” 私有子网，那里没有返回本地的路由，只允许 Internet 出站流量。确保在隔离子网中进行切换，以避免本地资源出现潜在问题，这一点至关重要。

先决条件：

1. 高级或高级支持级别。
2. 部署的 KMS 密钥 AMIs 的应用程序账户 IDs 。
3. 工具账户，如前所述。

AWS 应用程序迁移服务 (AWS MGN)

AWS 应用程序迁移服务 (AWS MGN) 可以通过在工具账户配置期间自动创建的 `AWSManagedServicesMigrationRole` IAM 角色在您的 MALZ Tools 账户中使用。您可以使用 AWS MGN 迁移在支持版本的 Windows 和 Linux 操作系统上运行的应用程序和数据库。

有关 AWS 区域 支持的大部分 up-to-date信息，请参阅AWS 区域服务列表。

如果 AWS MGN AWS 区域 目前不支持您的首选项，或者 AWS MGN 目前不支持运行应用程序的操作系统，请考虑改用工具账户中的CloudEndure 迁移。

正在请求 AWS MGN 初始化

AWS MGN 在首次使用前必须由 AMS 进行初始化。要申请新的 Tools 账户，请提交 Tools 账户中的管理 | 其他 | 其他 RFC，其中包含以下详细信息：

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
```

```
    to 'Create template' and complete the initialization process.
```

AMS 成功完成 RFC 并在您的 Tools 账户中初始化 AWS MGN 后，您可以使用编辑默认模板`AWSManagedServicesMigrationRole`以满足您的要求。

启用对新 AMS Tools 账户的访问权限

创建工具账户后，AMS 会为您提供账户 ID。下一步是配置对新账户的访问权限。执行以下步骤。

1. 将相应的 Active Directory 组更新为相应的帐户 IDs。

   AMS 创建的新账户将使用 ReadOnly 角色策略以及允许用户申报的角色进行配置。 RFCs

   Tools 账户还有一个额外的 IAM 角色和用户可用：

   - IAM 角色：`AWSManagedServicesMigrationRole`
   - IAM 用户：`customer_cloud_endure_user`
2. 请求策略和角色以允许服务集成团队成员设置更高级别的工具。

   导航到 AMS 控制台并归档以下内容 RFCs：

   a. 创建 KMS 密钥。使用创建 KMS 密钥 (auto) 或创建 KMS 密钥（需要查看）。

      当您使用 KMS 加密提取的资源时，使用与其余多账户着陆区应用程序账户共享的单个 KMS 密钥可以为摄取的图像提供安全保护，这些图像可以在目标账户中解密。

   b. 共享 KMS 密钥。

      使用管理 | 高级堆栈组件 | KMS 密钥 | 共享（需要查看）更改类型 (ct-05yb337abq3x5) 请求将新的 KMS 密钥共享给已提取的应用程序账户。 AMIs

最终账户设置的示例图：

AMS 预先批准的 IAM CloudEndure 政策示例

要查看 AMS 预先批准的 IAM CloudEndure 政策：解压 WIGS Cloud Endure 着陆区域示例文件并打开。`customer_cloud_endure_policy.json`

测试 AMS Tools 账户连接和 end-to-end设置

1. 首先在要复制到 AMS 的服务器上配置 CloudEndure 和安装 CloudEndure 代理。

2. 在中创建项目 CloudEndure。
3. 通过 secrets Manager 输入执行先决条件时共享的 AWS 凭据。
4. 在 “复制” 设置中：
   a. 选择 AMS “Sentinel” 安全组（仅限私有和 EgressAll），选择 “选择要应用于复制服务器的安全组” 选项。
   b. 为计算机（实例）定义转换选项。有关信息，请参阅步骤 5。切开
   c. 子网：私有子网。
5. 安全组：
   a. 同时选择 AMS “Sentinel” 安全组（仅限私有和 EgressAll）。
   b. 切换实例必须与 AMS 管理的 Active Directory (MAD) 和公共终端节点通信： AWS
      i. 弹性 IP：无
      ii. 公有 IP：否
      iii. IAM 角色： customer-mc-ec双实例配置文件
   c. 按照您的内部标签惯例设置标签。
6. 在计算机上安装 CloudEndure 代理，然后在 EC2 控制台中查找要出现在您的 AMS 账户中的复制实例。

AMS 摄取过程：

AMS Tools 账户卫生

在账户中共享了 AMI 并且不再需要复制的实例之后，您需要进行清理：

- 实例 WIGs 摄取后：
  - 切换实例：至少在工作完成后，通过 AWS 控制台停止或终止此实例
  - 摄取前 AMI 备份：在接入实例且本地实例终止后将其删除
  - AMS 摄取的实例：在共享 AMI 后关闭堆栈或终止
  - AMS-inge AMIs sted：与目标账户共享完成后删除
- 迁移结束清理：记录通过开发人员模式部署的资源，以确保定期进行清理，例如：
  - 安全组
  - 通过云形成创建的资源
  - 网络 ACK

- 子网
- VPC
- 路由表
- 角色
- 用户和账户

大规模迁移-迁移工厂

请参阅 AWS CloudEndure 迁移工厂解决方案简介。

MALZ：核心账户入门

在登录 AWS 多账号 landing zone 核心账户时，您需要完成的关键任务如下:.

主题

- 在 AMS 中创建 AWS 多账号 landing zone 核心账号
- 创建 IAM 角色让 AMS 访问您的账户
- 在 AMS 中为 root 用户使用多重身份验证 (MFA) 保护新账户
- 订阅 AWS Marketplace 趋势科技端点防护 (EPS)
- 设置联网
- 设置访问管理

如有入门问题，请联系您的云架构师。

在 AMS 中创建 AWS 多账号 landing zone 核心账号

AMS 多账户着陆区需要配置一个新的亚马逊网络服务 (AWS) 账户，才能在 AMS 多账户登录区域环境中充当管理账户。要创建 AWS 账户，请按照以下 step-by-step说明操作：如何创建和激活新的亚马逊 Web Services 账户？

简单的步骤是：前往 “创建账户”，单击 “立即注册”，然后在打开的页面上单击 “创建新账户” AWS 账户。按照屏幕上的说明进行操作，包括接听电话和使用电话键盘输入 PIN。您还需要输入信用卡。AMS 使用此账户作为您的新多账户 landing zone 的管理账户或付款人账户。

Note

入职后，请咨询您的云服务交付经理 (CSDM)，了解如何将账单从信用卡转移到发票系统。将需要以下信息：

- 账单公司名称
- 账单联系人姓名
- 账单联系人电话号码
- 账单联系人电子邮件
- 账单地址

您的 CSDM 将帮助您完成此更新。完成后，要更改付款方式，请参阅管理您的 AWS 付款方式。

Note

请勿将您的新账户关联到现有的管理账户或付款人账户。
确保您的账户不是现有账户的一部分 AWS Organizations；有关信息，请参阅什么是 AWS Organizations？

Important

确保电子邮件地址（通讯组列表，而不是个人的电子邮件地址）和电话号码与该帐户相关联，这一点非常重要，这样您才能收到对潜在安全事件的响应。如果不重置账户密码，就无法更改账户的电话号码和电子邮件地址，这对 AMS 根账户来说是一项艰巨的任务。为确保这些值保持稳定，选择与个人无关的联系信息至关重要，这些信息可能会发生变化。选择可以指向群组的电子邮件别名。在选择电话号码时遵循同样的做法：选择一个可以指向群组或公司拥有的号码而不是个人的号码。

要详细了解您需要将 Core 账户登录 AMS 多账号登陆区的问题，请参阅附录：多账号 landing zone (MALZ) 入职注意事项清单。

创建 IAM 角色让 AMS 访问您的账户

既然您已经成功创建了新账户 AWS 账户，接下来该流程的下一步是允许 AMS 访问新账户，以创建和配置您的 AMS 环境，并满足正在进行的更改和配置请求。有关详细信息，请参阅使用 IAM 角色委派跨 AWS 账户访问权限。

AWS Identity and Access Management (IAM) 是一项 Web 服务，可帮助您安全地控制用户对 AWS 资源的访问权限。您可以使用 IAM 来控制谁可以使用您的 AWS 资源（身份验证）、他们可以使用哪些资源以及以何种方式（授权）。

激活 IAM 对 AWS 控制台的访问权限

1. 使用您的根账户凭据（您用于创建的电子邮件和密码 AWS 账户）登录 AWS 管理控制台。请勿使用其他 IAM 凭证登录。 AWS 管理控制台主页打开。
2. 在顶部导航栏中，打开账户名称的下拉菜单，然后选择账户。账单主页打开。
3. 向下滚动到 IAM 用户和角色对账单信息的访问权限，然后选择编辑。将打开 “激活 IAM” 访问区域。
4. 选中该复选框，然后选择 “更新”。您现在可使用 IAM policy 控制用户可访问的页面。

创建一个 IAM 角色供 AMS 使用

1. 获取一个 JSON 或 YAML 文件，该文件定义了 AMS 用于创建您的基础设施的 IAM 角色。或者：
   - 您的 AMS 云架构师 (CA) 会为您提供一个 JSON 或 YAML 文件。
   - 你可以下载 onboarding_iam_roles.zip 并选择以下选项之一：
     - onboarding_role_admin.json（较短，授予完全管理员访问权限）
     - onboarding_role_minimal.json（时间更长，授予的权限最小）
2. 登录 AWS 管理控制台 并在 https://console.aws.amazon.com/cloudformation 上打开 CloudFormation 控制台。
3. 选择创建堆栈。您将看到以下页面。
4. 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。

5. **ams-onboarding-role**进入堆栈名称部分，继续向下滚动并选择下一步，直到到达此页面。

6. 确保选中该复选框，然后选择创建堆栈。
7. 确保堆栈已成功创建。

在 AMS 中为 root 用户使用多重身份验证 (MFA) 保护新账户

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM 获取说明或前往 AWS Artifact 入门。

订阅 AWS Marketplace 趋势科技端点防护 (EPS)

趋势科技端点保护 (EPS) 是 AMS 中用于操作系统安全的主要组件。要在开始创建 AMS 着陆区后设置 EPS，您需要登录共享服务核心账户并订阅趋势科技趋势科技服务器深度安全防护系统 AMI AWS Marketplace。您的 CSDM 或 CA 将为您提供建议。

1. 使用您在入职调查问卷中指定的角色或用户登录 AWS 控制台 `CustomerEPSSubscriptionIAMRoleOrUser`
2. 导航到 “切换角色” 屏幕。

- 账户：由 AMS 提供
- 角色：`EPSMarketplaceSubscriptionRole`
- 显示名称：EPS 订阅时段

要在中订阅趋势科技趋势科技趋势科技服务器深度安全防护系统 AWS Marketplace，请在控制台中切换角色后执行以下步骤：

1. 导航到 AWS Marketplace。
2. 在 “查找满足您需求的 AWS Marketplace 产品” 下，选择以下选项：
   a. 供应商：趋势科技
   b. 定价计划：如果您有许可证，请自带许可证，或者按房东计费

c. 配送方式：Amazon 机器映像

3. 在右侧面板中单击 “继续订阅”。
4. 查看条款和条件，然后点击右上角的 “接受条款”。
5. 注销该帐户，然后向您的云架构师确认该过程已完成。

此时，AMS 将基础设施部署到您的 AMS 环境中，在您连接网络并设置访问权限后，该环境便可供您使用。

设置联网

AMS 环境中的联网主要由网络核心账户处理。

要为 AWS Managed Services (AMS) 设置联网，需要完成几个流程：

- 为您的 AMS 环境分配 IP 空间
- 建立专用网络连接 AWS
- 设置防火墙以允许 AMS 操作

为您的 AMS 环境分配 IP 空间

在填写入职问卷时，你应该已经与云架构师合作定义了 AMS 环境的 IP 空间。

AWS 在 AMS 中建立专用网络连接

AWS 使用 VPN 连接提供私有连接，通过 Di AWS rect Connect 提供专用线路。可以通过两种方式设置私有连接：

- 使用 Transit Gateway 实现集中边缘
- 将 Direct Connect and/or VPN 连接到 VPCs

使用 Transit Gateway 实现集中边缘

AWS Transit Gateway 是一项服务，可让您将 Amazon 虚拟私有云 (VPCs) 和本地网络连接到单个网关。Transit Gateway 可用于整合您现有的边缘连接并将其路由到单个 ingress/egress 点。有关更多详细信息，请参阅 T AWS ransit Gateway。

将 Direct Connect 连接到 Transit

您可以使用现有的 Direct Connect 连接，也可以在现有 AWS 账户中创建新的 Direct Connect 连接。Direct Connect 连接应该是以 1 Gbps 或更高的速度运行的专用或托管连接。

> **Note**
>
> 有关在 AWS 服务中使用 Direct Connect 的信息，请参阅 Di AWS rect Connect 位置入门。

要使用现有的 Direct Connect 专用连接，该连接上创建的传输虚拟接口不得超过 3 个。这是因为 Direct Connect 专用连接每个连接的传输虚拟接口上限为 4 个。

有关 Direct Connect 限制的更多信息，请参阅 AWS Direct Connect 限制。

Direct Connect 连接可用后，会发生以下情况：

1. AMS 在网络账户中创建一个 Direct Connect 网关。您必须为 Direct Connect 网关提供自治系统编号 (ASN) 以及必须从 Direct Connect 网关发布的前缀。此 ASN 用作亚马逊 ASN。
2. 您可以创建新的 Transit VIF 并将虚拟接口所有者设置为网络账户。
3. AMS 登录网络账户并接受连接提案。
4. AMS 将传输网关与 Direct Connect 网关关联起来。
5. AMS 将附件与本地 Transit Gateway 路由表关联起来。

> **Note**
>
> 为 Direct Connect 网关和 Transit Gateway 提供的 ASN 必须不同。

为了提高连接的弹性，最佳做法是将来自不同的 Direct Connect 位置的至少 2 个中转虚拟接口连接到 AWS Direct Connect 网关。有关更多信息，请参阅Direct Connect 弹性建议。

连接到 Transit Gateway

要将 VPN 连接连接到中转网关，必须指定客户网关。有关客户网关要求的更多信息，请参阅 Amazon VPC 网络管理员指南中的客户网关要求。

您需要提供 BGP ASN 号码、静态公有 IP 地址和路由选项（静态或动态）。提供这些详细信息后，AMS 将创建 VPN 连接并将该附件与本地 Transit Gateway 路由表关联起来。

有关 Transit Gateway 附件的更多详细信息，请参阅公交网关 VPN 附件。

将直接连接 and/or VPN 连接到账户 VPCs

您也可以直接连接到 Direct Connect 或 VPN。 VPCs 流量直接从流向 Direct Connect 或 VPN，无需通过传输网关。 VPCs

> **Note**
>
> 共享服务 VPC 和应用程序账户 VPCs 必须连接到 Direct Connect 或 VPN 连接才能建立私有连接。

Direct Connect 在 AMS 中设置

设置在您的 Direct Connect AMS 管理的 VPC 和您的内部网络之间进行通信。

> **Note**
>
> 有关在 AWS 服务中使用 Direct Connect 的信息，请参阅Direct Connect 位置入门。

要设置 Direct Connect 连接，请完成以下步骤：

1. 注册 Amazon Web Services（AWS）
2. 提交 Direct Connect 连接请求。
3. 完成 Cross Connect。
4. （可选）使用配置冗余连接 Direct Connect。
5. 由 AMS 执行：创建虚拟接口。
6. 由 AMS 执行：下载路由器配置。
7. 验证您的虚拟接口。

VPN 设置

AMS 在设置 VPN 以在您的 AMS 管理的 VPC 和内部网络之间进行通信时遵循的基本步骤。

> **Note**
>
> 要全面了解如何将 VPN 与 AWS 服务结合使用，请参阅什么是 AWS Site-to-Site VPN 和您的客户网关（您的 VPN 设备）。

我们按照 AWS VPN 用户指南入门和测试 Site-to-Site VPN 连接部分完成以下步骤：

1. 在您的 AWS VPC 中，创建客户网关。
2. 在您的 AWS VPC 中，创建虚拟专用网关。
3. 在您的 AWS VPC 中，在您的路由表中启用路由传播。
4. 在您的 AWS VPC 中，更新您的安全组以启用入站 SSH、RDP 和 ICMP 访问权限。
5. 在您的内部网络中，创建 VPN 连接并配置客户网关。
6. 测试 VPC 和您的内部网络之间的 VPN 连接。

设置访问管理

使用由 AWS Managed Services (AMS) 管理的网络意味着授予 AMS 管理您的云基础设施的权限。您需要配置一种在私有网络和 AMS 之间安全连接的方法。首先要做出一些决定：

- AMS API/CLI 和控制台访问权限：您需要安装 AMS CLI（本文档中提供了相关说明）。您可以使用 AMS 变更管理 API 向 AMS 提出变更请求，使用 AMS SKMS API 来了解您的 AMS 管理的资源。使用 Active Directory 联合身份验证服务 (AD FS)，您可以访问 AMS 控制台。
- 用户访问权限：需要在 AMS 端的 AD（通过目录服务）与您用来管理用户的目录之间建立连接。
- 实例访问：实例级访问通过单向信任配置完成。目录服务信任您的 CORP AD 中的凭据，允许 AMS 端内的堆栈允许使用 CORP 凭据登录。

> **Note**
>
> AMS 设置信任的 Active Directory (AD) 必须是拥有您授权访问您的 AWS 资源的用户账户的目录。

建立活动目录信任

要建立信任，AMS 需要您的域控制器 “本地策略”-> “安全选项”-> “网络访问：可以匿名访问的命名管道”，列出 Netlogon 和 l sarpc 管道。这些管道默认列出，但出于安全考虑，有时会被删除。信任建立后，可以再次将其从列表中删除。

配置条件转发器

1. 在 AD DNS 管理器-> 创建新的条件转发器中，在 DNS 域下：使用 AMS 提供给您的域名；例如 A523434123 .amazonaws.com（将其更改为在入职调查问卷中选择的域名）。
2. 在主服务器的 IP 地址下：添加 AMS 提供的 IP 地址。验证两个地址，确保没有连接问题。
3. 选择 “将此条件转发器存储在 Active Directory 中”，然后按如下方式进行复制：此域中的所有 DNS 服务器，然后按确定。

配置 AD 信任

关注这篇 Microsoft AD 文章使用本节中描述的设置和选项，为信任的一方创建单向传入的林信任。

1. 打开 “开始”-> “管理工具”-> “活动目录域和信任” 对话框。右键单击要与之建立信任的域的域节点，然后单击 “属性”-> “信任”-> “新建信任” 以打开 “新建信任向导”。输入 AMS 提供给您的域名作为信任名称，然后按下一步。
2. 在 “信任类型” 下，选择适当的信任级别（例如森林信任）。按 “下一步”。
3. 在 “信任指示” 下，选择 “单向：传入”。按 Next（下一步）。
4. 在 “信任方” 下，选择 “仅限此域”。按 Next（下一步）。
5. 在 “信任密码” 下，键入您选择的密码。按 Next（下一步）。
6. 要使信任选择已完成且信任创建已完成，只需按下一步即可。
7. 在 “确认传入信任” 下，选择 “否，不确认传入信任”。按 Next（下一步）。
8. 在 “已完成新建信任向导” 下，选择 “完成”，然后选择 “确定” 关闭。
9. 提供信任密码（出于安全考虑，请通过您的 CSDM 的电话号码联系我们）。AMS 将完成信任配置。

活动目录网站和服务

要减少登录延迟，请将 VPC CIDR 范围添加到您的 Active Directory 站点和服务（“开始”-> “管理工具”-> “活动目录” 站点和服务）。将 VPC CIDR 范围添加到包含最接近 AWS 的域控制器的 Active Directory 站点。

向 CSDM 提供您专门用于 AMS 的网站的广告网站名称。AMS 将在 AD 的 AMS 一侧重命名默认站点，使其与提供的名称相匹配。

活动目录名称后缀路由

建立单向林信任后，请完成以下步骤以验证后缀路由：

1. 在开始 > 所有程序 > 管理工具下，单击 A ctive Directory 域和信任。

   Active Directory 域和信任控制台打开。
2. 右键单击您的公司域名，然后单击 “属性”

   将打开该域的属性对话框。
3. 单击 “信任” 选项卡。

   将打开 “信任” 页面。
4. 单击 Amazon 域名，然后单击 “属性”。

   将打开 Amazon 域名信任的 “属性” 页面。
5. 单击 “名称后缀路由”，然后单击 “刷新”。

   确保没有冲突，以确保服务主体名称 (SPNs) 可以通过信任来解决。

将您的活动目录与 AMS IAM 角色联合起来

将您的目录与 AMS IAM 角色联合的目的是使企业用户能够使用其公司证书与 AWS 控制台和 AWS 进行交互 APIs，从而与 AMS 控制台和 AMS 控制台进行交互。 APIs

联合过程示例

此示例使用 Active Directory 联合身份验证服务 (AD FS)；但是，支持任何支持 AWS IAM 联合身份验证的技术。有关 AWS 支持的 IAM 联合身份验证的更多信息，请参阅 IAM 合作伙伴和身份提供商以及联合。您的 CSDM 将帮助您完成此过程，这需要与您的 AD 团队和 AMS 共同努力。

有关集成 SAML 进行 API 访问的详细信息，请参阅此 AWS 博客《如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问》。

有关安装 AMS CLI 和 SAML 的示例，请参阅附录：AD FS 声明规则和 SAML 设置。

向 AMS 控制台配置联合 (MALZ)

下表中详述的 IAM 角色和 SAML 身份提供商（可信实体）已作为 AMS 基础设施的一部分进行配置。这些角色允许您审核和查看 AMS 核心账户。

角色	权限
AWSManagedServicesReadOnlyRole	允许您在核心账户中查看 AMS 基础架构。
AWSManagedServicesCaseRole	允许您查看新应用程序账户中的资源并提交 AMS 事件和服务请求。
AWSManagedServicesChangeManagementRole	允许您查看核心账户中的 AMS 基础设施、提交 AWS Support 票证并申请一些 RFCs。

有关不同账户下可用角色的完整列表，请参阅AMS 中的 IAM 用户角色。

验证控制台访问权限

设置 ADFS 并拥有用于身份验证的 AMS 网址后，请按照以下步骤操作。

使用 Active Directory 联合服务 (ADFS) 配置，您可以按照以下步骤操作：

1. 打开浏览器窗口，进入为您的帐户提供的登录页面。您的账户的 ADFS IdpInitiatedSignOn页面随即打开。
2. 选择 “登录到以下任一站点” 旁边的单选按钮。登录网站选择列表变为活动状态。
3. 选择 s ignin.aws.amazon.com 网站并点击登录。输入您的凭证的选项已打开。
4. 输入您的 CORP 凭据，然后单击 “登录”。 AWS 管理控制台 开场了。
5. 将 AMS 控制台的 URL 粘贴到地址栏中，然后按 Enter。AMS 控制台打开。

验证 API 访问权限

AMS 使用 AWS API，其中包含一些特定于 AMS 的操作，您可以在 AMS API 参考中阅读这些操作。

AWS 提供了几种 SDKs 可供您访问的亚马逊网络服务工具。如果您不想使用 SDK，则可以直接调用 API。有关身份验证的信息，请参阅签署 AWS API 请求。如果您没有使用软件开发工具包，也没有直接发出 HTTP API 请求，则可以使用 AMS CLIs 进行变更管理 (CM) 和 SKMS。

安装 AMS CLIs

AWS CLI 是使用 AMS CLIs（变更管理和 SKMS）的先决条件。

1. 要安装 AWS CLI，请参阅安装 AWS 命令行界面，然后按照相应的说明进行操作。请注意，该页面底部有使用不同安装程序（Linux、MS Windows、mac O S、虚拟环境、捆绑安装程序（Linux、 macOS 或 Unix）的说明。
2. 安装完成后，运行 aws help 以验证安装情况。
3. 安装 AWS CLI 后，要安装或升级 AMS CLI，请下载 AMS 可发行文件 zip 文件并解压缩。您可以通过 AMS 控制台左侧导航栏中的 “文档” 链接访问 AMS CLI 发行版，或者请您的云服务交付经理 (CSDM) 向您发送 zip 文件。
4. 根据您的操作系统，打开托管云分发文件-> CLI-> Windows 或托管云发行文件-> CLI-> Linux/macOS 目录，然后：
5. 对于 Windows，请执行相应的安装程序（此方法仅适用于 Windows 32 或 64 位系统）：
   - 32 位： ManagedCloudAPI_x86.msi
   - 64 位： ManagedCloudAPI_x64.msi
6. 对于 Mac/Linux，运行以下命令执行名为：MC_CLI.sh 的文件：sh MC_CLI.sh。请注意，amscm 和 amsskms 目录及其内容必须与 MC_CLI.sh 文件位于同一个目录中。
7. 如果您的公司证书是通过与 AWS 的联合身份验证（AMS 默认配置）使用的，则必须安装可以访问您的联合身份验证服务的凭证管理工具。例如，您可以使用此 AWS 安全博客如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问来帮助配置您的凭证管理工具。
8. 安装完成后，运行`aws amscm help`或`aws amsskms help`并查看命令和选项。

MALZ：应用程序账户入门

在申请新的应用程序账户之前，您必须使用核心账户设置多账户 AWS Managed Services (AMS) 环境。以下是设置环境后需要采取的步骤。

主题

- 申请新的应用程序账户
- 设置 Active Directory 以统一对 AMS IAM 角色的访问权限
- 使用新的应用程序帐户设置联网
- 在应用程序账户 VPCs 中设置其他账户

有关入门问题，请联系您的云服务交付经理 (CSDM)。另请参阅应用程序账户：AMS 托管、开发者模式、客户管理。有关模式的一般信息，请参阅 AMS 模式AWS Managed Services 中的服务管理。

有关应用程序账户的不同模式的信息，请参阅应用程序账户：AMS 托管、开发者模式、客户管理。有关模式的一般信息，请参阅 AMS 模式。

申请新的应用程序账户

在申请新的应用程序账户之前，您必须使用核心账户设置多账户 AWS Managed Services (AMS) 环境。有关使用核心账户设置多账户环境的信息，请参阅MALZ：核心账户入门。

您可以为应用程序账户中的初始 VPC 选择以下 Amazon VPC 类型之一：

- 私有：此 VPC 没有连接互联网网关。这适用于不需要访问互联网 to/from 的私有应用程序。
- 公有：此 VPC 连接了 Internet 网关，并有公有子网和私有子网。这适用于需要访问互联网 to/from 的公共应用程序。

您可以通过提交 Deployment | Managed landing zone | 管理账户 | 创建应用程序账户（使用 VPC）(ct-1zdasmc2ewzrs) RFC 并在 RFC 中提供以下值来申请新的应用程序账户：

- 账户名：账户的自定义名称。请注意，账户名称的最大长度为 50 个字符。
- 账户电子邮件：账户的通讯组列表电子邮件。此电子邮件 ID 用于创建 AWS 账户。
- 支持级别：AWS Support 级别，高级版或高级版。
- VPC 名称：VPC 的名称。
- 可用区数量 (AZs)：2 或 3。
- VPC CIDR：VPC 的 CIDR 块。
- 路径类型：可以是`routable`或`isolated`。 `Routable`表示与 Transit Gateway (TGW) 应用程序路由表 VPCs 关联的应用程序可以连接到此 VPC。 `Isolated`表示与 TGW 应用程序路由表 VPCs 关联的应用程序无法连接到此 VPC。默认值为 `routable`。
- Transit Gateway 应用程序路由表：应用程序账户 VPC 必须与之关联的 Transit Gateway 路由表。如果未提供任何值，`defaultAppRouteDomain`则使用默认值，这意味着该账户将能够与同一路由表下的所有其他账户通信。
- PublicSubnet可用区 1 中公有子网的 AZ *<1-3>* CIDRCIDR：可用区 1 中公有子网的 CIDR。
- PrivateSubnet*<1-10>*可用区 1 中公有子网的 AZ *<I-3>* CIDRCIDR：可用区 1 中公有子网的 CIDR。

此时，AMS 使用指定的 VPC 配置将新的应用程序账户部署到您的 AMS 管理账户。

设置 Active Directory 以统一对 AMS IAM 角色的访问权限

将您的目录与 AMS IAM 角色联合起来，使企业用户能够使用其公司证书与 AWS 控制台和 AWS 以及 AMS APIs 控制台和 AM APIs S 进行交互。

联合过程示例

此示例使用 Active Directory 联合身份验证服务 (ADFS)。但是，支持任何支持 AWS IAM Federation 的技术。有关 AWS 支持的 IAM 联合身份验证的更多信息，请参阅 IAM 合作伙伴和身份提供商以及联合。您的 CSDM 将帮助您完成此过程，这需要与您的 AD 团队和 AMS 共同努力。

有关集成 SAML 进行 API 访问的详细信息，请参阅此 AWS 博客《如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问》。

有关安装 AMS CLI 和 SAML 的示例，请参阅《AMS 用户指南》中的附录：AD FS 声明规则和 SAML 设置。

向 AMS 控制台配置联合

下表中详述的 IAM 角色和 SAML 身份提供商（可信实体）已在您的新应用程序账户中配置。这些角色允许您访问新的应用程序帐户和文件 RFCs、写入 S3 存储桶以及执行其他操作。

角色	权限
AWSManagedServicesReadOnlyRole	允许您查看新应用程序账户中的资源。
AWSManagedServicesCaseRole	允许您查看新应用程序账户中的资源并提交 AWS Support 票证。
AWSManagedServicesChangeManagementRole	允许您在应用程序账户中查看 AMS 基础设施、归档 RFCs AWS Support 票证、写入 S3 存储桶、管理 Secrets Manager 密钥以及管理亚马逊弹性计算云 (Amazon EC2) 预留实例。
AWSManagedServicesSecurityOpsRole	允许您查看应用程序账户中的 AMS 基础设施、管理 Secrets Manager 密钥、管理 Web 应用程序防火墙规则、管理证书和提交 AWS Support 票证。

角色	权限
AWSManagedServicesAdminRole	允许您查看应用程序账户中的 AMS 基础设施、管理 Marketplace 订阅、管理 Secrets Manager 密钥、管理 Web 应用程序防火墙规则、管理证书、创建、管理 Amazon 预留 EC2 实例 RFCs、写入 S3 存储桶、提交 AWS Support 票证以及管理 AWS Artifacts 协议。

向 AMS 提交联盟申请

如果这是您的第一个帐户，请与您的 CSDM C and/or loud Architect 合作，为您的身份提供商提供元数据 XML 文件。

如果您正在注册其他账户或身份提供商，并且可以访问管理账户或所需的应用程序帐户，请按照以下步骤操作。

1. 从 AMS 控制台创建服务请求。

> **Note**
>
> - 如果为应用程序账户创建身份提供商，请从应用程序账户本身或管理账户提交此请求。
> - 如果为 AMS 核心账户创建身份提供商，请从管理账户提交此请求。
> - 如果为管理账户创建身份提供商，请通过管理账户提交此请求，或者联系您的 CSDM 寻求帮助。

在服务请求中，提供添加身份提供者所需的详细信息：

- AccountId 将在哪个账户中创建新的身份提供商。
- 所需的身份提供商名称（如果未提供），则默认为 customer-saml；通常，该名称必须与联合身份提供商中配置的设置相匹配。
- 对于现有账户，请说明是应将新的身份提供者传播到所有现有的控制台角色，还是提供应信任新身份提供商的角色列表。
- 将从联合代理导出的元数据 XML 文件作为文件附件附加到服务请求。

2. 在您创建服务请求的同一个账户中，使用 CT-ID ct-1e1xtak34nx76（管理 | 其他 | 其他 | 其他 | 创建）创建一个新的 RFC，其中包含以下信息。

   - 标题：“<Name>账户 < AccountId > 的加载 SAML IDP”。
   - AccountId 将在哪个账户中创建身份提供商。
   - 身份提供者名称。
   - 对于现有账户：是否应将身份提供者传播到所有现有的控制台角色，还是应信任新身份提供者的角色列表。
   - 在步骤 1 中创建的服务请求的案例 ID，其中附加了元数据 XML 文件。

验证控制台访问权限

设置 AD FS 并获得 AMS URL 用于身份验证后，您可以执行以下步骤。

使用 Active Directory 联合服务 (AD FS) 配置，您可以按照以下步骤操作：

1. 打开浏览器窗口，进入为您的帐户提供的登录页面。您的账户的 AD FS IdpInitiatedSignOn 页面随即打开。
2. 选择 “登录到以下任一站点” 旁边的单选按钮。登录网站列表变为活动状态。
3. 选择 signin.aws.amazon.com 网站并选择 “登录”。输入您的凭证的选项已打开。
4. 输入您的 CORP 凭据并选择 “登录”。AWS 管理控制台打开。
5. 将 AMS 控制台的 URL 粘贴到地址栏中，然后按 Enter。AMS 控制台打开。

验证 API 访问权限

AMS 使用 AWS API，其中包含一些特定于 AMS 的操作，您可以在 AMS API 参考中阅读这些操作。

AWS 提供了 SDKs 一些可供您访问的亚马逊网络服务工具。如果您不想使用 SDK，则可以直接调用 API。有关身份验证的信息，请参阅签署 AWS API 请求。 。如果您没有使用 SDK，也没有直接发出 HTTP API 请求，则可以使用 AMS CLIs 进行变更管理 (CM) 和 SKMS。

使用新的应用程序帐户设置联网

为应用程序帐户设置联网包括配置防火墙规则以及可能设置其他 Transit Gateway (TGW) 路由表。

设置防火墙

要使用在 AMS 环境中部署的应用程序，必须创建一些防火墙规则。您不需要这些规则即可访问您的实例，您可以跳过堡垒进入您的实例。

应用程序访问的防火墙规则

必须为通过防火墙的流量打开以下端口：

- 从您的本地网络到您的新应用程序 VPC CIDRs ，包括入口和出口方向。
- 从您的新应用程序 VPC CIDRs 到您的本地网络，包括入口和出口方向（如果您的云应用程序需要访问您的本地应用程序）。

端口	协议	服务	自/至	到/自
80	TCP	HTTP 网络访问	本地网络	AMS 应用程序 VPC
443	TCP	HTTPS 网络访问	本地网络	AMS 应用程序 VPC

设置其他公交网关应用程序路由表

AWS Managed Services (AMS) 网络非常灵活，支持各种联网用例。

- 同一账户 VPCs 中的应用程序之间的通信。
- 不同账户 VPCs 中的应用程序之间的通信。
- 不同账户 VPCs 中的应用程序之间的隔离。
- 同一账户 VPCs 中的应用程序之间的隔离。

如果您有网络 unique/special 需求，请联系您的 AMS 云架构师，他们将制定计划，让 AMS 网络架构满足您的需求。

根据为应用程序账户做出的联网决定 VPCs，您可以通过提交部署 | 托管着陆区 | 网络账户 | 创建公交网关路由表 (ct-3dscwaeyi6cup) RFC 来创建多个 Transit Gateway (TGW) 应用程序路由表。

更改类型要求您指定TransitGatewayRouteTableName（TGW 路由表的有意义的名称）TransitGatewayId、和TGWRouteTableType。

> **Note**
>
> 如果选择 “ createCustomRoute域” TGWRouteTableType，则创建的路由表为空。你必须向部署 | 托管着陆区 | 网络账户 | 添加静态路由 (ct-3r2ckznmt0a59) 更改类型提交 R FC。

在应用程序账户 VPCs 中设置其他账户

您可以通过提交部署 | 托管着陆区 | 应用程序账户 | 创建 VPC (ct-1j3503fres5a5) RFC 来申请额外的应用程序账户 VPC。

这与为新应用程序账户配置 VPC 的方式相同。有关详细信息，请参阅申请新的应用程序账户。

附录：多账号 landing zone (MALZ) 入职注意事项清单

在规划 AMS 多账户 landing zone 部署时，您需要考虑许多关键注意事项。您的选择将为 AMS 提供所需的信息，以确定您需要的基础设施组件。您的云架构师 (CA) 将为您提供一份调查问卷，以协助您完成这项工作。

主题

- AMS 多账号 landing zone 账户配置
- AMS 多账户 landing zone 监控警报
- 网络配置
- 活动目录配置
- 趋势科技端点防护 (EPS)
- 访问权限：堡垒、SSH 和 RDP
- 联合身份验证

> **Note**
>
> 有关实例类型的更多信息，请参阅 Amazon EC2 实例类型。
> 有关数据库实例类型的更多信息，请参阅 Amazon RDS 实例类型。
> 如果您需要直接连接，请参阅 AMS 单账号登陆区域入门指南来创建 Direct Connect 连接。

您将收到来自云服务交付经理 (CSDM) 的入职调查问卷，其中包含有关您的账户所需配置设置的问题。在继续操作之前，请与您的 CSDM 合作完成调查问卷。

AMS 多账号 landing zone 账户配置

- 新账户 ID

  您为 AMS 多账号 landing zone 创建的 AWS 账户 ID。不应成为 AWS 组织的一部分。
- 服务区域

  部署 AMS 多账户 landing zone 环境的主要区域。
- 用于发送通知的核心账户电子邮件。（它们应该都在同一个域中）。为每人提供一个电子邮件地址：
  - 共享服务账户
  - 社交账号
  - 登录账号
  - 安全账户
- 您的服务类型，高级版或高级版

  这决定了解决您的环境中问题的服务级别协议 (SLAs)

AMS 多账户 landing zone 监控警报

AMS 为您提供了一种直接收到某些监控警报的提醒（而不是获取 AMS 服务通知）的方式。要注册，请确保您的云架构师 (CA) 或云服务交付经理 (CSDM) 收到以下信息：

直接警报电子邮件：这些是您希望 AMS 向其发送某些基于资源的警报的电子邮件地址。有关哪些警报直接发送到电子邮件的详细信息，请参阅《AMS 高级用户指南》中的 AMS 基线监控警报。有关 AMS 监控的更多信息，请参阅 AMS 单账户登录区域用户指南中的监控管理。

网络配置

- Transit Gateway ASN 编号

  这是边界网关协议 (BGP) 会话中 AWS 端的自治系统编号 (ASN)，它必须是唯一的，并且不能与用于您的 Direct Connect 或 VPN 的相同。 16 位的范围为 64512 到 65534（含）。 ASNs
- 您的 AMS 多账户着陆区域基础设施 VPC CIDR 范围。

这些 CIDR 范围不能与您的本地网络重叠

您可以包含 /22 CIDR 范围，也可以单独提供每个 VPC CIDR。请注意，仅允许使用以下 CIDR 范围：

- 10.0.0.0 - 10.255.255.255（10/8 前缀）
- 172.16.0.0 - 172.31.255.255（172.16/12 前缀）
- 192.168.0.0 - 192.168.255.255（192.168/16 前缀）

请注意，不得使用 IP 范围 198.18.0.0/15（由 AWS Directory Service 保留）。

- 核心基础设施 VPC CIDR 范围（推荐 /22 范围）
- 网络 VPC CIDR 范围（推荐 /24 范围）
- 共享服务 VPC CIDR 范围（推荐 /23 范围）
- DMZ VPC CIDR 范围（推荐 /25 范围）

- VPN ECMP（启用或禁用）

  对于 VPN ECMP support (VPN ECMP 支持)，如果您在 VPN 连接之前需要等价多路径 (ECMP) 路由支持，则选择 enable (启用)。如果连接通告相同 CIDRs，则流量将在它们之间平均分配。

网络访问控制列表 (NACL)

网络访问控制列表 (NACL) 是您的 VPC 的可选安全层，它充当防火墙，用于控制进出一个或多个子网的流量。您可以使用 ACLs 与您的安全组相似的规则来设置网络，以便为您的 VPC 增加额外的安全层。有关安全组和网络之间差异的更多信息 ACLs，请参阅安全组和网络的比较 ACLs。

但是，在 AMS 多账户 landing zone 中，为了让 AMS 有效地管理和监控基础设施，使用 NACLs 仅限于以下范围：

- NACLs 不支持多账户 landing zone 核心账户：管理、联网、共享服务、日志和安全。
- NACLs 支持多账户 landing zone 应用程序帐户，前提是它们仅用作 “拒绝” 列表。此外，他们必须配置 “Allow All All”，以确保 AMS 的监控和管理运行。

在大规模的多账户环境中，您还可以利用集中式出口防火墙等功能来控制出站流量和/或 AMS 多账户着陆区中的 Tr AWS ansit Gateway 路由表来隔离网络流量。 VPCs

活动目录配置

AMS 托管活动目录的域 FQDN

趋势科技端点防护 (EPS)

- 您的实例和 Auto Scaling 组的 EC2 实例大小

  趋势科技端点保护 (EPS) 是 AMS 中用于操作系统安全的主要组件。该系统由趋势科技服务器深度安全防护系统管理中心 (DSM) EC2 EC2 实例、中继实例以及存在于所有 AMS 数据平面和您的 EC2 实例中的代理组成。

  - 中继实例类型（AMS 支持的最小值为 m5.large）
  - 数据库实例大小（推荐 200 GB）
  - RDS 实例类型（仅允许 db.m5.large 或 db.m5.xlarge）
- DSM 许可证类型（Marketplace 或 BYOL）

  如果您已经有许可证，请选择 BYOL（自带许可证）。AMS 将与您联系以获取有关许可证的必要信息。
- AWS 趋势科技服务器深度安全防护系统订阅的 IAM 用户或角色亚马逊资源名称 (ARN)（角色 ARN：arn: aws: iam::: role/）*ACCOUNT_IDROLE_NAME*

  向我们提供一个 IAM 角色、ARN 或您有权访问的现有 AWS 账户 角色中的 IAM 用户 ARN。AMS 在您的 AMS 多账户 landing zone Shared Services 账户中创建一个 IAM 角色，并在共享服务中添加由 IAM 角色信任提供的角色或用户，这样您就可以代入该角色来订阅趋势科技服务器深度安全防护系统。 AWS Marketplace

访问权限：堡垒、SSH 和 RDP

- SSH 堡垒设置

  AMS 在您的共享服务账户中提供 SSH 堡垒，用于访问 AMS 环境中的主机。要以 SSH 用户身份访问 AMS 网络，您必须使用 SSH 堡垒作为入口点。网络路径来自本地网络，经过传输网关 (TGW)，然后路由 DX/VPN 到共享服务 VPC。一旦您能够访问堡垒，就可以跳转到 AMS 环境中的其他主机，前提是已批准了正确的访问请求。

  - 所需的实例数（推荐 2）
  - 最大实例数（推荐 4 个）

  - 最低实例数（推荐 2 个）
  - 实例类型（推荐 m5.large）
  - 入口 CIDRs：网络中的用户将从中访问 SSH 堡垒的 IP 地址范围（IP 范围 1、IP 范围 2、IP 范围 3 等）
- RDP 堡垒设置

  AMS 可选择在您的共享服务账户中提供 RDP 堡垒，以访问 AMS 环境中的主机。要以 RDP 用户身份访问 AMS 网络，您必须使用 RDP 堡垒作为入口点。网络路径来自本地网络，经过 TGW，然后路由 DX/VPN 到共享服务 VPC。一旦您能够访问堡垒，就可以跳转到 AMS 环境中的其他主机，前提是已批准了正确的访问请求。
  - 实例类型（推荐 t3.medium）
  - 所需的最少会话次数（推荐 2 次）
  - 所需的最大会话数（推荐 10 次）
- RDP Bastion 配置类型、共享标准或共享 HA（默认为共享标准）

  SecureStandard = 一个用户收到一个堡垒，但只有一个用户可以连接到堡垒。

  SecureHA = 用户在两个不同的可用区收到两个堡垒可供连接，并且只有一个用户可以连接到堡垒。

  SharedStandard = 一个用户收到一个要连接的堡垒，两个用户可以同时连接到同一个堡垒。

  SharedHA = 用户在两个不同的 AZ 中收到两个堡垒可供连接，两个用户可以同时连接到同一个堡垒。

联合身份验证

身份提供商 (IDP) 名称

默认值为 `customer-saml`

AMS 单账号 landing zone (SALZ) 入门

AMS SALZ 入职流程

要注册 AMS 单账户 landing zone (SALZ) 账户，你需要采取以下步骤：

1. 创建一个新的 AWS 账户，AMS 将其配置为网络账户来托管防火墙。在您的 AWS 组织内创建新账户（如果有）。AMS 将遵循创建普通 AMS 账户的程序，因此必须收集所需的所有信息（例如 CIDR、EPS 许可证和用户）。注意：CIDR 分配为 /24 就不错了。
2. 指定是否要从出口流量账户中删除 Internet 网关 (IGWs)。
3. 确定您已批准的域名。AMS 通过维护已批准的域名列表来启用目标筛选；该列表可以稍后修改。
4. 根据您的预期吞吐量确认要使用的实例大小。默认情况下，该实例是在我们发现防火墙吞吐量为 350Mbps 的 m4.xlarge 实例中创建的。AMS 可以将大小增加到预期吞吐量为 1.25 Gbps 的 C4.8xLarge 实例。
5. 在 AMS 和您的私有网络之间设置网络。这涉及几个任务：
    a. 分配 IP 空间
    b. 建立与 AWS 的私有网络连接
    c. 设置防火墙
    d. 设置访问管理
    e. 计划备份
6. 向 AMS 提供对已创建账户的访问权限。
7. 验证 AMS 服务是否正常运行。

AMS 将能够在最初申请之日起 2 周（10 个工作日）内对您的账户进行账户扩建（入职）。任何后续活动都可以使用 AMS 计划事件管理 (PEM) 执行。

> **Note**
>
> - 美国东部（弗吉尼亚）
> - 美国西部（加利福尼亚北部）
> - 美国西部（俄勒冈州）
> - 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）
- 欧盟西部（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）

经常会添加新区域。有关最新列表，请参阅 AWS 区域和可用区。

SALZ 网络架构

下图描述了 AWS Managed Services (AMS) 单账户着陆区 (SALZ) VPC 网络布局，是高可用性设置的示例。

AMS 根据我们的标准模板和您在入职期间提供的选择选项为您配置网络的各个方面。标准的 AWS 网络设计适用于您的 AWS 账户，然后为您创建虚拟私有云 (VPC)，并通过 VPN 或 Direct Connect 连接到 AMS。在 AWS Direct Connect 上详细了解 Direct Connect。标准 VPCs包括 DMZ、共享服务和应用程序子网。在入职过程中， VPCs 可能会要求并创建其他内容以满足您的需求（例如，客户部门、合作伙伴）。入门后，你会得到一张网络图。这是一份环境文档，说明你的网络是如何设置的。

> **Note**
>
> 要了解所有活动服务的默认服务限制和限制，请参阅 AWS 服务限制文档。

我们的网络设计围绕 Amazon 的 “最低权限原则” 构建。为了实现这一目标，除了来自可信网络的流量外，我们通过网关路由所有流量，包括入站和出站流量。唯一可信的网络是通过使用 VPN 和 AWS

Direct Connect (DX) 在您的本地环境和 VP and/or C 之间配置的网络。通过使用堡垒实例授予访问权限，从而防止直接访问任何生产资源。您的所有应用程序和资源都位于可通过公共负载均衡器访问的私有子网中。公共出口流量通过我们的正向代理流向 Internet Gateway，然后流向互联网。或者，流量可以通过您的 VPN 或 Direct Connect 流向您的本地环境。

AMS 单账号 landing zone 共享服务

共享服务子网包含 AMS 目录服务、自动配置和常见任务的管理主机、防病毒 (TrendMicro) 管理服务器和内部堡垒主机：

- AMS 目录服务 = AD 域控制器

  在 AMS 账户中创建 Active Directory，创建 AMS 域，在启动时将托管堆栈加入该域。
- 管理主机 = AMS 管理主机（ 自动配置和常见任务 ）

  充当 API 端点 Directory Service，用于修改和与 Directory Service 域控制器交互。
- 安全服务：防病毒 (TrendMicro) 管理服务器 = EPS DSM + EPS Relay

  利用趋势科技™ 趋势科技趋势科技服务器深度安全防护系统软件 (DSM)，在客户端服务器模式下运行，并具有后端数据库，包括趋势科技服务器深度安全防护系统管理器、代理和中继。
- 内部堡垒主机 = 客户堡垒

  特殊用途的服务器旨在作为互联网的主要接入点，并充当您的其他 Amazon EC2 实例的代理。

SALZ：为 AMS 创建一个新 AWS 账户

为 AWS Managed Services (AMS) 创建新 AWS 账户的五个步骤是：

1. 创建一个 AWS 账户
2. 设置整合账单——将新账户关联到付款人账户
3. 配置您 AWS 账户 的 AMS 访问权限
4. 在 AMS 中为 root 用户使用多重身份验证 (MFA) 保护新账户
5. 订阅 E AWS Marketplace PS

如果您有任何疑问，请联系您的客户服务交付经理 (CSDM)。

创建一个 AWS 账户

AMS 计划要求配置新的亚马逊 Web Services (AWS) 账户。以下视频中提供了分步说明：如何创建和激活新的亚马逊 Web Services 账户？ 简单的步骤是：

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS 管理控制台在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

> **Note**
>
> 如果您已经有一个账户，则可以前往定AWS 价页面，然后点击创建免费账户。请务必至少注册该EC2 服务。注册一项服务即可访问中的所有服务 AWS。您只需为使用的服务付费。
> 如果您计划将新账户与付款人账户关联以进行整合账单，则无需在出现提示时输入付款方式信息。相反，进入屏幕输入信用卡信息后，只需导航离开即可。您需要提供与付款人账户关联的电子邮件地址才能发送整合 billing/linked 账户申请，详情将在下一节中详细介绍。

> **Important**
>
> 请务必确保将电子邮件地址和电话号码与该帐户关联，这样您才能收到对潜在安全事件的响应。如果不重置账户密码，就无法更改账户的电话号码和电子邮件地址，这对 AMS 根账户来说是一项艰巨的任务。为确保这些值保持稳定，选择与个人无关的联系信息至关重要，这些信息可能会发生变化。选择可以指向群组的电子邮件别名。在选择电话号码时遵循同样的最佳做法：选择一个可以指向群组或公司拥有的号码而不是个人的号码。

设置整合账单——将新账户关联到付款人账户

如果您希望将新的 AMS 管理 AWS 账户 账单计入现有 AWS Organizations 管理账户的付款，则需要设置整合账单并关联账户。有关执行此操作的详细信息，请参阅

- 整合账单 AWS Organizations和AWS 多账户账单策略。
- 邀请 AWS 账户 加入您的组织

> **Note**
>
> 您可以在将账户移交给 AMS 之前执行这些步骤。移交后，可以通过变更管理流程完成加入组织的步骤（如上所述）。如果需要帮助，请咨询您的云服务交付经理 (CSDM) 或云架构师 (CA)。

有关包括管理整合账单在内的一般账单信息，请参阅什么是 AWS 账单。有关账户如何协同工作的一般 AWS Organizations 信息，请参阅什么是 AWS Organizations。有关管理账户的规范性指导，请参阅 AWS Organizations 管理账户、可信访问权限和委派管理员

配置您 AWS 账户 的 AMS 访问权限

完成上述步骤后，您已成功获得新的安全保障， AWS 账户 并确保相关费用得到适当的计费。该过程的最后一步是允许 AMS 访问新账户，以进行初始堆栈配置，并满足正在进行的更改和配置请求。有关详细信息，请阅读使用 IAM 角色委派跨 AWS 账户访问权限。本节描述了基本步骤。

激活 AWS 网站访问权限

要授予您的 IAM 用户访问您账户账单信息和工具的权限，您必须激活该功能。

按照以下步骤进行操作：

1. AWS 管理控制台 使用您的根账户凭证（您用来创建的电子邮件和密码 AWS 账户）登录。请不要使用您的 IAM 用户凭证登录。

   AWS 管理控制台 主页打开。

2. 在顶部导航栏中，打开账户名称的下拉菜单，然后选择 “我的账户”。

   账单主页打开。

3. 向下滚动到 “IAM 用户访问账单信息” 区域，然后单击右侧的编辑。 *The area does not appear unless you are logged in with root credentials*。

   将打开 “激活 IAM” 访问区域。

4. 选中该复选框并单击 “更新”。

   您现在可使用 IAM policy 控制用户可访问的页面。

有关此过程的更多详细信息 AWS，请参阅管理访问权限概述。

创建具有 AWS 网站访问权限的 IAM 角色

AWS Identity and Access Management (IAM) 是一项 Web 服务，可帮助您安全地控制用户对 AWS 资源的访问权限。您可以使用 IAM 来控制谁可以使用您的 AWS 资源（身份验证）、他们可以使用哪些资源以及以何种方式（授权）。

1. 前往 IAM 管理控制台，单击左侧导航窗格中的角色。

   角色管理页面打开，其中包含有关 IAM 角色的信息、“创建角色” 选项和现有角色列表。

2. 单击 “创建角色”。

   将打开 “创建角色选择可信实体的类型” 页面。单击 “ AWS 账户其他”，下方将打开一个设置区域。

   输入 AMS 向您提供的 AMS 可信账户 ID。取消选中 “需要外部 ID” 和 “需要 MFA” 选项。

3. 单击 Next: Permissions。

   创建角色附加权限策略页面打开，其中包含用于创建新策略、
   刷新页面和搜索现有策略的选项。提供了现有政策的列表。

4. 选择AdministratorAccess策略，然后单击 “下一步：查看”。

   将打开 “创建角色审阅” 页面。

5. 将新角色命名为 aws_managedservices_onboarding_role，然后在角色描述中键入 “AMS 入职角色”。查看新角色的设置，如果满意，请单击 “创建角色”。

   角色管理页面打开，其中列出了您的新角色。

订阅 E AWS Marketplace PS

AMS 端点安全 (EPS) 的最新更改要求您通过订阅 TrendMicro 趋势科技服务器深度安全防护系统 AWS Marketplace 并接受软件条款。

TrendMicro 提供两种许可模式：按受保护实例小时数和自带许可证 (BYOL)。

- BYOL：
  1. 您可以使用通过外部渠道购买的自己的许可证。
  2. 您必须向 AMS 提供所有许可证密钥才能构建 EPS 基础架构。您可以提供许可所有模块的激活码，也可以提供许可特定模块的单个激活码。AMS 仅创建与您提供的激活码对应的许可证文件。由于许可证激活是在入职期间进行的，因此您可以在 AMS 首席工程师和 CSDM 在场的情况下共享该信息。
  3. 此外，您必须订阅 BYOL TrendMicro Market Place AMI 订阅。请参阅趋势科技趋势科技服务器深度安全防护系统 (BYOL)。
- 每个受保护实例小时数：
  1. 在此订阅中，您无需拥有任何先前购买的 Trend 许可证。
  2. 但是，您必须订阅 Marketplace 订阅。
  3. 在此模型中，不需要与 AMS 共享许可证密钥，因为趋势使用量是自动计量的，包括软件许可证+ EC2 基础设施的使用情况。请参阅趋势科技趋势科技服务器深度安全防护系统。

要订阅趋势科技，请执行以下步骤：

1. 登录到你的 AWS 账户.
2. 导航到趋势科技趋势科技服务器深度安全防护系统（BYOL 或按受保护实例小时数）产品页面。

3. 在右侧面板中单击 “继续订阅”。
4. 点击右上角的 “接受条款”。

在趋势科技趋势科技服务器深度安全防护系统中启用 IDS 和 IPS

您可以请求 AMS 为您的账户启用趋势科技入侵检测系统 (IDS) 和入侵防护系统 (IPS)（非默认功能）。

为此，请提交更新请求（管理 | 其他 | 其他 | 更新），并附上用于接收 IDS 和 IPS 通知的电子邮件地址列表。这些地址将添加到您账户中的 SNS 主题中，AMS 会为您创建该主题。

> **Note**
>
> AMS 不能添加任何可能干扰我们提供其他 AMS 服务的趋势科技服务。

下一步: 在 AMS 中为 root 用户使用多重身份验证 (MFA) 保护新账户

订阅 Cent AWS Marketplace OS 7.6

AMS 现在提供 CentOS 7 (x86_64)，其中更新的 HVM 由 Centos.org 作为 AMS AMI 出售。要使用此 AMI，您必须选择免费的 Cent OS 许可证，并在所有 AMS 账户上接受该许可。

要订阅，请前往AWS Marketplace并按照选择加入的说明进行操作。

您不会因为使用本产品而产生软件费用，但您仍需承担其他 AWS 费用，包括 EC2 使用费。如果这是 “自带许可证” 产品，则必须拥有有效的软件许可证才能使用。

你可以在 CentOS 7 (x86_64) 上查看此软件的信息，以及更新 HVM。

在 AMS 中为 root 用户使用多重身份验证 (MFA) 保护新账户

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM 获取说明或前往 AWS Artifact 入门。

SALZ：设置网络

要为 AWS Managed Services (AMS) 设置联网，需要完成几个流程：

1. 为您的 AMS 环境分配 IP 空间
2. 建立与 AWS 的私有网络连接
3. 设置防火墙以允许 AMS 操作

为您的 AMS 环境分配 IP 空间

AMS 是使用 /16 CIDR 块作为推荐的网络分配进行设计和测试的。连接到 AMS 的可信网络必须使用与分配给 AMS 的 CIDR 块不重叠的 CIDR 块，这一点很重要。这些地址是设置虚拟私有云 (VPC) 和子网所必需的。有关 AWS 的更多信息 VPCs，请参阅亚马逊 VPC 限制和亚马逊 VPC FAQs。

虽然 /16 CIDR 块可能看起来像很多 IP 地址，但是 VPC 一旦创建，就无法扩展。因此，这种分配可确保您的 AMS 管理的 VPC 能够在相当长的一段时间内正常运行。在 CIDR 块中，您必须至少为两个私有子网和两个公有子网分配 IP 地址范围。

AWS 接受通过原生 AWS 虚拟专用网络 (VPN) 功能与 AMS 环境的连接。就您而言，这可以通过 AWS Direct Connect (DX)、硬件 VPN 或软件 VPN 来实现。在 AMS 方面，我们使用虚拟网关的功能 VPCs。

基本环境组件

用户 Network-to-Amazon VPC 连接选项	
硬件 VPN	建立从远程网络上的网络设备到连接到 VPC 上的 AMS 管理的网络设备的硬件 VPN 连接。
AWS Direct Connect (DX)	利用 AWS Direct Connect 建立从您的远程网络到 Amazon VPC 的私有逻辑连接（如果与 VPN 一起使用则为加密连接）。
软件 VPN	建立从远程网络上的设备到 Amazon VPC 内运行的用户管理的软件 VPN 设备的 VPN 连接。

> **Note**
>
> AMS 建议将冗余私有 VPN 连接到 DX 连接。您的客户服务交付经理 (CSDM) 将在您注册账户时协助进行设置。

建立与 AWS 的私有网络连接

将 AMS 添加到您的公司活动目录以建立连接。您可能需要通过专用网络连接执行管理操作或用户访问权限。AWS 通过提供 VPN 连接和专用线路 Direct Connect。以下步骤说明如何与 AMS 合作建立任一（或两者）连接方式。

VPN 设置

本节介绍设置 VPN 以在 AMS 管理的 VPC 和内部网络之间进行通信的基本步骤。

> **Note**
>
> 要全面了解如何将 VPN 与 AWS 服务配合使用，请参阅什么是 AWS Site-to-Site VPN 以及有关您的客户网关（您的 VPN 设备）的所有信息。

按照 AWS VPN 用户指南入门和测试 Site-to-Site VPN 连接部分完成以下步骤。

- 步骤 1：在您的 AWS VPC 中，创建客户网关
- 步骤 2：在您的 AWS VPC 中，创建虚拟私有网关
- 步骤 3：在您的 AWS VPC 中，在您的路由表中启用路由传播
- 步骤 4：在您的 AWS VPC 中，更新您的安全组以启用入站 SSH、RDP 和 ICMP 访问权限
- 步骤 5：在您的内部网络中，创建 VPN 连接并配置客户网关
- 步骤 6：测试 VPC 和您的内部网络之间的 VPN 连接

Direct Connect 设置

本节介绍设置 Direct Connect (DX) 以在您的 AMS 管理的 VPC 和内部网络之间进行通信的基本步骤。

> **Note**
>
> 有关将 DX 与 AWS 服务配合使用的信息，请参阅Direct Connect 地点入门。

要设置 DX 连接，您需要完成以下步骤：

1. 注册亚马逊 Web Services
2. 提交 AWS Direct Connect 连接请求

3. 完成 Cross Connect
4. （可选）使用 AWS Direct Connect 配置冗余连接
5. 由 AMS 执行：创建虚拟接口
6. 由 AMS 执行：下载路由器配置
7. 验证您的虚拟接口

设置您的防火墙

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM 获取说明或前往 AWS Artifact 入门。

应用程序迁移/入职期间的 AMS 堡垒选项

为了在迁移过程中为您提供最佳体验，以下是 AMS 目前可以利用的潜在选项：

- 选项 1：绕过堡垒仅用于迁移工作（出于安全考虑，作为临时措施，您必须签署此协议）。

  注意：审核功能仍将到位，以确保 AMS 可以查看每个请求。
- 选项 2：使用所选工具进行 SSH 隧道传输；例如 PuTTy，如图所示。

  对于此选项，所描述的环境组件已经需要准备就绪。

  AMS 将提供其他说明和说明。

使用 Pu 进行 SSH 隧道传输的步骤：TTy

在 PuTTY 中，您将使用堡垒主机的公有 IP 创建 SSH 会话，在 AUTH 部分提供 PEM 密钥，然后创建隧道。隧道的源端口应是未使用的本地端口（例如 5000），IP 将是附加了 RDP 端口的目标主机（您要访问的 Windows 盒子）的 IP（3389）。请务必保存您的配置，因为您不想在每次登录框时都要这样做。连接到堡垒主机，然后登录。然后，启动 localhost: 5000（或您选择的任何端口）的 RDP 会话。

1. 设置堡垒主机的主机名或公有 IP

2. 在 SSH->Auth 中，将私钥文件设置为.ppk 格式

3. 在 SSH->隧道中，添加新的转发端口。源端口应为任意未使用的端口，目标应为堡垒主机后面的目标服务器的 IP，并附加 RDP 端口。

4. 通过 Putty 连接到堡垒主机并登录。

5. 启动与 localhost: 5000 的 RDP 会话以到达目标服务器。

SALZ：设置访问管理

使用由 AWS Managed Services (AMS) 管理的网络意味着授予 AMS 管理您的云基础设施的权限。您需要配置一种在私有网络和 AMS 之间安全连接的方法。首先要决定您要提供的访问权限类型：

- 要@@ 访问 AMS API/CLI 和控制台：您需要安装 AMS CLI（本文档中提供了相关说明）。您可以使用 AMS 变更管理 API 向 AMS 提出变更请求，使用 AMS SKMS API 来了解您的 AMS 管理的资源。使用 Active Directory 联合身份验证服务 (AD FS)，您可以访问 AMS 控制台。

  > **Note**
  >
  > 如果您要设置自己的 ITSM，则需要使用 AWS Support API (SAPI) 来处理服务请求和事件报告。SAPI 已记录在《Su AWS pport API 参考》中。

- 对于用户访问：无论您是使用 Windows Active Directory (AD) 还是 Linux/LDAP 解决方案管理用户，都需要在 AMS 端的 AD（通过目录服务）与您的目录之间建立连接。
- 例如访问：实例级访问是通过单向森林信任配置完成的。目录服务信任其 CORP AD 中的凭据，允许 AMS 端内的堆栈允许使用 CORP 凭据登录。

  请注意，AMS 设置信任的 Active Directory (AD) 必须是拥有您授权访问您的 AWS 资源的用户账户的目录。

> **Important**
>
> 要设置森林信任，AMS 需要您的域控制器本地策略-> 安全选项-> 网络访问：可以匿名访问的命名管道，列出 Netlogon 和 l sarpc 管道。这些管道默认列出，但出于安全考虑，有时会被删除。信任建立后，可以再次将其从列表中删除。

建立活动目录 (AD) 信任

在开始为您的 AWS Managed Services (AMS) 账户建立活动目录 (AD) 信任之前，请确保已打开相应的防火墙端口。

AMS 管理的 Active Directory 和您的公司目录服务的信任允许您使用公司管理的凭据访问 AMS 管理的实例，以执行开发、测试或管理功能。

创建信任连接的练习分为两部分：

首先，配置条件转发，即 DNS 配置，以便 DNS 查询知道要访问哪个 DNS 服务器。

其次，配置信任，即 Active Directory (AD) 结构，允许一个域中的用户访问另一个域中的资源。

配置条件转发器

按照这篇 Microsoft AD 文章为域名分配条件转发器，然后使用以下设置和选项：

1. 在 AD DNS 管理器-> 创建新的条件转发器中，在 DNS 域下：使用 AMS 提供给您的域名；例如，*A523434123.amazonaws.com*。
2. 在主服务器的 IP 地址下：添加 AMS 提供的 IP 地址。验证两个地址，确保没有连接问题。
3. 选择 “将此条件转发器存储在 Active Directory 中”，然后按如下方式进行复制：此域中的所有 DNS 服务器，然后按确定。

配置信任

要为您的 AWS Managed Services (AMS) 账户配置信任，请按照这篇 MicroSoft 广告文章使用本节中描述的设置和选项为信任的一方创建单向传入林信任。

1. 打开 “开始”-> “管理工具”-> “活动目录域和信任” 对话框。右键单击要与之建立信任的域的域节点，然后单击 “属性”-> “信任”-> “新建信任” 以打开 “新建信任向导”。输入 AMS 提供给您的域名作为信任名称，然后按下一步。
2. 在 “信任类型” 下，选择 “林信任”。按 Next（下一步）。
3. 在 “信任指示” 下，选择 “单向：传入”。按 Next（下一步）。
4. 在 “信任方” 下，选择 “仅限此域”。按 Next（下一步）。
5. 在 “信任密码” 下，键入您选择的密码。按 Next（下一步）。
6. 要使信任选择已完成且信任创建已完成，只需按下一步即可。

7. 在 “确认传入信任” 下，选择 “否，不确认传入信任”。按 Next（下一步）。
8. 在 “已完成新建信任向导” 下，选择 “完成”，然后选择 “确定” 关闭。
9. 提供信任密码（出于安全考虑，请通过您的 CSDM 的电话号码联系我们）。AMS 将完成信任配置。

活动目录网站和服务

要减少登录延迟，请将 VPC CIDR 范围添加到您的 Active Directory 站点和服务（“开始”-> “管理工具”-> “活动目录” 站点和服务）。将 VPC CIDR 范围添加到包含最接近 AWS 的域控制器的 Active Directory 站点。

活动目录名称后缀路由

建立单向林信任后，请完成其他步骤。

1. 在开始 > 所有程序 > 管理工具下，单击 A ctive Directory 域和信任。

   Active Directory 域和信任控制台打开。
2. 右键单击您的公司域名，然后单击 “属性”

   将打开该域的属性对话框。
3. 单击 “信任” 选项卡。

   “信任” 页面打开。
4. 单击 Amazon 域名，然后单击 “属性”。

   将打开 Amazon 域名信任的 “属性” 页面。
5. 单击 “名称后缀路由”，然后单击 “刷新”。

   这些步骤可确保服务主体名称 (SPNs) 能够通过信任进行解析。

问题排查

如果遇到麻烦，可以尝试一些方法：

- 需要允许由 AMS 管理的 Active Directory 出站安全组通过您的 CIDR 块（例如 10.27.0.0/16）连接到您的域控制器。

- 在 AWS 控制台中追踪从域控制器到域控制器的路线，检查沿途的所有安全组。
- 如果允许互联网控制消息协议 (ICMP)，请确保你能够 ping 由 AMS 管理的 Active Directory 域控制器。
- 确保您的域控制器可以与 AWS 目录服务通信。
- 确保条件转发器解析并经过验证。
- 如果您在 “新建信任” 向导中没有看到 Fores t Trust，则您的条件转发器可能无法正常工作：
  - 使用 nslookup 来测试分辨率
  - 尝试重新启动域控制器

AMS 托管活动目录

AMS 现在提供了一项名为 “托管活动目录”（又名托管 AD）的新服务，它允许 AMS 管理您的活动目录 (AD) 基础设施运营，同时让您控制活动目录的管理。

AMS 对托管 AD 的支持与 AMS 对亚马逊关系数据库服务 (Amazon RDS) 的支持类似。在这两种情况下， AWS （包括 AMS）都支持创建和管理运行服务的基础架构，同时您可以执行访问控制和所有管理功能。该模型具有以下优点：

- 限制安全风险： AWS 而且 AMS 不需要您的域名的管理权限。
- 直接集成：您可以使用当前的授权模型并将其与 AD 集成，而无需与 AMS 接口。

备注：

- AMS 和您都无法访问您的托管 AD 域控制器，因此无法在域控制器上安装任何软件。这一点很重要，因为不允许要求在域控制器上安装软件的第三方解决方案。

  访问权限的工作原理是这样的：

  - AWS Directory Service 团队：有权访问域控制器。
  - AMS：有权访问 Directory Service APIs 以对域名执行某些操作。这些操作包括拍摄 AD 快照、更改 AD 架构和其他操作。
  - 您：可以访问域 (AD) 以创建用户、群组等。
- 我们建议您在迁移企业 AD 之前对托管 AD 进行概念验证，因为并非传统 AD 环境中的所有功能都可以在托管 AD 环境中使用。
- AMS 不会管理您的广告管理或提供有关您的广告管理的指导。例如，AMS 不会就组织单位结构、组策略结构、AD 用户命名约定等提供指导。

它的工作原理是这样的：

1. AMS AWS 账户 为您安装了一个新的，与您的 AMS 账户分开并添加到您的 AMS 账户之外，并通过 Directory Service 配置活动目录 (AD) 环境（另请参阅什么是 AWS AWS Directory Service？）。

   以下是系统集成商需要从您那里收集的信息，以便让 AMS 加入托管 AD：

   - 账户信息
     - 为您的 AMS 管理 AWS 账户 的广告创建的账户 ID：数字 AWS 账户
     - 要将托管广告加载到的区域： AWS 区域
   - 托管活动目录信息：
     - 微软 AD 版：标准版/企业版。AWS Microsoft AD（标准版）包括 1 GB 的目录对象存储空间。此容量最多可支持 5,000 个用户或 30,000 个目录对象，包括用户、群组和计算机。AWS Microsoft AD（企业版）包含 17 GB 的目录对象存储空间，最多可支持 100,000 个用户或 500,000 个对象。

       有关更多信息，请参阅 AWS Directory Service FAQs。
     - 域名 FQDN：您的 AMS 托管 AD 域名的 FQDN。
     - 域 NetBIOS 名称：您的 AMS 托管 AD 域的 NetBIOS 名称。
     - 您希望与托管 AD 集成的 AMS 标准账户的账号（AMS 配置从 AMS 标准账户的 AD 到托管 AD 的单向信任）
     - 是否需要修改活动目录架构？如果需要，需要进行哪些修改？
     - 默认情况下，会配置两个域控制器。你还需要更多吗？ 如果是，你需要多少？出于什么原因？
   - 托管活动目录的联网信息：
     - 域控制器的托管 AD VPC CIDR（托管 AD 域控制器的私有子网范围内的 CIDR）：
       - 域控制器的子网 CIDR 1：[您的 CIDR，必须是 AMS 托管 AD VPC CIDR 的一部分]
       - 域控制器的子网 CIDR 2：[您的 CIDR，必须是 AMS 托管 AD VPC CIDR 的一部分]

       例如：
       - 托管 AD VPC CIDR：192.168.0.0/16
       - 域控制器的 CIDR 1：192.168.1.0/24
       - 适用于域控制器的 CIDR 2：192.168.2.0/24

       为避免 IP 地址冲突，请确保您指定的托管 AD VPC CIDR 与您在公司网络中使用的任何其他私有子网 CIDR 不冲突。
     - VPN 技术（可选）：[Direc Connect/Direct t Connect 和 VPN]

- 您的网关的 BGP 自治系统编号 (ASN)：[客户提供的 ASN]
- 网关外部接口的互联网可路由的 IP 地址，该地址必须是静态的：[客户提供的 IP 地址]
- 您的 VPN 连接是否需要静态路由：[是/否]

2. AMS 为您提供 AD 环境的管理员账户密码，并要求您重置密码，这样 AMS 工程师就无法再访问您的 AD 环境了。
3. 要重置管理员帐户密码，请使用 Active Directory 用户和计算机 (ADUC) 连接到您的 Active Directory 环境。ADUC 和其他远程服务器管理工具 (RSAT) 应在您在非 AMS 基础架构上配置的管理主机上安装和运行。Microsoft 有保护此类管理主机的最佳实践。有关信息，请参阅实现安全的管理主机。您可以使用这些管理主机来管理 Active Directory 环境。
4. 在日常操作中，AMS 会管理 AWS 账户 直到 AWS Directory Service 方面的事情；例如 VPC 配置、AD 备份、AD 信任的创建和删除等。您使用和管理您的 AD 环境；例如，用户创建、群组创建、群组策略创建等。

有关最新的 RACI 表，请参阅 “查看服务说明” 中的 “角色和职责” 部分。

将 Active Directory 与 AMS AWS Identity and Access Management 角色联合

将您的目录与 AMS IAM 角色联合的目的是使企业用户能够使用其公司凭证与 AWS 管理控制台 和进行交互 AWS APIs，从而与 AMS 控制台和 APIs。

联合过程示例

此示例使用 Active Directory 联合身份验证服务 (AD FS)；但是，支持任何支持 AWS Identity and Access Management 联合身份验证的技术。有关 AWS 支持的 IAM 联合身份验证的更多信息，请参阅 IAM 合作伙伴和身份提供商以及联合。您的 CSDM 将帮助您完成此过程，这需要与您的 AD 团队和 AMS 共同努力。

有关集成 SAML 进行 API 访问的详细信息，请参阅此 AWS 博客《如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问》。

> **Note**
>
> 有关安装 AMS CLI 和 SAML 的示例，请参阅附录： ActiveDirectory 联合身份验证服务 (ADFS) 声明规则和 SAML 设置。

向 AMS 控制台配置联合 (SALZ)

下表中详述的 IAM 角色和 SAML 身份提供商（可信实体）已作为账户注册的一部分进行配置。这些角色允许您提交和监控 RFCs服务请求和事件报告，以及获取有关您的 VPCs 和堆栈的信息。

角色	身份提供商	权限
客户 _ _角色 ReadOnly	SAML	适用于标准 AMS 账户。允许您提交 RFCs 以更改 AMS 管理的基础架构，以及创建服务请求和事件。
客户管理的广告用户角色	SAML	适用于 AMS 托管活动目录账户。允许您登录 AMS 控制台以创建服务请求和事件（否 RFCs）。

有关不同账户下可用角色的完整列表，请参阅AMS 中的 IAM 用户角色。

入职团队的一名成员将您的联合身份验证解决方案中的元数据文件上传到预先配置的身份提供商。如果您想在兼容 SAML 的 IdP（身份提供商）（例如 Shibboleth 或 Active Directory 联合身份验证服务）之间建立信任，以便组织中的用户可以访问 AWS 资源，则可以使用 SAML 身份提供商。IAM 中的 SAML 身份提供商在具有上述角色的 IAM 信任策略中用作委托人。

虽然其他联合解决方案提供了 AWS 的集成说明，但 AMS 有单独的说明。使用以下博客文章《使用 Windows Active Directory、AD FS 和 SAML 2.0 启用与 AWS 的联合》，以及下面给出的修改，将使您的企业用户能够通过单个浏览器访问多个 AWS 账户。

根据博客文章创建信赖方信任后，按以下方式配置索赔规则：

- NameId: 关注博客文章。
- RoleSessionName: 使用以下值：
  - 声明规则名称： RoleSessionName
  - 属性存储：活动目录
  - LDAP 属性： SAM-Account-Name
  - 发出的索赔类型： https://aws.amazon.com/SAML/属性/ RoleSessionName
- 获取广告组：关注博客文章。
- 角色声明：关注博客文章，但对于自定义规则，请使用以下内容：

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

使用 AD FS 时，必须按照下表所示的格式为每个角色创建 Active Directory 安全组（customer_managed_ad_user_role 仅适用于 AMS 托管 AD 账户）：

组	角色
AWS-[AccountNo]-客户 _ _角色 ReadOnly	客户 _ _角色 ReadOnly
AWS-[AccountNo]-customer_managed_ad_user_role	客户管理的广告用户角色

有关更多信息，请参阅为身份验证响应配置 SAML 断言。

> **Tip**
>
> 要帮助进行故障排除，请下载适用于您的浏览器的 SAML tracer 插件。

向 AMS 提交联盟申请

如果这是您的第一个帐户，请与您的 CSDM C and/or loud Architect 合作，为您的身份提供商提供元数据 XML 文件。

如果您正在注册其他账户或身份提供商，并且可以访问管理账户或所需的应用程序帐户，请按照以下步骤操作。

1. 从 AMS 控制台创建服务请求，提供添加身份提供商所需的详细信息：
   - AccountId 将在哪个账户中创建新的身份提供商。
   - 所需的身份提供商名称（如果未提供），则默认为 customer-saml；通常，该名称必须与联合身份提供商中配置的设置相匹配。
   - 对于现有账户，请说明是应将新的身份提供者传播到所有现有的控制台角色，还是提供应信任新身份提供商的角色列表。

- 将从联合代理导出的元数据 XML 文件作为文件附件附加到服务请求。

2. 在您创建服务请求的同一个账户中，使用 CT-ID ct-1e1xtak34nx76（管理 | 其他 | 其他 | 其他 | 创建）创建一个新的 RFC，其中包含以下信息。

   - 标题：“<Name>账户 < AccountId > 的加载 SAML IDP”。
   - AccountId 将在哪个账户中创建身份提供商。
   - 身份提供者名称。
   - 对于现有账户：是否应将身份提供者传播到所有现有的控制台角色，还是应信任新身份提供者的角色列表。
   - 在步骤 1 中创建的服务请求的案例 ID，其中附加了元数据 XML 文件。

验证控制台访问权限

设置 ADFS 并拥有用于身份验证的 AMS 网址后，请按照以下步骤操作。

使用 Active Directory 联合服务 (ADFS) 配置，您可以按照以下步骤操作：

1. 打开浏览器窗口，进入为您的帐户提供的登录页面。您的账户的 ADFS IdpInitiatedSignOn页面随即打开。
2. 选择 “登录到以下任一站点” 旁边的单选按钮。登录网站选择列表变为活动状态。
3. 选择 s ignin.aws.amazon.com 网站并点击登录。输入您的凭证的选项已打开。
4. 输入您的 CORP 凭据，然后单击 “登录”。 AWS 管理控制台 开场了。
5. 将 AMS 控制台的 URL 粘贴到地址栏中，然后按 Enter。AMS 控制台打开。

验证 API 访问权限

AMS 使用 AWS API，其中包含一些特定于 AMS 的操作，您可以在 AMS API 参考中阅读这些操作。

AWS 提供了 SDKs 一些可供您访问的亚马逊网络服务工具。如果您不想使用 SDK，则可以直接调用 API。有关身份验证的信息，请参阅签署 AWS API 请求。如果您没有使用 SDK，也没有直接发出 HTTP API 请求，则可以使用 AMS CLIs 进行变更管理 (CM) 和 SKMS。

安装 AMS CLIs

有关安装用于 SAML 的 AWS Managed Services (AMS) CLI 的示例，请参阅附录： ActiveDirectory 联合身份验证服务 (ADFS) 声明规则和 SAML 设置。

如果您需要临时访问权限才能获取和安装 AWS Managed Services (AMS) SDKs，请参阅临时 AMS 控制台访问权限。

> **Note**
>
> 您必须具有管理员凭据才能执行此过程。

AWS CLI 是使用 AWS Managed Services (AMS) CLIs （变更管理和 SKMS）的先决条件。

1. 要安装 AWS CLI，请参阅安装 AWS 命令行界面，然后按照相应的说明进行操作。请注意，该页面底部有使用不同安装程序（Linux、MS Windows、mac O S、虚拟环境、捆绑安装程序（Linux、macOS 或 Unix）的说明。

   安装完成后，运行`aws help`以验证安装。

2. 安装 AWS CLI 后，要安装或升级 AMS CLI，请下载 AMS AMS C LI 或 AMS SDK 可分发文件 zip 文件并解压缩。您可以通过 AMS 控制台左侧导航栏中的开发者资源链接访问 AMS CLI 发行版。

3. README 文件提供了任何安装的说明。

   打开任一选项：

   - CLI zip：仅提供 AMS CLI。
   - 软件开发工具包压缩包：提供所有 AMS APIs 和 AMS CLI。

   对于 Windows，请运行相应的安装程序（仅限 32 位或 64 位系统）：

   - 32 位：ManagedCloudAPI_x86.msi
   - 64 位：ManagedCloudAPI_x64.msi

   对于 Mac/Linux，请运行以下命令运行名为:AWSManagedServices_InstallCLI.sh 的文件：。`sh AWSManagedServices_InstallCLI.sh`请注意，amscm 和 amsskms 目录及其内容必须与.sh 文件位于同一个目录中。AWSManagedServices_InstallCLI

4. 如果您的公司证书是通过与 AWS 的联合身份验证（AMS 默认配置）使用的，则必须安装可以访问您的联合身份验证服务的凭证管理工具。例如，您可以使用此 AWS 安全博客如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问来帮助配置您的凭证管理工具。

5. 安装完成后，运行`aws amscm helpaws amsskms help`并查看命令和选项。

> **Note**
>
> 必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的 “AMS 信息资源” 部分。您可能需要添加身份验证`--profile`选项；例如，`aws amsskms` *`ams-cli-command`* `--profile SAML`。您可能还需要添加该`--region`选项，因为所有 AMS 命令都将使用 us-east-1；例如。`aws amscm` *`ams-cli-command`* `--region=us-east-1`

在 VPC 级别安排 AMS 备份

分配目标实例的 VPC 中的 AWS Managed Services (AMS) 备份计划是在账户注册期间创建的，在 VPC 创建架构中使用默认标签。备份系统根据该 VPC 标签来安排快照的执行。可以通过创建服务请求来修改时间表。有关更多信息，请参阅 VPC 标签和默认值。

有关备份默认值，请参阅了解 AMS 默认值

SALZ：默认设置

您的 AWS Managed Services (AMS) 网络采用标准化方式配置，大多数服务均采用默认设置。

本节介绍 AMS 用于安全、访问、监控、日志记录、连续性以及修补和管理的默认设置。

有关基础架构成本的示例，请参阅基本组件。

中提供了防火墙规则 设置您的防火墙

端点安全 (EPS)

您在 AMS Advanced 环境中配置的资源自动包括安装端点安全 (EPS) 监控客户端。此过程可确保全天候监控和支持 AMS Advanced 管理的资源。此外，AMS Advanced 会监控所有代理活动，如果检测到任何安全事件，就会创建事件。

> **Note**
>
> 安全事件作为事件处理；有关更多信息，请参阅事件响应。

端点安全提供反恶意软件保护，具体而言，支持以下操作：

- EC2 向 EPS 注册的实例
- EC2 从 EPS 取消注册的实例
- EC2 实例实时反恶意软件保护
- EPS 代理启动的心跳
- EPS 恢复隔离的文件
- EPS 事件通知
- 每股收益报告

AMS Advanced 使用趋势科技实现端点安全 (EPS)。这些是默认 EPS 设置。要了解有关趋势科技的更多信息，请参阅趋势科技服务器深度安全防护系统帮助中心；请注意，非亚马逊链接可能会更改，恕不另行通知。

以下章节介绍了 AMS 高级多账户着陆区 (MALZ) 的默认设置；有关非默认 AMS 多账户着陆区 EPS 设置，请参阅 AMS 高级多账户着陆区 EPS 非默认设置。

> **Note**
>
> 你可以自备 EPS，请参阅 AMS 自带 EPS。

常规 EPS 设置

端点安全常规网络设置。

每股收益默认值

设置	Default
防火墙端口（实例的安全组）	EPS 趋势科技服务器深度安全防护系统管理中心代理 (DSMs) 必须打开端口 4120 Agent/Relay 才能与管理中心通信，为管理中心控制台打开端口 4119。EPS 中继必须打开端口 4122 Manager/Agent 才能与中继通信。不应为客户实例的入站通信打开特定的端口，因为代理会启动所有请求。

设置	Default
沟通方向	客户端/设备已启动
心跳间隔	十分钟
警报前错过的心跳次数	二
服务器时间之间允许的最大偏差（差）	无限制
对处于非活动状态（已注册但未联机）的虚拟机引发脱机错误	否
默认策略	基本政策（下文将介绍）
使用相同主机名激活多台计算机	被允许
已发出待定更新的警报	七天后
更新日程安排	AMS 的目标是趋势科技趋势科技服务器深度安全防护系统管理中心 (DSM) /趋势科技服务器深度安全防护系统客户端 (DSA) 软件更新的每月发布周期。但是，AMS 不维护更新的 SLA。在部署期间，AMS 开发团队在整个舰队范围内执行更新。 DSA/DSA 更新记录在趋势科技 DSM 系统事件中，AMS 默认在本地保留这些事件 13 周。有关供应商文档，请参阅趋势科技趋势科技服务器深度安全防护系统帮助中心中的系统事件。日志还会导出到亚马逊 CloudWatch的日志组/ aws/ams/eps/var/log/DSM .log。
更新源代码	趋势科技更新服务器 (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
删除事件或日志数据	事件和日志将在七天后从 DSM 数据库中删除。
代理软件版本已保留	最多五个

设置	Default
最新规则更新已保存	最多十个
日志存储	默认情况下，日志文件安全地存储在 Amazon S3 中，但您也可以将其存档到 Amazon Glacier，以帮助满足审计和合规要求。

基本政策

端点安全基础策略默认设置。

每股收益基本政策

设置	Default
已启用的模块	防恶意软件
已禁用的模块	网络信誉
	防火墙
	入侵防护
	完整性监控
	日志审查
	应用程序控制

反恶意软件

端点安全防恶意软件设置。

EPS 防恶意软件默认值

设置	Default	备注
实时扫描	扫描所有内容	隔离所有可疑病毒。启用 IntelliTrap 和

设置	Default	备注
	每 Day/All 天（24 小时）	spyware/grayware 保护。 间谍软件和灰色软件会触发防恶意软件并导致该项目被隔离。
手动扫描	扫描所有内容	必须请求，然后遵循默认的实时扫描配置。
预设扫描	扫描所有内容	定于每个月的最后一个星期日，早上 6 点。
智能防护	已禁用	不适用
隔离的文件	趋势科技趋势科技服务器深度安全防护系统管理中心 (DSM)	预留大约 1GB 的磁盘用于隔离。
扫描限制	趋势科技 DSM	扫描各种大小的文件。
允许的间谍软件或灰色软件	无	不适用
本地事件通知	是	不适用

安全组

在 AWS 中 VPCs，AWS 安全组充当虚拟防火墙，控制一个或多个堆栈（一个或一组实例）的流量。堆栈启动时，它会与一个或多个安全组相关联，这些安全组决定了允许哪些流量到达堆栈：

- 对于公有子网中的堆栈，默认安全组接受来自所有位置（互联网）的 HTTP (80) 和 HTTPS (443) 流量。这些堆栈还接受来自您的公司网络和 AWS 堡垒的内部 SSH 和 RDP 流量。然后，这些堆栈可以通过任何端口导出到互联网。它们还可以输出到您的私有子网和公有子网中的其他堆栈。

- 私有子网中的堆栈可以输出到私有子网中的任何其他堆栈，并且堆栈中的实例可以通过任何协议相互完全通信。

> **Important**
>
> 私有子网上堆栈的默认安全组允许私有子网中的所有堆栈与该私有子网中的其他堆栈通信。如果要限制私有子网内堆栈之间的通信，则必须创建描述限制的新安全组。例如，如果您想限制与数据库服务器的通信，使该私有子网中的堆栈只能通过特定端口从特定的应用程序服务器进行通信，请请求特殊的安全组。本节将介绍如何执行此操作。

默认安全组

MALZ

下表描述了堆栈的默认入站安全组 (SG) 设置。SG 名为“SentinelDefaultSecurityGroupPrivateOnly-vpc-id”，其中是 *ID* AMS 多账户着陆区账户中的 VPC ID。允许所有流量通过此安全组出站到 SentinelDefaultSecurityGroupPrivateOnly “mc-initial-garden-”（允许堆栈子网内的所有本地流量）。

第二个安全组 “” 允许所有流量出站到 0.0.0.0/0。SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> 如果您为 AMS 更改类型（例如 EC2 创建或 OpenSearch 创建域）选择安全组，则应使用此处描述的默认安全组之一，或者使用您创建的安全组。您可以在 AWS EC2 控制台或 VPC 控制台中找到每个 VPC 的安全组列表。

还有其他用于内部 AMS 目的的默认安全组。

AMS 默认安全组（入站流量）

类型	协议	端口范围	源
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnly （限制同一安全组成员的出站流量）

类型	协议	端口范围	源
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制出站流量）
HTTP、HS、SSH、	TCP	80/443（来源 0.0.0.0/0） 允许从堡垒访问 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制出站流量）
MALZ 堡垒：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客户提供的本地部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡垒：			
SSH	TCP	22	mc-initial-garden-LinuxBastion SG
SSH	TCP	22	mc-initial-garden-LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastion SG
RDP	TCP	3389	mc-initial-garden-WindowsBastion DMZSG

SALZ

下表描述了堆栈的默认入站安全组 (SG) 设置。SG 名为 “mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-*ID*”，其中*ID*是唯一标识符。允许所有流量通过此安全组出站到 SentinelDefaultSecurityGroupPrivateOnly “mc-initial-garden-”（允许堆栈子网内的所有本地流量）。

第二个安全组 “mc-initial-garden--” 允许所有流量出站到 0.0.0.0/0。SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> 如果您为 AMS 更改类型（例如 EC2 创建或 OpenSearch 创建域）选择安全组，则应使用此处描述的默认安全组之一，或者使用您创建的安全组。您可以在 AWS EC2 控制台或 VPC 控制台中找到每个 VPC 的安全组列表。

还有其他用于内部 AMS 目的的默认安全组。

AMS 默认安全组（入站流量）

类型	协议	端口范围	源
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnly（限制同一安全组成员的出站流量）
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制出站流量）
HTTP、HS、SSH、	TCP	80/443（来源 0.0.0.0/0） 允许从堡垒访问 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制出站流量）
MALZ 堡垒：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客户提供的本地部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡垒：			
SSH	TCP	22	mc-initial-garden-LinuxBastion SG
SSH	TCP	22	mc-initial-garden-LinuxBastion DMZSG

类型	协议	端口范围	源
RDP	TCP	3389	mc-initial-garden-WindowsBastion SG
RDP	TCP	3389	mc-initial-garden-WindowsBastion DMZSG

创建、更改或删除安全组

您可以请求自定义安全组。如果默认安全组不能满足您的应用程序或组织的需求，则可以修改或创建新的安全组。此类申请将被视为需要批准，并将由AMS运营团队进行审查。

要在堆栈之外创建安全组 VPCs，请使用`Deployment | Advanced stack components | Security group | Create (review required)`更改类型 (ct-1oxx2g2d7hc90) 提交 RFC。

要修改活动目录 (AD) 安全组，请使用以下更改类型：

- 添加用户：使用管理 | Directory Service | 用户和群组 | 将用户添加到群组 [ct-24pi85mjtza8k] 提交 RFC
- 要移除用户：使用管理 | Directory Service | 用户和群组 | 从群组中移除用户 [ct-2019s9y3nfml4] 提交 RFC

> **Note**
>
> 使用 “需要审核” 时 CTs，AMS 建议您使用 “尽快安排” 选项（在控制台中选择 “尽快”，在 AP I/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

查找安全组

要查找附加到堆栈或实例的安全组，请使用 EC2 控制台。找到堆栈或实例后，您可以看到与其关联的所有安全组。

有关在命令行中查找安全组并筛选输出的方法，请参阅`describe-security-groups`。

EC2 IAM 实例配置文件

实例配置文件是 IAM 角色的容器，您可以使用该容器在 EC2 实例启动时将角色信息传递给实例。

MALZ

有两个 AMS 默认实例配置文件customer-mc-ec2-instance-profile和customer-mc-ec2-instance-profile-s3。这些实例配置文件提供下表中所述的权限。

政策描述

配置文件	策略
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore ：允许 Ec2 实例使用 SSM 代理。
	AMSInstanceProfileLoggingPolicy ：允许 Ec2 实例将日志推送到 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy ：允许 Ec2 实例执行启动操作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy ：允许 Ec2 实例向 AMS 监控服务报告调查结果。
	AMSInstanceProfilePatchPolicy ：允许 Ec2 实例接收补丁。
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy ：允许 Ec2 实例使用 AMS 自带 EPS。
	AMSInstanceProfileLoggingPolicy ：允许 Ec2 实例将日志推送到 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy ：允许 Ec2 实例执行启动操作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy ：允许 Ec2 实例向 AMS 监控服务报告调查结果。
	AMSInstanceProfilePatchPolicy ：允许 Ec2 实例接收补丁。
	AMSInstanceProfileS3WritePolicy ：允许 Ec2 实例 read/write 访问客户的 S3 存储桶。

SALZ

有一个 AMS 默认实例配置文件`customer-mc-ec2-instance-profile`，用于授予 IAM 实例策略中的权限`customer_ec2_instance_profile_policy`。此实例配置文件提供下表中所述的权限。该配置文件向在实例上运行的应用程序授予权限，而不是向登录实例的用户授予权限。

策略通常包含多个语句，其中每个语句授予对不同资源集的权限或在特定条件下授予权限。

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。

EC2 默认 IAM 实例配置文件权限

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
亚马逊弹性计算云（亚马逊 EC2）			
EC2 消息操作	允许	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	允许在你的账户中执行 S EC2 ystems Manager 的消息传送操作。
Ec2 描述	允许	* (全部)	允许控制台显示您账户 EC2 中的配置详细信息。
我正在获取角色 ID	允许	GetRole	EC2 允许从`aws:iam::*:role/customer-*` 和获取您的 IAM ID `aws:iam::*:role/customer_*` 。
上传日志事件的实例	允许	创建日志组	允许在以下位置创建日志：`aws:logs:*:*:log-group:i-*`

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
		创建日志流	允许将日志流式传输到：`aws:logs:*:*:log-group:i-*`
CW for MMS	允许	DescribeAlarms, PutMetricAlarm, PutMetricData	CloudWatch 允许在您的账户中检索警报。 允许 CW 创建或更新警报并将其与指定指标关联。 允许 CW 向您的账户发布指标数据点。
Ec2 标签	允许	CreateTags, DescribeTags,	允许在您账户中的指定实例上添加、覆盖和描述标签。
明确拒绝 CW 日志	拒绝	DescribeLogStreams, FilterLogEvents, GetLogEvents	不允许列出、筛选或获取以下内容的日志流：`aws:logs:*:*:log-group:/mc/*`
亚马逊 S EC2 imple Systems Manager (SSM)			
SSM 操作	允许	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	允许在您的账户中使用各种 SSM 功能。

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
S3 中的 SSM 访问权限	允许	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	允许上的 SSM 获取和更新中的对象，中止向中多部分上传的多部分对象，并列出可供多部分上传的端口和存储桶。 EC2 `aws:s3:::mc-*-internal-*/aws/ssm*`
亚马逊 EC2 简单存储服务 (S3) Simple Storage Service			
在 S3 中获取对象	允许	获取 列表	允许 EC2 应用程序检索和列出您账户中 S3 存储桶中的对象。
客户加密日志 S3 访问权限	允许	PutObject	允许 EC2 应用程序更新中的对象 `aws:s3:::mc-*-logs-*/encrypted/app/*`
修补数据放置对象 S3	允许	PutObject	允许 EC2 应用程序将修补数据上传到您的 S3 存储桶，网址为 `aws:s3:::awsms-a*-patch-data-*`
将自己的日志上传到 S3	允许	PutObject	允许 EC2 应用程序将自定义日志上传到：`aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
明确拒绝 MC 命名空间 S3 日志	拒绝	GetObject* 看跌*	不允许 EC2 应用程序从以下位置获取或放置任何对象： `aws:s3:::mc-*-logs-*/encrypted/mc*` ， `aws:s3:::mc-*-logs-*/mc/*`， `aws:s3:::mc-a*-logs-*-audit/*`
明确拒绝 S3 删除	拒绝	* (全部)	不允许 EC2 应用程序对以下对象执行任何操作： `aws:s3:::mc-a*-logs-*/*` ， `aws:s3:::mc-a*-internal-*/*` ，
明确拒绝 S3 CFN 存储桶	拒绝	Delete*	不允许 EC2 应用程序从以下位置删除任何对象：`aws:s3:::cf-templates-*`
明确拒绝列出存储桶 S3	拒绝	ListBucket	不允许您列出来自以下内容的任何加密、审核日志或保留 (mc) 对象：`aws:s3:::mc-*-logs-*`
AWS Secrets Manager 在亚马逊 EC2			

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
趋势云一号秘密访问权限	允许	GetSecretValue	EC2 允许亚马逊访问 Trend Cloud One 迁移的机密： `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` ， `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` ， `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` ， `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service 在亚马逊 EC2			
Trend Cloud One 解密密钥	允许	Decrypt	EC2 允许亚马逊使用别名/-migration解 AWS KMS 密密钥 ams/eps/cloudone `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

如果您不熟悉 Amazon IAM 政策，请参阅 IAM 政策概述了解重要信息。

> **Note**
>
> 策略通常包含多个语句，其中每个语句授予对不同资源集的权限或在特定条件下授予权限。

监控指标默认值

下表显示了监控的内容和默认警报阈值。您可以通过变更管理变更请求 (RFC) 更改默认值。

> **Note**
>
> CloudWatch 2016 年 11 月 1 日推出了延长指标保留期。有关更多信息，请参阅CloudWatch 限制。

来自基线监控的警报

服务	安全警报	警报名称和触发条件	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，这些提醒可以直接发送到您的电子邮件中（如果您已选择加入 Direct-Customer-Alerts SNS 主题）。			
Application Load Balancer (ALB) 实例	否	RejectedConnectionCount 总和 > 0，持续 1 分钟，连续 5 次。	CloudWatch 如果因为负载均衡器达到最大值而被拒绝的连接数就会发出警报。
Application Load Balancer (ALB) 目标	否	TargetConnectionErrorCount 总和 > 0，持续 1 分钟，连续 5 次。	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。
亚马逊 EC2 实例 — Windows	否	SecureChannelFailure 在最后 15 个数据点中，有 10 个数据点大于 0.0。	CloudWatch 在 Windows 实例上发出警报，以便在安全通道连接失败时发出警报。

服务	安全警报	警报名称和触发条件	备注
Aurora 实例	否	CPUUtilization 大于 85%，持续 5 分钟，连续 2 次。	CloudWatch 警报。
AWS Backup	是	DeleteRecoveryPoint 意外的 IAM 角色委托人或 IAM 用户委托人删除了 AWS Backup 恢复点。	CloudWatch 事件。删除备份恢复点时发出。
AWS Outposts	是	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% 持续 5 分钟，连续 12 次。	CloudWatch 对 AWS Outposts 资源的实例系列容量可用性发出警报。
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% 持续 5 分钟，连续 12 次。	CloudWatch 对 AWS Outposts 资源的实例类型容量可用性发出警报。
		AMSOutpostsConnectedStatusConnectedStatus < 1，持续 5 分钟，连续 1 次。	CloudWatch AWS Outposts 服务链路连接时发出警报，少于 1 个计数受损。
		AMSOutpostsCapacityExceptionCapacityExceptions 0 表示 5 分钟，连续 1 次。	CloudWatch 实例启动时出现容量不足错误时发出警报 AWS Outposts .
EC2 实例-全部 OSs	否	CPUUtilization* 大于 95%，持续 5 分钟，连续 6 次。	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。

服务	安全警报	警报名称和触发条件	备注
		StatusCheckFailed > 0，持续 5 分钟，连续 3 次。	CloudWatch 警报。
		根卷使用情况 大于 95%，持续 5 分钟，连续 6 次。	
		非 root 卷使用情况 大于 85%，持续 5 分钟，连续 2 次。 默认情况下处于禁用状态；有关更多信息，请参阅https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info。	
		内存可用 * MemoryFree 小于 5%，持续 5 分钟，连续 6 次。	
	是	EPS恶意软件 在实例中发现了恶意软件。	CloudWatch 事件。
亚马逊 EC2 实例-Linux	否	根卷索引节点使用情况 连续 6 次，5 分钟内平均值大于 95%。	CloudWatch 警报。仅适用于 Linux 实例。

服务	安全警报	警报名称和触发条件	备注
		免费交换 * 内存交换 < 5%，持续 5 分钟，连续 6 次。	
ElastiCache 集群	否	CurrConnections = 65000	此警报通知 AMS ElastiCache 主机的最大连接限制。 CloudWatch 警报。如果您想更新此阈值，请联系 AMS 支持人员。

服务	安全警报	警报名称和触发条件	备注
ElastiCache 节点	否	CPUUtilization 平均值 > 预定义值，持续 2 次，持续 15 分钟。	CloudWatch 警报。默认值为 90。如果是 Redis，则根据实例类型使用以下值之一： • cache.t1.micro：90% • cache.m1.small：90% • cache.m1.medium：90% • cache.m1.large：45% • cache.m1.xlarge：22.5% • cache.m2.xlarge：45% • cache.m2.4xlarge：11.25% • cache.c1.xlarge：11.25% • cache.t2.micro：90% • cache.t2.small：90% • cache.t2.medium：45% • cache.m3.medium：90% • cache.m3.large：45% • cache.m3.xlarge：22.5% • cache.m3.2xlarge：11.25% • cache.r3.large：45% • cache.r3.xlarge：22.5% • cache.r3.2xlarge：11.25% • cache.r3.4xlarge：5.625% • cache.r3.8xlarge：2.8125%
ElastiCache 节点-内存缓存	否	SwapUsage 连续 5 次，5 分钟内最大值大于 50,000,000 字节。	CloudWatch 警报。仅适用于内存缓存。

服务	安全警报	警报名称和触发条件	备注
OpenSearch 集群	否	ClusterStatus.red 最大值为 >= 1，持续 1 分钟，连续 1 次。 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	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 Red 集群状态。
OpenSearch 域	否	KMSKey错误 >= 1 持续 1 分钟，连续 1 次。	CloudWatch 警报。用于在您的域中加密静态数据的 KMS 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 OpenSearch 服务服务的静态数据加密。
		ClusterStatus. 黄色 最大值为 >= 1，持续 1 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	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。
		FreeStorageSpace 最小值为 <= 20480，持续 1 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	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。
		ClusterIndexWritesBlocked >= 1 持续 5 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	集群正在阻止写入请求。要了解更多信息，请参阅 ClusterBlockException。

服务	安全警报	警报名称和触发条件	备注
		节点 最小值为 < x，持续 1 天 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	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。
		CPUUtilization 连续 3 次，15 分钟内平均值大于 80% 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	100% 的 CPU 利用率很常见，但是持续的高平均利用率是有问题的。考虑使用更大的实例类型或添加实例。
		JVMMemory压力 最大值为 >= 80%，持续 5 分钟，连续 3 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	如果使用量增加，群集可能会遇到内存不足错误。请考虑垂直扩展。Amazon ES 将实例内存的一半用于 Java 堆，堆大小不超过 32 GiB。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。
		大师 CPUUtilization 15 分钟内平均值大于 50%，连续 3 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	考虑为您的专用主节点使用更大的实例类型。由于专用主节点在集群稳定性和 blue/green 部署中的作用，因此其平均 CPU 使用率应低于数据节点。

服务	安全警报	警报名称和触发条件	备注
		主JVMMemory压力 最大 >= 80%，持续 15 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	考虑为您的专用主节点使用更大的实例类型。由于专用主节点在集群稳定性和 blue/green 部署中的作用，因此其平均 CPU 使用率应低于数据节点。
OpenSearch 实例	否	AutomatedSnapshotFailure 最大值为 >= 1，持续 1 分钟，连续 1 次。	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。参见红色集群状态。
弹性负载均衡实例	否	SurgeQueueLength 大于 100，持续 1 分钟，连续 15 次。	CloudWatch 如果有多余的请求等待路由，则发出警报。
		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。
		SpilloverCount > 1，持续 1 分钟，连续 15 次。	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。
GuardDuty 服务	是	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。	支持的 GuardDuty 查找类型列表位于 GuardDuty 活动查找类型上。

服务	安全警报	警报名称和触发条件	备注
Health	变化	AWS Health Dashboard	与 AMS 支持的基准服务相关的 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。
AWS Managed Microsoft AD	否	活动目录状态 AWS Managed Microsoft AD 实例发送活动状态事件。	服务事件。在事件发生后目录正常运行时发出。
		受损的目录状态 AWS Managed Microsoft AD 实例发送受损的目录状态事件。	服务事件。当目录以降级状态运行时发出。检测到一个或多个问题，可能有的目录操作未在完全有效地工作。
		无法操作的目录状态 AWS Managed Microsoft AD 实例发送无法操作的状态事件。	服务事件。当目录不起作用时发出。所有目录终端节点都报告有问题。
		正在删除目录状态 AWS Managed Microsoft AD 实例发送删除目录状态事件。	服务事件。当前正在删除目录时发出。
		失败的目录状态 AWS Managed Microsoft AD 实例发送失败状态事件。	服务事件。无法创建目录时发出。
		RestoreFailed 目录状态 AWS Managed Microsoft AD 实例发送恢复失败的目录状态事件。	服务事件。从快照恢复目录失败时发出。

服务	安全警报	警报名称和触发条件	备注
亚马逊 RDS 实例	否	当为数据库实例分配的存储空间用完时，将触发存储空间不足警报。	RDS-EVENT-0007，详情请参阅使用亚马逊 RDS 事件通知。
		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。	服务事件。RDS-EVENT-0031、Amazon RDS 事件类别和事件消息。
		未尝试故障切换 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。	服务事件。RDS-EVENT-0034、Amazon RDS 事件类别和事件消息。
		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，因此客户的操作是修改内存参数并重启数据库实例。	服务事件。RDS-EVENT-0035、Amazon RDS 事件类别和事件消息。
		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、Amazon RDS 事件类别和事件消息。
		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，请参阅排除 MySQL 只读副本问题。	服务事件。RDS-EVENT-0045、Amazon RDS 事件类别和事件消息。
		数据库实例读取复制已结束 只读副本上的复制已结束。	服务事件。RDS-EVENT-0057、Amazon RDS 事件类别和事件消息。

服务	安全警报	警报名称和触发条件	备注
		创建 statspack 用户账户时出错 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、Amazon RDS 事件类别和事件消息。
		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、Amazon RDS 事件类别和事件消息。
		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。
		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、Amazon RDS 事件类别和事件消息。
		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。
		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	RDS-EVENT-0089，请在 Amazon RDS 事件类别和事件消息中查看详情。

服务	安全警报	警报名称和触发条件	备注
		Aurora 无服务器数据库集群扩展失败时的通知服务。	RDS-EVENT-0143，请在 Amazon RDS 事件类别和事件消息中查看详情。
		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。
		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。
		此事件表示 RDS 实例存储无法自动扩展，自动扩缩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。
		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。
		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。
		RDS 无法为代理预调配容量，因为您的子网中没有足够的 IP 地址可用。	RDS-EVENT-0243，请在 Amazon RDS 事件类别和事件消息中查看详情。
		您的 AWS 账户的存储空间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。
		CPUUtilization 连续 2 次，15 分钟内 CPU 平均利用率大于 90%。	CloudWatch 警报。

服务	安全警报	警报名称和触发条件	备注
		DiskQueueDepth 总和大于 75，持续 1 分钟，连续 15 次。	
		FreeStorageSpace 连续 2 次，5 分钟内平均值小于 1,073,741,824 字节。	
		SwapUsage 连续 2 次，5 分钟内平均值 >= 104,857,600 字节。	
Amazon Redshift 集群	否	RedshiftClusterStatus 未处于维护模式时集群的生命值 < 1，持续 5 分钟。	1 表示集群运行状况良好。
Amazon Macie	是	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 Macie 警报类型的列表，请参阅分析亚马逊 Mac ie 调查结果。请注意，并非所有账户都启用 Macie。

默认日志保留和轮换

本节介绍 AMS 日志管理默认值；有关更多信息，请参阅日志管理。

- 轮换 = 实例内部的日志周转
- 保留期 = 我们在亚马逊日志和亚马逊简单存储服务 (S3) Simple Service 中保存 CloudWatch 日志的时间段

日志会根据需要保留在 CloudWatch 日志中（您可以对此进行配置），并保留在 S3 中。它们不会过期或被删除，并且受服务持久性的限制。有关 S3 持久性的详细信息，请参阅 Amazon S3 中的数据保护。

您可以请求更改所有日志的日志保留期，但 AWS CloudTrail 日志除外，出于审计和安全考虑，这些日志会无限期保存。

日志轮换是在实例内部配置的。默认情况下，如果操作系统和安全日志的容量超过 100MB，则每小时轮换一次，这样做是为了确保您在实例中不会出现磁盘不足的情况。

实例内部的日志代理将在线日志上传到 Lo CloudWatch gs，日志从那里存档到 S3。

日志以生成的原始格式存储在 CloudWatch Logs 和 S3 中，没有预处理。

连续性管理默认值

本节介绍 AMS 连续性管理默认值；有关 AMS 备份的更多信息，请参阅 AMS 用户指南连续性管理章节。

Backup 配置是在入职时完成的。这些是默认（推荐）备份设置。

VPC 标签和默认值

有关 AMS 备份的最新信息，请参阅连续性管理。

> **Important**
>
> 默认情况下， EC2 堆栈备份处于禁用状态（Backup = False）。您可以在创建实例时启用 EC2 实例备份，方法是在通过 RFC（CT ct-14027q0sjyt1h）请求 EC2 堆栈`Key: Backup, Value: True`时添加标签。如果要在创建实例后添加标签，请使用管理 | 高级堆栈组件 | 实例堆栈 | 更新 CT (ct-38s4s4tm4ic4u) 提交 RFC。 EC2

EC2 实例标签和默认值

EC2 堆栈备份标签指定堆栈是否需要附加 EBS 卷的快照。

标签 `Key: Backup`

标签 `Value: True, False`

默认情况下，值False为备份标签不存在，并且堆栈没有定时备份。

Key: Backup将标签更改为Value: True以启用备份，然后按照使用 VPC 备份标签设置的时间表完成备份。

> **Note**
>
> 标签值的大小写（仅限 Value）不敏感，因此 True/true 或 False/false 全部可以接受。

RDS 实例备份和默认值

Amazon 关系数据库 (RDS) Service 的默认值在堆栈模板中定义：

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

修补默认值

本节介绍了 AMS 修补默认值；有关 AMS 修补的更多信息，请参阅 AMS 用户指南补丁管理章节。

AMS 版本每月修补 AMIs 一次；所有新的堆栈请求都应使用最新的 AMS AMI 进行配置。

> **Important**
>
> AMS Patch Orchestrator 是一种基于标签的补丁，它使用 AWS Systems Manager (SSM) 功能来允许您标记实例或为您设置 AMS 标签，并使用基准和您配置的窗口对这些实例进行修补。要了解更多信息，请参阅 Patch Orchestrator：基于标签的修补模型。

AMS 标准、基于账户、补丁：对于每个拥有接收就地补丁的堆栈的账户，都会在 “补丁星期二” 之后不久发出即将发布的适用补丁的通知。该通知包含所有堆栈和适用补丁的列表以及建议的补丁窗口。对于关键补丁，窗口设置的时间不超过提前 10 天，标准修补的时间不超过提前 14 天。如果您不回复通知，则不会进行修补。如果您想排除某些补丁，请回复通知或提交服务请求。如果您在回复时同意修补，但没有特别要求不同的时间表，则会按照您收到的通知中所述应用补丁。

> **Note**
>
> 补丁服务通知是发送给账户联系人的电子邮件，其中包含指向 AWS Support 控制台的链接。您可以通过 AWS Support 控制台或 AMS 服务请求页面进行回复，在该页面中，通知显示为服务通知。

在 AMS 标准修补过程中，AMS 会执行以下操作：

1. 在建议的补丁窗口到来前 14 天，您会收到一条修补服务通知。修补服务通知通过电子邮件发送到您在账户中存档的联系人电子邮件地址。
2. 根据修补 EC2 通知中提供的堆栈列表识别堆栈中所有可访问的实例。在本例中，“可访问” 是指处于 “正在运行” EC2 状态且运行命令代理已完全 EC2 运行的实例。
3. AMS 执行修补的方式可以确保有足够数量的 EC2 实例同时运行（通过`healthy-host-threshold`设置进行配置），从而使堆栈保持正常运行。
4. 所有 EC2 实例的修补操作完成后，AMS 会将 RFC 更新为修补状态：成功、部分成功或失败。对于除 Success 之外的任何状态，系统都会创建一张工单，供操作员跟进修补结果并采取任何纠正措施。

验证 AMS 服务 (SALZ)

为了验证 AWS Managed Services (AMS) 服务是否按预期运行，本章介绍了您可以做的一些练习。

查找 AMS 账户设置

用于创建 AMS RFCs、设置日程安排和确定谁接收通知的账户设置。

有些设置是在入职期间创建的，需要服务请求才能更改。您应该记下这些账户信息，因为您将在与 AMS 通信时使用这些信息：

- 凭证：如果您需要检索 AMS 用户名或密码，请联系您的本地 IT 管理员——AMS 使用您的公司 Active Directory。
- 云服务交付经理 (CSDM)：此人是您与 AMS 的联络人，可以回答服务问题。您将在入职时获得此人的联系信息，并应将其提供给组织中与 AMS 互动的所有人。您可以期望从此人那里收到有关您的 AMS 服务的月度报告。
- 控制台访问权限：您可以通过专门为您的账户设置的 URL 访问 AMS 控制台。您可以从 CSDM 获取网址。

- AMS CLI：您可以通过 AMS 控制台开发者资源页面获取 AMS CLI，也可以通过 CSDM 获得的可分发软件包获取。获得发行版软件包后，请按照安装或升级 AMS CLI 中概述的步骤进行操作。
- 维护时段：您的维护时段决定何时对您的 EC2 实例进行修补。AWS Managed Services 维护窗口（或维护窗口）为 AWS Managed Services (AMS) 执行维护活动，并在太平洋时间每个月的第二个星期四下午 3 点至下午 4 点重复。AMS 可能会在 48 小时通知后更改维护时段。您可能在入职时选择了不同的时段，请记录您选择的维护时段。
- 监控：AMS 默认提供一组 CloudWatch 指标，但您也可以请求其他指标。如果你这样做，请记录下来。
- 日志：默认情况下，您的日志存储在 ams-a-*ACCOUNT_ID* log-management 中，*REGION*这是生成日志的区域。*REGION*
- 缓解：在入职时，AMS 会记录您选择的缓解措施，以防发现针对您的资源的恶意软件攻击。例如，联系某些人。让组织中与 AMS 互动的所有人都能获得这些信息。
- 区域：您可以在 AMS 控制台中查看 VPC 详情页面。您也可以在安装 AMS SKMS CLI 后运行此命令（此命令使用 SAML 配置文件，如果您的身份验证方法不同，请将其删除）：

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

AMS API/CLI（amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

在 AMS FQDNs 中查找

AWS Managed Services (AMSCTs) 访问权限更改类型 () 要求您的 AMS 信任域的完全限定域名或 FQDN，格式为。C844273800838.amazonaws.com要发现您的 AWS FQDN，请执行以下任一操作：

- AWS 控制台：在 AWS Directory Service 控制台的 “目录名称” 列中查看。

- CLI：登录域名时使用以下命令：

  Windows（返回用户和 FQDN）：

```
whoami /upn
```

  或 (DC+DC+DC=FQDN)

```
whoami /fqdn
```

  Linux：

```
hostname --fqdn
```

> **Note**
>
> AMS API/CLI（amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。`us-east-1`根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令`--region us-east-1`时进行添加。如果这是您的身份验证方法`--profile saml`，则可能还需要添加。

在 AMS 中查找可用区 (AZs)

可用区：所有账户都至少有两个可用区。要准确找到您的可用区名称，您必须先知道关联的子网 ID。

- AMS 控制台：如有必要 VPCs，在导航窗格中单击，然后单击相关的 VPC。在 VPCs 详细信息页面上，在子网表中选择相关的子网，打开带有关联可用区名称的子网详细信息页面。
- AMS SMS SMS API/CLI：

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> AMS API/CLI （amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

在 AMS 中查找 SNS 话题

您的 SNS 主题决定了在各种情况下谁会收到通知。AMS 提供有关 AMI 通知（参见带有 SNS 的 AMS AMI 通知）、 CloudWatch 警报和 EC2 资源（请参阅接收 AMS 生成的警报）等的 SNS 主题。要发现您现有的 SNS 话题，请执行以下操作：

- AWS 控制台：使用 SNS 控制台查看所有主题、应用程序和订阅以及消息图表。还可以创建、删除、订阅和发布主题。
- API/CLI（登录您的 AMS 账户后，需要 AWS CLI）：

  列出你的 SNS 话题：

  ```
  aws sns list-topics
  ```

  列出您的 SNS 订阅：

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> AMS API/CLI （amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

在 AMS 中查找备份设置

备份和快照由 AMS 通过本机AWS Backup服务进行管理。

配置通过 AWS Backup 计划进行管理。您可以 AWS Backup 制定多个计划，将带标签的资源与备份计划和保留策略相关联。要查找您的 AMS 账户 AWS Backup 设置，请使用 https://console.aws.amazon.com/backup 控制台或 AWS CLI 命令参考获取备份命令。

有关 AMS 和的更多信息 AWS Backup，请参阅连续性管理。

查找实例 ID 或 IP 地址

您需要一个实例 IP 地址才能登录实例。

- 要请求访问实例、登录实例或创建 AMI，您必须拥有实例 ID。对于 EC2 实例（独立实例或堆栈的一部分）或数据库实例，可以通过几种不同的方式查找 ID：
  - ASG 堆栈中实例的 AMS 控制台：在 RFC 详细信息页面上查看创建堆栈的 RFC。在 “执行输出” 部分，您将找到 ASG 堆栈的堆栈 ID，然后可以转到 EC2 控制台 A uto Scaling Gro ups 页面搜索该堆栈 ID 并为其查找实例。找到实例后，将其选中，页面底部将打开一个包含详细信息的区域，其中包含包括 IP 地址在内的详细信息。
  - 独立实例 EC2 或数据库 (DB) 实例的 AMS 控制台：在 RFC 详细信息页面上查看创建 EC2 堆栈或数据库实例的 RFC。在执行输出部分，您将找到实例 ID 和 IP 地址。
  - AWS EC2 控制台：
    1. 在导航窗格中，选择 Instances (实例)。将打开 “实例” 页面。
    2. 点击你想要 ID 的实例。实例详细信息页面打开并显示 ID 和 IP 地址。
  - AWS 数据库控制台：
    1. 在主页上，选择数据库实例。将打开 “实例” 页面。
    2. 筛选您想要 ID 的数据库实例。实例详细信息页面打开并显示 ID。
  - AMS CLI/API。

> **Note**
>
> 必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅用户指南中的 AMS 信息资源部分。您可能需要添加身份验证`--profile`选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该`--region`选项，因为所有 AMS 命令都将使用 us-east-1；例如。`aws amscm ams-cli-command --region=us-east-1`

> **Note**
>
> AMS API/CLI（amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

运行以下命令以获取堆栈执行输出详细信息：

```
aws amsskms get-stack --stack-id STACK_ID
```

输出如下所示， InstanceId 显示在底部附近Outputs（显示的值为示例）：

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
```

```
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```


DNS 友好的堡垒名称

MALZ

对于多账户着陆区 (MALZ)，将在 AMS 管理的 Active Directory 的 FQDN 中为堡垒创建 DNS 记录。AMS 根据需要取代 Linux 和 Windows 的堡垒。例如，如果必须部署新的堡垒 AMI，堡垒 DNS 记录会动态更新以指向新的有效堡垒。

1. 要访问 SSH (Linux) 堡垒，请使用如下所示的 DNS 记录：`sshbastion(1-4).Your_Domain.com`

   例如，域名为`Your_Domain`：

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`

2. 要访问 RDP (Windows) 堡垒，请使用像这样的 DNS 记录：。`rdp-Username.Your_Domain.com`

例如，其中用户名是alextest、demobob、或，域是*Your_Domain*.com：

- rdp-alex.*Your_Domain*.com
- rdp-test.*Your_Domain*.com
- rdp-demo.*Your_Domain*.com
- rdp-bob.*Your_Domain*.com

SALZ

单账户着陆区 (SALZ) 可根据需要取代 Linux 和 Windows 堡垒。例如，如果必须部署新的堡垒 AMI，堡垒 DNS 记录会动态更新以指向新的有效堡垒。

1. 要访问 SSH (Linux) 堡垒，请使用如下所示的 DNS 记录：sshbastion*(1-4)*.A*AccountNumber*.amazonaws.com.

   例如，账号在123456789012哪里：

   - sshbastion1.A123456789012.amazonaws.com
   - sshbastion2.A123456789012.amazonaws.com
   - sshbastion3.A123456789012.amazonaws.com
   - sshbastion4.A123456789012.amazonaws.com

2. 要访问 RDP (Windows) 堡垒，请使用像这样的 DNS 记录：。rdpbastion*(1-4)*.A*ACCOUNT_NUMBER*.amazonaws.com

   例如，账号在123456789012哪里：

   - rdpbastion1.A123456789012.amazonaws.com
   - rdpbastion2.A123456789012.amazonaws.com
   - rdpbastion3.A123456789012.amazonaws.com
   - rdpbastion4.A123456789012.amazonaws.com

查找堡垒 IP 地址

AMS 客户可以使用前面DNS 友好的堡垒名称描述的 SSH 和 RDP 堡垒，也可以使用堡垒 IP 地址。

要查找您账户的堡垒 IP 地址（SSH 和 RDP），请执行以下操作：

1. 仅适用于多账户 landing zone：登录共享服务账户。
2. 打开 EC2 控制台并选择运行实例。

   将打开 “实例” 页面。
3. 在顶部的筛选框中，输入 ssh-bastion 或 rdp-bastion。

   在顶部的筛选框中，输入 customer-ssh 或 customer- rdp 。

   将显示您账户的 SSH and/or RDP 堡垒。

   请注意，除了 SSH 堡垒外，您还可能在列表中看到 AMS 外围网络堡垒，但这些堡垒不可用。
4. 选择 SSH 或 RDP 堡垒。如果你使用的是 Windows 计算机并想登录 Linux 实例，则可以使用 SSH 堡垒。如果你想登录 Windows 实例，你可以使用 RDP 堡垒。如果你使用的是 Linux 操作系统并想登录 Windows 实例，你可以通过 RDP 隧道使用 SSH 堡垒（这样你就可以访问 Windows 桌面）。要从 Linux 操作系统访问 Linux 实例，您需要使用 SSH 堡垒。

EC2 实例：创建

您可以使用 AMS 控制台或 API/CLI 创建 EC2 具有更多卷的 Amazon EC2 和亚马逊。

创建堆栈

使用控制台创建 EC2 实例

下面显示了 AMS 控制台中的此更改类型。

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。

- 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。

3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 创建 EC2 实例

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

模板创建：

1. 将此更改类型的执行参数输出到 JSON 文件；此示例将其命名为 Create EC2 params.json：

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. 修改并保存 “创建EC2参数” 文件。例如，你可以用这样的东西替换内容：

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
     "Parameters": {
       "InstanceAmiId": "ami-1234567890EXAMPLE",
       "InstanceDetailedMonitoring": false,
       "InstanceEBSOptimized": false,
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 3000,
       "InstanceRootVolumeType": "gp3",
       "InstanceType": "t2.large",
       "InstanceUserData": "",
       "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
       "EnforceIMDSV2": "false"
     }
   }
   ```

3. 将 RFC 模板输出到当前文件夹中的一个文件中；此示例将其命名为 Create r EC2 fc.json：

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. 修改并保存创建 EC2 rfc.json 文件。例如，你可以用这样的东西替换内容：。

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. 创建 RFC，指定创建 EC2 Rfc 文件和创建EC2参数文件：

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

> **安全组**
>
> 从此更改类型的 3.0 版本开始，如果您指定自己的安全组，AMS 不会附加默认 AMS 安全组。如果您未在请求中指定自己的安全组，AMS 会附加 AMS 默认安全组。在之前的版本中，无论您是否提供了自己的安全组，AMS 都会附加默认安全组。
> 目前，如果您指定自定义安全组，则还必须为您的账户指定默认 AMS 安全组，`mc-initial-garden-SG-name`以及`mc-initial-garden-SG-name`。 IDs

> **实例类型**
>
> AMS 不推荐 t2.micro/ t3.micro 和 t2.nano/t 3.nano 类型。这些是较小的实例类型，可能会降低您的应用程序和 AMS 工具的性能。 EC2 除了应用程序工作负载外，实例还需要足够的容量来支持 EPS、SSM 和 Cloudwatch 等 AMS 工具。有关更多信息，请参阅为您的应用程序选择正确的 EC2 实例类型。

要创建包含更多卷的 EC2 堆栈，请参阅 EC2 堆栈 | 创建（包含其他卷）。

您最多可以添加 50 个标签，但要这样做，您必须启用其他配置视图。

如果需要，请参阅EC2 实例堆栈创建失败。

创建堆栈（包含其他卷）

使用控制台创建 EC2 实例和其他卷

下面显示了 AMS 控制台中的此更改类型。

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 创建 EC2 实例和其他卷

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID（示例仅显示必填参数）。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

模板创建：

1. 将此更改类型的执行参数输出到名为 Cre EC2 AVParams ate.json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
```

2. 修改并保存创建EC2AVParams 文件（示例显示了大多数参数）。例如，你可以用这样的东西替换内容：

```
{
"Description":      "EC2-Create-1-Addl-Volumes",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-nn8v8ffhcal611bmo",
"Name":             "My-EC2-1-Addl-Volume",
"TimeoutInMinutes": 60,
"Parameters":   {
    "InstanceAmiId":    "AMI_ID",
    "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
    "InstanceCoreCount": 1,
    "InstanceThreadsPerCore": 2,
    "InstanceDetailedMonitoring": "true",
    "InstanceEBSOptimized": "false",
    "InstanceProfile": "customer-mc-ec2-instance-profile",
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. 将 RFC 模板输出到当前文件夹中的一个文件中；此示例将其命名为 Cre EC2 AVRfc ate.json：

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. 修改并保存创建 EC2 AVRfc .json 文件。例如，你可以用这样的东西替换内容：

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. 创建 RFC，指定创建EC2AVRfc 文件和创建EC2AVParams 文件：

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

Important

这种变更类型有一个新版本 v 4.0，它使用了不同的变更类型 StackTemplateId（stm-nn8v8ffhcal611bmo）。如果您要在命令行提交带有此更改类型的 RFC，则这一点很重要。新版本引入了两个新参数（RootVolumeKmsKeyId和 CreditSpecification），并更改了一个现有参数（InstanceType）的默认值。

实例类型

- 如果选择指定内核数或线程数，则必须为两者都指定值。使用参数`InstanceCoreCount`和`InstanceThreadsPerCore`。要查找内核/线程的有效组合，请参阅每种实例类型的 CPU 内核和每 CPU 内核的线程。
- AMS 不推荐使用 t2.micro/t3. micro 或 t2.nano/t3.nano 实例类型。它们太小，除了您的业务工作负载外，还无法支持 EPS、SSM 和 Cloudwatch 等 AMS 工具。有关更多信息，请参阅为您的应用程序选择正确的 EC2 实例类型。

- 在 4.0 版本中，默认类型从 t2.large 提升到 t3.larg e。默认情况下，T3 实例以 “无限积分” 启动。即使实例消耗了所有 CPU 积分，您也不会遇到 CPU 限制的情况。相反，您可以选择 T2 实例并使用 CreditSpecification 无限制选项。
- 有关亚马逊的更多信息 EC2，包括尺寸建议，请参阅亚马逊弹性计算云文档。

要在创建更多卷后使用其他卷更新堆 EC2 栈，请参阅EC2 实例堆栈：更新（使用其他卷）

访问，请求

申请管理访问权限

使用控制台请求管理员访问权限

下图显示了 AMS 控制台中的此更改类型。

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。

5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 请求管理员访问权限

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

模板创建：

1. 将此更改类型的执行参数 JSON 架构输出到文件中；此示例将其命名为 GrantAdminAccessParams .json：

```
aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 GrantAdminAccessParams.json
```

修改并保存该 GrantAdminAccessParams 文件。例如，你可以用这样的东西替换内容：

```
{
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Username":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

请注意，该TimeRequestedInHours选项默认为一小时。您最多可以申请十二小时。

2. 将 RFC 模板输出到当前文件夹中的一个文件中；此示例将其命名为 GrantAdminAccessRfc .json：

```
aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
```

3. 修改并保存 GrantAdminAccessRfc .json 文件。例如，你可以用这样的东西替换内容：

```
{
"ChangeTypeId":         "ct-1dmlg9g1l91h6",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-Admin-Access-to-EC2-RFC"
}
```

4. 创建 RFC，指定 GrantAdminAccessRfc 文件和 GrantAdminAcessParams 文件：

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

要通过堡垒登录实例，请按照下一个步骤 “实例访问示例” 进行操作。

提示

> **Note**
>
> 您可以在访问请求到期之前提交其更新。有关信息，请参阅堆栈管理员访问权限 | 更新。
> 要登录属于 ASG 的实例，您需要请求访问 ASG 堆栈，这样您就可以访问所有关联的实例。

有关请求 ReadOnly 访问权限的示例，请参阅ReadOnly 访问权限：请求。

申请 ReadOnly 访问权限

使用控制台请求 ReadOnly 访问权限

下图显示了 AMS 控制台中的此更改类型。

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。

4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 请求 ReadOnly 访问权限

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数（内联提供执行参数时使用转义引号）发出 create RFC 命令，然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
```

```
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

模板创建：

1. 将此更改类型的执行参数 JSON 架构输出到文件中；此示例将其命名为 GrantReadOnlyAccessParams .json：

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   修改并保存该 GrantReadOnlyAccessParams 文件。例如，你可以用这样的东西替换内容：

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Usernames":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   请注意，该TimeRequestedInHours选项默认为一小时。您最多可以申请十二小时。

2. 将 RFC 模板输出到当前文件夹中的一个文件中；此示例将其命名为 GrantReadOnlyAccessRfc .json：

   ```
   aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
   ```

3. 修改并保存 GrantReadOnlyAccessRfc .json 文件。例如，你可以用这样的东西替换内容：

   ```
   {
   "ChangeTypeId":         "ct-199h35t7uz6jl",
   "ChangeTypeVersion":    "3.0",
   "Title":                "Request-ReadOnly-Access-to-EC2-RFC"
   }
   ```

4. 创建 RFC，指定 GrantReadOnlyAccessRfc 文件和 GrantReadOnlyAcessParams 文件：

   ```
   aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
   execution-parameters file://GrantReadOnlyAccessParams.json
   ```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

要通过堡垒登录实例，请按照下一个步骤 “实例访问示例” 进行操作。

提示

> **Note**
>
> 您可以在访问请求到期之前提交其更新。有关详细信息，请参阅堆栈只读访问权限 | 更新。要登录属于 A EC2 uto Scaling 组 (ASG) 的实例，您需要请求访问 ASG 堆栈，这样您就可以访问所有关联的实例。

有关请求管理员访问权限的演练，请参阅管理员访问权限：请求。

其他 | 其他 RFC，正在创建 (CLI)

此示例说明如何使用管理 | 其他 | 其他 | 创建 CT (ct-1e1xtak34nx76) 请求更改所有可用 CTs 地址。

当您找不到所需更改类型时，请使用此 CT；但是，如果您不确定是否要在现有 CT 中指定参数，则最好提交服务请求以寻求帮助。有关提交服务请求的信息，请参阅服务请求示例。

这种类型的 RFC 需要获得批准，这意味着它需要 AMS 批准才能实施。提交 RFC 后，AMS 操作员将与您联系，讨论您要部署的堆栈。

> **Note**
>
> 使用 “需要审核” 时 CTs，AMS 建议您使用 “尽快安排” 选项（在控制台中选择 “尽快”，在 AP I/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

所需数据：

- `Comment`: RFC 的用途。
- `ChangeTypeId`和`ChangeTypeVersion`：使用 Other | Create (`ct-1e1xtak34nx76`) 请求新资源，使用 Other | Update (`ct-0xdawir96cy7k`) 更改现有资源；两者都是`v1`。

可选数据:`Priority`: 可接受的值为`High`、`Medium`、或`Low`。

内联创建：

- 使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时使用转义引号）。示例使用“其他 | 创建”。

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- 使用创建 RFC 操作中返回的 RFC 编号提交 RFC。在提交之前，RFC 仍处于该`Editing`状态，不会被付诸行动。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- 监控 RFC 状态并查看执行输出：

```
aws amscm get-rfc --rfc-id RFC_ID
```

模板创建：

1. 为执行参数创建并保存一个 JSON 文件；示例将其命名为 OtherParams .json，并包含可选`Priority`参数：

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. 为 RFC 参数创建并保存一个 JSON 文件；示例将其命名为 OtherRfc .json。

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. 创建 RFC，指定 OtherRfc 文件和 OtherParams 文件：

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

您会在回复 RfcId 中收到新 RFC 的信息。例如：

```
{
"RfcId": "RFC-ID"
}
```

4. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC-ID
```

如果未报告错误，则表示操作成功。

5. 要监控请求的状态并查看执行输出，请执行以下操作：

```
aws amscm get-rfc --rfc-id RFC-ID
```

任何堆栈：删除、重启、启动、停止

您可以使用 AMS 控制台或 API/CLI 删除、重启、启动或停止 AMS 堆栈。

删除堆栈

使用控制台删除堆栈

AMS 控制台中此更改类型的屏幕截图：

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。

- 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。

3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 删除堆栈

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分

（不是执行参数）。--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

模板创建：

1. 将 RFC 模板输出到当前文件夹中的一个文件中；此示例将其命名为 DeleteStackRfc .json：

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. 修改并保存 DeleteStackRfc .json 文件。

   ExecutionParameters JSON 扩展中的内部引号必须使用反斜杠 (\) 进行转义。没有开始和结束时间的示例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. 创建 RFC：

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

> **Note**
>
> 如果删除 S3 存储桶，则必须先将其中的对象清空。

> **Important**
>
> 删除堆栈可能会带来意想不到和意想不到的后果。有关重要注意事项，请参阅删除堆栈的 RFC 疑难解答部分RFCs 。

重启堆栈

使用控制台重启堆栈

AMS 控制台中此更改类型的屏幕截图：

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。

4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 重启堆栈

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

模板创建：

1. 将 RFC 模板输出到当前文件夹中的一个文件中。此示例将其命名为 RebootStackRfc .json。请注意，由于只有一个用于停止（重启或启动）实例的执行参数，因此执行参数可以位于架构 JSON 文件本身中，无需创建单独的执行参数 JSON 文件。

```
aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
```

2. 修改并保存 RebootStackRfc .json 文件。

   `ExecutionParameters`JSON 扩展中的内部引号必须使用反斜杠 (\) 进行转义。示例：

```
{
"ChangeTypeId":          "ct-02u0hoaa9grat",
"Title":                 "Reboot-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. 创建 RFC：

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

   您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

有关应用程序负载均衡器的信息，请参阅应用程序负载均衡器。

启动堆栈

使用控制台启动堆栈

AMS 控制台中此更改类型的屏幕截图：

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 启动堆栈

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何CreateRfc参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

模板创建：

1. 将 RFC 模板输出到当前文件夹中的一个文件中。此示例将其命名为 StartInstanceRfc .json。请注意，由于只有一个用于启动堆栈的执行参数，因此执行参数可以位于架构 JSON 文件本身中，无需创建单独的执行参数 JSON 文件。

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. 修改并保存 StartStackRfc .json 文件。例如，你可以用这样的东西替换内容：

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. 创建 RFC：

```
aws amscm create-rfc --cli-input-json file://StartStackRfc.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

有关应用程序负载均衡器的信息，请参阅应用程序负载均衡器。

停止堆栈

使用控制台停止堆栈

AMS 控制台中此更改类型的屏幕截图：

它是如何运作的：

1. 导航到 “创建 RFC” 页面：在 AMS 控制台的左侧导航窗格中，单击RFCs打开 RFCs 列表页面，然后单击 “创建 R FC”。
2. 在默认的 “浏览更改类型” 视图中选择常用更改类型 (CT)，或者在 “按类别选择” 视图中选择 CT。
   - 按更改类型浏览：您可以单击 “快速创建” 区域中的常用 CT，立即打开 “运行 RFC” 页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

     要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击 “创建 RFC” 打开 “运行 RFC” 页面。如果适用，“创建 RFC” 按钮旁边会出现 “使用旧版本创建” 选项。
   - 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示 “使用旧版本创建” 选项（如果适用）。单击 “创建 RFC” 打开 “运行 RFC” 页面。
3. 在 “运行 RFC” 页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在 “浏览更改类型” 视图中选择 CT，则会为您填写此主题）。打开 “其他配置” 区域以添加有关 RFC 的信息。

   在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。
4. 完成后，单击 “运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。

5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 停止堆栈

它是如何运作的：

1. 使用 Inline Create（您发出包含所有 RFC 和执行参数的`create-rfc`命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出`create-rfc`命令。这里描述了这两种方法。
2. 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id` *`ID`* 命令。

   监控 RFC: `aws amscm get-rfc --rfc-id` *`ID`* 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> 您可以将任何`CreateRfc`参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`有关所有 CreateRfc 参数的列表，请参阅《AMS 变更管理 API 参考》。

内联创建：

使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时请转义引号），然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

模板创建：

1. 将 RFC 模板输出到当前文件夹中的一个文件中。此示例将其命名为 StopStackRfc .json。请注意，由于只有一个用于停止（重启或启动）实例的执行参数，因此执行参数可以位于架构 JSON 文件本身中，无需创建单独的执行参数 JSON 文件。

```
aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
```

2. 修改并保存 StopStackRfc .json 文件。例如，你可以用这样的东西替换内容：

```
{
"ChangeTypeId":          "ct-3dgbnh6gpst4d",
"Title":                 "Stop-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. 创建 RFC：

```
aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
```

   您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

除非您使用 AMS 资源计划程序计划重启，否则已停止的实例将保持停止状态。

如果需要，请参阅EC2 实例堆栈停止失败。

访问示例

这些示例显示了在获得 RFC 访问权限后，如何通过堡垒登录实例。有关授予访问权限的详细信息，请参阅访问请求。

> **Note**
>
> 通过 Auto Scaling 组创建的 EC2 实例将具有循环进出的 IP 地址，您必须使用 EC2 控制台来查找该 IP 地址。

所需数据：

- 堡垒 DNS 友好名称或 IP 地址：使用中所述的 DNS 友好名称DNS 友好的堡垒名称或按中所述查找堡垒 IP 地址。查找堡垒 IP 地址
- 用户名（例如 username@customerdomain.com）和密码：账户的凭证。
- 堆栈 IP 地址：要获取此信息，请查看 AMS 控制台堆栈页面，找到您要登录的堆栈，然后在 EC2 控制台中筛选您账户的堆栈 ID。对于单个 EC2 实例，您也可以使用 AMS SKMS 命令有关 AMS SKMS API 参考，请参阅 AWS Artifact 控制台中的 “报告” 选项卡。要查找堆栈 ID，然后要查看 AMS SKMS API 参考，请参阅 AWS Artifact 控制台中的 “报告” 选项卡。要查找堆栈 IP 地址。

根据需要访问堡垒 IP 地址（SSH 或 RDP），然后使用以下过程之一登录。

从 Linux 计算机到 Linux

使用 SSH 连接到 SSH 堡垒，然后连接到 Linux 实例。

MALZ

有关友好堡垒名称的更多信息，请参阅 DNS 堡垒。

要连接到 Linux 实例，您必须先连接到 SSH 堡垒。

1. 打开 shell 窗口并输入：

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

如果你的 domain_FQDN 是 “corp.domain.com”，你的账号是 “123456789123”，你的域名是 “amazonaws.com”，你选择堡垒 “4”，你的用户名是 “”，那会是这样：JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 使用您的公司活动目录凭据登录。
3. 当出现 Bash 提示时，使用 SSH 登录实例，然后输入：

```
ssh Domain_FQDN\\Username@Instance_IP
```

或者，你可以使用登录标志 (-l)：

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

有关友好堡垒名称的更多信息，请参阅 DNS 堡垒。

要连接到 Linux 实例，您必须先连接到 SSH 堡垒。

1. 打开 shell 窗口并输入：

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
    or SSH_BASTION_IP
```

如果你的账号是 123456789123，你选择堡垒 4，你的用户名是： JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 使用您的公司活动目录凭据登录。
3. 当出现 Bash 提示时，使用 SSH 登录实例，然后输入：

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

或者，你可以使用登录标志 (-l)：

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 计算机到 Windows 实例

使用 SSH 隧道和 RDP 客户端从你的 Linux 计算机连接到 Windows 实例。

MALZ

此过程需要适用于 Linux 的远程桌面连接客户端；该示例使用 Microsoft 远程桌面（用于连接到 Windows 远程桌面服务的开源 UNIX 客户端）。Rdesktop 是另一种选择。

> **Note**
>
> 登录 Windows 实例的方式可能会因所使用的远程桌面客户端而异。

首先建立 SSH 隧道，然后登录。

有关友好堡垒名称的更多信息，请参阅DNS 友好的堡垒名称。

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅访问请求。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).Your_Domain
```

如果你的 domain_FQDN 是 “corp.domain.com”，你的 AMS 管理的 Your_Domain_Domain 是 “amazonaws.com”，你选择堡垒 “4”，你的用户名是 “”，那会是这样：JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅查找实例 ID 或 IP 地址。

1. 通过 SSH 隧道设置 RDP，从 Linux 桌面到 Windows 实例。要使用正确的值发出ssh命令，有以下几种方法可以继续：

   - 在 Linux 外壳中，设置变量，然后输入 SSH 连接命令：

   ```
   BASTION="sshbastion(1-4).Your_Domain""
   WINDOWS="Windows_Instance_Private_IP"
   AD="AD_Account_Number"
   USER="AD_Username"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   例如，如果使用以下值：

   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

```
AD="ACORP_example"

USER="john.doe"
```

- 将变量值直接添加到ssh命令中。

无论哪种情况，呈现的请求都是这样（假设变量值相同）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. 任一：打开远程桌面客户端，输入环回地址和端口 127.0.0. 1:3389，然后打开连接。

   或者，从新的 Linux 桌面外壳登录到 Windows 实例。如果使用 RDesktop，则命令如下所示：

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows 实例的远程桌面窗口将显示在您的 Linux 桌面上。

   > **Tip**
   >
   > 如果远程桌面会话无法启动，请在步骤 1 中验证是否允许通过 shell 的端口 3389 通过 SSH 堡垒与 Windows 实例建立网络连接（适当替换private_ip_address_of_windows_instance）：
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 成功：
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >         netstat -anvp | grep 3389
   >         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

单账户登录区域的此过程需要适用于 Linux 的远程桌面连接客户端；该示例使用 Microsoft 远程桌面（用于连接到 Windows 远程桌面服务的开源 UNIX 客户端）。Rdesktop 是另一种选择。

> **Note**
>
> 登录 Windows 实例的方式可能会因所使用的远程桌面客户端而异。

首先建立 SSH 隧道，然后登录。

有关友好堡垒名称的更多信息，请参阅DNS 友好的堡垒名称。

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅访问请求。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

如果你的账号是 123456789123 然后你选择堡垒 4，那会是这样：

```
sshbastion4.A123456789123.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅查找实例 ID 或 IP 地址。

1. 通过 SSH 隧道设置 RDP，从 Linux 桌面到 Windows 实例。要使用正确的值发出ssh命令，有以下几种方法可以继续：

   - 在 Linux 外壳中，设置变量，然后输入 SSH 连接命令：

     ```
     BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
     WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
     AD="AD_ACCOUNT_NUMBER"
     USER="AD_USERNAME"
     ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
     ```

     例如，如果使用以下值：

     ```
     BASTION="sshbastion4.A123456789123.amazonaws.com"

     WINDOWS="172.16.3.254"

     AD="ACORP_example"
     ```

```
USER="john.doe"
```

- 将变量值直接添加到ssh命令中。

无论哪种情况，呈现的请求都是这样（假设变量值相同）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 任一：打开远程桌面客户端，输入环回地址和端口 127.0.0. 1:3389，然后打开连接。

   或者，从新的 Linux 桌面外壳登录到 Windows 实例。如果使用 RDesktop，则命令如下所示：

   ```
   rdesktop 127.0.0.1:3389
   ```

   Windows 实例的远程桌面窗口将显示在您的 Linux 桌面上。

   > **Tip**
   >
   > 如果远程桌面会话无法启动，请在步骤 1 中验证是否允许通过 shell 的端口 3389 通过 SSH 堡垒与 Windows 实例建立网络连接（适当替换private_ip_address_of_windows_instance）：
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```
   >
   > 成功：
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >         Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >         netstat -anvp | grep 3389
   >         tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

Windows 计算机到 Windows 实例

使用 Windows 远程桌面连接客户端从你的 Windows 计算机连接到 Windows 实例。

MALZ

有关友好堡垒名称的更多信息，请参阅DNS 友好的堡垒名称。

1. 打开远程桌面连接程序（标准的 Windows 程序），然后在“主机名”字段中输入 Windows 堡垒的友好 DNS 名称。

2. 选择连接。远程桌面连接尝试与堡垒建立 RDP 连接。

   如果成功，则会打开一个凭据对话框。要获得访问权限，请使用您的公司 Active Directory 凭据，就像使用 Windows 实例一样。

3. 在堡垒上打开远程桌面连接程序，输入要连接的 Windows 实例的 IP 地址（例如 10.0.0.100），然后选择 Connect。在连接到 Windows 实例之前，再次需要您的公司 Active Directory 凭据。

SALZ

有关友好堡垒名称的更多信息，请参阅DNS 友好的堡垒名称。

1. 打开远程桌面连接程序（标准的 Windows 程序），然后在主机名字段中输入 Windows 堡垒的友好 DNS 名称；例如`rdpbastion`*`(1-4)`*`.A`*`AMSAccountNumber`*`.amazonaws.com`，如果你的账号是 123456789123 并且你选择了堡垒 4，则该名称将如下所示。`rdpbastion4.A123456789123.amazonaws.com`

2. 选择连接。远程桌面连接尝试与堡垒建立 RDP 连接。

   如果成功，则会打开一个凭据对话框。要获得访问权限，请使用您的公司 Active Directory 凭据，就像使用 Windows 实例一样。

3. 在堡垒上打开远程桌面连接程序，输入要连接的 Windows 实例的 IP 地址（例如 10.0.0.100），然后选择 Connect。在连接到 Windows 实例之前，再次需要您的公司 Active Directory 凭据。

Windows 计算机到 Linux 实例

要从 Windows 环境中对 SSH 堡垒进行 RDP，请按照以下步骤操作。

MALZ

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅访问请求。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).YOUR_DOMAIN
```

如果 YOUR_DOMAIN 是 myamsaddomain.com” 然后你选择堡垒 4，那会是这样：

```
sshbastion4.myamsaddomain.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅查找实例 ID 或 IP 地址。

要从 Windows 计算机连接到 Linux 实例，必须先连接到 SSH 堡垒。

使用原生 Windows OpenSSH 客户端或者在本地计算机上安装 P uTTY。要了解有关 OpenSSH 的更多信息，请参阅 Windows 中的 Op en SSH。

1. 使用本机 Windows 或打开 PuTTY 并输入 SSH 堡垒的主机名或 SSH 堡垒的 IP 地址。例如，10.65.2.214（22 是用于 SSH 的端口；默认情况下将设置该端口）。
2. OpenSSH 或 PuTTY 尝试通过 SSH 连接到堡垒并打开外壳窗口。
3. 使用您的公司 Active Directory 凭据来获得访问权限，就像使用 RDP 主机一样。
4. 当出现 Bash 提示时，使用 SSH 进入实例。输入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅访问请求。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

如果你的账号是 123456789123 然后你选择堡垒 4，那会是这样：

```
sshbastion4.A123456789123.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅查找实例 ID 或 IP 地址。

要从 Windows 计算机连接到 Linux 实例，必须先连接到 SSH 堡垒。

使用原生 Windows OpenSSH 客户端或者在本地计算机上安装 P uTTY。要了解有关 OpenSSH 的更多信息，请参阅 Windows 中的 Op en SSH。

1. 使用本机 Windows 或打开 PuTTY 并输入 SSH 堡垒的主机名或 SSH 堡垒的 IP 地址。例如，10.65.2.214（22 是用于 SSH 的端口；默认情况下将设置该端口）。
2. OpenSSH 或 PuTTY 尝试通过 SSH 连接到堡垒并打开外壳窗口。
3. 使用您的公司 Active Directory 凭据来获得访问权限，就像使用 RDP 主机一样。
4. 当出现 Bash 提示时，使用 SSH 进入实例。输入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

举报事件

使用 AMS 控制台报告事件。为每个新问题或问题创建一个新事件很重要。在打开与旧查询相关的案例时，提供相关的案例编号会很有帮助，这样我们就可以参考以前的信件。

> **Note**
>
> 如果案例信件偏离了原始问题，AMS 操作员可能会要求您举报新的事件。

要使用 AMS 控制台报告事件，请执行以下操作：

1. 从左侧导航栏中选择 “事件”

   事件列表打开：

如果您的事件列表为空，则清除筛选器选项会将过滤器重置为 “任意” 状态。

如果您知道要使用电话或聊天，请单击 “在支持中心创建事件”，在 Support Center Console 中打开事件创建页面，该页面会自动填充 AMS 服务类型。

> **Important**
>
> - 以开头的电话 支持 会被录音，以便更好地提高响应能力。如果来电掉线，你必须通过 Support Center 案例回电， AWS 没有回电的机制。
> - 电话和聊天支持旨在帮助解决支持案例、事件和服务请求，而不是 RFC 或安全问题。
> - 对于 RFC 问题，请使用相关 RFC 详细信息页面上的通信选项联系 AMS 工程师。
> - 对于安全问题，请创建高优先级（P1 或 P2）支持案例。实时聊天功能不适用于安全事件。

2. 如果要查找现有事件，请在下拉列表中选择事件状态筛选器。

	• 所有尚未解决的事件。 • 尚未分配的新事件。 • 已分配的事件。 • 你重新审理的事件。 • 一个已分配的、复杂的事件。 • 需要您在下一步之前提供反馈的事件。 • 您最近提交信息的事件。 • 一个已经结束的事件。 • 账户中的所有事件。

3. 选择创建。

   创建事件页面打开：

4. 选择优先级：

- 低：您的业务服务或应用程序中与 AWS/AMS 资源相关的非关键功能受到影响。
- 中：与 AWS/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。您的应用程序中与 AWS/AMS 资源相关的关键功能不可用。专为影响生产系统的最严重的停机而设计。

5. 选择一个类别。

> **Note**
>
> 如果您要测试事件功能，请在事件标题中添加不采取行动标志 (AMSTestNoOpsActionRequired)。

6. 输入以下信息：

- 主题：事件报告的描述性标题。
- 抄送电子邮件：一份电子邮件地址列表，供你想向其通报事件报告和解决方案的人使用。
- 详细信息：全面描述事件、受影响的系统以及解决方案的预期结果。回答预设的问题，或者将其删除并输入任何相关信息。

要添加附件，请选择 “添加附件”，浏览到所需的附件，然后单击 “打开”。要删除附件，请单击 “删除” 图
标：
。

7. 选择提交。

将打开一个详细信息页面，其中包含有关事件的信息，例如类型、主题、已创建、ID 和状态，以及一个包含您创建的请求描述的 “通信” 区域。

单击 “回复” 以打开通信区域，并提供更多详细信息或状态更新。

事件解决后，单击 “关闭案例”。

如果信件数量超过一页所能容纳的信件数量，请单击 “加载更多”。

别忘了给沟通打分！

您的事件将显示在事件列表页面上。

创建服务请求

要使用 AWS Managed Services (AMS) 控制台创建服务请求，请执行以下操作：

1. 从左侧导航栏中选择 “服务请求”。

   服务请求列表打开。

   如果您的服务请求列表为空，则清除筛选器选项会将筛选器重置为 “任意” 状态。

   如果您知道要使用电话或聊天，请单击 Support Cent er 中的 “创建服务请求”，在 Supp ort Center Console 中打开服务请求创建页面，该页面会自动填充 AMS 服务类型。

   > **Note**
   >
   > 通过 支持 中心发起的电话会被录音，以更好地提高响应能力。如果来电掉线，你必须通过 Support Center 案例回电， AWS 没有回电的机制。

   > **Important**
   >
   > 电话和聊天支持旨在帮助处理支持案例、事件和服务请求。如果 RFC 问题，请使用相关 RFC 详细信息页面上的通信选项联系 AMS 工程师。

2. 如果要查找现有服务请求，请在下拉列表中选择服务请求状态筛选器。

	• 所有尚未解决的服务请求。 • 尚未分配的新服务请求。 • 已分配的服务请求。 • 您重新打开的服务请求。 • 已分配的、复杂的服务请求。 • 需要您在下一步之前提供反馈的服务请求。 • 您最近向其提交信息的服务请求。 • 服务请求已结束。

- 账户中的所有服务请求。

3. 选择创建。

   将打开 “创建服务请求” 页面。

4. 选择一个类别。

   > **Note**
   >
   > 如果您要测试服务请求功能，请在服务请求标题中添加无操作标志AMSTestNoOpsActionRequired。

5. 输入以下信息：

   - 主题：这将在列表页上创建指向服务请求详细信息的链接。
   - 抄送电子邮件：除了您的默认电子邮件联系人外，这些电子邮件还会接收信件。
   - 详情：请在此处提供尽可能多的信息。

   要添加附件，请选择 “添加附件”，浏览到所需的附件，然后单击 “打开”。要删除附件，请单击 “删除” 图标：。

6. 选择提交。

   将打开一个详细信息页面，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，以及一个包含您创建的请求描述的通信区域。

   此外，您的服务请求会显示在服务请求列表页面上。当您收到警报但尚未收到来自 AMS 的消息时，请使用此选项。

   单击 “回复” 以打开通信区域并提供更多详细信息或状态更新。

   服务请求解决后，单击 “解决问题”。

   单击 “加载更多” 可查看不适合初始页面的其他信件。

   别忘了给沟通打分！

对于账单相关查询，请使用 AMS 控制台中的其他类别；AMS CM API `ChangeTypeId` `ct-1e1xtak34nx76` 中的或 AWS Support API `IssueType=AMS` 中的。

入职后的步骤

既然您已经注册了 AMS 账户，您需要阅读更多 AMS 文档。请参阅以下文档：

- 接下来，使用 HA 双层堆栈 CT 创建功能齐全的 WordPress 堆栈的教程提供了完整的 AMS 体验。
- AMS 用户指南：AMS 用户指南描述了 AMS 的功能，列出了关键术语、操作、接口，并概述了典型的 AMS 托管基础设施架构。此外，还提供了访问管理详细信息和 AMS 默认值。还提供了有关如何使用 AMS 变更管理系统的详细说明，并提供了一些演练。还描述了其他管理概念。
- AMS API 参考：此 API 参考提供了所有 API 调用的描述，包括请求、响应和示例。
- AMS 应用指南：《AMS 应用指南》描述了在 AMS 中部署和维护应用程序的不同选项和方法。

教程

以下教程详细介绍了使用高可用性（高级）CT（ct-06mjngx5flwto）、使用 CLI 和使用控制台创建两层堆栈的步骤。提供了有关部署 Linux Auto Scaling 组 (ASG) 和部署 Windows ASG 的教程。

所有 CT 选项（包括）的描述均 ChangeTypeId 可在 AMS 更改类型参考中找到。

CLI 教程：高可用性双层堆栈 (Linux/RHEL)

本节介绍如何使用 AMS CLI 将高可用性 (HA) 双层堆栈部署到 AMS 环境中。

> **Note**
>
> 本部署演练已在 AMZN Linux 和 RHEL 环境中进行了测试。

任务和所需任务摘要 RFCs：

1. 创建基础架构（HA 双层堆栈）
2. 为 CodeDeploy 应用程序创建 S3 存储桶
3. 创建 WordPress 应用程序包并将其上传到 S3 存储桶
4. 使用部署应用程序 CodeDeploy

5. 访问该 WordPress 网站并登录以验证部署

开始前的准备工作

部署 | 高级堆栈组件 | 高可用性双层堆栈高级 | 创建 CT 可创建 Auto Scaling 组、负载均衡器、数据库以及 CodeDeploy 应用程序名称和部署组（与您为应用程序指定的名称相同）。有关信息，CodeDeploy 请参阅什么是 CodeDeploy？

本演练使用高可用性双层堆栈（高级）RFC，其中包括 UserData 并描述了如何创建可部署的 WordPress CodeDeploy 捆绑包。

示例中UserData显示的通过查询 http://169.254.169.254/latest/meta-data/ 上提供的实例元数据服务，从正在运行的实例中获取 EC2 实例元数据，例如实例 ID、区域等。用户数据脚本中的这一行：`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`，将可用区名称从元数据服务检索到我们支持区域的 $REGION 变量中，并使用它来填写下载代理的 S3 存储桶的 URL。 CodeDeploy 169.254.169.254 IP 只能在 VPC 内路由（所有人都可以查询该服务）。 VPCs 有关该服务的信息，请参阅实例元数据和用户数据。另请注意，以身份输入 UserData 的脚本以 “root” 用户身份执行，不需要使用 “sudo” 命令。

本演练将以下参数保留为默认值（如图所示）：

- Auto Scaling 群组：`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`。
- Load Balancer：`HealthCheckInterval=30, HealthCheckTimeout=5`。
- 数据库：`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`。

- 应用程序：DeploymentConfigName=CodeDeployDefault.OneAtATime。
- S3 存储桶：AccessControl=Private。

其他设置：

RequestedStartTimeRequestedEndTime如果你想安排 RFC：你可以使用 Time.is 来确定正确的 UT C 时间。必须对所提供的示例进行适当调整。如果开始时间已过，RFC 将无法继续。或者，您可以省略这些值以创建一个 ASAP RFC，该RFC将在批准通过后立即执行。

> **Note**
>
> 您可以选择设置许多与所示不同的参数。示例中显示的这些参数的值已经过测试，但可能不适合您。

创建基础架构

在开始之前收集以下数据可以加快部署速度。

必需的数据有堆栈：

- AutoScalingGroup:
  - UserData：本教程中提供了此值。它包括为其设置资源 CodeDeploy 和启动 CodeDeploy 代理的命令。
  - AMI-ID：此值决定了您的 Auto Scaling 组 (ASG) 将启动哪种 EC2 实例。请务必在您的账户中选择以 “customer-” 开头且具有所需操作系统的 AMI。 IDs 使用 AMS SKMS API 参考查找 AMI，请参阅 AWS Artifact 控制台的 “报告” 选项卡。操作 (CLI: list-amis) 或 AMS 控制台-> 详情页面。VPCs VPCs 本演练适用于 ASGs 配置为使用 Linux AMI。
- 数据库：
  - 尽管示例中显示的值已经过测试，但这些参数EngineVersion、、和LicenseModel应根据您的情况进行设置。DBEngine
  - 部署应用程序包时需要MasterUserPassword这些参数RDSSubnetIdsDBNameMasterUsername、、、和。对于 RDSSubnet ID，请使用两个私有子网。
- LoadBalancer:
  - 尽管示例中显示的值已经过测试，但这些参数EngineVersion、、和LicenseModel应根据您的情况进行设置。DBEngine

  - ELBSubnetIds：使用两个公有子网。
- 应用程序：该ApplicationName值设置 CodeDeploy 应用程序名称和 CodeDeploy 部署组名称。你可以用它来部署你的应用程序。它在账户中必须是唯一的。要查看您的账户中的 CodeDeploy 姓名，请访问 CodeDeploy 控制台。该示例使用 “WordPress”，但是，如果您要使用该值，请确保该值尚未被使用。

此过程使用高可用性双层堆栈（高级）CT（ct-06mjngx5flwto）和创建 S3 存储 CT（ct-1a68ck03fn98r）。在经过身份验证的账户中，在命令行中执行以下步骤。

1. 启动基础架构堆栈。

   a. 将 HA 双层堆栈 CT 的执行参数 JSON 架构输出到当前文件夹中名为 CreateStackParams .json 的文件中。

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

   b. 修改架构。根据需要*variables*更换。例如，对于 ASG 将要创建的 EC2 实例，使用所需的操作系统。记录下来ApplicationName，因为您稍后将使用它来部署应用程序。请注意，您最多可以添加 50 个标签。

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
```

```
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. 将 CreateRfc JSON 模板输出到当前文件夹中名为 CreateStackRfc .json 的文件中：

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. 按如下方式修改 RFC 模板并保存，即可删除和替换内容。请注意，RequestedStartTime和现在RequestedEndTime是可选的；排除它们会创建一个 ASAP RFC，该RFC在获得批准后立即执行（通常会自动发生）。要提交计划的 RFC，请添加这些值。

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. 创建 RFC，指定 CreateStackRfc .json 文件和.js CreateStackParams on 执行参数文件：

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

您在响应中收到 RFC ID。保存 ID 以供后续步骤使用。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

如果 RFC 成功，则不会收到任何输出。

g. 要检查 RFC 状态，请运行

```
aws amscm get-rfc --rfc-id RFC_ID
```

记下 RFC ID。

2. 启动 S3 存储桶

在开始之前收集以下数据可以加快部署速度。

必需的数据 S3 存储桶：

- VPC-ID：此值决定您的 S3 存储桶将位于何处。使用您之前使用的 VPC ID。
- BucketName：此值设置 S3 存储桶名称，您可以使用它来上传您的应用程序包。它在账户所在区域内必须是唯一的，并且不能包含大写字母。不要求将您的账户 ID 作为其中的 BucketName 一部分，但可以更轻松地在以后识别存储桶。要查看账户中存在哪些 S3 存储桶名称，请访问您的账户的 Amazon S3 控制台。

a. 将 S3 存储创建 CT 的执行参数 JSON 架构输出到名为 createS3 StoreParams .json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3StoreParams.json
```

b. 按如下方式修改架构，可以删除和替换其中的内容。*VPC_ID*适当地更换。示例中的值已经过测试，但可能不适合您。

> **Tip**
>
> 在账户所在区域内BucketName必须是唯一的，并且不能包含大写字母。不要求将您的账户 ID 作为其中的 BucketName 一部分，但可以更轻松地在以后识别存储桶。要查看账户中存在哪些 S3 存储桶名称，请访问您的账户的 Amazon S3 控制台。

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. 将的 JSON 模板输出 CreateRfc 到当前文件夹中名为 createS3 StoreRfc .json 的文件中：

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. 修改并保存 createS3 StoreRfc .json 文件，你可以删除和替换其中的内容。请注意，RequestedStartTime和现在RequestedEndTime是可选的；排除它们会创建一个 ASAP RFC，该RFC在获得批准后立即执行（通常会自动发生）。要提交计划的 RFC，请添加这些值。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. 创建 RFC，指定 createS3 StoreRfc .json 文件和 createS3 .json StoreParams 执行参数文件：

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

您会在回复 RfcId 中收到新 RFC 的信息。保存 ID 以供后续步骤使用。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，则不会收到任何输出。

g. 要检查 RFC 状态，请运行

```
aws amscm get-rfc --rfc-id RFC_ID
```

创建、上传和部署应用程序

首先，创建 WordPress 应用程序包，然后 CodeDeploy CTs 使用创建和部署应用程序。

1. 下载 WordPress、解压缩文件并创建. /scripts 目录。

   Linux 命令：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows：粘贴`https://github.com/WordPress/WordPress/archive/master.zip`到浏览器窗口并下载 zip 文件。

   创建用于组装软件包的临时目录。

   Linux：

   ```
   mkdir /tmp/WordPress
   ```

   Windows：创建一个 “WordPress” 目录，稍后将使用该目录路径。

2. 将 WordPress 源代码解压缩到 “WordPress” 目录并创建一个。 /scripts 目录。

   Linux：

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   ```

```
rm -f master
cd /tmp/WordPress
mkdir scripts
```

Windows：转到你创建的 “WordPress” 目录并在那里创建一个 “脚本” 目录。

如果您在 Windows 环境中，请务必将脚本文件的中断类型设置为 Unix (LF)。在 Notepad ++ 中，这是窗口右下角的一个选项。

3. 在 WordPress 目录中创建 CodeDeploy appsec.yml 文件（如果复制示例，请检查缩进，每个空格都很重要）。重要：确保将 WordPress 文件（在本例中为 WordPress 目录中）复制到预期目标 (/var/www/html/WordPress) 的 “源” 路径是正确的。在示例中，appsec.yml 文件位于文件所在的目录中，因此只需要 “/”。 WordPress 另外，即使你在 Auto Scaling 组中使用了 RHEL AMI，也要保留 “操作系统：linux” 一行不变。appspec.yml 文件示例：

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. 在中创建 bash 文件脚本。 WordPress /scripts 目录。

首先，`config_wordpress.sh`使用以下内容创建（如果您愿意，可以直接编辑 wp-config.php 文件）。

> **Note**
>
> *DBName*替换为 HA 堆栈 RFC 中给出的值（例如，wordpress）。
> *DB_MasterUsername*替换为 HA 堆栈 RFC 中给出的MasterUsername值（例如，admin）。
> *DB_MasterUserPassword*替换为 HA 堆栈 RFC 中给出的MasterUserPassword值（例如，p4ssw0rd）。
> 在 HA 堆栈 RFC 的执行输出中替换*DB_ENDPOINT*为终端节点 DNS 名称（例如srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com）。你可以通过GetRfc操作（CLI：get-rfc--rfc-id RFC_ID）或之前提交的 HA Stack RFC 的 AMS 控制台 RFC 详情页面中找到这一点。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 在同一个目录中创建install_dependencies.sh包含以下内容的内容：

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS 是在启动时作为用户数据的一部分安装的，以便运行状况检查从一开始就起作用。

6. 在同一个目录中创建start_server.sh包含以下内容的内容：

- 对于亚马逊 Linux 实例，请使用以下命令：

```
#!/bin/bash
service httpd start
```

- 对于 RHEL 实例，请使用以下命令（额外的命令是允许 SELINUX 接受的策略）： WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. 在同一个目录中创建`stop_server.sh`包含以下内容的内容：

```
#!/bin/bash
service httpd stop
```

8. 创建 zip 捆绑包。

   Linux：

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows：前往 “WordPress” 目录选择所有文件并创建一个 zip 文件，一定要将其命名为 wordpress.zip。

1. 将应用程序包上传到 S3 存储桶。

   要继续部署堆栈，捆绑包需要准备就绪。

   您可以自动访问自己创建的任何 S3 存储桶实例。您可以通过堡垒或 S3 控制台访问它，然后上传 WordPress 捆绑包 drag-and-drop或浏览并选择 zip 文件。

   您也可以在 shell 窗口中使用以下命令；请确保您的 zip 文件路径正确：

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. 部署 WordPress 应用程序包。

   在开始之前收集以下数据可以加快部署速度。

   必填数据：

   - VPC-ID：此值决定您的 S3 存储桶将位于何处。使用您之前使用的 VPC ID。
   - CodeDeployApplicationName和CodeDeployApplicationName：你在 HA 2 层堆栈 RFC 中使用的ApplicationName值设置 CodeDeployApplicationName 和。CodeDeployDeploymentGroupName该示例使用 “WordPress”，但您可能使用了不同的值。
   - S3Location: 对于 S3BucketBucketName，请使用您之前创建的。S3BundleType和来自S3Key您放在 S3 商店中的捆绑包。

   a. 将 CodeDeploy 应用程序部署 CT 的执行参数 JSON 架构输出到名为 Deploy p CDApp arams.json 的 JSON 文件中。

   ```
   aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    DeployCDAppParams.json
   ```

   b. 按如下方式修改架构并将其另存为，您可以删除和替换内容。

   ```
   {
   "Description":                          "DeployWPCDApp",
   "VpcId":                                "VPC_ID",
   "Name":                                 "WordPressCDAppDeploy",
   "TimeoutInMinutes":                     60,
   "Parameters":   {
       "CodeDeployApplicationName":                "WordPress",
       "CodeDeployDeploymentGroupName":            "WordPress",
       "CodeDeployIgnoreApplicationStopFailures":   false,
       "CodeDeployRevision": {
         "RevisionType": "S3",
         "S3Location": {
           "S3Bucket":     "BUCKET_NAME",
           "S3BundleType": "zip",
           "S3Key":        "wordpress.zip" }
           }
       }
   }
   ```

c. 将的 JSON 模板输出 CreateRfc 到当前文件夹中名为 Deploy CDApp rfc.json 的文件中：

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. 修改并保存 Deplo CDApp y rfc.json 文件，你可以删除和替换其中的内容。请注意，RequestedStartTime和现在RequestedEndTime是可选的；排除它们会创建一个 ASAP RFC，该RFC在获得批准后立即执行（通常会自动发生）。要提交计划的 RFC，请添加这些值。

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. 创建 RFC，指定 Deploy CDApp Rfc 文件和 De CDApp ploy Params 执行参数文件：

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

您会在回复 RfcId 中收到新 RFC 的信息。保存 ID 以供后续步骤使用。

f. 提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，则不会收到任何输出。

g. 要检查 RFC 状态，请运行

```
aws amscm get-rfc --rfc-id RFC_ID
```

验证应用程序部署

导航到先前创建的负载均衡器的终端节点 (ELB CName)， WordPress 部署的路径为：/。WordPress 例如：

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

拆除应用程序部署

完成本教程后，您将需要取消部署，这样您就无需为资源付费。

以下是一个通用的堆栈删除操作。您需要提交两次，一次用于 HA 2 层堆栈，一次用于 S3 存储桶堆栈。最后，提交服务请求，要求删除 S3 存储桶的所有快照（在服务请求中包括 S3 存储桶堆栈 ID）。它们会在 10 天后自动删除，但提早删除它们可以节省一点成本。

本演练提供了使用 AMS 控制台删除 S3 堆栈的示例；此过程适用于使用 AMS 控制台删除任何堆栈。

> **Note**
>
> 如果删除 S3 存储桶，则必须先将其中的对象清空。

必填数据：

- `StackId`: 要使用的堆栈。你可以通过查看 AMS Console Stack s 页面来找到它，该页面可通过左侧导航栏中的链接获得。使用 AMS SKMS API/CLI 运行有关 AMS SKMS API 参考，请参阅 AWS Artifact 控制台中的 “报告” 选项卡。操作（在 CLI 中`list-stack-summaries`）。
- 本演练的更改类型 ID 为`ct-0q0bic0ywqk6c`，版本为 “1.0”，要查找最新版本，请运行以下命令：

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

内联创建：

- 使用内联提供的执行参数发出 create RFC 命令（内联提供执行参数时使用转义引号）。E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- 使用创建 RFC 操作中返回的 RFC 编号提交 RFC。在提交之前，RFC 仍处于该`Editing`状态，不会被付诸行动。

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- 监控 RFC 状态并查看执行输出：

```
aws amscm get-rfc --rfc-id RFC_ID
```

模板创建：

1. 将 RFC 模板输出到当前文件夹中的一个文件中；示例将其命名为 DeleteStackRfc .json：

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. 修改并保存 DeleteStackRfc .json 文件。由于删除堆栈只有一个执行参数，因此执行参数可以在 DeleteStackRfc .json 文件本身中（无需创建带有执行参数的单独的 JSON 文件）。

   ExecutionParameters JSON 扩展中的内部引号必须使用反斜杠 (\) 进行转义。没有开始和结束时间的示例：

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. 创建 RFC：

   ```
   aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
   ```

   您会在回复 RfcId 中收到新 RFC 的信息。例如：

   ```
   {
   "RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
   }
   ```

   保存 ID 以供后续步骤使用。

4. 提交 RFC：

   ```
   aws amscm submit-rfc --rfc-id RFC_ID
   ```

   如果 RFC 成功，则不会在命令行收到任何确认。

5. 要监控请求的状态并查看执行输出，请执行以下操作：

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

控制台教程：高可用性双层堆栈 (Linux/RHEL)

本节介绍如何使用 AMS 控制台将高可用性 (HA) WordPress 站点部署到 AMS 环境中。

> **Note**
>
> 本部署演练已在 AMZN Linux 和 RHEL 环境中进行了测试。

任务和所需任务摘要 RFCs：

1. 创建基础架构（HA 双层堆栈）
2. 为 CodeDeploy 应用程序创建 S3 存储桶
3. 创建 WordPress 应用程序包并将其上传到 S3 存储桶
4. 使用部署应用程序 CodeDeploy
5. 访问该 WordPress 网站并登录以验证部署
6. 拆除部署

所有 CT 选项（包括 ChangeTypeId）的描述均可在 AMS 更改类型参考中找到。

开始前的准备工作

部署 | 高级堆栈组件 | 高可用性双层堆栈 | 创建 CT 可创建 Auto Scaling 组、负载均衡器、数据库以及 CodeDeploy 应用程序名称和部署组（与您为应用程序指定的名称相同）。有关信息， CodeDeploy 请参阅什么是 CodeDeploy？

本演练使用高可用性双层堆栈 RFC，其中包括`UserData`并描述了如何创建可部署的 WordPress CodeDeploy 捆绑包。

示例中`UserData`显示的通过查询 http://169.254.169.254/latest/meta-data/ 上提供的实例元数据服务，从正在运行的实例中获取 EC2 实例元数据，例如实例 ID、区域等。用户数据脚本中的这一行：`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`，将可用区名称从元数据服务检索到我们支持区域的 $REGION 变

量中，并使用它来填写下载代理的 S3 存储桶的 URL。 CodeDeploy 169.254.169.254 IP 只能在 VPC 内路由（所有人都可以查询该服务）。 VPCs 有关该服务的信息，请参阅实例元数据和用户数据。另请注意，以身份输入 UserData 的脚本以 “root” 用户身份执行，不需要使用 “sudo” 命令。

本演练将以下参数保留为默认值（如图所示）：

- Auto Scaling 群组：`Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`。
- Load Balancer：`HealthCheckInterval=30, HealthCheckTimeout=5`。
- 数据库：`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`。
- 应用程序：`DeploymentConfigName=CodeDeployDefault.OneAtATime`。

变量参数：

控制台为开始时间提供了 “尽快” 选项，本演练建议使用该选项。ASAP 会在批准通过后立即执行 RFC。

> **Note**
>
> 您可以选择设置许多与所示不同的参数。示例中显示的这些参数的值已经过测试，但可能不适合您。示例中仅显示必填值。应更改*replaceable*字体值，因为它们是您的帐户所特有的。

创建基础架构

此过程使用高可用性双层堆栈 CT，然后使用 Create S3 存储 CT。

在开始之前收集以下数据可以加快部署速度。

必需的数据有堆栈：

- AutoScalingGroup:
  - UserData：本教程中提供了此值。它包括为其设置资源 CodeDeploy 和启动 CodeDeploy 代理的命令。
  - AMI-ID：此值决定了您的 Auto Scaling 组 (ASG) 将启动的 EC2 实例的操作系统。在您的账户中选择一个以 “customer-” 开头且具有所需操作系统的 AMI。 IDs 在 AMS 控制台 VPCs -> VPCs 详情页面中查找 AMI。本演练适用于 ASGs 配置为使用亚马逊 Linux 或 RHEL AMI。
- 数据库：
  - 尽管示例中显示的值已经过测试，但这些参数EngineVersion、、和LicenseModel应根据您的情况进行设置。DBEngine本教程分别使用以下值：*MySQL*、*8.0.16*、*general-public-license*。
  - 部署应用程序包时需要MasterUsername这些参数DBNameMasterUserPassword、、和。本教程分别使用以下值：*wordpressDB*、*p4ssw0rd*、*admin*。请注意， DBName 只能包含字母数字字符。
  - 当您输入 RDS 数据库时，它将以明文形式显示，因此请尽快登录数据库并更改密码以确保您的安全。MasterUsername
  - 对于 RDSSubnetID，请使用两个私有子网。每次输入一个，然后按 “Enter”。 IDs 使用 AMS SKMS API 参考查找子网，请参阅 AWS Artifact 控制台中的报告选项卡。操作 (CLI: list-subnet-summaries) 或 AMS 控制台-> VPCs VPC 详细信息页面。
- LoadBalancer:
  - 将此参数 Public 设置为 true，因为本教程使用公有 ELB 子网。
  - ELBSubnetID：使用两个公有子网。每次输入一个，然后按 “Enter”。 IDs 使用 AMS SKMS API 参考查找子网，请参阅 AWS Artifact 控制台中的报告选项卡。操作 (CLI: list-subnet-summaries) 或 AMS 控制台-> VPCs VPC 详细信息页面。
- 应用程序：该ApplicationName值设置 CodeDeploy 应用程序名称和 CodeDeploy 部署组名称。你可以用它来部署你的应用程序。它在账户中必须是唯一的。要查看您的账户中的 CodeDeploy 姓名，请访问 CodeDeploy 控制台。该示例使用了，*WordPress*但是，如果您要使用该值，请确保该值尚未被使用。

1. 启动高可用性堆栈。

a. 在 “创建 RFC” 页面上，从列表中选择类别 “部署”、“标准堆栈” 子类别、“高可用性双层堆栈” 和 “创建” 操作。

b. 重要：选择 “高级”，然后如图所示设置值。

   您只需要为已加星标 (*) 的选项输入值，示例中显示了测试值；您可以将非必填的空选项留空。

c. 对于 RFC 描述部分：

```
Subject: WP-HA-2-Tier-RFC
```

d. 在 “资源信息” 部分，为 “数据库” AutoScalingGroup、“应用程序” 和 “标签” 设置参数。LoadBalancer

   此外，“AppName” 标签密钥的目的是让您可以轻松地在 EC2 控制台中搜索 ASG 实例；您可以将此标签密钥称为 “名称” 或任何其他您想要的密钥名称。请注意，您最多可以添加 50 个标签。

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:              AMI-ID
Description:        WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
```

```
    MasterUsername:       admin
    DBName:               wordpressDB

LoadBalancer:
    Public:               true (USE RADIO BUTTON)
    ELBSubnetIds:         PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:      WordPress

Tags:
    Name:                 WP-Rhel-Stack
```

e. 完成后单击 “提交”。

2. 登录到您创建的数据库并更改密码。
3. 启动 S3 存储桶堆栈。

   在开始之前收集以下数据可以加快部署速度。

   必需的数据 S3 存储桶：

   - VPC-ID：此值决定您的 S3 存储桶将位于何处。 IDs 使用有关 AMS SKMS API 参考查找 VPC，请参阅 AWS Artifact 控制台中的报告选项卡。操作 (CLI: list-vpc-summaries) 或 AMS 控制台 VPCs 页面中。
   - BucketName：此值设置 S3 存储桶名称，您可以使用它来上传您的应用程序包。它在账户所在区域内必须是唯一的，并且不能包含大写字母。不要求将您的账户 ID 作为其中的 BucketName 一部分，但可以更轻松地在以后识别存储桶。要查看账户中存在哪些 S3 存储桶名称，请访问您的账户的 Amazon S3 控制台。

   a. 在 “创建 RFC” 页面上，从 RFC CT 选择列表中选择部署类别、子类别 “高级堆栈组件”、“项目 S3 存储” 和 “创建” 操作。

   b. 保留默认的 “基本” 选项，并如图所示设置值。

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
```

```
TimeoutInMinutes:     60
```

c. 完成后单击 “提交”。使用此更改类型部署的存储桶允许对整个账户进行完全 read/write 访问权限。

创建、上传和部署应用程序

首先，创建 WordPress 应用程序包，然后 CodeDeploy CTs 使用创建和部署应用程序。

1. 下载 WordPress、解压缩文件并创建. /scripts 目录。

   Linux 命令：

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows：粘贴`https://github.com/WordPress/WordPress/archive/master.zip`到浏览器窗口并下载 zip 文件。

   创建用于组装软件包的临时目录。

   Linux：

   ```
   mkdir /tmp/WordPress
   ```

   Windows：创建一个 “WordPress” 目录，稍后将使用该目录路径。

2. 将 WordPress 源代码解压缩到 “WordPress” 目录并创建一个。 /scripts 目录。

   Linux：

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows：转到你创建的 “WordPress” 目录并在那里创建一个 “脚本” 目录。

   如果您在 Windows 环境中，请务必将脚本文件的中断类型设置为 Unix (LF)。在 Notepad ++ 中，这是窗口右下角的一个选项。

3. 在 WordPress 目录中创建 CodeDeploy appsec.yml 文件（如果复制示例，请检查缩进，每个空格都很重要）。重要：确保将 WordPress 文件（在本例中为 WordPress 目录中）复制到预期目标 (/var/www/html/WordPress) 的 “源” 路径是正确的。在示例中，appsec.yml 文件位于文件所在的目录中，因此只需要使用 “/”。 WordPress 另外，即使你在 Auto Scaling 组中使用了 RHEL AMI，也要保留 “操作系统：linux” 一行不变。appspec.yml 文件示例：

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. 在中创建 bash 文件脚本。 WordPress /scripts 目录。

   首先，`config_wordpress.sh`使用以下内容创建（如果您愿意，可以直接编辑 wp-config.php 文件）。

> **Note**
>
> *DBName*替换为 HA 堆栈 RFC 中给出的值（例如，`wordpress`）。
> *DB_MasterUsername*替换为 HA 堆栈 RFC 中给出的`MasterUsername`值（例如，`admin`）。
> *DB_MasterUserPassword*替换为 HA 堆栈 RFC 中给出的`MasterUserPassword`值（例如，`p4ssw0rd`）。

在 HA 堆栈 RFC 的执行输出中替换*DB_ENDPOINT*为终端节点 DNS 名称（例如`srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com`）。你可以通过GetRfc操作（CLI：get-rfc--rfc-id RFC_ID）或者在之前提交的 HA Stack RFC 的 AMS 控制台 RFC 详情页面中找到它。

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. 在同一个目录中创建`install_dependencies.sh`包含以下内容的内容：

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS 是在启动时作为用户数据的一部分安装的，以便运行状况检查从一开始就起作用。

6. 在同一个目录中创建`start_server.sh`包含以下内容的内容：

   - 对于亚马逊 Linux 实例，请使用以下命令：

   ```
   #!/bin/bash
   service httpd start
   ```

   - 对于 RHEL 实例，请使用以下命令（额外的命令是允许 SELINUX 接受的策略）： WordPress

   ```
   #!/bin/bash
   setsebool -P  httpd_can_network_connect_db 1
   ```

```
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. 在同一个目录中创建stop_server.sh包含以下内容的内容：

```
#!/bin/bash
service httpd stop
```

8. 创建 zip 捆绑包。

   Linux：

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows：前往 “WordPress” 目录选择所有文件并创建一个 zip 文件，一定要将其命名为 wordpress.zip。

1. 将应用程序包上传到 S3 存储桶

   要继续部署堆栈，软件包需要准备就绪。

   您可以自动访问自己创建的任何 S3 存储桶实例。您可以通过 Bastions（请参阅访问实例）或 S3 控制台对其进行访问，然后使用 drag-and-drop文件或浏览并选择文件来上传 CodeDeploy 软件包。

   您也可以在 shell 窗口中使用以下命令；请确保您的 zip 文件路径正确：

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. 部署 WordPress CodeDeploy 应用程序包

   必需的数据代码部署应用程序部署：

   - CodeDeployApplicationName: 你给 CodeDeploy 应用程序起的名字。
   - CodeDeployGroupName：由于 CodeDeploy 应用程序和组都是根据您在 HA 堆栈 RFC 中为 CodeDeploy 应用程序指定的名称创建的，因此该名称与。CodeDeployApplicationName
   - S3Bucket：你给 S3 存储桶起的名字。

- S3 BundleType 和 S3Key：它们是您部署的 WordPress 应用程序包的一部分。
- VpcId：相关的 VPC。

a. 在 “创建 RFC” 页面上，从 RFC CT 选择列表中选择 “部署”、“CodeDeploy 应用程序” 子类别、“应用程序” 和 “操作” 部署类别。

b. 保留默认的 “基本” 选项，并如图所示设置值。

> **Note**
>
> 引用之前创建的 CodeDeploy 应用程序、 CodeDeploy 部署组、S3 存储桶和捆绑包。

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

c. 完成后单击 “提交”。

验证应用程序部署

导航到先前创建的负载均衡器的终端节点 (LoadBalancerCName)， WordPress 部署的路径为：/。WordPress例如：

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

你应该会看到这样的页面：

拆除高可用性部署

要取消部署，您可以提交针对 HA 双层堆栈和 S3 存储桶的 Delete Stack CT，然后可以请求删除 RDS 快照（它们将在十天后自动删除，但在此期间确实会花费少量费用）。收集 HA 堆栈 IDs 和 S3 存储桶的堆栈，然后按照以下步骤操作。参见堆栈 | 删除。

附录：SALZ 入职问卷

主题

这是您在注册账户之前需要考虑的一些信息。

部署摘要

部署的描述。例如：

- 此帐户用于 Line-of-Business应用程序部署（而不是产品应用程序部署）。
- 部署涉及账户的公有子网或 DMZ 子网内的自动扩展 ARP（经过身份验证的反向代理）。
- Web 和应用程序服务器将部署在账户的私有子网中。
- 还将在账户的私有子网中部署 RDS（Amazon Relational Database Service）实例。
- 服务器（ARP、Web、应用程序、数据库、负载均衡器等）分为不同的安全组。
- 该账户需要跨可用区 () 的 HA（高可用性AZs）设计，即 “多可用区”。

环境架构注意事项

在决定如何配置环境和架构时，请考虑以下标准。

- 您的虚拟数据中心能否重新连接到您的公司网络？

  - 您有现有 AWS DirectConnect 服务还是需要新 DirectConnect 服务？
  - 您是否已有 VPN 连接或者需要新的 VPN 服务？
- 您可以分配的内部地址的可用的 CIDR 块范围是多少？（推荐 /16，不得与公司网络范围重叠）
- 您的虚拟数据中心是否需要互联网接入？
- 您打算使用哪个区域？(Sydney/N. Virginia/Dublin)
- 是否需要共享服务子网来托管与所有其他子网相连的应用程序？
- 您希望将哪些组织部门作为单独的子网托管。对于每个：
  - 您需要与其他子网的什么连接？
  - 子网是否需要互联网接入？
  - 该子网是否有任何应用程序部署限制？
  - 该子网是否有任何特定的网络要求？
- 您想要单独的开发 and/or 测试环境吗？（将包括共享服务副本，便于随时访问）
- 您的快照备份要求是什么？
- 您是否有想要保留的现有维护流程或补丁窗口？
- 您的域名注册要求是什么？
- 您有任何单点登录要求吗？（例如 AD、LDAP）
- 您的总体预期操作系统和预期容量需求是多少？

单账户着陆区监控警报

AMS 为您提供了一种直接收到某些监控警报的提醒（而不是获取 AMS 服务通知）的方式。要注册，请确保您的云架构师（CA）或云服务交付经理 (CSDM) 收到以下信息：

直接警报电子邮件：这些是您希望 AMS 向其发送某些基于资源的警报的电子邮件地址。有关哪些警报直接发送到电子邮件的详细信息，请参阅《AMS 单账户着陆区用户指南》中的 AMS 基线监控警报。有关 AMS 监控的更多信息，请参阅 AMS 单账户登录区域用户指南中的监控管理。

维护时段

您需要创建一个维护窗口，以考虑不同的应用程序需求 AWS 区域、不同的压力期和不同的压力期。您的维护时段是 AMS 应用补丁的时间。下面是一些指导方针：

- 要限制对用户的影响，请根据您的环境部署 AWS 区域 位置来规划维护时段。
- 安排在正常工作时间之外以及预计生产服务器上的流量最少的时段。

- 通常，基础架构堆栈需要每月更新。
- 将维护时段安排至少 300 分钟。操作系统修补需要 60-90 分钟，基础设施堆栈修补需要 180-300 分钟。

后续步骤

AMS 入职团队将协助您完成向 AMS 注册账户的每一步工作。这些是入职要求：

- 配置一个新的 AWS 账户 用于 AMS 并提供一个 AWS 账户 ID。
- 注册即可获得所需的 Support 级别。
- 创建跨账户 IAM 角色以授予 AMS 配置账户访问权限并将角色名称提供给 AMS。
- 将账户 753102745277 添加为可信实体。

附录： ActiveDirectory 联合身份验证服务 (ADFS) 声明规则和 SAML 设置

有关如何安装和配置 AD FS 的详细 step-by-step说明，请参阅使用 Windows Active Directory、ADFS 和 SAML 2.0 启用与 AWS 的联合。

ADFS 声明规则配置

如果您已经有 ADFS 实现，请进行以下配置：

- 依赖方信任
- 索赔规则

信赖方信任和索赔规则的步骤是从 “使用 Windows Active Directory、AD FS 和 SAML 2.0 向 AWS 启用联合身份验证” 博客中介绍的

- 索赔规则：
  - Nameid：每篇博客文章的配置
  - RoleSessionName: 按如下方式进行配置
    - 声明规则名称：**RoleSessionName**
    - 属性存储：**Active Directory**
    - LDAP 属性：**SAM-Account-Name**
    - 发出的索赔类型：**https://aws.amazon.com/SAML/Attributes/RoleSessionName**
    - 获取 AD 组：每篇博客文章的配置
    - 角色声明：按如下方式进行配置

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web 控制台

您可以使用以下链接访问 AWS Web 控制台，将其*[ADFS-FQDN]*替换为 ADFS 实施的 FQDN。

https://*[ADFS-FQDN]*/adfs/ls/IdpInitiatedSignOn.aspx

您的 IT 部门可以通过组策略将上述链接部署到用户群中。

使用 SAML 访问 API 和 CLI

如何使用 SAML 配置 API 和 CLI 访问权限。

python 软件包来自以下博客文章：

- NTLM：如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问
- 表单：如何使用 SAML 2.0 实现联合 API/CLI 访问的通用解决方案
- PowerShell: 如何使用 Windows 设置对 AWS 的联合 API 访问权限 PowerShell

脚本配置

1. 使用 Notepad++ 将默认区域更改为正确的区域
2. 使用 Notepad++，在测试和开发环境中禁用 SSL 验证
3. 使用 Notepad++ 配置 idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Windows 配置

以下说明适用于 python 软件包。生成的证书将在 1 小时内有效。

1. 下载并安装 python (2.7.11)
2. 下载并安装 AWS CLI 工具
3. 安装 AMS CLI：

    a. 下载您的云服务交付经理 (CSDM) 提供的 AMS 可发行文件 zip 文件并解压缩。

    有几个目录和文件可用。

b. 根据您的操作系统，打开托管云分发文件-> CLI-> Windows 或托管云发行文件-> CLI-> Linux/macOS 目录，然后：

   对于 Windows，请执行相应的安装程序（此方法仅适用于 Windows 32 或 64 位系统）：

   - 32 位： ManagedCloudAPI_x86.msi
   - 64 位： ManagedCloudAPI_x64.msi

   对于 Mac/Linux，请执行名为 MC_CLI.sh 的文件。你可以通过运行这个命令来做到这一点:sh `MC_CLI.sh`. 请注意，amscm 和 amsskms 目录及其内容必须与 MC_CLI.sh 文件位于同一个目录中。

c. 如果您的公司证书是通过与 AWS 的联合身份验证（AMS 默认配置）使用的，则必须安装可以访问您的联合身份验证服务的凭证管理工具。例如，您可以使用此 AWS 安全博客如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问来帮助配置您的凭证管理工具。

d. 安装完成后，运行`aws amscm help`或`aws amsskms help`并查看命令和选项。

4. 下载所需的 SAML 脚本

   下载到 c:\aws\scripts

5. 下载 PIP

   下载到 c:\aws\downloads

6. 使用 PowerShell，安装 PIP

   <pythondir>。 \ python.exe c:\aws\downloads\get-pip.py

7. 使用 PowerShell，安装 boto 模块

   <pythondir\ scripts>pip 安装启动器

8. 使用 PowerShell、安装请求模块

   <pythondir\ scripts>pip 安装请求

9. 使用 PowerShell、安装请求安全模块

   <pythondir\ scripts>pip 安装请求 [安全]

10. 使用 PowerShell，安装 beautifulsoup 模块

    <pythondir\ scripts>pip 安装 beautifulsoup4

11. 使用 PowerShell，在用户配置文件中创建一个名为.aws 的文件夹 (%userprofile%\ .aws)

mkdir .aws

12. 使用 PowerShell，在.aws 文件夹中创建凭证文件

    新物品凭证类型文件 —force

    凭证文件不能有文件扩展名

    文件名必须全部为小写并具有名称凭证

13. 使用记事本打开凭证文件并粘贴以下数据，指定正确的区域

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. 使用 PowerShell SAML 脚本和登录

    <pythondir>。 \ python.exe c:\aws\scripts\samlapi.py

    用户名：[用户名] @upn

    选择你想担任的角色

Linux 配置

生成的证书将在 1 小时内有效。

1. 使用 WinSCP 传输 SAML 脚本
2. 使用 WinSCP 传输根 CA 证书（对于测试和开发，请忽略）
3. 将 ROOT CA 添加到受信任的根证书中（对于测试和开发，请忽略）

   $ openssl x509-inform der-in [certname] .cer out certificate.pem（测试和开发时忽略）

   将 certificate.pem 的内容添加到/ etc/ssl/certs/ca-bundle.crt 文件的末尾（对于测试开发人员来说，忽略此操作）

4. 在 home/ec2-user 5 中创建.aws 文件夹

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. 使用 WinSCP 将证书文件传输到.aws 文件夹
6. 安装 boto 模块

   $ sudo pip 安装启动程序
7. 安装请求模块

   $ sudo pip 安装请求
8. 安装漂亮的汤模块

   $ sudo pip 安装 beautifulsoup4
9. 将脚本复制到 home/ec2-user

   设置所需的权限

   执行脚本：samlapi.py

文档历史记录

下表描述了自上次发布 AMS 以来对文档所做的重要更改。

- API 版本：2019-05-21
- 最新文档更新：2025 年 9 月 23 日

更改	描述	日期
在 AWS Managed Services 常见问题解答部分更新了 A SageMaker I 中终端节点自动扩展的更改类型	使用 AMS SSP 在你的 AMS 账户中配置 SageMaker Amazon AI。 使用管理 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | 更新实体或策略（需要审查）更改类型 (ct-27tuth19k52b4) 提交 RFC，以临时或永久提升自动扩展权限，因为自动缩放需要对服务的许可访问权限。 CloudWatch	2025年9月25日
精确的更改类型参考	创建、更改或删除安全组。 添加用户：使用 “管理” | “目录服务” | “用户和群组” 提交 RFC | 将用户添加到群组 [ct-24pi85mjtza8k] 和删除用户：使用管理提交 RFC | 目录服务 | 用户和群组 | 从群组中移除用户 [ct-2019s9y3nfml4]	2025年8月8日
已移除目录链接	已移除 TOC AWS 词汇表链接。	2025年8月8日
添加了处方指导链接	设置整合账单——将新账户关联到付款人账户.	2025年5月8日
更新了激活 IAM 访问权限的说明 AWS 管理控制台	澄清了激活 IAM 访问权限的说明 AWS 管理控制台。	激活 IAM 对 AWS 控制台的访问权限

更改	描述	日期
更新了 Direct Connect 专用连接上允许的传输虚拟接口数量	Direct Connect 专用连接现在每个连接最多只能有 4 个传输虚拟接口	将 Direct Connect 连接到 Transit
改进措辞。	指定 “仅用作 “拒绝” 列表” 必须包含 “Allow All All”，以确保 AMS 监控和管理运行。	网络配置
有关使用 AMS CLI 的更多信息。	“新增注意某些 CLI 命令可能需要该`--region`选项”	安装 AMS CLIs
更新：为了保持一致性和可读性，章节标题已移至更合适的章节	“变更管理模式” 是 “变更管理” 的新标题	更改管理模式
更新了内容	以前称为 “变更管理模式” 或 “标准 CM 模式” 的 AMS 模式现在被称为 “RFC 模式”。模式部分已扩展。	RFC 模式.
更新了内容	以前称为 “变更管理模式” 或 “标准 CM 模式” 的 AMS 模式现在被称为 “RFC 模式”。模式部分已缩短，并添加了有关模式的 “AMS 高级用户指南” 部分的链接。	AMS 模式.
MALZ：更新的网络架构图	网络账户架构m	2022 年 6 月 16 日
将主题列表移至开头段落下方	AWS Managed Services 入职简介	2022 年 6 月 16 日
更新内容，包容性语言倡议	“管理账户” 而不是 “主账户”。	AMS 中的 IAM 用户角色，“政策示例” 部分
更新了内容、工具账号角色名称	已将角色名称更新 CustomerMigrationAccessRole 为 AWSManagedServicesMigrationRole。	AWS 应用程序迁移服务 (AWS MGN)

更改	描述	日期
SALZ：连续性管理默认值	更新了链接并从中删除了过时的信息 VPC 标签和默认值	2022 年 2 月 28 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。