aws

用户指南

AWS License Manager

AWS License Manager: 用户指南

Table of Contents

什么是 AWS License Manager？

AWS License Manager 是一项服务，可让您更轻松地在本地环境中集中管理来自软件供应商（例如 Microsoft、SAP、Oracle 和 IBM）的软件许可证。 AWS 这可以控制和查看许可证的使用情况，使您能够限制许可超额并降低不合规和误报的风险。

在构建云基础架构时 AWS，您可以利用自带许可模式 (BYOL) 机会来节省成本。也就是说，您可以重新调整现有许可证清单的用途，以便与您的云资源一起使用。

License Manager 通过与 AWS 服务直接相关的库存跟踪来降低许可超额和处罚的风险。通过基于规则的许可证消耗控制，管理员可以对新的和现有的云部署设置硬限制或软限制。基于这些限制，License Manager 可以帮助在不合规的服务器使用发生之前予以阻止。

License Manager 的内置控制面板可让您随时掌握许可证使用情况，并能协助供应商审核。

License Manager 支持跟踪根据虚拟内核 (vCPU)、物理内核、套接字或计算机数量许可的任何软件。这包括来自 Microsoft、IBM、SAP、Oracle 和其他供应商的各种软件产品。

借 AWS License Manager助，您可以通过保持所有已结账权利的计数，集中跟踪许可证并在多个地区实施限制。License Manager 还会跟踪与每次签出相关的最终用户身份和底层资源标识符（如果有）以及签出时间。这些时间序列数据可以通过 CloudWatch指标和事件追踪到 ISV。ISV 可以将该数据用于分析、审计和其他类似目的。

AWS License Manager 已与 AWS MarketplaceAWSData Exchange 以及以下 AWS 服务集成：AWS Identity and Access Management (IAM) AWS Organizations、Service Quotas AWS CloudFormation、、 AWS 资源标记和AWS X-Ray。

托管权限

使用 License Manager，许可管理员可以跨账户和整个组织分配、激活和跟踪软件许可。

独立软件供应商 (ISV) 可以通过托管授权 AWS License Manager 来管理和向最终用户分发软件许可证和数据。作为颁发者，您可以使用 License Manager 控制面板集中跟踪卖家颁发的许可证的使用情况。作为交易工作流程的一部分，通过销售的独立软件供应商 AWS Marketplace 受益于自动创建和分发许可证。ISV 还可以使用 License Manager 为没有 AWS 帐户的客户创建许可证密钥和激活许可证。

License Manager 使用开放、安全的行业标准来表示许可证，并允许客户以加密方式验证其真实性。License Manager 支持各种不同的许可模式，包括永久许可模式、浮动许可模式、订阅许可模式和

基于使用情况的许可模式。如果您拥有必须锁定节点的许可证，License Manager 会提供以这种方式使用您的许可证的机制。

您可以在中创建许可证， AWS License Manager 并使用 IAM 身份或通过生成的数字签名令牌将其分发给最终用户。 AWS License Manager使用的最终用户 AWS 可以进一步将许可证权利重新分配给各自 AWS 组织中的身份。拥有分布式权限的最终用户可以通过您的软件与 AWS License Manager 集成，从该许可证中签出并签入所需的权限。每次签出许可证都指定权限、关联数量和签出时间段，例如在 1 小时内签出 10 个 **`admin-users`**。可以根据分布式许可证的底层 IAM 身份或 AWS License Manager 通过该 AWS License Manager 服务生成的长期代币来执行此项检查。

License Manager 使用案例

以下是 License Manager 为各种使用案例提供的功能示例：

- License Manager 中的自管理许可证— 用于根据企业协议的条款定义许可规则，这些条款决定了如何 AWS 处理使用这些许可证的命令。
- 卖家在 License Manager 中颁发的许可证 — 用于管理并向最终用户分配软件许可证。
- 在 License Manager 中已授予的许可证— 用于管理从 AWS Marketplace AWS Data Exchange、或直接从将软件与托管权利集成的卖家那里获得的许可证的使用。
- License Manager 中的许可证类型转换— 用于在 AWS 提供的许可和自带许可模式 (BYOL) 之间更改许可证类型，而无需重新部署工作负载。
- License Manager 中的库存搜索— 用于使用 AWS Systems Manager 清单和许可规则发现和跟踪本地应用程序。
- License Manager 中的基于用户的订阅 — 用于购买完全合规的 Amazon 提供的受支持软件的许可证，并按用户收取订阅费。
- License Manager 中的 Linux 订阅 — 用于查看和管理您拥有并在 AWS上运行的商用 Linux 订阅。

相关服务

License Manager 已与亚马逊 EC2、Amazon RDS AWS Marketplace、 AWS Systems Manager、和集成 AWS Organizations。

Amazon EC2 集成让您能够跟踪以下资源的许可证，并在整个资源生命周期中强制执行许可规则：

- Amazon EC2 实例
- 专用实例

- 专属主机
- 竞价型实例和竞价型实例集
- 托管式节点

同时使用 License Manager 时 AWS Systems Manager，可以管理托管在外部的物理或虚拟服务器上的许可 AWS。您可以将 License Manager 与配 AWS Organizations 合使用，集中管理所有组织帐户。

此外，您可以管理从 AWS Marketplace AWS Data Exchange、或直接从与其软件集成的卖家那里购买的许可证的使用 AWS License Manager。您可以使用 AWS License Manager 将使用权（称为授权）分配给特定用户 AWS 账户。

License Manager 与适用于 Oracle 的 Amazon RDS 和基于 Db2 vCPU 的 BYOL 许可证的 Amazon RDS 集成。通过这种集成，您可以了解适用于 Oracle 的 RDS 和适用于 Db2 的 RDS 数据库实例的 vCPU 使用情况。您可以使用此数据根据您与数据库管理系统供应商签订的许可条款计算所消耗的许可证数量。有关更多信息，请参阅 Amazon RDS 用户指南中的以下相关链接。

- 适用于甲骨文的 RDS 许可选项
- 适用于 Db2 的 RDS 许可选项

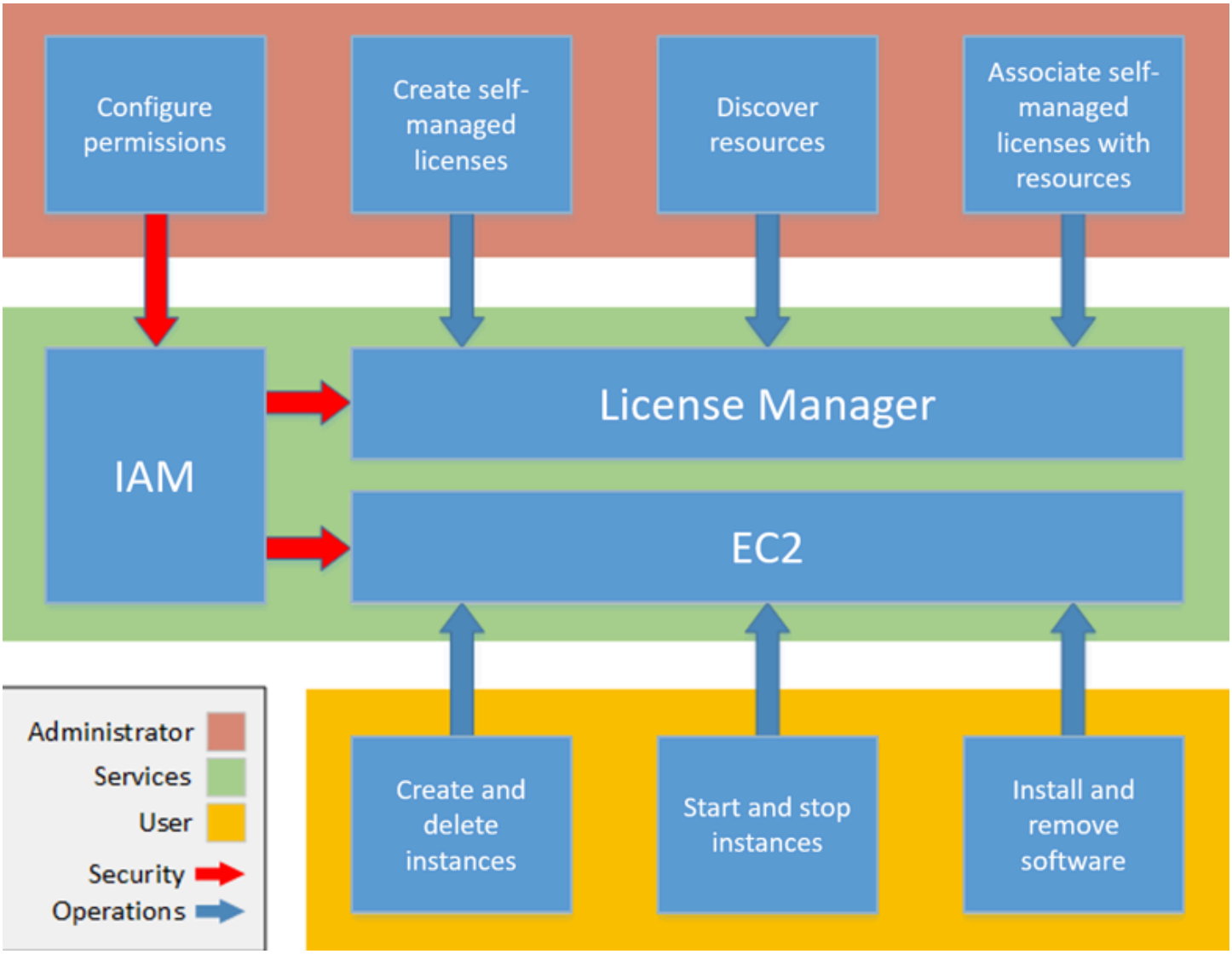
License Manager 的工作原理

有效的软件许可证管理取决于以下因素：

- 熟悉企业许可协议中的语言
- 适当地限制访问使用许可证的操作
- 准确地跟踪许可证清单

企业可能指派专门的人员或团队负责其中的每个领域。因而，有效地进行沟通成为一个难题，特别是在许可证专家和系统管理员之间。License Manager 提供了一种方法以汇集各个领域的信息。至关重要的是，它还与 AWS 服务内在集成在一起；例如，与 Amazon EC2 控制面板集成在一起，可以在其中创建和删除实例。这意味着，License Manager 规则和限制捕获业务和运营信息，并且还会转换为对实例创建和应用程序部署的自动控制。

下图说明了许可证管理员（管理权限和配置 License Manager）和用户（通过 Amazon EC2 控制台创建、管理和删除资源）的不同但相互协调的职责。



如果您负责管理组织中的许可证，您可以使用 License Manager 设置许可规则，将其附加到资源启动中以及跟踪使用情况。然后，组织中的用户可以添加和删除使用许可证的资源，而无需执行额外的工作。

许可专家管理整个组织中的许可证，从而确定资源清单需求，监督许可证采购以及推动合规地使用许可证。在使用 License Manager 的企业中，该工作是通过 License Manager 控制台整合的。正如图中所示，这涉及设置服务权限，创建自管理许可证，清点本地和云中的计算资源，以及将此类许可证与找到的资源相关联。实际上，这可能表示将许可证配置与一个批准的亚马逊机器映像 (AMI) 相关联；IT 部门将该 AMI 作为所有 Amazon EC2 实例部署的模板。

由于避免了违规使用许可证，License Manager 节省了很多成本。内部审计仅在事后发现违规行为，从而无法避免因违规行为而受到处罚，而 License Manager 可以防止发生这种代价高昂的事件。License Manager 使用内置的控制面板简化了报告过程，从而显示许可证使用情况和跟踪的资源。

入门 AWS License Manager

以下各节将指导您设置 AWS 账户 和用户，以及如何开始使用 License Manager。有关在遵循 AWS 最佳做法的同时管理用户、群组和角色使用 License Manager 的权限的更多信息，请参阅适用于 AWS License Manager 的 Identity and Access Management。有关设置与 License Manager 集成的 Amazon EC2 资源的更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南中的设置以使用 Amazon EC2。

主题

设置

以下部分详细介绍了您 AWS 账户 和用户的设置。

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/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，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。作为安全最佳实践，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。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 Management Console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》中的以根用户身份登录。
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》中的启用 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》中的创建权限集。
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》中的添加组。

已上线即可使用 License Manager AWS Management Console

要开始使用 License Manager，需要执行以下步骤。完成初始要求后，您可以继续使用 License Manager 来处理所需的使用案例。

License Manager 入门

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 系统将提示您配置 License Manager 及其支持服务的权限。按照说明配置所需的权限。
3. 初始设置完成后，您可以根据需要继续使用 License Manager 来处理所需的 License Manager 使用案例。

使用 AWS License Manager

可以将 License Manager 应用于具有包含 AWS 资源和本地资源的混合基础设施的企业的标准方案。您可以创建自管理许可证，清点使用许可证的资源，将此类许可证与资源相关联以及跟踪清单和合规性。

AWS Marketplace 产品许可

通过使用 License Manager，您现在可以通过 Amazon EC2 启动模板、AWS CloudFormation 模板或 Service Catalog 产品将许可规则与 AWS Marketplace BYOL AMI 产品相关联。在每种情况下，您都会从集中式许可证跟踪和合规性实施中受益。

> **Note**
>
> License Manager 不会改变您从 Marketplace 中获取和激活 BYOL AMI 的方式。在启动后，您必须提供直接从卖家获取的许可证密钥以激活任何第三方软件。

在本地数据中心跟踪资源的许可证

借助 License Manager，您可以使用 Systems Manager 清单发现在 AWS 外部运行的应用程序，然后将许可规则附加到这些应用程序。在附加许可规则后，您可以在 License Manager 控制台中跟踪本地服务器以及 AWS 资源。

区分随附许可证和 BYOL

使用 License Manager，您可以确定哪些资源拥有产品随附的许可证，哪些资源使用您自己的许可证。这样，您能够准确报告 BYOL 许可证的使用情况。该筛选条件需要 SSM 版本 2.3.722.0 或更高版本。

跨 AWS 账户的 License Manager

通过 License Manager，您能够跨 AWS 账户管理许可证。您可以在 AWS Organizations 管理账户中创建许可证配置一次并使用 AWS Resource Access Manager 或通过 License Manager 设置链接 AWS Organizations 账户来跨账户共享这些配置。此外，这使您能够执行跨账户发现来跨 AWS 账户搜索清单。

目录

- License Manager 中的许可证规则
- License Manager 中的使用情况报告
- License Manager 中的许可证类型转换
- AWS License Manager 中的主机资源组
- License Manager 中的库存搜索
- 在 License Manager 中已授予的许可证
- 卖家在 License Manager 中颁发的许可证
- License Manager 中的基于用户的订阅
- License Manager 中的 Linux 订阅
- AWS License Manager 中的设置
- AWS License Manager 中的控制面板

License Manager 中的自管理许可证

自管理许可证是 License Manager 的核心。自管理许可证以前被称为“许可证配置”。自管理许可证包含基于您的企业协议条款的许可规则。您创建的规则决定了如何 AWS 处理消耗许可证的命令。在创建自管理许可证时，请与组织的合规性团队密切合作以审核您的企业协议。

限制

- 每种资源的自管理许可证数量：10
- 自管理许可证总数：25
- Systems Manager 托管实例必须与 vCPU 和实例类型自管理许可证相关联。

内容

- 自管理许可证参数和规则
- 通过供应商许可证构建 License Manager 规则
- 创建自管理许可证
- 共享自管理许可证
- 编辑自管理许可证
- 停用自管理许可证
- 删除自管理许可证

自管理许可证参数和规则

自管理许可证包括基本参数和根据参数值变化的规则。您还可以为自管理许可证添加标签。创建自管理许可证后，管理员可以修改许可证数量和使用限制，以反映不断变化的资源需求。

可用参数和规则包括：

- 自管理许可证名称 — 自管理许可证的名称。
- （可选）描述 — 自管理许可证的描述。
- 许可证类型 — 用于对许可证计数的指标。支持的值为 vCPU、内核、套接字和实例。
- （可选）<option> 数 — 资源使用的许可证数量。
- 状态 — 指示配置是否处于活动状态。
- 产品信息 — 用于自动化发现的产品的名称和版本。支持的产品是 Windows Server、SQL Server、适用于 Oracle 的 Amazon RDS 和适用于 Db2 的 Amazon RDS。
- （可选）规则 — 这些规则包括以下内容。可用规则因计数类型而异。
  - 许可证关联到主机（以天为单位） — 在指定的天数内限制主机使用许可证。范围为 1 至 180。计数类型必须是内核或套接字。关联期过后，许可证将在 24 小时内可供重用。
  - 最大内核数 — 资源的最大内核数。
  - 最大套接字数 — 资源的最大套接字数。
  - 最大 vCPU 数 — 资源的最大 vCPU 数。
  - 最小内核数 — 资源的最小内核数。
  - 最小套接字数 — 资源的最小套接字数。
  - 最小 vCPU 数 — 资源的最小 vCPU 数。
  - 租赁 — 将许可证的使用限制在指定的 EC2 租赁范围内。如果计数类型为内核或套接字，则需要专属主机。如果计数类型为实例或 vCPU，则支持共享租赁、专属主机和专用实例。控制台（和 API）名称如下：
    - 共享 (`EC2-Default`)
    - 专用实例 (`EC2-DedicatedInstance`)
    - 专属主机 (`EC2-DedicatedHost`)
    - vCPU 优化 — License Manager 与 Amazon EC2 中的 CPU 优化支持集成，使您能够自定义实例上的 vCPU 数量。如果此规则设置为 True，License Manager 则根据自定义内核和线程计数来对 vCPU 计数。否则，License Manager 会对该实例类型的默认 vCPU 进行计数。

下表描述了每种计数类型都有哪些许可证规则可用。

控制台名称	API 名称	内核	实例	套接字	vCPU
许可证关联到主机（以天为单位）	`licenseAffinityToHost`	✓		✓	
最大内核数	`maximumCores`	✓	✓		
最大套接字数	`maximumSockets`		✓	✓	
最大 vCPU 数	`maximumVcpus`		✓		✓
最小内核数	`minimumCores`	✓	✓		
最小套接字数	`minimumSockets`		✓	✓	
最小 vCPU 数	`minimumVcpus`		✓		✓
租赁	`allowedTenancy`	✓	✓	✓	✓
vCPU 优化	`honorVcpuOptimization`				✓

通过供应商许可证构建 License Manager 规则

您可以根据软件供应商许可证的语言创建 License Manager 规则集。下面的示例并非用作实际使用案例的蓝图。在许可协议的任何实际应用场合中，可以根据您的特定本地服务器环境的架构和许可历史记录选择所需的方案。所选的方案还取决于计划将资源迁移到 AWS的详细信息。

这些示例尽可能做到与供应商无关，而是侧重于通常适用的硬件和软件分配问题。供应商许可条款也与 AWS 要求和限制相互作用。应用程序所需的许可证数量因所选的实例类型和其他因素而异。

> **Important**
>
> AWS 不参与软件供应商的审核流程。客户负责满足合规性要求，并负责根据其许可协议仔细了解规则并将其捕获到 License Manager 中。

示例：实施操作系统许可证

该示例涉及一个服务器操作系统的许可证。许可语言对每个服务器的 CPU 内核类型、租赁和最小许可证数量施加了限制。

在该示例中，许可条款包括以下规定：

- 物理处理器内核决定许可证计数。
- 许可证数量必须等于内核数量。
- 服务器必须至少运行 8 个内核。
- 操作系统必须在非虚拟化主机上运行。

此外，客户还做出了以下决定：

- 购买了 96 个内核的许可证。
- 施加了硬限制以将许可证使用限制为购买的数量。
- 每个服务器最多需要 16 个内核。

下表将 License Manager 规则生成参数与它们捕获并自动填写的供应商许可要求相关联。示例值仅用于说明目的；您应在自己的自管理许可证中指定所需的值。

License Manager 规则	设置
许可证计数类型	许可类型设置 设置为**Cores**。
许可证计数	内核数 设置为 **96**。
最小/最大 vCPU 或内核数	最小内核数 设置为 **8**。 最大内核数 设置为 **16**。
许可证计数硬限制	选择了 Enforce license limit (强制实施许可证限制)。
允许的租赁	

License Manager 规则	设置
	租赁设置为 **Dedicated Host**。

创建自管理许可证

自管理许可证代表与您的软件供应商签订的协议中的许可条款。您的自管理许可证指定了您的许可证应如何计数（例如，按照 vCPU 或实例数量）。它还规定了您的使用限制，这样您就可以防止使用量超过分配的许可证数量。此外，它还可以为您的许可证指定其他限制，例如租赁类型。

适用于 Oracle 的 Amazon RDS 和适用于 Db2 数据库的 Amazon RDS 的注意事项

当您添加产品信息以配置自动发现适用于 Oracle 的 Amazon RDS 或适用于 Db2 数据库的 Amazon RDS 时，以下要求适用：

- 受支持的许可证计数类型是 vCPU。
- 不支持规则。
- 不支持硬许可证限制。
- 每个自管理许可证可以跟踪一个产品版本。
- 您无法使用相同的自管理许可证跟踪 Amazon RDS 数据库和其他产品。

使用控制台创建自管理许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择创建自管理许可证。
4. 在 Configuration details (配置详细信息) 面板中提供以下信息：
   - 自管理许可证名称 — 自管理许可证的名称。
   - 描述 — 自管理许可证的可选描述。
   - 许可证类型 — 该许可证的计数模型（vCPU、内核、套接字或实例）。
   - <option> 数 — 显示的选项取决于许可证类型。在超出许可证限制时，License Manager 会通知您（软限制）或禁止部署资源（硬限制）。
   - 强制执行许可证限制 — 如果选中，则许可证限制为硬限制。

- 规则 — 一条或多条规则。对于每个规则，选择一个规则类型，提供一个规则值，然后选择 Add rule (添加值)。显示的规则类型取决于许可证类型。例如，最小值、最大值和租期。如果您不指定租赁类型，则接受所有值。

5. （可选）在自动化发现规则面板中，执行以下操作：

   a. 为要使用自动化发现功能发现和跟踪的每个产品选择产品名称、产品类型和资源类型。

   b. 选择在卸载软件时停止跟踪实例，以便在 License Manager 检测到软件已卸载并且已过任何许可证关联期限后，许可证可供重用。

   c. （可选）如果您的账户是某个组织的 License Manager 管理账户，则必须选择定义要从自动化发现中排除的资源。为此，请选择添加排除规则，选择要筛选的属性，支持 AWS 账户 ID 和资源标签，然后输入用于标识该属性的信息。

6. （可选）展开标签面板以将一个或多个标签添加到自管理许可证配置。标签是键/值对。为每个标签提供以下信息：

   - 键 — 键的可搜索名称。
   - 值 — 键的值。

7. 选择提交。

使用命令行创建自管理许可证配置

- create-license-configuration (AWS CLI)
- new-licm () LicenseConfigurationAWS Tools for PowerShell

共享自管理许可证

您可以使用 AWS Resource Access Manager 与任何 AWS 账户或通过 AWS Organizations任何账户共享您的自我管理许可证。有关更多信息，请参阅《AWS RAM 用户指南》中的共享 AWS 资源。

支持的账户配额

如果您在 2023 年 10 月 14 日 AWS License Manager 之前启用了许可证共享，则您的组织中 License Manager 支持的最大账户数量的配额将小于新的默认最大值。您可以通过使用下一节中提供 AWS RAM 的 API 操作来增加此配额。有关 License Manager 中默认配额的更多信息，请参阅 AWS 一般参考 指南中的使用许可证的配额。

先决条件

要完成以下步骤，您必须以组织管理账户中的主题身份登录并且必须拥有以下权限：

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

增加受支持的账户配额

以下步骤会将 `Number of accounts per organization for License Manager`的当前配额增加到当前默认最大数量。

增加 License Manager 的受支持账户配额

1. 使用describe-organization AWS CLI 命令通过以下操作来确定组织的 ARN：

```
aws organizations describe-organization

{
 "Organization": {
  "Id": "o-abcde12345",
  "Arn": "arn:aws:organizations::111122223333:organization/o-abcde12345",
  "FeatureSet": "ALL",
  "MasterAccountArn": "arn:aws:organizations::111122223333:account/o-
abcde12345/111122223333",
  "MasterAccountId": "111122223333",
  "MasterAccountEmail": "name+orgsidentifier@example.com",
  "AvailablePolicyTypes": [
    {
     "Type": "SERVICE_CONTROL_POLICY",
     "Status": "ENABLED"
    }
  ]
 }
}
```

2. 使用get-resource-shares AWS CLI 命令通过以下操作来确定组织的 ARN：

```
aws ram  get-resource-shares --resource-owner SELF --tag-filters
 tagKey=Service,tagValues=LicenseManager --region us-east-1

{
 "resourceShares": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "name": "licenseManagerResourceShare-111122223333",
    "owningAccountId": "111122223333",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "tags": [
     {
      "key": "Service",
      "value": "LicenseManager"
     }
    ],
    "creationTime": "2023-10-04T12:52:10.021000-07:00",
    "lastUpdatedTime": "2023-10-04T12:52:10.021000-07:00",
    "featureSet": "STANDARD"
  }
 ]
}
```

3. 使用enable-sharing-with-aws-organization AWS CLI 命令通过以下方式启用资源共享 AWS RAM：

```
aws ram enable-sharing-with-aws-organization

{
 "returnValue": true
}
```

您可以使用list-aws-service-access-for-organization AWS CLI 命令来验证 Organizations 列表是否已为 License Manager 启用服务主体，以及 AWS RAM：

```
aws organizations list-aws-service-access-for-organization

{
 "EnabledServicePrincipals": [
```

```
  {
    "ServicePrincipal": "license-manager.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.814000-07:00"
  },
  {
    "ServicePrincipal": "license-manager.member-account.amazonaws.com",
    "DateEnabled": "2023-10-04T12:50:59.565000-07:00"
  },
  {
    "ServicePrincipal": "ram.amazonaws.com",
    "DateEnabled": "2023-10-04T13:06:34.771000-07:00"
  }
 ]
}
```

> **Important**
>
> 您的组织可能需要长达六个小时 AWS RAM 才能完成此操作。必须先完成此过程，然后才能继续。

4. 使用associate-resource-share AWS CLI 命令将您的 License Manager 资源共享与您的组织相关联：

```
aws ram associate-resource-share --resource-share-arn arn:aws:ram:us-
east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --
principals arn:aws:organizations::111122223333:organization/o-abcde12345 --
region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATING",
    "external": false
  }
 ]
}
```

您可以使用get-resource-share-associations AWS CLI 命令来验证资源共享关联是否status为ASSOCIATED：

```
aws ram get-resource-share-associations --association-type "PRINCIPAL" --principal
 arn:aws:organizations::111122223333:organization/o-abcde12345--resource-share-
arns arn:aws:ram:us-east-1:111122223333:resource-share/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 --region us-east-1

{
 "resourceShareAssociations": [
  {
    "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "resourceShareName": "licenseManagerResourceShare-111122223333",
    "associatedEntity": "arn:aws:organizations::111122223333:organization/o-
abcde12345",
    "associationType": "PRINCIPAL",
    "status": "ASSOCIATED",
    "creationTime": "2023-10-04T13:12:33.422000-07:00",
    "lastUpdatedTime": "2023-10-04T13:12:34.663000-07:00",
    "external": false
  }
 ]
}
```

编辑自管理许可证

您可以在自管理许可证中编辑以下字段的值：

- 自管理许可证名称
- 描述
- <option> 数
- 强制执行许可证类型限制

编辑自管理许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。

3. 选择自管理许可证。
4. 选择 Actions（操作）和 Edit（编辑）。
5. 根据需要编辑详细信息，然后选择更新。

使用命令行编辑自管理许可证

- update-license-configuration (AWS CLI)
- update-licm () LicenseConfigurationAWS Tools for PowerShell

停用自管理许可证

在停用自管理许可证时，使用该许可证的现有资源不会受到影响，仍然可以启动使用该许可证的 AMI。不过，不再跟踪许可证使用情况。

停用自管理许可证后，不得将其附加到任何正在运行的实例。停用后，无法使用自管理许可证执行启动。

停用自管理许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证。
4. 选择操作，停用。当系统提示您确认时，请选择 Deactivate (停用）。

使用命令行停用自管理许可证

- update-license-configuration (AWS CLI)
- update-licm () LicenseConfigurationAWS Tools for PowerShell

删除自管理许可证

在可以删除自管理许可证之前，您必须解除关联所有资源。如果您需要重新开始使用新的许可规则，则可以删除自管理许可证。如果软件供应商的许可条款发生变更，您可以解除关联现有资源，删除自管理许可证，创建新的自管理许可证以反映更新的条款，并将其与现有资源关联。

使用控制台删除自管理许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证的名称以打开许可证详细信息页面。
4. 选择每个资源（单独或批量），然后选择取消关联资源。重复该操作，直到列表为空。
5. 依次选择 Actions（操作）和 Delete（删除）。当系统提示进行确认时，选择 Delete（删除）。

使用命令行删除自管理许可证

- delete-license-configuration (AWS CLI)
- Remove-licm LicenseConfiguration ()AWS Tools for PowerShell

License Manager 中的许可证规则

在创建自管理许可证规则后，可以将其附加到相关的启动机制，它们可以在其中直接禁止部署不合规的新资源。组织中的用户可以从指定的 AMI 中无缝地启动 EC2 实例，管理员可以通过内置的 License Manager 控制面板跟踪许可证清单。可以通过启动控件和控制面板警报更轻松地实施合规性。

> **Important**
>
> AWS 不参与软件供应商的审核流程。客户负责满足合规性要求，并负责根据其许可协议仔细了解规则并将其捕获到 License Manager 中。

许可证跟踪从将规则附加到实例时开始，一直跟踪到实例终止。您可以定义使用限制和许可规则，License Manager 将跟踪部署，同时还提醒您违反规则的情况。如果配置了硬限制，License Manager 可能会禁止启动资源。

在停止或终止跟踪的服务器时，将释放其许可证并退回到可用的许可证池。

由于组织采用不同的方法实施操作和合规性，因此，License Manager 支持多种启动机制：

- 手动将自管理许可证与 AMI 相关联 — 要跟踪操作系统或其他软件的许可证，您可以在发布 AMI 之前附加许可规则，以便在组织中更广泛地使用。将使用 License Manager 自动跟踪来自这些 AMI 的任何部署，而无需用户执行任何其他操作。您还可以将许可规则附加到当前 AMI 构建机制，例如 Systems Manager Automation、VM Import/Export 和 Packer。

- Amazon EC2 启动模板和 AWS CloudFormation — 如果将许可规则附加到 AMI 不是首选选项，则可以在 EC2 启动模板或AWS CloudFormation 模板中将其指定为可选参数。将使用 License Manager 跟踪使用这些模板进行的部署。您可以通过在自我管理许可证字段中指定一个或多个自行管理的许可证 ID，对 EC2 启动 AWS CloudFormation 模板或模板强制执行规则。

AWS 将许可证跟踪数据视为敏感的客户数据，只能通过拥有该数据的 AWS 帐户进行访问。 AWS 无法访问您的许可证跟踪数据。您可以控制许可证跟踪数据，并且可以随时将其删除。

将自管理许可证和 AMI 相关联

以下过程演示如何使用 License Manager 控制台将自管理许可证与 AMI 相关联。该过程假设您至少有一个现有的自管理许可证。您可以将自管理许可证与您有权访问的任何 AMI 相关联，无论是您拥有的还是共享的。如果与您共享了 AMI，则可以将其与当前账户中的自管理许可证相关联。否则，您可以指定 AMI 是与所有账户的自管理许可证相关联，还是仅与当前账户中的自管理许可证相关联。

如果您将 AMI 与所有账户的自管理许可证相关联，则可以跨账户跟踪从 AMI 启动的实例。当达到硬限制时，License Manager 会阻止启动其他实例。当达到软限制时，License Manager 会通知您其他实例已启动。

如果您在同一区域内复制 AMI，并且该 AMI 关联了许可配置，则这些许可配置将自动与新 AMI 关联。当您从新 AMI 启动实例时，License Manager 会对其进行跟踪。同样，如果您从具有相关许可配置的正在运行的实例创建新 AMI，则这些许可配置将自动与新 AMI 关联，License Manager 会跟踪您从新 AMI 启动的实例。

> **Warning**
>
> License Manager 不支持跨区域实例跟踪。如果您将关联许可配置的 AMI 复制到其他区域，License Manager 会阻止从新 AMI 启动所有实例。

将自管理许可证和 AMI 相关联

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证的名称以打开许可证详细信息页面。要查看当前关联的 AMI，请选择已关联 AMI。
4. 选择关联 AMI。

5. 对于可用 AMI，选择一个或多个 AMI，然后选择关联。
   - 如果您的账户至少拥有一个 AMI，则系统会提示您为自己拥有的 AMI 选择 AMI 关联范围。从其他账户共享的任何 AMI 仅与您的账户关联。选择确认。
   - 如果 AMI 是通过其他账户与您共享的，则它们仅与您的账户关联。

   新关联的 AMI 现在显示在许可证详细信息页面的已关联 AMI 选项卡上。

解除自管理许可证和 AMI 的关联

以下过程说明了如何使用 License Manager 控制台解除自管理许可证和 AMI 的关联。无法解除对已注销的 AMI 的关联。License Manager 每 8 小时检查一次已注销的 AMI，并自动将其解除关联。

解除自管理许可证和 AMI 的关联

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证的名称以打开许可证详细信息页面。
4. 选择 Associated AMIs (关联的 AMI)。
5. 选择 AMI 并选择取消关联 AMI。

License Manager 中的使用情况报告

使用 AWS License Manager，您可以通过安排对许可证使用情况进行定期快照来跟踪自管理许可证的历史记录。通过设置使用情况报告，License Manager 会根据您的规范要求自动将您的自管理许可证报告上传到 S3 存储桶。使用情况报告以前称为报告生成器。您可以设置多个使用情况报告，以有效地跟踪环境中不同许可证类型的配置。

> **Note**
>
> AWS License Manager 不存储您的报告。License Manager 报告会直接发布到 S3 存储桶。删除使用情况报告后，报告将不再发布到您的 S3 存储桶。

创建使用情况报告

创建使用情况报告时，您可以指定 License Manager 要跟踪的自管理许可证类型、定义报告生成频率间隔以及报告类型。所有报告均以 CSV 格式生成并发布到 S3 存储桶。使用情况报告可以生成以下一种或多种报告类型。

自管理许可证摘要报告

此报告类型包含有关已使用的许可证数量的信息以及有关自管理许可证的详细信息。列出了跟踪的自管理许可证类型，其中包含许可证计数、许可证规则以及许可证在不同资源类型的分布等详细信息。

资源使用情况报告

此报告类型为您提供有关您跟踪的资源及其许可证使用的详细信息。使用指定的自管理许可证类型的每个跟踪资源都将列出详细信息，例如许可证 ID、资源状态和拥有该资源的 AWS 账户 ID。

创建使用情况报告

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从导航窗格中，选择使用情况报告。
3. 选择创建使用情况报告，然后从创建使用情况报告窗格中定义报告的参数：
   a. 为您的使用情况报告输入名称和可选描述。
   b. 从下拉列表中选择自管理许可证类型。这是使用情况报告将生成数据的许可证类型。
   c. 选择要生成的报告类型。
   d. 选择 License Manager 发布报告的频率，您可以选择每 24 小时一次、每 7 天一次或每 30 天一次。
   e. （可选）添加标签以跟踪使用情况报告资源。
4. 选择创建使用情况报告。

新的使用情况报告将在 60 分钟或更短的时间内开始发布报告。

如果您的账户还没有关联的 S3 存储桶，则当您创建使用情况报告时，License Manager 将在您的账户中创建一个新的 Amazon S3 存储桶。如果您之前启用了跨账户库存搜索，则在启用跨账户库存搜索后，报告将发送到 License Manager 创建的 S3 存储桶。

报告使用以下 Amazon S3 URI 模式存储在您的存储桶中：

```
s3://aws-license-manager-service-*/Reports/usage-report-name/year/months/day/report-id.csv
```

编辑使用情况报告

您可以随时从 License Manager 控制台查看和更改使用情况报告。使用情况报告表列出了为您的账户创建的所有使用情况报告，您可以从该表中概览不同的报告，转到与您的使用情况报告关联的 Amazon S3 存储桶，并查看报告生成状态。

编辑使用情况报告

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从导航窗格中，选择使用情况报告。
3. 从表格中选择要编辑的使用情况报告，然后选择查看详细信息。
4. 选择编辑可对使用情况报告进行更改。
5. 对使用情况报告进行所需的更改，然后选择保存更改。

更新后的使用情况报告将在一小时内生成一份新报告。

> **Note**
>
> 更改使用情况报告的名称后，今后的报告将发送到 License Manager S3 存储桶中反映新名称的新文件夹。

删除使用情况报告

删除使用情况报告后，会停止生成新报告，但是，您的 Amazon S3 存储桶和之前的所有报告都不会受到影响。

> **Note**
>
> 如果自管理许可证关联了使用情况报告，则无法将其从您的账户中删除。必须先删除该使用情况报告。

编辑使用情况报告

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从导航窗格中，选择使用情况报告。
3. 从表格中选择要编辑的使用情况报告，然后选择查看详细信息。
4. 选择删除。此操作将永久删除使用情况报告。

License Manager 中的许可证类型转换

借助 License Manager，您可以根据业务需求的变化，在 AWS 提供的许可和自带许可模式 (BYOL) 或自带订阅模式 (BYOS) 之间更改许可证类型。无需重新部署现有工作负载即可更改许可证类型。

您可以使用许可证类型转换功能针对以下情况优化许可证清单：

将本地工作负载迁移到 Amazon EC2

在迁移期间，您可以将工作负载部署到亚马逊弹性计算云 (Amazon EC2)，并 AWS 使用提供的许可。迁移完成后，使用 License Manager 许可证类型转换功能来更改实例的许可证类型。您可以更改为 BYOL 或 BYOS，以便可以使用迁移期间发布的许可证。

在许可协议即将到期的情况下继续运行工作负载

您可以使用 License Manager 许可类型转换从 BYOL 或 BYOS 切换到 AWS 提供的许可。此开关允许您使用灵活的 pay-as-you go 许可模式提供的完全合规 AWS 的软件许可证继续运行工作负载。如果您与操作系统的软件供应商（例如 Microsoft 或 Canonical）签订的许可协议即将到期，并且您不打算续订，则可以选择这样操作。

优化成本

对于小型或不规则的工作负载， AWS 提供的许可证（包括许可证）实例可能更具成本效益。当您选择使用 BYOL 或 BYOS 时，此类选项可能需要长期订阅。在这种情况下，您可以使用 License Manager 许可证类型转换功能将您的实例切换为随附许可证，以优化许可相关成本。如果您的实例是从您自己的虚拟机 (VM) 映像启动的，则可以切换回 BYOL 或 BYOS。当工作负载更加稳定或可预测时，你可以选择这样操作。

扩展维护

如果您的 Ubuntu 操作系统的标准支持已到期，则可以添加 Ubuntu Pro 的付费订阅。添加 Ubuntu Pro 订阅，可在较长时间内提供安全更新。有关更多信息，请参阅 Canonical 文档中的 Ubuntu Pro。

主题

符合许可证类型转换条件的许可证类型

您可以将 License Manager 许可证类型转换与 Windows Server 和Microsoft SQL Server 许可证支持的版本和组合一起使用。您也可以在 Ubuntu Linux 订阅中使用许可证类型转换功能。

目录

适用于 Windows Server 和 SQL Server 符合条件的许可证类型

> **Important**
>
> 最初从 Amazon 提供的亚马逊机器映像 (AMI) 启动的实例不符合将许可类型转换为 BYOL 的条件。

Windows Server 和 SQL Server 必须满足某些要求才有资格进行许可证类型转换。

主题

- 使用操作值
- 媒体兼容性
- 转换路径

SQL Server 版本

License Manager 支持以下 SQL Server 版本：

- SQL Server 标准版
- SQL Server 企业版
- SQL Server Web 版

SQL Server 版本

License Manager 支持以下 SQL Server 版本：

- SQL 服务器 2005
- SQL Server
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

使用操作值

许可证类型转换会更改与您的实例关联的使用操作值。下表显示了每个受支持的操作系统的使用情况值。有关更多信息，请参阅 AMI 计费信息字段。

操作系统详细信息	使用情况操作
Windows Server 为 BYOL 模式	RunInstances:0800
Windows Server 为 BYOL 模式	RunInstances:0800

操作系统详细信息	使用情况操作
SQL Server（任何版本）为 BYOL 模式	
Windows Server 使用随附许可证	RunInstances:0002
Windows Server 使用随附许可证 SQL Server（任何版本）为 BYOL 模式	RunInstances:0002
Windows Server 使用随附许可证 SQL Server Web 使用随附许可证	RunInstances:0202
Windows Server 使用随附许可证 SQL Server Standard 使用随附许可证	RunInstances:0006
Windows Server 使用随附许可证 SQL Server Enterprise 使用随附许可证	RunInstances:0102

媒体兼容性

下表确认了哪些媒体可以在哪些实例许可模式上使用。

来源	目标	
	BYOL	随附许可证
AWS 提供了 Windows 服务器镜像	否	是
AWS 提供了 SQL 服务器镜像	否	是
您的 Windows Server 媒体[1]	是	是
您的 SQL Server 媒体[2]	是	是

[1] 表示该实例最初是从您自己导入的虚拟机 (VM) 启动的。您可以使用 VM Import/Export 或 AWS Application Migration Service 等服务导入 VM。

[2] 表示您已获取自己的 SQL Server 安装媒体（.iso、.exe）。

转换路径

下表确认了来源许可证模式是否可以在 BYOL 和随附许可证之间转换为另一种模式。有关更多信息，请参阅 转换许可证类型。

> **Important**
>
> - Windows Server 为 BYOL 模式且 SQL Server 使用随附许可证，这种配置不受支持。
> - 指定为“不需要”的转换不会更改使用操作值。

来源	目标					
	Windows Server 为 BYOL 模式	Windows Server 使用随附许可证	Windows Server 为 BYOL 模式 SQL Server 为 BYOL 模式	Windows Server 使用随附许可证 SQL Server 为 BYOL 模式	Windows Server 为 BYOL 模式 SQL Server 使用随附许可证	Windows Server 使用随附许可证 SQL Server 使用随附许可证
Windows Server 为 BYOL 模式（您的媒体）	不需要	是	不需要	是[1]	不支持	是[1]
Windows Server 使用随附许可	是[2]	不需要	是的 [1、2]	不需要 [3]	不支持	是[1]

来源	目标					
证（您的媒体）						
包含许可的 Windows 服务器（AWS 提供的图片）	不是 ✗	不需要	不是 ✗	不需要 [3]	不支持	是[1]
Windows Server 为 BYOL 模式（您的媒体）	不需要 [4]	是	不需要	是	不支持	是
SQL Server 为 BYOL 模式（您的媒体）						
Windows Server 使用随附许可证（您的媒体）	是[2]	不需要 [4]	是[2]	不需要	不支持	是
SQL Server 为 BYOL 模式（您的媒体）						

来源	目标					
包含许可的 Windows 服务器（AWS 提供的图片）	不是 ✗	不需要 [4]	不是 ✗	不需要	不支持	是
SQL Server 为 BYOL 模式（您的媒体）						
Windows Server 为 BYOL 模式（您的媒体）	不支持	不支持	不支持	不支持	不支持	不支持
SQL Server 使用随附许可证						
包含许可的 Windows 服务器（AWS 提供的图像或您的媒体）	不是 ✗	不是 ✗	不是 ✗	不是 ✗	不支持	不需要
包含许可证的 SQL Server（AWS 提供的图片）						

来源	目标					
Windows Server 使用随附许可证（您的媒体）	是的[2、5、6]	是[5]	是[2]	是	不支持	不需要
SQL Server 使用随附许可证（您的媒体）						
包含许可的 Windows 服务器（AWS 提供的图片）	不是 ✗	是[5]	不是 ✗	是	不支持	不需要
SQL Server 使用随附许可证（您的媒体）						

✗ 您必须使用替代配置部署新实例，因为不支持转换为目标许可证类型。有关更多信息，请参阅 媒体兼容性。

对于其他转换方案，您可能需要采取以下步骤来执行许可证转换：

[1] 在针对 SQL Server 转换为 BYOL 模式之前，必须先安装 SQL Server。

[2] 必须先修改您的 Windows 配置，才能使用自己的 KMS 服务器激活许可证。有关更多信息，请参阅 Convert Windows Server from license included to BYOL。

[3] 从不使用 SQL Server 的来源转换为使用 SQL Server 的目标时，必须先安装 SQL Server（不管 SQL Server 许可证类型如何）。

[4] 从使用 SQL Server 的来源转换为不使用 SQL Server 的目标时，必须先卸载 SQL Server（不管 SQL Server 许可证类型如何）。

[5] 在转换为随附许可证的 SQL Server 之前，必须先卸载 SQL Server。

[6] 必须先执行 [2] 和 [5] 的步骤。完成这些步骤后，必须将许可证类型转换为“Windows Server 使用随附许可证”，然后将许可证类型再次转换为“Windows Server 为 BYOL 模式”。

符合条件的 Linux 订阅类型

受支持的 Ubuntu 版本可以进行许可证类型转换。受支持的版本包括例如 Ubuntu 18.04.1 LTS 之类的更新。当您将订阅转换为 Ubuntu Pro 时，将再提供五年的安全更新。有关更多信息，请参阅 Canonical 文档中的 Ubuntu Pro。

您可以在以下 Ubuntu 版本中使用许可证类型转换功能：

- Ubuntu 16.04 LTS
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Ubuntu 22.04 LTS

操作系统详细信息	使用情况操作
Linux/Unix	RunInstances
Ubuntu Pro	RunInstances:0g00

Linux 的转换路径

你可以将任何受支持的 Ubuntu LTS 版本转换为 Ubuntu Pro。如果您需要从 Ubuntu Pro 转换为 Ubuntu LTS，则需要向 AWS Support提出请求。有关更多信息，请参阅创建支持案例。

转换先决条件

要使用 License Manager 转换许可证类型，需要满足常规先决条件和特定于操作系统的先决条件。

主题

- 常规
- Windows
- Linux

常规

在执行许可证类型转换之前，您必须满足以下常规先决条件：

- 您 AWS 账户 必须已加入 License Manager。请参阅 入门 AWS License Manager。
- 在转换许可证类型之前，目标实例必须处于停止状态。有关更多信息，请参阅 Amazon EC2 用户指南中的停止和启动您的实例。
- 如果在目标实例上启用了停止保护，则转换过程将失败。有关更多信息，请参阅 排查许可证类型转换问题。
- 目标实例必须使用 S AWS ystems Manager 清单进行配置。有关更多信息，请参阅 AWS Systems Manager 用户指南中的为 EC2 实例设置 Systems Manager 和 AWS Systems Manager 清单。
- 用户或角色必须包括以下权限：
  - `ssm:GetInventory`
  - `ssm:StartAutomationExecution`
  - `ssm:GetAutomationExecution`
  - `ssm:SendCommand`
  - `ssm:GetCommandInvocation`
  - `ssm:DescribeInstanceInformation`
  - `ec2:DescribeImages`
  - `ec2:DescribeInstances`
  - `ec2:StartInstances`
  - `ec2:StopInstances`
  - `license-manager:CreateLicenseConversionTaskForResource`
  - `license-manager:GetLicenseConversionTask`
  - `license-manager:ListLicenseConversionTasks`
  - `license-manager:GetLicenseConfiguration`
  - `license-manager:ListUsageForLicenseConfiguration`
  - `license-manager:ListLicenseSpecificationsForResource`

- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`

有关 Systems Manager Inventory 的更多信息，请参阅 AWS Systems Manager 清单。

Windows

Windows 实例必须满足以下先决条件：

- 最初从 Amazon 提供的亚马逊机器映像 (AMI) 启动的实例不符合将许可类型转换为 BYOL 的条件。必须从您自己的虚拟机 (VM) 映像启动原始 Amazon EC2 实例。有关将 VM 转换为 Amazon EC2 的更多信息，请参阅 VM Import/Export。
- 要将您的 SQL Server 许可证更改为 BYOL，必须使用您自己的媒体安装 SQL Server。

Linux

Linux 实例必须满足以下先决条件：

- 实例必须运行 Ubuntu LTS。
- Ubuntu Pro 客户端必须安装在您的 Ubuntu 操作系统中。
  - 运行以下命令确认是否安装了 Ubuntu Pro 客户端：

    ```
    pro --version
    ```

  - 如果找不到该命令，或者需要更新版本，请运行以下命令来安装 Ubuntu Pro 客户端：

    ```
    apt-get update && apt-get dist-upgrade
    ```

- 实例必须能够访问多个终端节点才能激活其 Ubuntu Pro 订阅并接收更新。您必须允许来自实例的出站流量通过 TCP 端口 443 到达以下终端节点：
  - contracts.canonical.com — 用于激活 Ubuntu Pro。
  - esm.ubuntu.com — 用于访问大多数服务的 APT 存储库。
  - api.snapcraft.io — 用于安装和运行快照。
  - dashboard.snapcraft.io — 用于安装和运行快照。
  - login.ubuntu.com — 用于安装和运行快照。
  - cloudfront.cdn.snapcraftcontent.com — 用于从内容开发网络 (CDN) 下载内容。

- livepatch.canonical.com — 用于从 Livepatch 服务器下载补丁。

有关更多信息，请参阅 Ubuntu Pro Client 文档中的 Ubuntu Pro Client 网络要求和 Canonical Snapcraft 文档中的网络要求。

转换许可证类型

您可以使用 License Manager 控制台或 AWS CLI转换 Windows 许可证、Microsoft SQL Server 许可证和 Ubuntu Linux 订阅。您可能需要完成其他步骤才能在实例的操作系统中转换许可证或订阅。

您可以使用 License Manager 控制台或 AWS CLI转换许可证类型。当您创建许可证类型转换时，License Manager 会验证您的实例上的计费产品。如果这些初步验证成功，License Manager 将创建许可证类型转换。您可以使用`list-license-conversion-tasks`和 `get-license-conversion-task` AWS CLI 命令检查许可证类型转换的状态。

作为许可类型转换的一部分，License Manager 可能会更新与您的自管理许可证关联的资源。具体来说，对于具有自动化发现规则类型为`License Included`的任何自管理许可证，如果`license included`自动化发现规则明确排除该资源，则 License Manager 会解除许可类型转换中的资源与许可证的关联。

例如，如果您的自管理许可证包含两条自动化发现规则，并且每条规则都不包括随附许可证的 Windows Server，则许可证类型从 BYOL 转换为随附许可证的 Windows Server 会导致实例与自管理许可证解除关联。但是，如果两条自动化发现规则中只有一条`License Included`规则，则该实例不会解除关联。

在许可证类型转换过程中，您不应启动或停止实例。许可证类型转换成功后，其状态将由 `IN_PROGRESS` 更改为 `SUCCEEDED`。如果 License Manager 在工作流程中遇到问题，它会将许可证类型转换的状态更新为 `FAILED`，并使用错误消息更新状态消息。

> **Note**
>
> 转换许可证类型时，用于启动实例的 AMI 上的计费产品信息不会发生变更。要检索准确的账单信息，请使用 Amazon EC2 `DescribeInstances` API。此外，如果您现有的工作流程可以从 AMI 中搜索账单信息，请更新此类工作流程以使用 `DescribeInstances`。

目录

转换适用于 Windows Server 和 SQL Server 的许可证类型

你可以使用 License Manager 控制台或转换符合条件的 Windows 和 SQL Server 实例的许可类型。AWS CLI

主题

许可证类型转换限制

> **Important**
>
> Microsoft 软件的使用受 Microsoft 许可条款的约束。您有责任遵守 Microsoft 许可条款。提供本文档是为了方便起见，您无权依赖其描述。本文件不构成法律建议。如果您对 Microsoft 软件的许可权利有任何疑问，请咨询您的法律团队、Microsoft 或 Microsoft 分销商。

License Manager 限制了您可以根据 Microsoft 服务提供商许可协议 (SPLA) 创建的许可证转换类型。下面列出了许可证类型转换需要遵守的一些限制。这不是一份完整列表，可能会发生变化。

- 必须从您自己的虚拟机 (VM) 映像启动 Amazon EC2 实例。
- 随附许可证的 SQL Server 不能在专属主机上运行。
- 随附许可证的 SQL Server 实例必须至少具有四个 vCPU。

使用 License Manager 控制台转换许可证类型

您可以使用 License Manager 控制台转换许可证类型。

> **Note**
>
> 仅显示处于停止状态且已通过 AWS Systems Manager 清单关联的实例。

在控制台中开始许可证类型转换

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择许可证类型转换，然后选择创建许可证类型转换。
3. 对于源操作系统，请选择要转换的实例的平台：
    1. Ubuntu LTS
    2. Windows BYOL
    3. Windows 随附许可证
4. （可选）通过为实例 ID 或使用操作值指定值来筛选可用实例。
5. 选择要转换其许可证的实例，然后选择下一步。
6. 输入许可证类型的使用操作值，选择要转换到的许可证，然后选择下一步。
7. 确认您对许可证类型转换配置感到满意，然后选择开始转换。

您可以从许可证类型转换面板查看许可证类型转换的状态。转换状态列将转换状态显示为正在进行中、已完成或失败。

> **Important**
>
> 如果您将 Windows Server 的模式从随附许可证转换为 BYOL，则必须根据 Microsoft 许可协议激活 Windows。请参阅Convert Windows Server from license included to BYOL了解更多信息。

使用转换许可证类型 AWS CLI

在 AWS CLI中开始许可证类型转换：

确定实例的许可证类型

1. 确认已安装并设置 AWS CLI。有关更多信息，请参阅安装、更新和卸载 AWS CLI 以及配置 AWS CLI。

   > **Important**
   >
   > 在以下步骤中，您可能需要更新 AWS CLI 才能运行某些命令并接收所有必需的输出。

2. 验证您是否有权运行该`create-license-conversion-task-for-resource` AWS CLI 命令。如需帮助，请参阅为 License Manager 创建 IAM 策略。
3. 要确定当前与您的实例关联的许可证类型，请运行以下 AWS CLI 命令。将实例 ID 替换为要确定其许可证类型的实例的 ID。

   ```
   aws ec2 describe-instances --instance-ids <instance-id> --query
    "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
    PlatformDetails, UsageOperation: UsageOperation, UsageOperationUpdateTime:
    UsageOperationUpdateTime}"
   ```

4. 以下是 `describe-instances` 命令的示例响应。请注意，`UsageOperation` 值是与许可证关联的账单信息代码。`UsageOperationUpdateTime` 是账单代码的更新时间。有关更多信息，请参阅 Amazon EC2 API 参考中的 DescribeInstances。

   ```
   "InstanceId": "i-0123456789abcdef",
   "Platform details": "Windows with SQL Server Enterprise",
   "UsageOperation": "RunInstances:0800",
   "UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
   ```

> **Note**
>
> 具有 SQL Server Enterprise BYOL 的 Windows Server 的使用操作与 Windows BYOL 的使用操作相同，因为它们的计费方式相同。

将 Windows Server 从随附许可证转换为 BYOL

当您将 Windows Server 从随附许可证转换为 BYOL 时，License Manager 不会自动激活 Windows。您必须将您的实例的 KMS 服务器从 AWS KMS 服务器切换到您自己的 KMS 服务器。

> **Important**
>
> 要从随附许可证转换为 BYOL，必须从您自己的虚拟机 (VM) 映像启动原始 Amazon EC2 实例。有关将 VM 转换为 Amazon EC2 的更多信息，请参阅 VM Import/Export。最初从亚马逊机器映像 (AMI) 启动的实例没有不符合转换为 BYOL 的条件。

查看您的 Microsoft 许可协议，确定可以使用哪些方法来激活 Microsoft Windows Server。例如，如果您使用的是 KMS 服务器，则必须从实例的原始 BYOL 配置中获取 KMS 服务器的地址。

1. 要转换您的实例的许可证类型，请运行以下命令，将 ARN 替换为您要转换的实例的 ARN：

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0002 \
    --destination-license-context UsageOperation=RunInstances:0800
```

2. 要在转换许可证后激活 Windows，必须将操作系统的 Windows Server KMS 服务器指向您自己的 KMS 服务器。登录到 Windows 实例并运行以下命令：

```
slmgr.vbs /skms <your-kms-address>
```

将 Windows Server 从 BYOL 转换为随附许可证

当你将 Windows Server 从 BYOL 转换为包含许可证时，License Manager 会自动将你的实例的 KMS 服务器切换到 AWS KMS 服务器。

要将您的实例的许可证类型从 BYOL 转换为随附许可证，请运行以下命令，将 ARN 替换为要转换的实例的 ARN：

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0800 \
    --destination-license-context UsageOperation=RunInstances:0002
```

将 Windows Server 和 SQL Server 从 BYOL 转换为包含的许可证

您可以同时切换多款产品。例如，您可以通过一次许可证类型转换来转换 Windows Server 和 SQL Server。

要将 Windows Server 实例的许可证类型从 BYOL 转换为随附许可证，将 SQL Server Standard 从 BYOL 转换为随附许可证，请运行以下命令，将 ARN 替换为要转换的实例的 ARN：

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances:0800 \
    --destination-license-context UsageOperation=RunInstances:0006
```

转换适用于 Linux 的许可证类型

您可以使用 License Manager 控制台或转换符合条件的 Ubuntu LTS 实例的许可证类型。 AWS CLI

主题

许可证类型转换注意事项

下面列出了许可证类型转换需要考虑的一些注意事项。这不是一份完整列表，可能会发生变化。

- 该实例必须运行 Ubuntu LTS 才能将许可证类型转换为 Ubuntu Pro。
- 您不能对 Ubuntu Pro 订阅使用许可证类型转换功能。要移除 Ubuntu Pro 订阅，请参阅移除 Ubuntu Pro 订阅。
- Ubuntu Pro 不可用作预留实例。如需通过按需型实例定价节省费用，建议您使用配套 Savings Plans 的 Ubuntu Pro。有关更多信息，请参阅 Amazon EC2 用户指南中的预留实例和什么是储蓄计划？在 Savin gs Plans 用户指南中。

使用 License Manager 控制台转换许可证类型

您可以使用 License Manager 控制台转换许可证类型。

> **Note**
>
> 仅显示处于停止状态且已通过 AWS Systems Manager 清单关联的实例。

在控制台中开始许可证类型转换

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择许可证类型转换，然后选择创建许可证类型转换。
3. 对于源操作系统，请选择要转换的实例的平台：
    1. Ubuntu LTS
    2. Windows BYOL
    3. Windows 随附许可证
4. （可选）通过为实例 ID 或使用操作值指定值来筛选可用实例。
5. 选择要转换其许可证的实例，然后选择下一步。
6. 输入许可证类型的使用操作值，选择要转换到的许可证，然后选择下一步。
7. 确认您对许可证类型转换配置感到满意，然后选择开始转换。

您可以从许可证类型转换面板查看许可证类型转换的状态。转换状态列将转换状态显示为正在进行中、已完成或失败。

使用转换许可证类型 AWS CLI

要在中开始许可证类型转换 AWS CLI，您应确认您的实例的许可证类型符合条件，然后执行许可证类型转换以更改为所需的订阅。有关符合条件的订阅类型的更多信息，请参阅符合条件的 Linux 订阅类型。

确定实例的许可证类型

确认已安装并设置 AWS CLI。有关更多信息，请参阅安装、更新和卸载 AWS CLI 以及配置。 AWS CLI

> **Important**
>
> 在以下步骤中，您可能需要更新 AWS CLI 才能运行某些命令并接收所有必需的输出。验证您是否有权运行该`create-license-conversion-task-for-resource` AWS CLI 命令。有关更多信息，请参阅 为 License Manager 创建 IAM 策略。

要确定当前与您的实例关联的许可证类型，请运行以下 AWS CLI 命令。将实例 ID 替换为要确定其许可证类型的实例的 ID：

```
aws ec2 describe-instances --instance-ids <instance-id> --query
 "Reservations[*].Instances[*].{InstanceId: InstanceId, PlatformDetails:
 PlatformDetails, UsageOperation: UsageOperation, UsageOperationUpdateTime:
 UsageOperationUpdateTime}"
```

以下是 `describe-instances` 命令的示例响应。该UsageOperation值是与许可证关联的账单信息代码。使用操作值为 `RunInstances` 表示实例正在使用 AWS 提供的许可。`UsageOperationUpdateTime` 是账单代码的更新时间。有关更多信息，请参阅 Amazon EC2 API 参考中的 DescribeInstances。

```
"InstanceId": "i-0123456789abcdef",
"Platform details": "Linux/UNIX",
"UsageOperation": "RunInstances",
"UsageOperationUpdateTime: "2021-08-16T21:16:16.000Z"
```

转换为 Ubuntu Pro

当您将实例从 Ubuntu LTS 转换为 Ubuntu Pro 时，您必须拥有该实例的出站 Internet 访问权限，才能从 Canonical 服务器检索许可证令牌并安装 Ubuntu Pro 客户端。有关更多信息，请参阅 转换先决条件。

将 Ubuntu LTS 转换为 Ubuntu Pro：

1. 在指定实例的 ARN 的 AWS CLI 同时运行以下命令：

```
aws license-manager create-license-conversion-task-for-resource \
    --resource-arn <instance_arn> \
    --source-license-context UsageOperation=RunInstances \
    --destination-license-context UsageOperation=RunInstances:0g00
```

2. 在实例中运行以下命令以检索有关您的 Ubuntu Pro 订阅状态的详细信息：

```
pro status
```

3. 确认您的输出表明该实例已订阅有效的 Ubuntu Pro：

```
ubuntu@ip-                pro status
SERVICE                   STATUS    DESCRIPTION
cc-eal          yes       disabled  Common Criteria EAL2 Provisioning Packages
cis             yes       disabled  Security compliance and audit tools
esm-apps        yes       disabled  Expanded Security Maintenance for Applications
esm-infra       yes       enabled   Expanded Security Maintenance for Infrastructure
fips            yes       disabled  NIST-certified core packages
fips-updates    yes       disabled  NIST-certified core packages with priority security updates
livepatch       yes       enabled   Canonical Livepatch service

Enable services with: pro enable <service>

               Account:
          Subscription:
           Valid until: Fri Dec 31 00:00:00 9999 UTC
Technical support level: essential
```

移除 Ubuntu Pro 订阅

许可证类型转换只能用于从 Ubuntu LTS 转换为 Ubuntu Pro。如果您需要从 Ubuntu Pro 转换为 Ubuntu LTS，则需要向 AWS Support提出请求。有关更多信息，请参阅创建支持案例。

租赁转换

您可以更改实例的租赁，使其最适合您的使用案例。你可以使用 m odify-instance-placemence-placemence- AWS CLI placem ence 命令在

- 共享
- 专用实例
- 专属主机
- 主机资源组

您的账户必须有一台具有可用容量的专属主机才能启动实例，才能切换到专属主机租赁类型。有关使用专属主机的更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南中的使用专属主机。

要移至主机资源组租赁类型，您的账户中必须至少有一个主机资源组。要将实例启动到主机资源组中，该实例必须具有与主机资源组关联的相同许可证集。有关更多信息，请参阅 AWS License Manager 中的主机资源组。

租赁转换限制

以下限制适用于租赁转换：

- 所有租赁类型都允许使用 Linux 账单代码。
- 共享租赁不允许使用 Windows BYOL 账单代码。
- 所有租赁类型都允许使用 Windows Server 随附许可证的账单代码。
- 共享租赁和专用实例允许使用所有受支持的 SQL Server 版本、Red Hat (RHEL) 和 SUSE (SLES) 随附许可证的账单代码。但是，专属主机和主机资源组不允许使用这些账单代码。
- 除了 Windows Server 之外，不允许在专属主机和主机资源组上使用随附许可证的账单代码。

使用更改实例的租期 AWS CLI

实例必须处于 `stopped` 状态才能更改其租赁属性。

要停止实例，请运行以下命令：

```
aws ec2 stop-instances --instance-ids <instance_id>
```

要将实例从任何租赁更改为 `default` 或 `dedicated` 租赁，请运行以下命令：

`default`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy default
```

`dedicated`

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy dedicated
```

要使用自动放置功能将实例从任何租赁更改为 `host` 租赁，请运行以下命令：

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --affinity default
```

要将实例从任何租赁更改为 `host` 租赁，针对特定专属主机，请运行以下命令：

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --affinity host --host-id <host_id>
```

要使用主机资源组将实例从任何租赁更改为host 租赁，请运行以下命令：

```
aws ec2 modify-instance-placement --instance-id <instance_id> \
  --tenancy host --host-resource-group-arn <host_resource_group_arn>
```

排查许可证类型转换问题

故障排除主题

- Windows 激活
- 实例 [实例] 是从 Amazon 拥有的 AMI 启动的。提供最初从 BYOL AMI 启动的实例。
- 无法验证该实例 [实例] 是从 BYOL AMI 启动的。确保 SSM 代理正在实例上运行。
- 调用CreateLicenseConversionTaskForResource操作时出现错误 (InvalidParameterValueException)： ResourceId -[实例] 处于无效状态，无法更改许可证类型。
- EC2 实例 [实例] 未能停止。确保您拥有 EC2 StopInstances. 的权限

Windows 激活

许可证类型转换包含多个步骤。在某些情况下，当您将 Windows Server 实例从 BYOL 转换为随附许可证时，实例上的计费产品会成功更新。但是，KMS 服务器可能无法切换到 AWS KMS 服务器。

要解决此问题，请按照为什么 EC2 Windows 实例上的 Windows 激活失败？中的步骤进行操作使用 Systems Manager AWSSupport-ActivateWindowsWithAmazonLicense 自动运行手册激活 Windows，或者登录实例并手动切换到 AWS KMS 服务器。

实例 [实例] 是从 Amazon 拥有的 AMI 启动的。提供最初从 BYOL AMI 启动的实例。

您必须从已导入的 AMI 启动您的 Amazon EC2 Windows 实例，才能将许可证类型转换为自带许可模式 (BYOL)。最初从 Amazon 拥有的 AMI 启动的实例不符合将许可证类型转换为 BYOL 的条件。有关更多信息，请参阅 转换先决条件。

无法验证该实例 [实例] 是从 BYOL AMI 启动的。确保 SSM 代理正在实例上运行。

要成功转换许可类型，您的实例必须先处于在线状态并由 Systems Manager 管理，才能收集其清单。AWS Systems Manager 代理（SSM 代理）将从您的实例收集清单，其中包括有关操作系统的详细信息。有关更多信息，请参阅 AWS Systems Manager 用户指南中的检查 SSM 代理状态并启动代理和 SSM 代理故障排除。

调用**CreateLicenseConversionTaskForResource**操作时出现错误 (InvalidParameterValueException)： ResourceId -[实例] 处于无效状态，无法更改许可证类型。

要执行许可证类型转换，目标实例必须处于停止状态。有关更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南中的转换先决条件和排查实例的停止问题。

EC2 实例 [实例] 未能停止。确保您拥有 EC2 **StopInstances.** 的权限

您必须具有在目标实例上执行 `StopInstances` EC2 API 操作的权限。此外，如果在目标实例上启用了停止保护，则转换过程将失败。有关更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南 中的为正在运行或已停止的实例禁用停止保护。

AWS License Manager 中的主机资源组

Amazon EC2 专属主机是指 EC2 实例容量完全专供您专用的物理服务器。主机资源组是专属主机的集合，您可以将其作为单个实体进行管理。当您启动实例时，License Manager 会根据您配置的设置分配主机并在这些主机上启动实例。您可以将现有专属主机添加到主机资源组中，并通过 License Manager 利用自动化主机管理功能。有关更多信息，请参阅 Amazon EC2 用户指南中的专属主机。

您可以使用主机资源组按用途区分主机，例如开发测试主机与生产、组织单位或许可限制。将专属主机添加到主机资源组后，您无法直接在专属主机上启动实例，必须使用主机资源组启动这些实例。

设置

您可以为主机资源组配置以下设置：

- 自动分配主机 — 表示如果在该主机资源组中启动实例会超出其可用容量，Amazon EC2 是否可以代表您分配新主机。
- 自动释放主机 — 表示 Amazon EC2 是否可以代表您释放未使用的主机。未使用的主机没有正在运行的实例。
- 自动恢复主机 — 表示 Amazon EC2 能否将实例从意外出现故障的主机转移到新主机。
- 关联的自管理许可证 — 可用于启动该主机资源组中实例的自管理许可证。
- （可选）实例系列 — 您可以启动的实例类型。默认情况下，您可以启动专属主机上受支持的任何实例类型。如果您启动基于 Nitro 的实例，则可以在同一主机资源组中启动具有不同实例类型的实例。否则，您必须只启动同一主机资源组中具有相同实例类型的实例。

目录

创建主机资源组

配置主机资源组以允许 License Manager 管理您的专属主机。要充分利用最昂贵的许可证，可以将一个或多个基于内核或套接字的自管理许可证与主机资源组关联起来。为了最大限度地优化主机利用率，可以在主机资源组中允许所有基于内核或套接字的自管理许可证。

创建主机资源组

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择主机资源组。
3. 选择创建主机资源组。
4. 有关主机资源组详细信息，请指定主机资源组的名称和描述。
5. 对于 EC2 专属主机管理设置，请根据需要启用或禁用以下设置：
   - 自动分配主机
   - 自动释放主机
   - 自动恢复主机
6. （可选）对于其他设置，请选择可以在主机资源组中启动的实例系列。
7. 对于自管理许可证，请选择一个或多个基于内核或套接字的自管理许可证。
8. （可选）对于标签，请添加一个或多个标签。
9. 选择创建。

共享主机资源组

您可以使用 AWS Resource Access Manager 通过 AWS Organizations 共享您的主机资源组。共享主机资源组和自管理许可证后，成员账户可以在共享主机资源组中启动实例。新主机在拥有该主机资源组的账户中分配。成员账户拥有实例。有关更多信息，请参阅 AWS RAM 用户指南。

向主机资源组添加专属主机

您可以通过 AWS Management Console、AWS CLI 或 AWS API 将现有主机添加到主机资源组。要添加主机，您必须是创建专属主机和主机资源组的 AWS 账户所有者。如果您的主机资源组列出了允许的自管理许可证和实例类型，则添加的主机必须符合这些要求。

> **Note**
>
> 假设您停止实例并想要对其重启。您必须执行以下两个任务：
>
> - 修改实例以指向主机资源组。
> - 关联自管理许可证以匹配主机资源组。

有关更多信息，请参阅 AWS Resource Groups 用户指南。

请使用以下步骤向资源组添加一台或多台专属主机：

1. 登录 License Manager 控制台，网址为 https://console.aws.amazon.com/license-manager/。
2. 选择主机资源组。
3. 在主机资源组名称列表中，单击要在其中添加专属主机的主机资源组的名称。
4. 选择专属主机。
5. 选择添加。
6. 选择一台或多台要添加到主机资源组的专属主机。
7. 选择添加。

   添加主机可能需要 1-2 分钟，然后它就会出现在专属主机列表中。

在主机资源组中启动实例

启动实例时，您可以指定主机资源组。例如，您可以使用以下 run-instances 命令。您必须将基于内核或套接字的自管理许可证与 AMI 关联。

```
aws ec2 run-instances --min-count 2 --max-count 2 \
--instance-type c5.2xlarge --image-id ami-0abcdef1234567890 \
--placement="Tenancy=host,HostResourceGroupArn=arn"
```

您还可以使用 Amazon EC2 控制台。有关更多信息，请参阅 Amazon EC2 用户指南中的在主机资源组中启动实例。

修改主机资源组

您可以随时修改主机资源组的设置。您不能将主机限制值设置为少于主机资源组中现有主机的数量。如果主机资源组中正在运行该类型的实例，则无法移除该类型的实例。

修改主机资源组

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择主机资源组。
3. 选择主机资源组，然后选择操作、编辑。
4. 根据需要修改设置。
5. 选择保存更改。

从主机资源组中移除专属主机

从主机资源组中移除主机后，该主机上运行的实例仍保留在主机上。连接到主机资源组的实例仍与该组关联，通过关联直接连接到主机的实例保持相同的属性。如果您与其他 AWS 账户共享主机资源组，License Manager 会自动移除共享主机，并且使用者会收到驱逐通知，要求他们在 15 天内将其实例从主机中移出。要使用已从主机资源组中移除的专属主机，请参阅 Amazon EC2 用户指南中的使用专属主机。

使用以下步骤将专属主机移至主机资源组：

1. 登录 License Manager 控制台，网址为 https://console.aws.amazon.com/license-manager/。
2. 选择主机资源组。
3. 单击要移除专属主机的主机资源的名称。
4. 选择专属主机。
5. 选择要从主机资源组中删除的专属主机。或者，您可以按主机 ID、主机类型、主机状态或可用区搜索专属主机。

6. 选择移除。
7. 再次选择移除以确认。

删除主机资源组

如果主机资源组没有主机，则可以将该组删除。

删除主机资源组

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择主机资源组。
3. 选择主机资源组，然后选择操作、删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

License Manager 中的库存搜索

License Manager 允许您使用 Systems Manager 清单查找本地应用程序，然后将许可规则附加到这些应用程序。将许可规则附加到这些服务器后，您可以在 License Manager 控制面板中跟踪它们以及您的 AWS 服务器。

不过，License Manager 无法在启动或终止时验证这些服务器的许可规则。要保留有关非AWS 服务器的信息 up-to-date，必须使用 License Manager 控制台的 “清单” 搜索部分定期刷新清单信息。

Systems Manager 将数据存储为清单数据 30 天。在此期间，License Manager 会将托管实例计为活动实例，即使无法对该实例进行 Ping 操作也是如此。在从 Systems Manager 中清除清单数据后，License Manager 会将实例标记为非活动状态并更新本地清单数据。为了确保托管实例计数准确，我们建议在 Systems Manager 中手动取消注册实例，以便 License Manager 能够运行清理操作。

查询 Systems Manager 库存需要资源数据同步才能将库存存储在 Amazon S3 存储桶中，Amazon Athena 需要汇总来自组织账户的库存数据， AWS Glue 并提供快速的查询体验。有关更多信息，请参阅 将服务相关角色用于 AWS License Manager。

如果您的组织不限制 AWS 用户创建 AMI 派生的实例或在运行的实例上安装其他软件，资源清单跟踪也是非常有用的。License Manager 为您提供了一种机制以使用清单搜索轻松查找这些实例和应用程序。您可以将规则附加到这些找到的资源，并使用与通过管理的 AMI 创建的实例相同的方式跟踪和验证它们。

内容

- 使用库存搜索
- 自动发现清单

使用库存搜索

License Manager 使用 Systems Manager 清单来发现本地软件使用情况。将自管理许可证与本地服务器关联后，License Manager 会定期收集软件清单，更新许可信息，并刷新其控制面板以报告使用情况。

任务

- 设置库存搜索
- 使用库存搜索
- 向自管理许可证添加自动化发现规则
- 将自管理许可证与库存搜索相关联
- 解除自管理许可证和资源的关联

设置库存搜索

在使用资源库存搜索之前，请完成以下要求：

- 通过将 License Manager 与您的账户集成，启用跨 AWS Organizations 账户库存发现。有关更多信息，请参阅 AWS License Manager 中的设置。
- 为要管理的服务器和应用程序创建自管理许可证。例如，创建一个自管理许可证，该许可证反映了您与 Microsoft 签订的 SQL Server Enterprise 许可协议的条款。

使用库存搜索

请完成以下步骤以搜索资源库存。您可以按名称（例如，以“SQL Server”开头的名称）和随附许可证类型（例如，不适用于“SQL Server Web”的许可证）搜索应用程序。

搜索您的资源清单

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择 库存搜索。
3. （可选）您可以指定筛选选项以简化搜索结果，如下所示。

亚马逊 EC2 资源

筛选条件名称	描述	逻辑运算符	支持的值
资源 ID	资源的 ID。	Equals, Not equals	
账户 ID	拥有资源的 AWS 账户的 ID。	Equals, Not equals	
平台名称	资源的操作系统平台。	Equals, Not equals, Begins with, Contains	
应用程序名称	应用程序的名称。	Equals, Begins with	
包含许可证的名字	包括的许可证类型。	Equals, Not equals	• SQL Server Enterprise • SQL Server Standard • SQL Server Web • Windows Server Datacenter

筛选条件名称	描述	逻辑运算符	支持的值
标签	分配给资源的元数据标签键和可选值。 请注意，Not equals逻辑运算符仅在启用跨账户发现时才可用。	Equals, Not equals	

Amazon RDS 资源

筛选条件名称	描述	逻辑运算符	支持的值
引擎版本	数据库引擎版本。	Equals	• oracle-ee • oracle-se • oracle-se1 • oracle-se2 • db2-se • db2-ae

筛选条件名称	描述	逻辑运算符	支持的值
许可证包（仅限 Oracle）	与 Amazon RDS for Oracle 许可证关联的管理包。	Equals	• Spatial and Graph • Active Data Guard • Label Security • Oracle On-Line Analytical Processing (OLAP) • Diagnostic Pack and Tuning Pack

有关 Amazon RDS 数据库产品许可证的更多信息，请参阅 A mazon RDS 用户指南中的 RDS for Oracle 许可选项或 RDS for Db2 许可选项。

向自管理许可证添加自动化发现规则

将产品信息添加到自管理许可证后，License Manager 可以跟踪安装了这些产品的实例的许可证使用情况。有关更多信息，请参阅 自动发现清单。

向自管理许可证添加自动化发现规则

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 打开库存搜索页面。
3. 选择资源，然后选择添加自动化发现规则。
4. 对于自管理许可证，请选择自管理许可证。

5. 指定要发现和跟踪的产品。
6. （可选）选择在卸载软件时停止跟踪实例，以便在 License Manager 检测到软件已卸载并且已过任何许可证关联期限后，许可证可供重用。
7. （可选）要从自动发现中排除资源，请选择添加排除规则。

> **Note**
>
> 排除规则不适用于亚马逊 RDS 产品（例如 Oracle 的 RDS 和适用于 Db2 的 RDS）。

   a. 选择要筛选的属性，目前支持账户 ID 和标签。
   b. 输入用于标识该属性的信息。对于账户 ID，请指定 12 位数的 AWS 账户 ID 作为值。对标签，请输入键/值对。
   c. 重复步骤 7 以添加其他规则。
8. 选择 添加。

将自管理许可证与库存搜索相关联

确定需要管理的未管理资源后，可以手动将其与自管理许可证相关联，而不必使用自动化发现功能。

将自管理许可证与资源相关联

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 打开库存搜索页面。
3. 选择资源，然后选择关联自管理许可证。
4. 对于自管理许可证名称，请选择自管理许可证。
5. （可选）选择与我的所有成员账户共享自管理许可证。
6. 选择关联。

解除自管理许可证和资源的关联

如果软件供应商的许可条款发生变化，则可以解除手动关联的资源，然后删除自管理许可证。

解除自管理许可证和资源的关联

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。

2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证的名称。
4. 选择资源。
5. 选择要与自行管理的许可证取消关联的每个资源，然后选择取消关联资源。

自动发现清单

License Manager 使用 Systems Manager 清单来发现 Amazon EC2 实例和本地实例上的软件使用情况。您可以将产品信息添加到您的自管理许可证中，License Manager 将跟踪安装了这些产品的实例。此外，您可以根据许可协议指定排除规则，以决定要排除哪些实例。您可以将属于 AWS 账户 ID 的实例或与资源标签关联的实例排除在自动化发现范围之外

可以将自动化发现添加到新的许可证集、现有的自管理许可证或库存中的资源中。可以随时使用 UpdateLicenseConfigurationAPI 命令通过 CLI 编辑自动发现规则。要在控制台中编辑规则，您必须删除现有自管理许可证并创建新的许可证。

要使用自动化发现功能，您必须将产品信息添加到您的自管理许可证中。在使用库存搜索创建自管理许可证时可以执行此操作。

您无法手动解除关联通过自动化发现功能跟踪的实例。默认情况下，在卸载软件后，自动化发现功能不会解除与跟踪的实例的关联。您可以配置自动化发现功能，以在卸载软件时停止跟踪实例。

配置自动化发现功能后，您可以通过 License Manager 控制面板跟踪许可证使用情况。

先决条件

- 通过将 License Manager 与您的账户集成，启用跨 AWS Organizations 账户库存搜索。有关更多信息，请参阅 AWS License Manager 中的设置。

  > **Note**
  >
  > 单个账户可以设置自动化发现功能，但不能添加排除规则。

- 在您的实例上安装 Systems Manager 清单。

在创建自管理许可证时配置自动化发现功能

在创建自管理许可证时，您可以配置自动化发现规则和排除规则。有关更多信息，请参阅 创建自管理许可证。

向现有自管理许可证添加自动化发现规则

使用以下过程通过控制台将自动化发现规则添加到现有的自管理许可证，您也可以从库存搜索窗格中执行此操作，方法是选择资源 ID 并选择添加自动化发现规则。

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择自管理许可证。
3. 选择自管理许可证的名称以打开许可证详细信息页面。
4. 在自动化发现规则选项卡上，选择添加自动化发现规则。
5. 指定要发现和跟踪的产品。
6. （可选）选择在卸载软件时停止跟踪实例，以便在 License Manager 检测到软件已卸载并且已过任何许可证关联期限后，许可证可供重用。
7. （可选）要定义要从自动化发现中排除的资源，请选择添加排除规则。

   > **Note**
   >
   > - 排除规则不适用于 RDS 数据库产品（例如适用于 Oracle 的 Amazon RDS 和适用于 Db2 的 Amazon RDS）。
   > - 排除规则只有在启用跨账户资源查找后才可用。

   a. 选择要筛选的属性，目前支持账户 ID 和标签。
   b. 输入用于标识该属性的信息。对于账户 ID，请指定 12 位数的 AWS 账户 ID 作为值。对标签，请输入键/值对。
   c. 重复步骤 7 以添加其他规则。
8. 完成后，选择添加以应用您的自动化发现规则。

在 License Manager 中已授予的许可证

已授予的许可证是贵组织从 AWS Marketplace、AWSData Exchange 购买，或直接从将软件与托管权限集成的卖方处购买的产品的许可证。许可证管理员可以使用 AWS License Manager 来管理此类许可证的使用，并将使用权（称为权限）分配给特定 AWS 账户。

分发给 AWS Data Exchange 产品的数据许可证可通过 AWS Data Exchange 提供给 AWS 账户。必须先启用订阅共享功能，然后才能从 AWS Marketplace 中分配许可证。有关更多信息，请参阅在组织中共享订阅。

在许可证管理员将权限从 AWS Marketplace 许可证分发给一个 AWS 账户，并且收件人接受并激活已授予的许可证后，该 AWS 账户就可以通过 AWS Marketplace 进行订阅了。该账户还可以访问产品。例如，如果许可管理员从 AWS Marketplace 购买亚马逊机器映像 (AMI)并将权限分配给您的 AWS 账户，则您可以使用 AWS Marketplace 和 Amazon EC2 从 AMI 启动 Amazon EC2 实例。

主题

查看已授予的许可证

License Manager 会显示选项卡，可根据您验证的权限查看和管理已授予的许可证。已授予的许可证页面可以显示以下选项卡：

我的许可证

任何有权在 License Manager 中查看已授予的许可证的用户都可以使用此选项卡。该选项卡有一个我已授予的许可证部分，其中包含有关每个许可证的信息，例如许可证 ID 和产品名称。在此页面上，您可以查看有关每个许可证的其他信息。

许可证摘要（仅限于组织管理员使用）

该选项卡仅限于组织管理员使用。该选项卡有一个总计部分，列出了组织中所有账户的产品总量和已授予的许可证。还显示了产品部分，其中包含一个表格，详细说明了每个产品的属性，例如产品名称和已授予许可证的数量。

汇总的许可证（仅限于组织管理员使用）

该选项卡仅限于组织管理员使用。此选项卡中有一个部分，详细介绍了我的组织已授予的许可证，其中包括有关每个许可证的信息，例如许可证 ID 和产品名称。在此页面上，您可以查看有关每个许可证的其他信息。

管理已授予的许可证

已授予的许可证将显示在 License Manager 控制台中。收件人必须接受并激活已授予的许可证，然后才能使用该产品。您接受和激活许可证的方式取决于该许可证是否来自 AWS Marketplace，您的账户是否是 AWS Organizations 组织中的成员账户，以及您的组织是否启用了所有功能。

已授予的许可证需要跨区域复制许可证元数据。License Manager 会自动将每个已授予的许可证及其相关信息复制给其他 AWS 区域。这样，您能够集中查看向您授予许可证的所有区域。

来自 AWS Marketplace 和 AWS Data Exchange 的许可证

- 系统会自动接受并激活您购买的订阅的许可证。
- 如果启用了所有功能的组织的管理账户购买了订阅并将许可证分配给成员账户，则成员账户将自动接受这些许可证。管理账户或成员账户可以稍后激活许可证。
- 如果仅启用整合账单功能的组织的管理账户购买了订阅并将许可证分配给成员账户，则每个成员账户都必须接受并激活许可证。

来自卖家的许可证

- 对于使用 License Manager 分配许可证的产品，您必须接受并激活许可证。
- 如果启用了所有功能的组织的管理账户购买了产品并将许可证分配给成员账户，则成员账户将自动接受这些许可证。管理账户或成员账户可以稍后激活许可证。
- 如果仅启用整合账单功能的组织的管理账户购买了产品并将许可证分配给成员账户，则每个成员账户都必须接受并激活许可证。

Console (My licenses)

您可以查看和管理单个 AWS 账户已授予的许可证。

管理账户中已授予的许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择已授予的许可证。
3. 如果当前选项不是我的许可证，请选择该选项卡。
4. （可选）使用筛选条件选项（如下所示）来确定显示的许可证列表的范围。

    - “产品 SKU”— 此许可证的产品标识符，由许可证颁发者在创建许可证时定义。同一产品 SKU 可能存在于多个 ISV 中。

- “收件人”— 许可证收件人的 ARN。
- “状态”— 许可证的状态。例如，可用。

5. 要查看有关许可证的其他信息，请选择许可证 ID 以打开许可证概览页面。
6. 如果许可证颁发者是 AWS Marketplace 以外的实体，则初始授予状态为待接受。请执行下列操作之一：
   - 选择接受并激活许可证。生成的授权状态为活跃。
   - 选择接受许可证。生成的授权状态为已禁用。准备好使用许可证后，选择激活许可证。
   - 选择拒绝许可证。生成的授权状态为已拒绝。拒绝许可证后，您将无法对其进行激活。

如果您不想继续使用已激活的许可证，可以返回许可证概览页面并选择停用许可证。如果要继续使用已停用的许可证，请返回许可证概览页面并选择激活许可证。

Console (Aggregated licenses)

您可以查看从组织中的所有账户中汇总的已授予的许可证。

> **Important**
>
> 要使用组织范围视图查看已授予的许可证，必须先使用 AWS License Manager 控制台设置关联 AWS Organizations。有关更多信息，请参阅AWS License Manager 中的设置。

管理 AWS Organizations 账户中已授予的许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择已授予的许可证。
3. 如果当前选项不是聚合许可证选项卡，请选择该选项卡。
4. （可选）使用筛选条件选项（如下所示）来确定显示的许可证列表的范围。
   - “产品 SKU”— 此许可证的产品标识符，由许可证颁发者在创建许可证时定义。同一产品 SKU 可能存在于多个 ISV 中。
   - “受益人”— 您组织中获得许可证的账户。
5. 要查看有关许可证的其他信息，请选择许可证 ID 以打开许可证详细信息页面。
6. 如果许可证颁发者是 AWS Marketplace 以外的其他实体，请执行以下操作之一：
   - 选择激活许可证。生成的授权状态为活跃。
   - 选择停用许可证。生成的授权状态为已停用。

如果您不想继续使用已激活的许可证，可以返回许可证概览页面并选择停用许可证。如果要继续使用已停用的许可证，请返回许可证概览页面并选择激活许可证。

AWS CLI

您可以使用 AWS CLI 来处理已授予的许可证。

要管理已授予的许可证，请使用 AWS CLI：

- accept-grant
- create-grant-version
- get-grant
- list-licenses
- list-received-grants
- list-received-grants-for-organization
- list-received-licenses
- list-received-licenses-for-organization
- reject-grant

分配权限

如果您是在组织的管理账户中操作并启用了所有功能的许可证管理员，则可以通过创建授权将已授予的许可证中的权限分配给您的组织。有关 AWS Organizations 的更多信息，请参阅 AWS Organizations 术语和概念。

您可以将授权的收件人指定为下列选项之一：

- AWS 账户，仅包括指定的账户。
- 组织根，包括您组织中的所有账户。
- 组织单位 (OU)（未嵌套），包括指定 OU 中的所有账户，以及指定 OU 下的嵌套 OU 中的所有账户。

> **Note**
>
> 您最多可以为每个许可证创建两千个授权。

您可以使用 AWS License Manager 控制台或 AWS CLI 来分配权限。在控制台中创建授权时，您可以指定组织 ID 或组织 ARN，但必须将 ARN 格式与 AWS CLI 一起使用。例如，ARN 如下：

组织 ID ARN

```
arn:aws:organizations::<account-id-of-management-account>:organization/
o-<organization-id>
```

组织 OU ARN

```
arn:aws:organizations::<account-id-of-management-account>:ou/
o-<organization-id>/ou-<organizational-unit-id>
```

Console

创建授权（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择已授予的许可证。
3. 选择许可证 ID 以打开许可证概览页面。
4. 从授权部分选择创建授权。
5. 在详细信息面板上，执行以下操作：
   a. 输入授权的名称，以帮助您标识授权的用途或收件人。
   b. 输入授予收件人的 AWS 账户 ID、AWS Organizations OU ID 或 ARN 或者 AWS Organizations ID 或 ARN。
   c. 选择创建授权。
6. 在许可证概览页面上，您将在授权面板中看到授权条目。授权的初始状态是待接受。当收件人接受授权时，状态将更改为活跃，当收件人拒绝授权时，将更改为已拒绝。

AWS CLI

您可以使用 AWS CLI 来分配权限。使用 AWS License Manager API 时，必须使用 ARN 格式指定组织 ID 或 OU。

使用 AWS CLI 创建和列出授权

- create-grant
- list-distributed-grants

授权详细信息页面显示您已授予访问权限的账户列表。向您的组织分配许可证后，您可以分别停用或激活每个账户的许可证。

授权接受和激活

为已授予的许可证创建授权时，该授权将分配给收件人。必须接受并激活已授予的许可证，然后授予收件人才能使用该许可证。授权激活过程可包括从 AWS Marketplace 获取已授予的许可证的其他选项。

默认情况下，已授予的许可证的授予概览页面的状态为 `Pending Acceptance`。您可以选择 `Accept`、`Accept and Activate` 或 `Reject` 授权。已接受但尚未激活的授权的状态为 `Disabled`。已接受且已激活的授权的状态为 `Active`。

必须接受并激活已授予的许可证，然后授予收件人才能使用该许可证。默认情况下，已授予许可证的授权详细信息页面的状态为待接受。您可以选择接受、接受并激活或拒绝许可证。已接受但尚未激活的授权的状态为已禁用。已接受且已激活的授权的状态均为活跃。

> **Tip**
>
> 您可以自动接受来自组织管理账户的授权。要启用自动接受授权功能，请在 AWS License Manager 控制台的设置页面上从管理账户关联您的组织账户。

您不能从 AWS Marketplace同时为同一产品激活两个许可证。如果您有两个订阅（例如，一个产品的公共套餐和私有套餐，或者一个产品的订阅的许可证和同一产品的已授予的许可证），则可以进行以下操作之一：

1. 禁用同一产品的现有授权，然后激活新的授权。
2. 激活新的授权，并指定要禁用的现有活跃授权，并用新授权替换现有的活跃授权。您可以使用 License Manager 控制台或 AWS CLI：
   a. 使用 License Manager 控制台激活新授权，同时选择是以替换活跃授权。
   b. 使用 `CreateGrantVersion` API，通过为 `Status` 是“`Active`”的 `ActivationOverrideBehavior` 指定 `ALL_GRANTS_PERMITTED_BY_ISSUER` 来激活新授权。

Console

您可以使用 License Manager 控制台来激活授权。当您激活来自 AWS Marketplace 的授权时，您可能会看到是否替换活跃授权的选项：

- 作为许可证管理员，您必须在激活授权时指定是否要替换活跃授权。
- 作为授予人，您可以选择在为组织中的其他账户激活授权时指定是否要替换活跃授权。
- 作为被授权者，如果创建分布式授权的授予人没有指定是否要替换活跃授权，则必须在激活授权时进行选择。

激活授权（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择已授予的许可证。
3. 选择许可证 ID 以打开许可证概览页面。
4. 选择授权名称以打开授权概览页面。
5. 如果出现以下选项，请选择一个激活选项以确定是否要替换活跃授权：
   a. 否 — 此选项将激活授权，而不会替换收件人（被授予者）的任何现有活跃授权。
   b. 是 — 此选项将禁用对同一产品的授权，并为定义的收件人（被授予者）激活新的授权：
      i. 指定的 AWS 账户。
      ii. 指定组织 OU 的成员账户。
      iii. 组织中的成员账户。
6. （可选）给出激活授权的原因。
7. 在输入框中输入 **`activate`**，然后选择激活。

AWS CLI

您可以使用 AWS CLI 来处理已授予的许可证。

使用 AWS CLI 来使用分布式授权：

- accept-grant
- create-grant-version
- list-received-grants
- list-received-grants-for-organization
- reject-grant

许可证状态

许可证有两种状态：许可证状态（显示许可证的总体可用性和可共享性）和授予状态（显示是否可以使用许可证）。

下表显示了已授予的许可证的不同状态：

状态	描述
AVAILABLE	该许可证可供使用和共享。
PENDING_AVAILABLE	由于许可证仍在处理中，因此无法使用。
DEACTIVATED	由于许可证颁发者已将其停用，因此无法使用该许可证。
SUSPENDED	该许可证已暂停，因此无法使用。
EXPIRED	该许可证无法使用，因为它已经到期了。
PENDING_DELETE	该许可证正在删除中，因此无法使用。
DELETED	由于许可协议已取消，该许可证无法使用。

下表显示了授权的不同状态：

状态	描述
PENDING_WORKFLOW	该授权正在分配过程中。
PENDING_ACCEPT	已创建授权，但授予收件人尚未接受。
REJECTED	该授权已被授予收件人拒绝。
ACTIVE (处于活动状态)	该授权已被接受并激活，供授予收件人使用。可以使用许可的资源。
FAILED_WORKFLOW	分配授权失败。
DELETED	该授权已被授予人删除。

状态	描述
PENDING_DELETE	正在删除分配的授权。
DISABLED	该授权已被授予收件人接受，但尚未激活使用。
WORKFLOW_COMPLETE	已向某组织分配或收回授权。授权详细信息显示组织中每个账户的子授权状态。

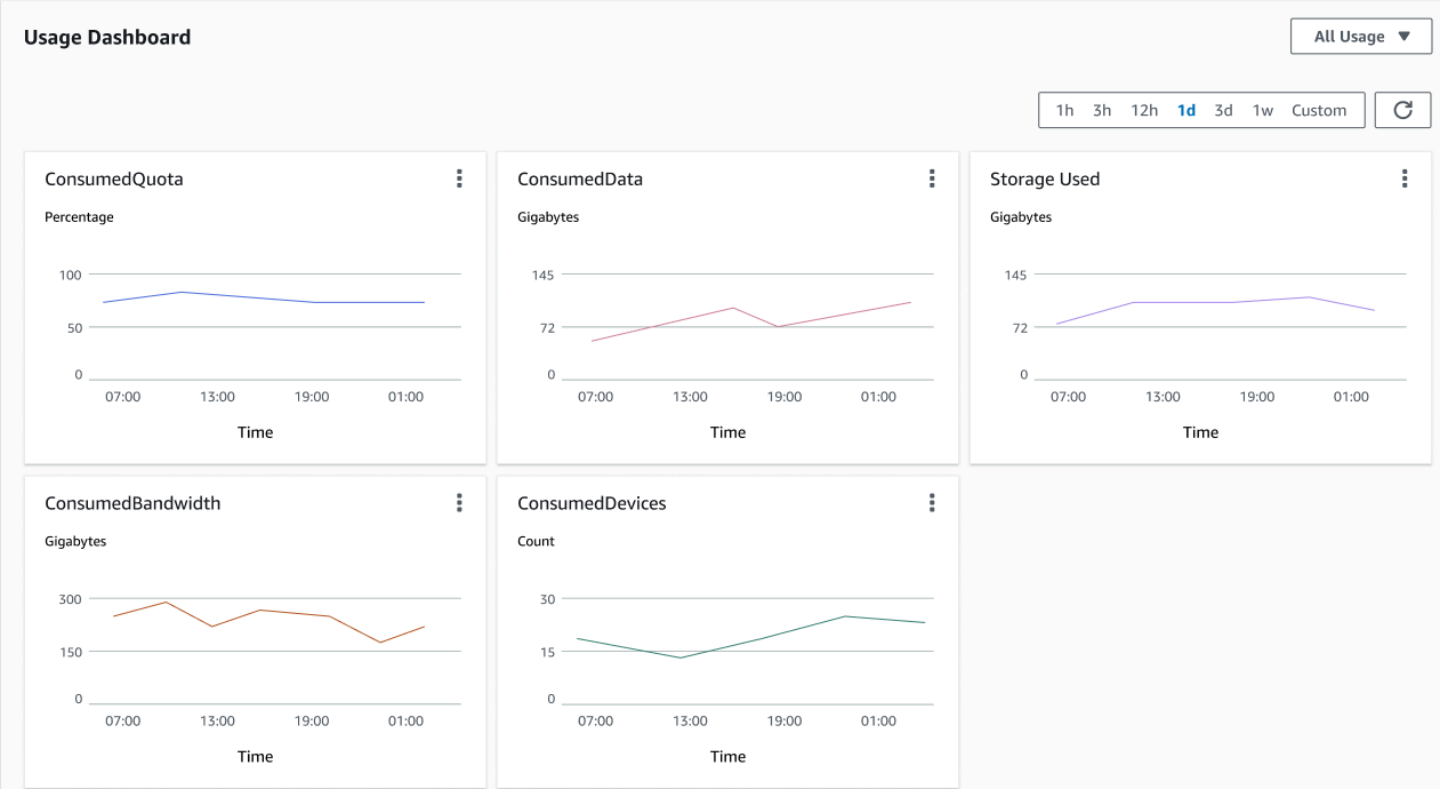
买家账户指标

当卖家颁发的许可证的授予配置为允许提交使用记录时，License Manager 会向卖家账户、根买家账户和记录使用情况的账户发布 CloudWatch 指标。买家账户是指已购买或获得卖方颁发的许可证的 AWS 账户。有关更多信息，请参阅向客户授予许可证。

使用情况控制面板

当卖方或独立软件供应商 (ISV) 应用程序根据买方账户的许可证记录使用情况时，记录使用情况的账户和根购买者账户将在 License Manager 控制台的使用情况控制面板页面上看到具有使用记录的 CloudWatch 小组件。买家还可以在 AWS Organizations 中查看他们已向其分配许可证的账户的指标。使用情况控制面板页面上的图表适用于已发送使用记录的每个许可证。

下图是使用情况控制面板的示例：



卖家在 License Manager 中颁发的许可证

独立软件供应商 (ISV) 可以使用 AWS License Manager 来管理和向最终用户分发软件许可证。作为颁发者，您可以使用 License Manager 控制面板集中跟踪卖家颁发的许可证的使用情况。

License Manager 使用开放、安全的行业标准来表示许可证，并允许客户以加密方式验证其真实性。License Manager 将每个许可证与一个非对称密钥相关联。作为 ISV，您拥有非对称 AWS KMS 密钥并将其存储在您的账户中。

卖家颁发的许可证要求跨区域复制许可证元数据。License Manager 会自动将每个卖家颁发的许可证及其相关信息复制到其他区域。

License Manager 支持多种不同的许可模式，包括：

- 永久模式 — 终身许可证无到期日期，授权用户无限期地使用该软件。
- 浮动模式 — 可与应用程序的多个实例共享许可证。许可证可以预付费，并向其中添加一组固定的权限。
- 订阅模式 — 具有到期日期的许可证，除非明确停用，否则可以自动续订。
- 基于使用情况模式 — 根据使用情况（如 API 请求数、事务数或存储能力）设定具体条款的许可证。

您可以在 License Manager 中创建许可证，然后使用 AWS IAM 身份或通过 License Manager 生成的持有者令牌将其分发给客户。拥有 AWS 账户的客户可以将许可证权限重新分配给各自组织中的 AWS 身份。拥有分布式权限的客户可以通过您的软件与 License Manager 集成，从该许可证中签出并签入所需的权限。

权限

License Manager 将许可证功能作为权限记录到许可证中。权限的特征是数量有限或不限数量。例如，“40GB 数据传输”就是有限权限的一个示例。“白金等级”就是无限量权限的一个示例。

许可证包含所有授予的权限、激活和到期日期以及颁发者的详细信息。许可证是一个受版本控制的实体，每个版本都是不可变的。每当许可证发生变化时，许可证版本都会更新。

要签出或签入有限权限，ISV 应用程序必须指定每项有限功能的数量。要获得无限权限，ISV 应用程序只需指定相关权限即可再次签入或签出。最后，有限功能还支持“超额”标志，该标志指示最终用户是否可以超出其初始权限的使用量。License Manager 会跟踪并向 ISV 报告使用情况以及任何超额情况。

许可证使用

License Manager 通过对所有已签出权限进行记录清点，可让您集中跟踪多个区域的许可证。License Manager 还会跟踪与每次签出相关的用户身份和底层资源标识符（如果有）以及签出时间。您可以通过 CloudWatch Events 事件跟踪此类时间序列数据。

许可证可能处于以下几种状态之一：

- 已创建 — 许可证已创建。
- 已更新 — 许可证已更新。
- 已停用 — 许可证已停用。
- 已删除 — 许可证已删除。

要求

要开始使用此功能，您需要具有调用以下 License Manager API 操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
```

```
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenses",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
            "license-manager:CheckInLicense",
            "license-manager:ExtendLicenseConsumption",
            "license-manager:GetLicenseUsage",
            "license-manager:CreateGrant",
            "license-manager:CreateGrantVersion",
            "license-manager:DeleteGrant",
            "license-manager:GetGrant",
            "license-manager:ListDistributedGrants"
        ],
        "Resource": "*"
      }
    ]
}
```

如果您要与 License Manager 集成，以便没有 AWS 账户的客户可以使用在 AWS Marketplace 之外销售的许可证，则必须创建一个角色，使软件应用程序能够调用 License Manager API。例如，您可以使用 AWS CLI。首先，使用 create-role 命令创建一个名为 AWSLicenseManagerConsumptionRole 的角色。

```
aws iam create-role
    --role-name AWSLicenseManagerConsumptionRole
    --description "Role used to consume licenses using AWS License Manager"
    --max-session-duration 3600
    --assume-role-policy-document file://trust-policy-document.json
```

以下是 `trust-policy-document.json` 文件。

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Federated": "openid-license-manager.amazonaws.com"
        },
```

```
        "Action": "sts:AssumeRoleWithWebIdentity",
        "Condition": {
            "StringLike": {
                "openid-license-manager.amazonaws.com:sub": "66a9bbf5-0896-460f-a1a9-
de535dcc175b"
            }
        }
    }
}
```

接下来，使用 attach-role-policy 命令将 AWSLicenseManagerConsumptionPolicy AWS 托管策略添加到 AWSLicenseManagerConsumptionRole 角色中。

```
aws iam attach-role-policy
    --policy-arn arn:aws:iam::aws:policy/service-role/
AWSLicenseManagerConsumptionPolicy
    --role-name AWSLicenseManagerConsumptionRole
```

创建卖家颁发的许可证

通过使用AWS Management Console 按以下步骤创建要向客户授予的许可证。或者，您可以使用 CreateLicense API 操作创建许可证。

使用控制台创建许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从左侧菜单中选择卖家颁发的许可证。
3. 选择创建许可证。
4. 对于许可证元数据，请提供以下信息：

   - 许可证名称 — 向买家显示的名称，最多 150 个字符。
   - 许可证描述 — 可选描述，用于将此许可证与其他许可证区分开来，最多 400 个字符。
   - 产品 SKU — 产品 SKU。
   - 收件人 — 收件人的姓名（公司或个人）。
   - 主区域 — 许可证所在的 AWS 区域。尽管可以在全球范围内使用许可证，但您只能在主区域更改许可证。创建许可证后，您无法更改许可证的主区域。
   - 许可证起始日期 — 激活日期。
   - 许可证结束日期 — 许可证的结束日期（如果适用）。

5. 对于使用配置，请提供以下信息：

   - 更新频率 — 是否每周、每月更新，还是根本不更新。
   - 使用配置 — 如果要将许可证用于持续连接，请选择临时使用配置选项。如果要离线使用许可证，请选择借用。输入最大生存时间（分钟）以设置许可证的可用时长。

6. 对于颁发者，请提供以下信息：

   - 输入 AWS KMS 密钥 — License Manager 使用此密钥对颁发者进行签名和验证。有关更多信息，请参阅许可证的加密签名。
   - 颁发者名称 — 卖家的公司名称。
   - 登记卖家 — 可选的公司名称。
   - 协议 URL — 许可协议的 URL。

7. 对于权限，请提供以下有关许可证向收件人授予的功能的信息：

   - 姓名 — 收件人的姓名。
   - 单位类型 — 选择单位类型，然后提供最大计数。
   - 如果收件人在更新之前必须签入许可证，请选中允许签入。
   - 如果收件人可以使用超过最大计数的资源，请选中所允许的超额。此选项可能会给收件人带来额外费用。

8. 选择创建许可证。

向客户授予许可证

添加新许可证后，您可以使用 AWS Management Console向拥有 AWS 账户的客户授予许可证。在使用许可证之前，收件人必须接受授权。有关更多信息，请参阅在 License Manager 中已授予的许可证。

或者，如果客户没有 AWS 账户，则可以使用 License Manager API 让客户能够使用许可证。

使用控制台向客户授予许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从左侧菜单中选择卖家颁发的许可证。
3. 选择许可证 ID 以打开其详细信息页面。
4. 对于授予，请选择创建授权。
5. 对于授予详细信息，请提供以下信息：

- 授予名称 — 授予名称。这用于启用搜索功能。
- AWS 账户 ID — 许可证收件人的 AWS 账号。
- 许可证权限
  - 如果收件人可以使用授予的权限，请选择使用。
  - 如果收件人可以将授予的权限分配给其他 AWS 账户，请选择分配。
  - 选择允许本地生成令牌，以便在不使用 AWS 身份或凭证的情况下对共享许可证进行身份验证。
  - 选择允许提交使用记录，以允许许可证收件人提交使用类型的使用记录。
- 主区域 — 许可证的 AWS 区域。

6. 选择创建授权。

为没有 AWS 账户的客户获取临时凭证

对于没有 AWS 账户的客户，您可以使用与拥有 AWS 账户的客户相同的方式使用权限。按以下步骤为没有 AWS 账户的客户获取临时 AWS 凭证。API 调用必须在主区域进行。

获取用于调用 License Manager API 的临时凭证

1. 调用 CreateToken API 操作以获取编码为 JWT 令牌的刷新令牌。
2. 调用 GetAccessToken 操作，指定您在上一步中从 `CreateToken` 中收到的刷新令牌，以接收临时访问令牌。
3. 调用 AssumeRoleWithWebIdentity API 操作，指定您在上一步中从 `GetAccessToken` 中收到的访问令牌以及您创建的 AWSLicenseManagerConsumptionRole 角色，以获取临时 AWS 凭证。

从 AWS License Manager 控制台创建令牌

1. 在 License Manager 控制台中，导航到许可证详细信息页面，查看您要在没有 AWS 账户的情况下使用的特定许可证权限。
2. 选择创建令牌以生成临时访问令牌。

> **Note**
>
> 首次生成临时访问令牌时，系统会要求您创建一个服务角色，以便 License Manager 可以代表您访问服务。创建了以下服务角色：`AWSLicenseManagerConsumptionRole`。

3. 下载 token.csv 文件，或者在生成令牌字符串时将其复制。

> **Important**
>
> 这是您查看或下载该令牌的唯一机会。我们建议您下载令牌并将文件存储在安全位置。您可以随时创建新令牌，但不得超过服务限制。

使用许可证

License Manager 允许多个用户同时使用单个许可证中具有有限功能的权限。调用 CheckoutLicense API 操作。以下是参数描述。

- 密钥指纹 — 可信许可证颁布者。

  示例：aws:123456789012:issuer:issuer-fingerprint

- 产品 SKU — 此许可证的产品标识符，由许可证颁发者在创建许可证时定义。同一产品 SKU 可能存在于多个 ISV 中。因此，可信密钥指纹起着重要作用。

  示例：1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE

- 权限 — 可签出的功能。如果您指定无限功能，则数量为零。示例：

```
"Entitlements": [
    {
        "Name": "DataTransfer",
        "Unit": "Gigabytes",
        "Value": 10
    },
    {
        "Name": "DataStorage",
        "Unit": "Gigabytes",
        "Value": 5
    }
]
```

- 受益人 — 软件即服务 (SaaS) ISV 可以通过包含客户标识符来代表客户签出许可证。License Manager 限制对在 SaaS ISV 账户中创建的许可证存储库的调用。

  示例：user@domain.com

- 节点 ID — 用于将许可证节点锁定到应用程序的单个实例的标识符。

示例：10.0.21.57

删除卖家颁发的许可证

删除许可证后，您可以进行重新创建。许可证及其数据将保留六个月，供许可证颁发者和许可证被授予者以只读模式使用。

按以下步骤删除您使用 AWS Management Console创建的许可证。或者，您可以使用 DeleteLicense API 操作删除许可证。

使用控制台删除许可证

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 从左侧菜单中选择卖家颁发的许可证。
3. 选择许可证旁边的单选按钮，将其选中删除。
4. 选择删除。如果提示进行确认，输入 **`delete`**，并选择删除。

License Manager 中的基于用户的订阅

使用基于用户的订阅 AWS License Manager，您可以购买完全合规的许可软件订阅。许可证由 Amazon 提供，按用户收取订阅费。Amazon EC2 为预配置的亚马逊机器映像 (AMI) 提供受支持的软件，以及包含许可证的 Windows 服务器许可证。无需长期许可订阅即可使用此类许可证。

要使用基于用户的订阅，您可以将来自 AWS Directory Service for Microsoft Active Directory（AWS Managed Microsoft AD）或您的自管理（本地）域的用户与提供软件的 EC2 实例关联起来。要使您的许可软件可用，您必须创建基于用户的订阅，并将其与从预配置的 AMI 启动的实例关联起来。AWS Systems Manager 将配置和强化您启动的包含许可证的实例。用户必须连接远程桌面软件才能访问提供该软件的实例。

包含许可证的实例的每个关联用户和 vCPU 都会产生费用。Amazon EC2 预留实例和 Savings Plan 定价模式可以帮助优化您的 Amazon EC2 成本。有关更多信息，请参阅 Amazon Elastic Compute Cloud 用户指南 中的预留实例。基于用户的订阅从上半月到月底计费。

目录

先决条件

在创建基于用户的订阅之前，必须在您的环境中实现以下先决条件。

- 您必须允许 License Manager 创建服务相关角色，才能为基于用户的订阅注册 AWS 账户 。License Manager 控制台的基于用户的订阅部分将出现一次提示，您可以在其中同意授予 License Manager

创建所需服务相关角色的权限。向 License Manager 授予权限后，可以选择创建以创建服务相关角色。有关更多信息，请参阅 将服务相关角色用于 AWS License Manager。

- 您必须创建 AWS Managed Microsoft AD 目录。 AWS Managed Microsoft AD 不支持已共享的目录。有关创建 AWS Managed Microsoft AD 目录的更多信息，请参阅《AWS Directory Service 用户指南》中的AWS Managed Microsoft AD 先决条件和创建您的 AWS Managed Microsoft AD 目录。
- 要使用基于用户的订阅，您必须将用户与您的 AWS Managed Microsoft AD 目录或自行管理的 Active Directory 关联起来。
  - 要将用户与关联 AWS Managed Microsoft AD，您必须在 AWS Managed Microsoft AD 目录中配置用户。有关更多信息，请参阅 AWS Directory Service 管理指南 中的管理 AWS Managed Microsoft AD中的用户和组。
  - 要关联自管理目录中的用户，必须在您的自管理目录和 AWS Managed Microsoft AD 目录之间建立双向林信任。有关更多信息，请参阅《管理指南》中的教程：在您 AWS Managed Microsoft AD 和您自行管理的 Active Directory 域之间创建信任关系。AWS Directory Service
  - 为您的目录配置的子网必须全部来自您的同一 VPC。 AWS 账户
- 必须配置来自提供基于用户的订阅的实例或 VPC 终端节点的出站 Internet 访问权限，您的实例才能与 AWS Systems Manager通信。有关更多信息，请参阅 AWS Systems Manager 用户指南中的为 EC2 实例设置 Systems Manager。
- License Manager 会创建两个网络接口，它们使用配置您 AWS Managed Microsoft AD 的 VPC 的默认安全组。此类接口用于实现目录所需的服务功能。确保您的默认安全组允许出站流量流向每个域控制器的网络接口 IPv4 地址或域控制器使用的安全组。有关更多信息，请参阅 AWS Directory Service 管理指南中的步骤 1：配置 AWS Directory Service for Microsoft Active Directory 和虚拟私有云 (VPC) 和创建的内容。

  预置过程完成后，您可以将不同的安全组关联到 License Manager 创建的接口。您选择的安全组还必须允许所需的流量流向每个域控制器的网络接口 IPv4 地址或安全组。有关更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的使用安全组。
- 除了您注册的基于用户的订阅外，您还必须为任何其他 VPC 配置 DNS 转发。 AWS Managed Microsoft AD 您可以使用 Amazon Route 53 或其它 DNS 服务进行 DNS 转发。有关更多信息，请参阅博客文章将 Directory Service 的 DNS 解析与 Amazon Route 53 Resolver 集成。
- 如果您使用基于用户的订阅来订阅 Microsoft Office，则必须：
  - 为 VPC 启用 DNS 主机名和 DNS 解析。有关更多信息，请参阅查看和更新 VPC 的 DNS 属性。
  - 确保为提供基于用户的 Microsoft Office 订阅而启动的实例有一条通往配置 VPC 终端节点的子网的路由。

- 为您的 VPC 终端节点识别或创建一个允许入站 TCP 端口 1688 连接的安全组。此安全组将在您配置虚拟私有云设置时指定。有关更多信息，请参阅使用安全组。在配置 VPC 时，License Manager 会将此安全组关联到它代表您创建的 VPC 终端节点。有关 VPC 终端节点的更多信息，请参阅 AWS PrivateLink 指南中的使用接口 VPC 终端节点访问 AWS 服务。
- 为启动的实例识别或创建安全组，以提供基于用户的订阅，允许从您批准的连接源进行入站 TCP 端口 3389 连接。安全组还应允许出站 TCP 端口 1688 连接到达 VPC 终端节点。有关更多信息，请参阅使用安全组。

  如果您已经准备好首次使用基于用户的订阅，请完成列出的先决条件并参阅基于用户的订阅入门。如果您已经设置了基于用户的订阅，并且想要将此类产品添加到您的 AWS Managed Microsoft AD 并为 Microsoft Office 产品配置 VPC，请完成列出的先决条件，然后参阅修改基于用户的订阅的目录设置。

- 您必须将实例配置文件角色附加到提供基于用户的订阅产品的实例，该产品允许由 AWS Systems Manager管理资源。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

  > **Warning**
  >
  > 提供基于用户的订阅的实例必须由 AWS Systems Manager 管理才能保持正常状态。此外，您的实例必须能够激活其基于用户的订阅许可，并在许可证激活后保持合规性。License Manager 将尝试恢复运行状况不佳的实例，但无法恢复正常状态的实例将被终止。有关如何让 Systems Manager 管理您的实例以及实例合规性的问题排查信息，请参阅本指南的排查基于用户的订阅问题章节。

- 要创建基于用户的订阅，您的用户或角色必须具有以下权限：
  - `ec2:CreateNetworkInterface`
  - `ec2:DeleteNetworkInterface`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:CreateNetworkInterfacePermission`
  - `ec2:DescribeSubnets`
  - `ds:DescribeDirectories`
  - `ds:AuthorizeApplication`
  - `ds:UnauthorizeApplication`
  - `ds:GetAuthorizedApplicationDetails`
  - `ds:DescribeDomainControllers`

- 要为 Microsoft Office 产品创建基于用户的订阅，您的用户或角色还必须具有以下额外权限：
  - `ec2:CreateVpcEndpoint`
  - `ec2:DeleteVpcEndpoints`
  - `ec2:DescribeVpcEndpoints`
  - `ec2:ModifyVpcEndpoint`
  - `ec2:DescribeSecurityGroups`

注意事项

在 License Manager 中使用基于用户的订阅时，请注意以下注意事项：

- Win 远程桌面服务 SAL 许可证不能与受支持的基于用户的订阅产品分开使用。
- 提供基于用户的订阅的实例一次最多支持两个活跃的用户会话。
- 当您在提供基于用户的订阅的实例上创建具有管理员权限的本地用户时，实例的运行状况可能会更改为不正常。License Manager 可以终止因不合规而运行状况不佳的实例。有关更多信息，请参阅排查实例合规性问题。
- 要停止因基于用户的订阅而产生的费用，您必须解除该用户与其关联的所有实例的关联。有关更多信息，请参阅 解除用户与基于用户的订阅的关联。
- 在使用 Microsoft Office 产品配置目录时，您的 VPC 必须至少在一个子网中预置 VPC 终端节点。如果要移除由 License Manager 创建的所有 VPC 终端节点资源，则必须执行以下操作：
  - 接触所有用户与其基于用户的订阅的关联。有关更多信息，请参阅 解除用户与基于用户的订阅的关联。
  - 从 License Manager 设置中移除配置的所有目录。有关更多信息，请参阅 移除基于用户的订阅的目录。
  - 终止所有提供基于用户的订阅产品的实例。有关更多信息，请参阅 终止提供基于用户的订阅的 EC2 实例。
- 不得更改或删除由 License Manager 为您的实例分配的值为 `UserSubscriptions` 的 `AWSLicenseManager` 标签键。
- 为了使服务正常运行，不得更改或删除为 License Manager 创建的两个弹性网络接口 (ENI)。
- 不得更改或删除 License Manager 在 AWS Managed Microsoft AD 目录的AWS 保留组织单位 (OU) 中创建的对象。

- 为基于用户的订阅部署的实例必须是具有 AWS Systems Manager 的托管节点，并且必须加入到同一个域中。有关如何让 Systems Manager 管理您的实例的信息，请参阅本指南的排查基于用户的订阅问题章节。

基于用户的订阅的软件

AWS License Manager 支持微软 Visual Studio 和微软 Office 的基于用户的订阅。每位用户都需要单独订阅 Windows Server 远程桌面服务订阅用户访问许可证 (RDS SAL)，才能访问包含许可证的实例，该实例提供基于用户的订阅产品。License Manager 将跟踪支持的软件的使用情况。有关更多信息，请参阅 基于用户的订阅入门。

支持的 Windows 操作系统 (OS) 平台

你可以找到包含适用于以下 Windows 操作系统平台的 RDS SAL 许可证所涵盖产品的 Windows AMI：

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

支持基于用户的订阅的软件

License Manager 支持使用以下软件进行基于用户的许可。

Microsoft Visual Studio

Microsoft Visual Studio 是一个集成式开发环境 (IDE)，开发人员能够创建、编辑、调试和发布应用程序。提供的 Microsoft Visual Studio AMI 包括 AWS Toolkit for .NET Refactoring 和 AWS Toolkit for Visual Studio。

支持的版本

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

下表详细说明了用于 License Manager 基于用户的订阅 API 操作的软件订阅名称及其关联产品值。

软件订阅名称	产品价值

软件订阅名称	产品价值
Visual Studio Enterprise 2022	VISUAL_STUDIO_ENTERPRISE
Visual Studio Professional 2022	VISUAL_STUDIO_PROFESSIONAL

Microsoft Office

Microsoft Office 是微软为各种生产用例开发的一系列软件，包括处理文档、电子表格和幻灯片演示文稿。

支持的版本

- Office LTSC Professional Plus 2021

下表详细说明了用于 License Manager 基于用户的订阅 API 操作的软件订阅名称及其关联产品值。

软件订阅名称	产品价值
Office LTSC Professional Plus 2021	OFFICE_PROFESSIONAL_PLUS

从支持的 AMI 启动

当你从支持Office LTSC Professional Plus微软 Visual Studio 的 AMI 启动实例时，启动时默认为最新的 Windows 操作系统平台版本的 AMI（例如 Windows Server 2022）。要使用较早版本的操作系统平台启动，请按照以下步骤操作。

1. 打开 AWS Marketplace 控制台，网址为 https://console.aws.amazon.com/marketplace。
2. 在导航窗格中，选择管理订阅。
3. 为了简化订阅结果，您可以搜索全部或部分订阅名称。例如，Office LTSC Professional Plus 2021 或 Visual Studio Enterprise。
4. 从订阅面板中选择 “启动新实例”。这将打开启动配置页面。
5. 要从基于早期版本的 Windows 操作系统平台的 AMI 启动实例，请选择软件版本下方的完整 AWS Marketplace 网站链接。此操作带您进入配置页面，您可以从版本列表中进行选择。

6. 该列表显示了支持的 Windows 操作系统平台的最新 AMI 版本。选择你要从中启动的 Windows 操作系统版本。

其他软件

您可以在您的实例上安装其他软件，此类软件不能作为基于用户的订阅提供。License Manager 不会跟踪其他软件的安装。这些安装必须使用默认在您的 AWS Managed Microsoft AD 目录中创建的管理员帐户来执行。有关更多信息，请参阅 AWS Directory Service 管理指南中的管理员帐户。

要使用管理员账户安装其他软件，您必须：

- 使用管理员账户订阅实例提供的产品。
- 将管理员账户与实例关联。
- 使用管理员账户连接到实例以执行安装。

有关更多信息，请参阅 基于用户的订阅入门。

基于用户的订阅入门

以下步骤详细介绍了如何开始使用基于用户的订阅。这些步骤假设您已经实现了所需的先决条件。有关更多信息，请参阅 先决条件 。

如果你已经为基于用户的订阅配置了 AWS Managed Microsoft AD 目录，并且还想使用 Microsoft Office，请参阅修改基于用户的订阅的 VPC 设置。

步骤

- 步骤 1：配置 AWS Directory Service for Microsoft Active Directory 和虚拟私有云 (VPC)
- 步骤 2：订阅产品
- 步骤 3：启动实例以提供基于用户的订阅
- 步骤 4：将用户关联到基于用户的订阅实例
- 步骤 5：连接到基于用户的订阅实例

步骤 1：配置 AWS Directory Service for Microsoft Active Directory 和虚拟私有云 (VPC)

License Manager 需要 AWS Managed Microsoft AD 将用户与基于用户的订阅关联起来。在配置目录时，您必须选择基于用户的订阅所需的所有产品，因为用户只能订阅已配置的产品。<directory_id>注

册 AWS Managed Microsoft AD 目录时，License Manager 将创建两个弹性网络接口 (ENI)，以便服务能够与您的目录通信，其描述类似于为LicenseManager 其AWS 创建的网络接口。

> **Important**
>
> 在继续操作之前，必须允许 License Manager 创建所需的服务相关角色。有关更多信息，请参阅 先决条件 。

要将 Microsoft Office 与基于用户的订阅一起使用，您必须授予许可证管理器更新您的 VPC 配置的权限。在您配置 VPC 时，License Manager 会代表您创建 VPC 终端节点。您的资源需要这些终端节点才能连接到激活服务器并保持合规性。

对于您注册的基于用户的订阅，您必须为任何其他 VPC 配置 DNS 转发。 AWS Managed Microsoft AD 如果您有多个基于用户的订阅 AWS 区域，则每个区域都必须有自己 AWS Managed Microsoft AD 的 DNS 转发配置，如下所示。

您可以使用以下方法之一配置基于用户的订阅的环境。

Console (Active Directory)

AWS Managed Microsoft AD 为基于用户的订阅进行配置（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中选择设置以导航至设置页面，或者在横幅中选择打开设置。
3. 在设置页面上的 AWS Managed Microsoft AD 部分下，选择配置。
4. 对于 AWS 托管目录名称和 ID，选择包含要为其创建基于用户的订阅的用户的目录。
5. 对于产品名称和 ID，选择所有必需的产品，然后选择配置。

   选择配置后，设置页面上的 AWS Managed Microsoft AD 部分将显示您的目录 ID，其状态为正在配置。配置过程完成后，状态将显示为已配置，您可以继续执行其余步骤。

Console (Active Directory and VPC)

AWS Managed Microsoft AD 为基于用户的订阅进行配置（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中选择设置以导航至设置页面，或者在横幅中选择打开设置。

3. 在设置页面上的 AWS Managed Microsoft AD 部分下，选择配置。
4. 对于 AWS 托管目录名称和 ID，选择包含要为其创建基于用户的订阅的用户的目录。
5. 对于产品名称和 ID，选择所有必需的产品。
6. 对于虚拟私有云，请选择一个 VPC 进行其他配置。
7. 对于 vpc-*x* 的子网，请至少选择一个用于预置 VPC 终端节点的子网。
8. 对于 vpc-*x* 的安全组，选择您创建的与 VPC 终端节点关联的安全组，然后选择配置。

   选择配置后，设置页面上的 AWS Managed Microsoft AD 和虚拟私有云部分将显示您的目录 ID 和 VPC ID，其状态为正在配置。配置过程完成后，每项状态都将显示为已配置，您可以继续执行其余步骤。

AWS CLI

AWS Managed Microsoft AD 为基于用户的订阅进行配置 ()AWS CLI

您可以通过该RegisterIdentityProvider操作将您 AWS Managed Microsoft AD 注册为基于用户的订阅的身份提供商。

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product-name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}"
```

为基于用户的订阅配置 AWS Managed Microsoft AD 和您的 VPC ()AWS CLI

您可以将您的身份注册 AWS Managed Microsoft AD 为身份提供商，并通过RegisterIdentityProvider操作将您的 VPC 配置为基于用户的订阅。

```
aws license-manager-user-subscriptions register-identity-
provider --product "<product_name>" --identity-provider
 "ActiveDirectoryIdentityProvider={DirectoryId=<directory_id>}" --settings
 "Subnets=[subnet-1234567890abcdef0,subnet-021345abcdef6789],SecurityGroupId=sg-1234567890ab
```

有关可用软件产品的更多信息，请参阅基于用户的订阅的软件。

步骤 2：订阅产品

要在中订阅配置的产品 AWS Marketplace

在使用所需产品配置目录后，您可能还需要订阅所需的产品。商城订阅状态为非活跃的产品要求您先订阅，然后才能将用户关联到实例并使用它们。

您的账户必须订阅 Windows 服务器远程桌面服务订阅用户访问许可证 (RDS SAL)。Microsoft 远程桌面服务 (RDS) 在 Windows Server 2008 及更低版本中被称为终端服务，是 Microsoft Windows 的组件之一，允许用户通过网络连接控制远程计算机或虚拟机。RDS 允许用户远程访问图形桌面和 Windows 应用程序。

与提供基于用户的订阅产品的实例关联的所有用户，除了他们想要使用的任何其他产品外，还必须具有该许可证的单个有效订阅。当您的用户订阅基于用户的订阅产品时，将代表他们订阅 RDS SAL。

> **Note**
>
> RDS SAL 许可不能与受支持的基于用户的订阅产品分开使用。有关更多信息，请参阅 注意事项。

您可以使用以下链接直接在上 AWS Marketplace 订阅您的产品：

- Visual Studio Professional
- Visual Studio Enterprise
- Office LTSC Professional Plus 2021
- Win 远程桌面服务 SAL

从 License Manager 控制台发现和订阅产品

您还可以从 License Manager 控制台发现需订阅的产品。

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅处选择产品。
3. 选择产品名称以显示订阅详细信息。
4. 选择 “查看方式” AWS Marketplace。
5. 查看订阅详细信息并选择继续订阅。
6. 如果要继续，请查看条款并选择接受条款。

如果您接受条款，则需要处理产品订阅。订阅在完成之前会有一条进行中信息。您可以对您需要的任何其他配置产品重复这些步骤。一旦所有必需的产品都具有有效的订阅，您就可以继续为用户订阅这些产品。

> **Note**
>
> 对于 AWS Billing中尚未结束的账单周期（标记为待处理账单状态），您的用户数量和相关费用的预估账单将需要 48 小时才能显示。有关更多信息，请参阅 AWS Billing 用户指南中的查看您的月度费用。

步骤 3：启动实例以提供基于用户的订阅

订阅产品后，您必须启动实例，供用户从包含该产品的 AWS Marketplace AMI 进行连接。启动实例后， AWS Systems Manager 将尝试将该实例加入域并对资源执行其他配置和强化。使实例可供使用的配置可能需要大约 20 分钟才能完成。在 License Manager 控制台的用户关联页面上，通过检查实例的运行状况是否为活跃，可以确认资源是否已准备就绪。

> **Important**
>
> 您启动的实例必须满足合规性所需的先决条件。无法完成初始配置的资源将被终止。有关更多信息，请参阅 先决条件 和 排查基于用户的订阅问题。

使用基于用户的订阅启动实例

1. 通过以下网址访问 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在图像下，选择 AMI 目录。
3. 选择 AWS Marketplace AMI。
4. 在搜索框中输入产品名称，然后按“Enter”。例如，您可能会搜索 **`Visual Studio`**。
5. 在发布者下，选择 Amazon Web Services。
6. 为要启动实例以提供基于用户的订阅的产品选择选择。
7. 选择继续以继续。
8. 选择使用 AMI 启动实例。
9. 完成向导，同时确保您：

a. 选择不基于 Graviton 而基于 Nitro 的实例类型。
b. 选择一个 VPC 和子网，您的实例可从该子网连接到您的 AWS Managed Microsoft AD 目录。
c. 选择一个允许从您的实例连接到您的 AWS Managed Microsoft AD 目录的安全组。
d. 展开高级详细信息并选择一个允许您的实例使用 Systems Manager 功能的 IAM 角色。

10. 选择启动实例。

在 AWS Marketplace AMI 中运行实例后，您必须为用户订阅该产品并将他们与实例相关联，这些实例提供产品，以便他们能够使用该产品。

步骤 4：将用户关联到基于用户的订阅实例

一旦您订阅了所需产品的 AWS Marketplace AMI，就可以为用户订阅产品并将他们关联到提供该产品的实例。您可以通过单个步骤或单独为用户订阅产品并将他们与实例关联。当您为用户订阅时，会检查目录以确保存在该用户身份。将为您订阅产品的每个用户创建一个订阅。

> **Note**
>
> 每个用户都必须订阅 Windows Server 远程桌面服务订阅用户访问许可证 (RDS SAL) 和他们将要使用的产品。您的账户按步骤 2：订阅产品中所述订阅 RDS SAL 后，当您的用户订阅基于用户的订阅产品时，您将代表他们订阅 RDS SAL。

License Manager 中的产品页面会通过将商城订阅状态列为活跃来显示有效订阅。在产品的详细信息页面中，License Manager 将显示状态为已订阅的有效用户订阅。

> **Important**
>
> 如果您的目录未配置该产品，则控制台顶部将出现一个通知栏，建议您调整目录的设置。在通知栏上，选择打开设置以访问 License Manager 中的设置页面并编辑您的目录。
> 每个用户都必须订阅 RDS SAL 和他们将要使用的产品。如果为用户订阅商城订阅状态为非活跃的产品，则会失败。

为用户订阅产品并将他们关联到实例

您可以通过以下过程为用户订阅产品，并将他们与实例关联起来。

为用户订阅并将其关联到实例

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅下，选择用户关联。
3. 选择要与用户关联的实例，然后选择订阅并关联用户。
4. 指定目录中最多存在的五个用户名，包括域名（如果这些用户名存在于可信域中），然后选择订阅并关联。

在用户关联页面上，您选择的用户应显示在关联状态为已关联的用户下。此外，在产品页面上，您可以通过选择产品名称来查看产品的详细信息页面。已订阅的用户将显示在状态为已订阅的用户下。

为用户订阅产品

您可以使用以下方法之一为用户订阅产品。

Console

为用户订阅产品（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅处选择产品。
3. 为用户选择商城订阅状态为活跃的产品进行订阅，然后选择订阅用户。
4. 指定目录中最多存在的五个用户名，包括域名（如果这些用户名存在于可信域中），然后选择订阅。

   已订阅的用户将显示在状态为已订阅的用户下。

AWS CLI

允许用户订阅产品 (AWS CLI)

您可以使用 StartProductSubscription 操作为用户订阅在您的身份提供商处注册的产品。

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 ""ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}"
```

使用自管理 Active Directory 为用户订阅产品 (AWS CLI)

您可以使用StartProductSubscription操作为自己管理的 Active Directory 中的用户订阅在您的 AWS Managed Microsoft AD 目录中注册的产品。

```
aws license-manager-user-subscriptions start-product-subscription
 --username <user_name> --product <product_name> --identity-provider
 'ActiveDirectoryIdentityProvider" = {"DirectoryId" = "<directory_id>"}' --
domain <self-managed-domain-name>
```

有关可用软件产品的更多信息，请参阅基于用户的订阅的软件。

已订阅的用户将显示在状态为已订阅的用户下。

将用户关联到实例

您可以使用以下方法之一将用户与实例关联。

> **Important**
>
> 在将产品与实例关联之前，您必须先为用户订阅产品。

Console

将用户关联到实例（控制台）

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅下，选择用户关联。
3. 选择要与用户关联的实例，然后选择关联用户。
4. 指定目录中最多存在的五个用户名，包括域名（如果这些用户名存在于可信域中），然后选择关联。

   在用户关联页面上，您选择的用户应显示在关联状态为已关联的用户下。

AWS CLI

将用户关联到实例 (AWS CLI)

您可以将用户与启动的实例关联起来，以便通过 AssociateUser 操作提供基于用户的订阅。

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}"
```

将自管理 Active Directory 用户关联到实例 (AWS CLI)

您可以将自管理 Active Directory 中的用户与启动的实例关联起来，以便通过 AssociateUser 操作提供基于用户的订阅。

```
aws license-manager-user-subscriptions associate-user --username <user_name> --
instance-id <instance_id> --identity-provider  ""ActiveDirectoryIdentityProvider" =
 {"DirectoryId" = "<directory_id>"}" --domain <self-managed-domain-name>
```

有关可用软件产品的更多信息，请参阅基于用户的订阅的软件。

在用户关联页面上，您选择的用户应显示在关联状态为已关联的用户下。

步骤 5：连接到基于用户的订阅实例

将用户与提供产品的实例关联后，如果实例的运行状况为活跃，他们就可以连接到该实例。用户需要使用域的用户凭证进行连接，才能以相关身份使用产品。

> **Important**
>
> 创建 EC2 实例并为用户准备该实例这一过程可能需要大约 20 分钟。实例的关联状态必须为活跃，才能访问该实例和使用该产品。

使用基于用户的订阅连接到实例

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅下，选择用户关联。
3. 在用户关联页面上，确认实例的运行状况为活跃。
4. 记下实例 ID，因为您将需要它来收集连接详细信息。
5. 按照使用 RDP 连接到 Windows 实例中列出的步骤进行操作，同时确保指定关联用户的完全限定用户名。

修改基于用户的订阅的目录设置

您可以在 License Manager 设置页面中配置的目录中添加或移除基于用户的订阅的产品。如果你使用的是 Microsoft Office 产品，则步骤会有所不同，因为 License Manager 必须为此类订阅创建 VPC 终端节点。

在没有 Microsoft Office 产品的情况下修改目录配置

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择 设置。
3. 在“设置”页面的 AWS Managed Microsoft AD 部分下，选择编辑。
4. 对于产品名称和 ID，选择其他产品并根据需要清除之前的选择，然后选择保存更改。

使用 Microsoft Office 产品修改目录配置

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中选择设置以导航至设置页面，或者在横幅中选择打开设置。
3. 在设置页面的 AWS Managed Microsoft AD 部分下，选择编辑。
4. 对于产品名称和 ID，选择所有必需的产品，包括 Microsoft Office。
5. 对于虚拟私有云，请选择一个 VPC 进行其他配置。
6. 对于 vpc-***x*** 的子网，请至少选择一个用于预置 VPC 终端节点的子网。
7. 对于 vpc-***x*** 的安全组，选择您创建的与 VPC 终端节点关联的安全组，然后选择保存更改。

   选择保存更改后，设置页面上的 AWS Managed Microsoft AD 和虚拟私有云部分将显示您的目录 ID 和 VPC ID，其状态为正在配置。您必须等到目录的状态为已配置且 VPC 的状态为活跃，然后才能将基于用户的订阅与 Microsoft Office 结合使用。

修改基于用户的订阅的 VPC 设置

如果您添加了 Microsoft Office 产品，则可以修改您的 VPC 的配置。License Manager 将在您指定的子网中代表您创建 VPC 终端节点，以便您的资源到达激活服务器并保持合规性。您必须指定至少一个子网。有关更多信息，请参阅 先决条件 。

> **Note**
>
> 仅当您的目录配置了 Microsoft Office 产品时，才能修改 VPC 设置。有关更多信息，请参阅 基于用户的订阅入门。
> 如果要移除所有 VPC 终端节点，请参阅注意事项。

修改目录配置

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择 设置。
3. 在“设置”页面的已配置的虚拟私有云部分下，选择编辑。
4. 根据需要更改已配置的 VPC 的子网和安全组，然后选择保存更改。

解除用户与基于用户的订阅的关联

您可以解除用户与实例的关联以移除对资源的访问权限。

> **Note**
>
> 从目录中删除用户不会改变用户关联或订阅。您必须在 License Manager 中解除用户与产品详细信息页面的关联，才能移除其与实例的关联。

解除基于用户的订阅用户的关联

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅下，选择用户关联。
3. 选择要解除用户关联的实例。
4. 选择要解除关联的用户名，然后选择解除关联用户。

从基于用户的订阅中取消用户订阅

您可以取消用户对产品的订阅，以删除访问权限并停止向其收取产品费用。

> **Important**
>
> 必须先解除用户与当前关联实例的关联，然后才能取消订阅。

从基于用户的订阅中取消用户订阅

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅处选择产品。
3. 选择要取消用户订阅的产品。
4. 选择要取消订阅的用户名，然后选择取消订阅用户。

终止提供基于用户的订阅的 EC2 实例

如果您不再需要提供基于用户的订阅的实例，您可以将其删除。这称为终止实例。您应该首先取消所有用户与实例的关联，然后从 Amazon EC2 控制台终止该实例。

> **Note**
>
> 必须取消用户与实例的关联，才能停止产生订阅费用。有关更多信息，请参阅 解除用户与基于用户的订阅的关联。

识别和终止提供基于用户的订阅的实例

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的基于用户的订阅下，选择用户关联。
3. 在用户关联页面上，选择实例 ID 以访问实例的详细信息页面。
4. 记下实例 ID，因为您需要它来终止实例。
5. 解除所有用户与实例的关联。
6. 按照终止实例中列出的步骤进行操作。

移除基于用户的订阅的目录

如果不想再将目录用于基于用户的订阅，则可以将其删除。从 License Manager 中移除目录的配置并不能删除目录本身。移除目录后，无法将用户与基于用户的订阅的目录相关联。

> **Important**
>
> 必须先解除用户关联并终止提供基于用户的订阅的实例，然后才能从 License Manager 中移除该目录。

移除目录

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择 设置。
3. 在 “设置” 页面的 AWS Managed Microsoft AD 部分下，选择 “删除”。
4. 输入所需的文本以确认您要移除该目录，然后选择移除。

选择移除后，设置页面上的 AWS Managed Microsoft AD 部分将显示您的目录 ID，状态为正在配置。配置过程完成后，应从 AWS Managed Microsoft AD 部分中移除该目录。

排查基于用户的订阅问题

以下是一些问题排查技巧，可帮助解决 AWS License Manager中基于用户的订阅可能出现的问题。

目录

排查实例合规性问题

提供基于用户的订阅的实例必须保持正常运行状态才能符合要求。标记为运行状况不佳的实例不再满足所需的先决条件。License Manager 将尝试将实例恢复到正常运行状态，但无法恢复正常运行状态的实例将被终止。

将终止为提供基于用户的订阅而启动但无法完成初始配置的实例。在这种情况下，您必须更正配置问题并启动新实例才能提供基于用户的订阅。有关更多信息，请参阅 先决条件 。

排查许可证合规性问题

如果您将目录配置为通过 Microsoft Office 提供基于用户的订阅，则必须确保您的资源可以连接到 License Manager 创建的 VPC 终端节点。终端节点需要 TCP 端口 1688 上的入站流量，这些流量来自提供基于用户的订阅的实例。

您可以使用 Reachability Analyzer 来帮助确认提供基于用户订阅的实例和 VPC 终端节点的网络配置是否正确。您可以指定在提供基于用户的订阅的子网中启动的实例 ID 作为来源，将为 Microsoft Office 产品预置的 VPC 终端节点指定为目标。将 TCP 指定为协议，将 1688 指定为要分析的路径的目标端口。有关更多信息，请参阅如何解决网关和接口 VPC 终端节点上的连接问题？。

排查实例连接问题

用户必须能够使用 RDP 连接到提供基于用户的订阅的实例，才能使用其中的产品。有关排除实例连接故障的更多信息，请参阅 Amazon EC2 用户指南中的 Windows 实例连接疑难解答。

对加入域名失败问题进行排查

用户必须能够通过 License Manager 设置中配置的目录，以其用户身份连接到提供基于用户的订阅产品的实例。将终止未能加入域的实例。

要进行问题排查，您可能需要启动实例并手动加入域，这样资源就不会被终止，然后才能进行调查。实例必须成功接收并执行 Systems Manager Run Command，并且该实例还必须能够在操作系统中完成域加入。有关更多信息，请参阅 AWS Systems Manager 用户指南中的了解命令状态和 Microsoft 网站上的如何排除将基于 Windows 的计算机连接到域时发生的错误。

排查 Systems Manager 连接问题

提供基于用户的订阅的实例必须由管理， AWS Systems Manager 否则它们将被终止。有关更多信息，请参阅 AWS Systems Manager 用户指南中的排查 SSM 代理问题和排查托管节点可用性问题疑难解答。

对 Systems Manager Run Command 进行故障排除

Run Command 是 Systems Manager 的一项功能，可与提供基于用户订阅的实例一起使用，以加入域、强化操作系统并对所含产品执行访问审核。有关更多信息，请参阅AWS Systems Manager 用户指南中的了解命令状态。

License Manager 中的 Linux 订阅

借助 AWS License Manager，您可以查看和管理您在 AWS 上拥有和运行的商业 Linux 订阅。可以跨 AWS 区域和账户跟踪许可证使用情况。一旦发现并汇总了数据，您就可以使用商用 Linux 订阅了解您的所有实例。此外，您发现的订阅数据将作为 Amazon CloudWatch 控制面板显示在 License Manager 控制台中。如果您的账户位于 Organizations 中，则可以将成员账户注册为委托管理员，以管理任务。有关更多信息，请参阅委托管理员。

您可以跟踪多个订阅的使用情况，例如：

- Red Hat Enterprise Linux (RHEL) 随附订阅
- 使用 Red Hat Cloud Access 程序的 RHEL 自带订阅模式 (BYOS)
- SUSE Linux Enterprise Server
- Ubuntu Pro

Linux 订阅使用最终一致性模型。一致性模型决定了在 Linux 订阅视图中加载和呈现数据的方式和时间安排。使用此模型，License Manager 可确保从您的资源中定期更新您的 Linux 订阅数据。如果某些数据在这些时间间隔内未被摄取，则将在下次指标发布时提供这些信息。此行为可能会造成资源（如新启动的 EC2 商业 Linux 实例）延迟显示在 Linux 订阅控制面板中。

> **Note**
>
> 完成初始资源发现最长可能需要 36 小时，发现和报告新启动的实例最长可能需要 12 小时。一旦发现您的资源，就会每小时发布一次 Linux 订阅数据的 Amazon CloudWatch 指标。

目录

管理 Linux 订阅的发现

您可以使用 License Manager 控制台管理 Linux 订阅的发现。当您为指定的 AWS 区域启用 Linux 订阅发现功能时，您可以选择将此发现功能扩展到 AWS Organizations 中的账户。如果您不再需要跟踪订阅使用情况，您也可以禁用发现功能。

> **Note**
>
> 默认情况下，每个 AWS 区域的每个账户最多可以发现和显示五千个资源。要申请上调限制，请使用限制上调表。

主题

启用 Linux 订阅的发现功能

要启用 Linux 订阅的发现功能，您需要在 License Manager 中配置所需的设置。在设置页面中，您可以创建服务相关角色、指定要在哪些 AWS 区域中启用发现功能以及是否跨 AWS Organizations 账户发现资源。

为 Linux 订阅启用发现功能

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择 Linux 订阅选项卡，然后选择配置。
4. 在源 AWS 区域 中，选择要发现 Linux 订阅的区域。

5. 如果您想在 AWS Organizations 中汇总各个账户的订阅数据，请选择关联 AWS Organizations。
6. 查看并确认该选项，该选项授予创建 Linux 订阅服务相关角色的 AWS License Manager 权限。
7. 选择 Save configuration。

资源发现状态原因

AWS License Manager 将显示您选择启用 Linux 订阅发现功能的每个 AWS 区域的状态和相应的状态原因。如果您将 Linux 订阅与 AWS Organizations 相关联，则状态原因会有所不同：

- 正在进行中
- 成功
- 失败

为您选择的每个区域显示的状态原因一次最多显示两个状态原因。下表提供了更多详细信息：

状态原因操作	描述
Account-onboard	注册单个账户。
Account-offboard	注销单个账户。
Org-onboard	注册整个组织。
Org-offboard	注销整个组织。

您可以调用 `UpdateServiceSettings` API 并随后调用 `GetServiceSettings` API 来监控启用 Linux 订阅的进度。每种状态和状态原因可以同时适用于多个区域。下表提供了有关状态和状态原因的更多详细信息：

状态	状态原因	描述
正在进行	`"Region": "Account-Onboard: Pending"`	正在为单个账户启用 Linux 订阅。
	`"Region": "Org-Onboard: Pending"`	正在为组织启用 Linux 订阅。

状态	状态原因	描述
	"Region": "Account-Offboard: Pending	正在禁用单个账户的 Linux 订阅。
	"Region": "Org-Offboard: Pending	正在禁用组织的 Linux 订阅。
成功	"Region": "Account-Onboard: Successful"	已成功为单个账户启用 Linux 订阅。
	"Region": "Org-Onboard: Successful"	已成功为组织启用 Linux 订阅。
	"Region": "Account-Offboard: Successful	已成功禁用单个账户的 Linux 订阅。
	"Region": "Org-Offboard: Successful	成功禁用组织的 Linux 订阅。
失败	"Region": "Account-Onboard: Failed - Service-linked role not present"	由于未创建所需的服务相关角色，为单个账户启用 Linux 订阅失败。创建所需的角色，然后重试。
	"Region": "Account-Onboard: Failed - An internal error occurred"	由于内部错误，为单个账户启用 Linux 订阅失败。
	"Region": "Org-Onboard: Failed - Account isn't the management account"	为组织启用 Linux 订阅失败，因为执行该操作的账户不是该组织的管理账户。登录管理账户，然后重试。
	"Region": "Org-Onboard: Failed - Account isn't part of an organization"	为组织启用 Linux 订阅失败，因为执行操作的账户不在组织中。尝试使用组织中的某个账户进行操作，或者将此账户添加到组织中，然后重试。

状态	状态原因	描述
	`"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"`	由于 License Manager 没有访问该组织的权限，因此为组织启用 Linux 订阅失败。创建 Linux 订阅的服务相关角色，然后重试。

禁用 Linux 订阅的发现功能

您可以从 AWS License Manager 设置页面禁用 Linux 订阅的发现功能。

> **Warning**
> 如果您禁用发现功能，则之前在 Linux 订阅中发现的所有数据都将从 AWS License Manager 中移除。

禁用 Linux 订阅的发现功能

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择设置。
3. 在设置页面上，选择 Linux 订阅选项卡，然后选择禁用 Linux 订阅发现。
4. 输入**`Disable`**，然后选择禁用以确认停用。
5. （可选）删除 Linux 订阅的服务相关角色。有关更多信息，请参阅删除 License Manager 的服务相关角色。
6. （可选）禁用 License Manager 与您的组织之间的可信访问权限。有关更多信息，请参阅 AWS License Manager 和 AWS Organizations：

查看发现的实例数据

完成初始资源发现后，您将能够查看在所选 AWS 区域中发现的 Linux 订阅。如果您选择关联 AWS Organizations，则还会汇总来自组织内账户的数据。您可以导航到 AWS License Manager 控制台的实例部分以查看数据表。您可以导航到 AWS License Manager 控制台的实例部分以查看数据表。

每个实例的数据包括以下内容：

- 实例 ID — 实例的 ID。
- 实例类型 — 实例的类型。
- 账户 ID — 拥有实例的账户的 ID。
- 状态 — 实例的状态。
- 区域 — 实例所在的 AWS 区域。
- 使用操作 — 实例的操作以及与 AMI 关联的账单代码。有关更多信息，请参阅使用操作值。
- 产品代码 — 用于启动实例的 AMI 关联的产品代码。有关更多信息，请参阅 AMI 产品代码。
- AMI ID — 用于启动实例的 AMI 的 ID。

主题

查看所有实例的数据

您可以查看所选区域内组织中各账户汇总的所有实例的数据。

查看所有实例的发现的数据

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的“Linux 订阅”下，选择实例。
3. 根据需要在控制台中查看数据。您可以按如下条件筛选数据：
    - 实例 ID
    - 账户
    - 区域
    - AMI ID
    - 使用情况操作
    - 产品代码
4. （可选）选择将视图导出为 CSV，将所有实例的数据导出为逗号分隔值文件 (CSV)。

查看每个订阅的实例数据

您可以查看所选区域内组织中各账户汇总的所有实例的数据。

查看使用特定订阅的实例的已发现数据

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的“Linux 订阅”下，选择订阅。
3. 在订阅名称列下，选择您要查看其数据的订阅。
4. 选择实例选项卡，然后根据需要在控制台中查看数据。您可以按如下条件筛选数据：
   - 实例 ID
   - 账户
   - 区域
   - AMI ID
   - 使用情况操作
   - 产品代码
5. （可选）选择将视图导出为 CSV，将使用此订阅的实例的数据导出为逗号分隔值文件 (CSV)。

Linux 订阅的账单信息

在 Amazon EC2 上运行的每个商用 Linux 订阅都将具有与亚马逊机器映像 (AMI) 关联的账单信息。商用 Linux 订阅将包含 Amazon EC2 使用操作、AWS Marketplace 产品代码或两者的组合。有关更多信息，请参阅适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南中的 AMI 账单信息字段和 AWS Marketplace 卖家指南中的 AMI 产品代码。

订阅名称	Amazon EC2 使用情况操作	AWS Marketplace 产品代码	订阅类型
Red Hat Enterprise Linux Server BYOS	RunInstances:00g0	✗	自带订阅模式 (BYOS)
Red Hat Enterprise Linux Server	RunInstances:0010	✗	随附 EC2 订阅
具有高可用性附加组件的 Red Hat Enterprise Linux	RunInstances:1010	✗	随附 EC2 订阅

订阅名称	Amazon EC2 使用情况操作	AWS Marketplace 产品代码	订阅类型
采用 SQL Server Standard 和高可用性的 Red Hat Enterprise Linux	RunInstances:1014	✗	随附 EC2 订阅
采用 SQL Server Enterprise 和高可用性的 Red Hat Enterprise Linux	RunInstances:1110	✗	随附 EC2 订阅
采用 SQL Server 标准版的 Red Hat Enterprise Linux	RunInstances:0014	✗	随附 EC2 订阅
采用 SQL Server Web 的 Red Hat Enterprise Linux	RunInstances:0210	✗	随附 EC2 订阅
采用 SQL Server 企业版的 Red Hat Enterprise Linux	RunInstances:0110	✗	随附 EC2 订阅
SUSE Linux Enterprise Server	RunInstances:000g	✗	随附 EC2 订阅
具有高可用性和更新服务的 Red Hat Enterprise Linux for SAP	RunInstances:0010	✓	AWS Marketplace 订阅 [1]
SUSE Linux Enterprise Server with SAP	✗	✓	AWS Marketplace 订阅
Ubuntu Pro	RunInstances:0g00	✓	AWS Marketplace 订阅

订阅名称	Amazon EC2 使用情况操作	AWS Marketplace 产品代码	订阅类型
Red Hat Enterprise Linux 工作站	✗	✓	AWS Marketplace 订阅

[1] 此订阅同时具有 Amazon EC2 使用操作和 AWS Marketplace 产品代码。

Linux 订阅的使用情况指标和 Amazon CloudWatch 警报

AWS License Manager 控制台的订阅部分列出了您在 AWS 上购买的或使用自带订阅模式 (BYOS) 引入的已发现的商业 Linux 订阅。所有商用 Linux 订阅均按实例进行许可。

每个发现的 Linux 订阅都有以下详细信息：

- 订阅名称
- 订阅类型
- 每个订阅的正在运行的实例数
- 已配置的 Amazon CloudWatch 警报

当您从摘要页面选择 Linux 订阅时，使用情况指标和警报选项卡将显示该订阅的数据。在此选项卡中，License Manager 控制台中显示所选订阅的 Amazon CloudWatch 控制面板。您可以调整控制面板以涵盖从选定日期开始的特定时间范围或评估范围，以小时、天或周为单位。

在使用情况指标和警报选项卡中，每个订阅都有一个警报部分，详细说明了以下内容：

- 警报名称 — 警报的名称。
- 状态 — 警报的状态。
- 维度 — 警报的维度。该维度将包括 AWS 区域和已定义的实例类型。
- 条件 — 警报的条件。条件将包括比较运算符和已定义的警报阈值。

您可以使用您定义的维度和条件创建 CloudWatch 警报，以便根据您当前的订阅使用情况进行跟踪和告警。Linux 订阅控制台显示摘要，包括正在使用的订阅名称、订阅类型、每个订阅的正在运行的实例数量以及警报状态。

以下是 CloudWatch 可能出现的警报状态：

- 正常 — 指标或表达式在定义的阈值范围内。
- 警报 — 指标或表达式超出定义的阈值。
- 数据不足 — 警报刚刚开始、指标不可用或没有足够数据可用于指标来确定警报状态。

主题

Linux 订阅的使用情况指标

以下指标和维度可用于 Linux 订阅：

指标	描述
RunningInstancesCount	当前账户中运行的按订阅名称或订阅名称和区域分组的实例总数。 单位：计数 维度： `SubscriptionName` ：订阅的名称。 `Region`：发现使用商业 Linux 订阅的资源的区域。

为 Linux 订阅创建警报

您可以为运行中的 EC2 实例上发现的每个商业 Linux 订阅创建警报。如有必要，您可以为每个订阅创建具有不同维度和条件的多个警报。

使用控制台为 Linux 订阅创建 CloudWatch 警报

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的“Linux 订阅”下，选择订阅。
3. 在订阅名称列下，选择要为其创建警报的订阅，然后选择创建警报。

4. 为警报指定以下内容：
   - 警报名称 — 指定类似 AWS-LM-LS-*AlarmName* 的名称。
   - “实例类型”— 选择将使用所选订阅的实例类型。
   - “使用区域”— 选择要为其创建警报的区域。
   - “比较运算符”— 警报阈值的比较运算符。
   - “警报阈值”— 警报的阈值。
5. 选择创建以创建警报。

修改 Linux 订阅的警报

您可以从 License Manager 控制台修改现有警报以适应不断变化的需求。

使用控制台修改 Linux 订阅的 CloudWatch 警报

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的“Linux 订阅”下，选择订阅。
3. 在订阅名称列下，选择要修改的订阅，然后选择编辑。
4. 根据需要修改定义的值。
5. 选择编辑以修改警报。

删除 Linux 订阅的警报

您可以从 License Manager 控制台中删除现有警报以适应不断变化的需求。

使用控制台删除 Linux 订阅的 CloudWatch 警报

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中的“Linux 订阅”下，选择订阅。
3. 在订阅名称列下，选择要修改的订阅，然后选择删除。

AWS License Manager 中的设置

AWS License Manager 控制台的设置部分显示当前账户的设置。您必须配置设置才能启用某些功能，例如向组织分配托管授权和自管理许可证，以及执行跨账户资源发现。

编辑 License Manager 设置

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择设置。
3. 选择包含您要配置或修改的设置的选项卡。例如，选择托管许可证以配置账户详细信息。
4. 为要配置或修改的设置选择相关操作。例如，您可以选择编辑或开启。

设置主题

托管许可证

以下设置适用于托管许可证。

账户详细信息

您可以查看账户详细信息以查看账户类型、AWS Organizations 中的账户是否已关联、账户的 License Manager S3 存储桶 ARN 以及 AWS Resource Access Manager 共享 ARN 等信息。您还可以使用此部分关联您的 AWS Organizations 账户。

要在组织内分配托管权限或自管理许可证，请选择关联 AWS Organizations 账户。您的所有成员账户都会自动接受托管权限的分配授权。当您选择此选项时，我们会向管理账户和成员账户添加服务相关角色。

> **Note**
>
> 要启用该选项，您必须登录到管理账户并在 AWS Organizations 中启用所有功能。有关更多信息，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。
> 此选项还会在您的管理账户中创建 AWS Resource Access Manager 资源共享，这样您就可以无缝共享自管理许可证。有关更多信息，请参阅 AWS Resource Access Manager 用户指南。

要禁用此选项，请调用 UpdateServiceSettings API。

跨账户资源查找

您可以开启跨账户资源发现，以便在 AWS Organizations 中管理所有账户的许可证使用情况。

要在组织中启用跨账户资源发现，请选择开启跨账户资源发现。当您开启跨账户资源发现功能时，AWS Organizations 将自动关联到您的所有账户中执行资源发现。

License Manager 使用 Systems Manager 清单来发现软件使用情况。确保已在所有资源上配置 Systems Manager 清单。查询 Systems Manager 清单需要满足以下条件：

- 资源数据同步以将清单存储在 Amazon S3 存储桶中。
- Amazon Athena 在 AWS Organizations 中汇总您账户中的清单数据。
- AWS Glue 提供快速的查询体验。

> **Note**
>
> 以下 AWS 区域不需要 Amazon Athena 或AWS Glue 来查询或汇总 Systems Manager 清单的清单数据以发现软件使用情况：
>
> - 亚太地区（雅加达）
> - 以色列（特拉维夫）

Simple Notification Service (SNS)

您可以将 Amazon SNS 配置为接收来自 License Manager 的通知和告警。

配置 Amazon SNS 主题

1. 选择Simple Notification Service (SNS)旁边的编辑。
2. 采用以下格式指定 SNS 主题 ARN：

   ```
   arn:<aws_partition>:sns:<region>:<account_id>:aws-license-manager-service-*
   ```

3. 选择保存更改。

Linux 订阅

您可以配置 Linux 订阅的设置，以控制订阅发现和汇总的执行方式。您可以选择要发现 Linux 订阅的区域，以及是否要在 AWS Organizations 中汇总各账户的订阅数据。有关更多信息，请参阅License Manager 中的 Linux 订阅。

基于用户的订阅

以下设置可用，具体取决于基于用户的订阅所需的产品。

AWS Managed Microsoft AD

License Manager 要求先配置 AWS Managed Microsoft AD，然后才能使用基于用户的订阅。有关更多信息，请参阅License Manager 中的基于用户的订阅。

虚拟私有云

当您在 Microsoft Office 中使用基于用户的订阅时，除了 AWS Managed Microsoft AD 之外，License Manager 还需要配置您的 VPC。有关更多信息，请参阅License Manager 中的基于用户的订阅。

委托管理员

您可以在 License Manager 中注册委托管理员来执行托管许可证和 Linux 订阅的管理任务。为了简化管理，我们建议使用 License Manager 控制台为 License Manager 的每项功能注册一个委托管理员。使用这种方法，您的组织中将有一个委托管理员来管理 License Manager。

使用 AWS CLI 或软件开发工具包，您可以将组织中的不同成员账户注册为每项受 License Manager 支持功能的委托管理员。这样可以让组织中的不同成员账户能够执行托管许可证和 Linux 订阅的管理任务。

> **Important**
>
> 要在 License Manager 控制台中使用委托管理功能，您必须将相同的成员账户注册为每项 License Manager 功能的委托管理员。如果您将多个成员账户注册为委托管理员，则必须先注销现有成员账户，然后为 License Manager 的每项功能注册相同的账户。

必须先使用 Organizations 启用可信访问权限，然后才能注册委托管理员。有关更多信息，请参阅邀请 AWS 账户加入您的组织和使用 AWS Organizations 启用可信访问权限。

以下是您可以注册委托管理员的功能：

托管许可证

您可以执行管理任务，例如与其他成员账户共享自管理许可证、执行跨账户资源发现以及将托管权限分配给其他成员账户。

Linux 订阅

您可以执行管理任务，如查看和管理您拥有的商业 Linux 订阅，并在 AWS Organizations 中跨 AWS 区域和账户运行。您还可以针对订阅 Linux 创建和管理 Amazon CloudWatch 告警。必须先发现并汇总数据，然后才能在 License Manager 控制台中显示这些数据，如果配置了告警，则所有告警都可以正常运行。

> **Important**
>
> 注册后，委托管理员就可以查看您组织中账户拥有的 EC2 实例。

AWS License Manager 控制台、AWS CLI 或 AWS 开发工具包可用于注册和取消注册委托管理员。

委托管理员支持的区域

以下区域支持 License Manager 委托的管理员：

- 美国东部（俄亥俄州）
- 美国东部（弗吉尼亚州北部）
- 美国西部（北加利福尼亚）
- 美国西部（俄勒冈）

- Asia Pacific (Mumbai)
- 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）
- 亚太地区（香港）
- 中东（巴林）
- 加拿大（中部）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲（伦敦）
- 欧洲（巴黎）
- Europe (Stockholm)
- 欧洲地区（米兰）
- 非洲（开普敦）
- 南美洲（圣保罗）

注册委托管理员

您可以使用 AWS CLI 或 AWS Management Console注册委托管理员。

Console

要使用 AWS License Manager 控制台注册委托管理员，请执行以下步骤：

1. 以管理账户管理员身份登录 AWS。
2. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
3. 从左侧导航窗格中，选择设置。
4. 选择委托管理选项卡。
5. 选择 Register delegated administrator (注册委派管理员)。
6. 输入要注册为委托管理员的成员账户 ID，确认要授予 License Manager 所需的权限，然后选择注册。
7. 将显示一条消息，表示指定账户是否已成功注册为 License Manager 的委托管理员。

AWS CLI

要使用 AWS CLI 注册托管许可证的委派管理员，请执行以下步骤：

1. 在命令行处，运行以下 AWS CLI 命令：

```
aws organizations register-delegated-administrator --service-principal=license-manager.amazonaws.com --account-id=<account-id>
```

2. 运行以下命令验证指定的账户是否已成功注册为委托管理员。

```
aws organizations list-delegated-administrators --service-principal=license-manager.amazonaws.com
```

要使用 AWS CLI 注册 Linux 订阅的委托管理员，请执行以下步骤：

1. 在命令行处，运行以下 AWS CLI 命令：

```
aws organizations register-delegated-administrator --service-principal=license-manager-linux-subscriptions.amazonaws.com --account-id=<account-id>
```

2. 运行以下命令验证指定的账户是否已成功注册为委托管理员。

```
aws organizations list-delegated-administrators --service-principal=license-manager-linux-subscriptions.amazonaws.com
```

注销委托管理员

您还可以使用 AWS CLI 或 AWS Management Console注销委托管理员。

Console

要使用 AWS License Manager 控制台注销委托管理员，请执行以下步骤：

1. 以管理账户管理员身份登录 AWS。
2. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
3. 从左侧导航窗格中，选择设置。
4. 选择委托管理选项卡。

5. 选择移除。
6. 输入文本 **remove** 以确认您要移除的 License Manager 委托管理员，然后选择移除。
7. 将显示一条消息，表示指定账户是否已成功移除 License Manager 的委托管理员。

AWS CLI

要使用 AWS CLI 注销托管许可证的委托管理员，请执行以下步骤：

1. 在命令行处，运行以下 AWS CLI 命令：

```
aws organizations deregister-delegated-administrator --service-
principal=license-manager.amazonaws.com --account-id=<account-id>
```

2. 运行以下命令验证指定的账户是否已成功取消注册为委托管理员。

```
aws organizations list-delegated-administrators --service-principal=license-
manager.amazonaws.com
```

要使用 AWS CLI 注销 Linux 订阅的委托管理员，请执行以下步骤：

1. 在命令行处，运行以下 AWS CLI 命令：

```
aws organizations deregister-delegated-administrator --service-
principal=license-manager-linux-subscriptions.amazonaws.com --account-
id=<account-id>
```

2. 运行以下命令验证指定的账户是否已成功取消注册为委托管理员。

```
aws organizations list-delegated-administrators --service-principal=license-
manager-linux-subscriptions.amazonaws.com
```

您可随时再次注册已注销的账户。

AWS License Manager 中的控制面板

License Manager 控制台的控制面板部分提供了使用情况详细信息，用于跟踪与每个自管理许可证、授予的许可证权限、基于用户的订阅的订阅用户以及正在运行的实例相关的许可证使用情况。控制面板还会显示由于违反许可证规则而产生的警报。

概述

概述部分提供了有关您的许可证的以下详细信息。

已授予的许可证

该区域此账户中已授予的许可证总量。

自管理许可证

该区域此账户中自管理许可证总量。

卖家颁发的许可证

该区域此账户中卖家颁发的许可证总量。

产品

产品部分提供了基于用户的订阅的以下详细信息。

产品名称

基于用户的订阅的名称产品。

已订阅用户

该产品的已订阅用户数。

已授予的许可证权限

已授予的许可证权限部分提供了以下详细信息。

产品名称

已授予的许可证的产品名称。

授权

授权的名称。

用量

权限的使用情况。

自管理许可证

自管理许可证提供以下详细信息。

许可证名称

自管理许可证的名称。

授权

授权的名称。

用量

权限的使用情况。

实例使用情况

实例使用情况部分提供了以下详细信息。

正在运行的实例计数

该区域中此账户中正在运行的实例总数。

汇总正在运行的实例计数

您在该区域的 AWS Organizations 内所有账户中汇总的正在运行的实例总数。此图表仅对管理账户和委托管理员账户可见。

监控 AWS License Manager

您可以使用 Amazon CloudWatch 监控 AWS License Manager 中跟踪的许可证和订阅的使用情况。CloudWatch 收集和处理原始数据，并将数据处理为便于读取的近乎实时的指标。您可以设置用于监控特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅使用 Amazon CloudWatch 监控许可证使用情况。

您可以使用 AWS CloudTrail 捕获由某个 AWS 账户发出或代表该账户发出的 API 调用和相关事件。事件会以日志文件的形式捕获，传送到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅使用 AWS CloudTrail 记录 AWS License Manager API 调用。

目录

使用 Amazon CloudWatch 监控许可证使用情况

您可以使用 Amazon CloudWatch 监控 License Manager 的指标统计数据。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。您可以设置用于监控特定阈值的警报，并在达到相应阈值时发送通知或执行操作。例如，您可以使用 `LicenseConfigurationUsagePercentage` 指标监控许可证的百分比，并在超过限制之前采取措施。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

License Manager 每小时在 `AWSLicenseManager/licenseUsage` 命名空间中发布以下指标：

指标	描述
RunningInstancesCount	当前账户中运行的按订阅名称分组的实例总数。 单位：计数 维度：

指标	描述
	SubscriptionName ：订阅的名称。
AggregateRunningInstancesCount	在当前 AWS 区域内 AWS Organizations 的所有账户中运行的汇总实例总数。 单位：计数 维度： SubscriptionName ：订阅的名称。
TotalLicenseConfigurationUsageCount	可用的许可证配置总数。 单位：计数 维度： • LicenseConfigurationArn ：许可证配置 Amazon 资源名称 (ARN)。 • LicenseConfigurationType ：许可证配置类型
LicenseConfigurationUsageCount	此配置中已使用的许可证总数。 单位：计数 维度： • LicenseConfigurationArn ：许可证配置 ARN。 • LicenseConfigurationType ：许可证配置类型
LicenseConfigurationUsagePercentage	该许可证配置的已用许可证百分比。 单位：百分比 维度： • LicenseConfigurationArn ：许可证配置 ARN。 • LicenseConfigurationType ：许可证配置类型。

创建警报来监控 License Manager 指标

您可以创建 CloudWatch 警报，使其在指标的值发生改变并导致报警改变状态时发送 Amazon Simple Notification Service (Amazon SNS) 消息。告警会按照您指定的时间段监控某个指标，并根据该指标在若干时间段相对于给定阈值的值执行操作。告警仅为持续状态更改调用操作。CloudWatch 告警不调用操作，因为这些操作处于特定状态；状态必须改变并保持指定时间。有关更多信息，请参阅使用 CloudWatch 警报。

使用 AWS CloudTrail 记录 AWS License Manager API 调用

AWS License Manager 已与 AWS CloudTrail 集成，后者作为一项服务，提供 License Manager 中由用户、角色或 AWS 服务所执行的操作的记录。CloudTrail 将 License Manager 的所有 API 调用作为事件捕获。捕获的调用包括来自 License Manager 控制台的调用和对 License Manager API 操作的代码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 License Manager 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 License Manager 发出了什么请求、发出请求的 IP 地址、请求方、请求时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 License Manager 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 License Manager 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 License Manager 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 License Manager 操作都由 CloudTrail 记录，并记录在 License Manager API 参考中。例如，对 CreateLicenseConfiguration、ListResourceInventory 和 DeleteLicenseConfiguration 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 License Manager 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 DeleteLicenseConfiguration 操作。


```
{
   "eventVersion":"1.05",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDAIF2U5EXAMPLEH5AP6",
      "arn":"arn:aws:iam::123456789012:user/Administrator",
      "accountId":"012345678901",
      "accessKeyId":"AKIDEXAMPLE",
      "userName":"Administrator"
   },
   "eventTime":"2019-02-15T06:48:37Z",
   "eventSource":"license-manager.amazonaws.com",
   "eventName":"DeleteLicenseConfiguration",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.83",
   "userAgent":"aws-cli/2.4.6 Python/3.8.8 Linux",
   "requestParameters":{
      "licenseConfigurationArn":"arn:aws:license-manager:us-
east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
```

```
    },
    "responseElements":null,
    "requestID":"3366df5f-4166-415f-9437-c38EXAMPLE48",
    "eventID":"6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
    "eventType":"AwsApiCall",
    "recipientAccountId":"012345678901"
}
```

AWS License Manager 中的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是AWS和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS Compliance Programs 的一部分。要了解适用于 License Manager 的合规性计划，请参阅按合规性计划提供的范围内 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 License Manager 时应用责任共担模式。它说明了如何配置 License Manager 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务来帮助您监控和保护 License Manager 资源。

目录

AWS License Manager 中的数据保护

AWS 责任共担模式适用于 AWS License Manager 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有

关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的博客文章 AWS Shared Responsibility Model and GDPR。

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

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

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

静态加密

License Manager 将数据存储在管理账户的 Amazon S3 存储桶中。该存储桶使用 Amazon S3 托管加密密钥 (SSE-S3) 进行配置。

适用于 AWS License Manager 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一种 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份认证（登录）并获得使用 AWS 资源的授权（具有权限）。您可以使用 IAM 在您的 AWS 账户下创建用户和组。您可以控制用户使用 AWS 资源执行任务所需的权限。使用 IAM 不会产生额外的费用。

默认情况下，用户无权管理 License Manager 资源和操作。要允许用户管理 License Manager 资源，您必须创建一个 IAM 策略，明确授予他们权限。

在将策略附加到一个用户或一组用户时，它会授权或拒绝用户使用指定资源执行指定任务。有关更多信息，请参阅 IAM 用户指南中的策略与权限。

创建用户、组和角色

您可以为自己的 AWS 账户 创建用户和组，然后为其分配所需权限。作为最佳实践，用户应通过担任 IAM 角色来获取权限。有关如何为 AWS 账户设置用户和组的更多信息，请参阅 入门 AWS License Manager。

IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色类似于 IAM 用户，因为它是一个 AWS 身份，具有确定其在 AWS 中可执行和不可执行的操作的权限策略。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。此外，角色没有关联的标准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。

IAM 策略结构

IAM policy 是包含一个或多个语句的 JSON 文档。每个语句的结构如下。

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
      }
    }
  ]
}
```

组成语句的各个元素如下：

- Effect：此 effect 可以是 `Allow` 或 `Deny`。默认情况下，用户没有使用资源和 API 操作的权限，因此，所有请求均会被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- 操作：操作是对其授予或拒绝权限的特定 API 操作。
- 资源：受操作影响的资源。有些 License Manager API 操作允许您在策略中包括该操作可以创建或修改的特定资源。要在语句中指定资源，您需要使用其Amazon 资源名称 (ARN)。有关更多信息，请参阅 AWS License Manager 定义的操作。

- 条件：条件是可选的。它们可以用于控制策略生效的时间。有关更多信息，请参阅 AWS License Manager 的条件键。

为 License Manager 创建 IAM 策略

在 IAM 策略语句中，您可以从支持 IAM 的任何服务中指定任何 API 操作。License Manager 使用以下前缀为 API 操作命名：

- `license-manager:`
- `license-manager-user-subscriptions:`
- `license-manager-linux-subscriptions:`

例如：

- `license-manager:CreateLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`
- `license-manager-user-subscriptions:ListIdentityProviders`
- `license-manager-linux-subscriptions:ListLinuxSubscriptionInstances`

有关可用的 License Manager API 的更多信息，请参阅以下 API 参考：

- AWS License Manager API 参考
- AWS License Manager 用户订阅 API 参考
- AWS License Manager Linux 订阅 API 参考

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": ["license-manager:action1", "license-manager:action2"]
```

您也可以使用通配符指定多项操作。例如，您可以指定名称以单词 List 开头的所有 License Manager API 操作，如下所示：

```
"Action": "license-manager:List*"
```

要指定所有 License Manager API 操作，请使用 * 通配符，如下所示：

```
"Action": "license-manager:*"
```

使用 License Manager 的 ISV 策略示例

通过 License Manager 分配许可证的 ISV 需要以下权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "license-manager:CreateLicense",
            "license-manager:ListLicenses",
            "license-manager:CreateLicenseVersion",
            "license-manager:ListLicenseVersions",
            "license-manager:GetLicense",
            "license-manager:DeleteLicense",
            "license-manager:CheckoutLicense",
            "license-manager:CheckInLicense",
            "kms:GetPublicKey"
        ],
        "Resource": "*"
        }
    ]
}
```

向用户、组和角色授予权限

创建所需的 IAM 策略后，必须向您的用户、组和角色授予这些权限。

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和组：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

将服务相关角色用于 AWS License Manager

AWS License Manager 使用 AWS Identity and Access Management（IAM）服务相关角色。服务相关角色是一种与 License Manager 直接关联的独特类型的 IAM 角色。服务相关角色由 License Manager 预定义，并包含服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可让您更轻松地设置 License Manager，因为您不必手动添加必要的权限。License Manager 定义其服务相关角色的权限，除非另外定义，否则只有 License Manager 可以代入该角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在先删除相关资源后，才能删除服务相关角色。这将保护您的 License Manager 资源，因为您不会无意中删除对资源的访问权限。

License Manager 操作取决于三个服务相关角色，如以下几节中所述。

服务相关角色

- License Manager — 核心角色
- License Manager — 管理账户角色
- License Manager — 成员账户角色
- License Manager — 基于用户的订阅角色
- License Manager — Linux 订阅角色

License Manager — 核心角色

License Manager 需要服务相关角色代表您管理许可证。

核心角色的权限

名为 `AWSServiceRoleForAWSLicenseManagerRole` 的服务相关角色允许 License Manager 访问 AWS 资源，从而代表您管理许可证。

AWSServiceRoleForAWSLicenseManagerRole 服务相关角色信任 license-manager.amazonaws.com 服务来代入角色。

要查看的权限 AWSLicenseManagerServiceRolePolicy，请参阅AWS 托管策略：AWSLicenseManagerServiceRolePolicy。要了解有关为服务相关角色配置权限的更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

为 License Manager 创建服务相关角色

您无需手动创建服务相关角色。在您首次访问 License Manager 控制台时填写 License Manager 首次运行体验表单时，将自动创建服务相关角色。

您也可以使用 IAM 控制台、AWS CLI 或 IAM API 手动创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。如果您在 2017 年 1 月 1 日之前使用 License Manager 服务，当它开始支持服务相关角色时，则 License Manager 会在您的账户中创建 AWSServiceRoleForAWSLicenseManagerRole 角色。有关更多信息，请参阅我的 IAM 账户中出现新角色。

您可以使用 License Manager 控制台创建服务相关角色。

创建服务相关角色

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 选择开始使用 License Manager。
3. 在 IAM 权限 (one-time-setup) 表单中，选择我授予AWS License Manager所需权限，然后选择继续。

您也可以使用 IAM 控制台为 License Manager 使用案例创建服务相关角色。或者，在 AWS CLI 或 AWS API 中，使用 IAM 通过 license-manager.amazonaws.com 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

如果删除该服务相关角色，您可以使用相同的 IAM 过程再次创建该角色。

编辑 License Manager 的服务相关角色

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

删除 License Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，建议您删除该角色。这样，您就只有主动监控或维护的实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

清除服务相关角色

您必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。这意味着要先解除任何自管理许可证与关联实例和 AMI 的关联，然后删除自管理许可证。

> **Note**
>
> 在您尝试删除资源时，如果 License Manager 正在使用该角色，删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除核心角色使用的 License Manager 资源：

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在导航窗格中，选择自管理许可证。
3. 选择您作为所有者的自管理许可证，并解除关联已关联 AMI 和资源选项卡中的所有条目。对每个许可证配置重复此过程。
4. 仍在自管理许可证的页面上，选择操作，然后选择删除。
5. 重复前面的步骤，直到删除所有自管理许可证。

手动删除 服务相关角色

使用 IAM 控制台、AWS CLI 或 AWS API 删除 AWSServiceRoleForAWSLicenseManagerRole 服务相关角色。如果您同时使用AWSServiceRoleForAWSLicenseManagerMasterAccountRole和AWSLicenseManagerMemberAccountRole，请先删除这些角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

License Manager — 管理账户角色

License Manager 需要服务相关角色才能执行许可证管理。

管理账户角色的权限

名为 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 的服务相关角色允许 License Manager 访问 AWS 资源，从而代表您管理集中管理账户的许可证管理操作。

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 服务相关角色信任 `license-manager.master-account.amazonaws.com` 服务来代入角色。

要查看的权限 AWSLicenseManagerMasterAccountRolePolicy，请参阅AWS 托管式策略：AWSLicenseManagerMasterAccountRolePolicy。要了解有关为服务相关角色配置权限的更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

创建管理账户服务相关角色

您无需手动创建该服务相关角色。在 AWS Management Console中配置跨账户许可证管理时，License Manager 将创建服务相关角色。

> **Note**
>
> 要在 License Manager 中使用跨账户支持，您必须使用 AWS Organizations。

如果您删除了此服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。

您也可以使用 IAM 控制台、AWS CLI 或 IAM API 手动创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。如果您在 2017 年 1 月 1 日之前使用 License Manager 服务，当它开始支持服务相关角色时，则 License Manager 会在您的账户中创建 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole`。有关更多信息，请参阅我的 IAM 账户中出现新角色。

您可以使用 License Manager 控制台创建该服务相关角色。

创建服务相关角色

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 选择 Settings (设置) 和 Edit (编辑)。
3. 选择 Link AWS Organizations accounts (关联 Amazon Organizations 账户)。
4. 选择应用。

您也可以使用 IAM 控制台通过 License Manager — 管理账户使用案例创建服务相关角色。或者，在 AWS CLI 或 AWS API 中，使用 IAM 通过 `license-manager.master-account.amazonaws.com` 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

如果删除该服务相关角色，您可以使用相同的 IAM 过程再次创建该角色。

编辑 License Manager 的服务相关角色

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

删除 License Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，建议您删除该角色。这样，您就只有主动监控或维护的实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

手动删除服务相关角色

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

License Manager — 成员账户角色

License Manager 需要一个允许管理账户管理许可证的服务相关角色。

成员账户角色的权限

名为 AWSServiceRoleForAWSLicenseManagerMemberAccountRole 的服务相关角色允许 License Manager 访问 AWS 资源，代表您从已配置的管理账户进行许可证管理操作。

AWSServiceRoleForAWSLicenseManagerMemberAccountRole 服务相关角色信任 license-manager.member-account.amazonaws.com 服务来代入角色。

要查看的权限 AWSLicenseManagerMemberAccountRolePolicy，请参阅AWS 托管式策略：AWSLicenseManagerMemberAccountRolePolicy。要了解有关为服务相关角色配置权限的更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

为 License Manager 创建服务相关角色

无需手动创建服务相关角色。您可以在 License Manager 控制台的设置页面上从管理账户启用与 AWS Organizations 的集成。您也可以使用 AWS CLI（运行 update-service-settings）或 AWS API（调用 UpdateServiceSettings）来执行此操作。当您进行该操作时，License Manager 会在 Organizations 成员账户中为您创建服务相关角色。

如果您删除了此服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。

您也可以使用 IAM 控制台、AWS CLI 或 AWS API 手动创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。如果您在 2017 年 1 月 1 日之前使用 License Manager 服务，当它开始支持服务相关角色时，则 License Manager 会在您的账户中创建 AWSServiceRoleForAWSLicenseManagerMemberAccountRole 角色。有关更多信息，请参阅我的 IAM 账户中出现新角色。

您可以使用 License Manager 控制台创建服务相关角色。

创建服务相关角色

1. 登录到您的 AWS Organizations 管理账户。
2. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。

3. 在左侧导航栏上，选择设置，然后选择编辑。
4. 选择 Link AWS Organizations accounts (关联 Amazon Organizations 账户)。
5. 选择应用。这将在所有子账户AWSServiceRoleForAWSLicenseManagerMemberAccountRole中创建角色AWSServiceRoleForAWSLicenseManagerRole和。

您也可以使用 IAM 控制台为 License Manager - Member account 使用案例创建服务相关角色。或者，在 AWS CLI 或 AWS API 中，使用 license-manager.member-account.amazonaws.com 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

如果删除该服务相关角色，您可以使用相同的 IAM 过程再次创建该角色。

编辑 License Manager 的服务相关角色

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

删除 License Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，建议您删除该角色。这样，您就只有主动监控或维护的实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

手动删除服务相关角色

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

License Manager — 基于用户的订阅角色

License Manager 需要一个服务相关角色，用于管理将提供基于用户的订阅的 AWS 资源。

基于用户的订阅角色的权限

名为 AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService 的服务相关角色允许 License Manager 使用 AWS Systems Manager 和管理提供基于用户的订阅的 Amazon EC2 资源，以及描述 AWS Directory Service 资源。

要查看的权限 AWSLicenseManagerUserSubscriptionsServiceRolePolicy，请参阅AWS 托管式策略：AWSLicenseManagerUserSubscriptionsServiceRolePolicy。要了解有关为服务相关角色配置权限的更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

为 License Manager 创建服务相关角色

您无需手动创建服务相关角色，因为在 License Manager 控制台基于用户的订阅页面上会提示您创建该角色。

如果您删除了此服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。

您也可以使用 IAM 控制台、AWS CLI 或 IAM API 手动创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

您可以使用 License Manager 控制台创建服务相关角色。

创建服务相关角色

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择用户关联或产品。
3. 同意 License Manager 创建基于用户的订阅角色的条款。
4. 选择创建。这样就创建了角色。

您也可以使用 IAM 控制台为 `License Manager - User-based subscriptions` 使用案例创建服务相关角色。或者，在 AWS CLI 或 AWS API 中，使用 `license-manager-user-subscriptions.amazonaws.com` 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

如果删除该服务相关角色，您可以使用相同的 IAM 过程再次创建该角色。

编辑 License Manager 的服务相关角色

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

删除 License Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，建议您删除该角色。这样，您就只有主动监控或维护的实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

手动删除服务相关角色

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

License Manager — Linux 订阅角色

License Manager 需要一个与服务相关的角色，用于管理提供 Linux 订阅的 AWS 资源。

Linux 订阅角色的权限

名为 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 的服务相关角色允许 License Manager 发现 Amazon EC2 和 AWS Organizations 资源，从而汇总 Linux 订阅的使用情况。

要查看的权限 AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy，请参阅AWS 托管式策略：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy。要了解有关为服务相关角色配置权限的更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

为 License Manager 创建服务相关角色

您无需手动创建服务相关角色，因为在 License Manager 控制台 Linux 订阅页面上会提示您创建该角色。

如果您删除了此服务相关角色然后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。

您也可以使用 IAM 控制台、AWS CLI 或 IAM API 手动创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

您可以使用 License Manager 控制台创建服务相关角色。

创建服务相关角色

1. 在 https://console.aws.amazon.com/license-manager/ 处打开 License Manager 控制台。
2. 在左侧导航窗格中，选择订阅或实例。

3. 同意 License Manager 创建 Linux 订阅角色的条款。
4. 选择创建。这样就创建了角色。

您也可以使用 IAM 控制台为 License Manager - Linux subscriptions 使用案例创建服务相关角色。或者，在 AWS CLI 或 AWS API 中，使用 license-manager-linux-subscriptions.amazonaws.com 服务名称创建服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。

如果删除该服务相关角色，您可以使用相同的 IAM 过程再次创建该角色。

编辑 License Manager 的服务相关角色

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

删除 License Manager 的服务相关角色

如果不再需要使用某个需要服务相关角色的特征或服务，建议您删除该角色。这样，您就只有主动监控或维护的实体。但是，您必须先清除您的服务相关角色，然后才能手动删除它。

手动删除服务相关角色

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

适用于 AWS License Manager 的 AWS 托管式策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 服务负责维护和更新 AWS 托管式策略。您无法更改 AWS 托管式策略中的权限。服务偶尔会向 AWS 托管策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管策略。服务不会从 AWS 托管策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管式策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅《IAM 用户指南》中的适用于工作职能的 AWS 托管策略。

AWS 托管策略：AWSLicenseManagerServiceRolePolicy

此策略将附加到名为 AWSServiceRoleForAWSLicenseManagerRole 的服务相关角色，这样 License Manager 可以代表您调用 API 操作来管理许可证。有关服务相关角色的更多信息，请参阅 核心角色的权限。

角色权限策略允许 License Manager 对指定的资源完成以下操作。

操作	资源 ARN
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*

操作	资源 ARN
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

要在中查看此策略的权限AWS Management Console，请参阅AWSLicenseManagerServiceRolePolicy。

AWS 托管式策略：AWSLicenseManagerMasterAccountRolePolicy

此策略附加AWSServiceRoleForAWSLicenseManagerMasterAccountRole到名为的服务相关角色，允许 License Manager 调用代表您为中央管理账户执行许可证管理的 API 操作。有关服务相关角色的更多信息，请参阅 License Manager — 管理账户角色。

角色权限策略允许 License Manager 对指定的资源完成以下操作。

操作	资源 ARN
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:GetBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*

操作	资源 ARN
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3:DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	请参阅脚注 [1]
glue:UpdateTable	请参阅脚注 [1]
glue:DeleteTable	请参阅脚注 [1]
glue:UpdateJob	请参阅脚注 [1]
glue:UpdateCrawler	请参阅脚注 [1]
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*

操作	资源 ARN
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram:DeleteResourceShare	*
resource-groups:PutGroupPolicy	*
iam:GetRole	*
iam:PassRole	arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*
cloudformation:UpdateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

操作	资源 ARN
cloudformation:CreateStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DeleteStack	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*
cloudformation:DescribeStacks	arn:aws:cloudformation:*:*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*

[1] 以下是为 AWS Glue 操作定义的资源：

- arn:aws:glue:*:*:catalog
- arn:aws:glue:*:*:crawler/LicenseManagerResourceSynDataCrawler
- arn:aws:glue:*:*:job/LicenseManagerResourceSynDataProcessJob
- arn:aws:glue:*:*:table/license_manager_resource_inventory_db/*
- arn:aws:glue:*:*:table/license_manager_resource_sync/*
- arn:aws:glue:*:*:database/license_manager_resource_inventory_db
- arn:aws:glue:*:*:database/license_manager_resource_sync

要在中查看此策略的权限AWS Management Console，请参阅AWSLicenseManagerMasterAccountRolePolicy。

AWS 托管式策略：AWSLicenseManagerMemberAccountRolePolicy

此策略将附加到名为 AWSServiceRoleForAWSLicenseManagerMemberAccountRole 的服务相关角色，这样 License Manager 可以代表您从配置的管理账户调用 API 操作来管理许可证。有关更多信息，请参见 License Manager — 成员账户角色。

角色权限策略允许 License Manager 对指定的资源完成以下操作。

操作	资源 ARN
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:GetLicenseConfiguration	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:CreateResourceDataSync	*
ssm:DeleteResourceDataSync	*
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

要在中查看此策略的权限AWS Management Console，请参阅AWSLicenseManagerMemberAccountRolePolicy。

AWS 托管策略：AWSLicenseManagerConsumptionPolicy

您可以将 AWSLicenseManagerConsumptionPolicy 策略附加到 IAM 身份。此策略授予的权限允许访问使用许可证所需的 License Manager API 操作。有关更多信息，请参见 许可证使用。

要查看此策略的权限，请参阅 AWS Management Console 中的 AWSLicenseManagerConsumptionPolicy。

AWS 托管式策略：AWSLicenseManagerUserSubscriptionsServiceRolePolicy

此策略将附加到名为 AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService 策略的服务相关角色，这样 License Manager 可以调用 API 操作来管理基于用户的订阅资源。有关更多信息，请参见 License Manager — 基于用户的订阅角色。

角色权限策略允许 License Manager 对指定的资源完成以下操作。

操作	资源 ARN
ds:DescribeDirectories	*
ds:GetAuthorizedApplicationDetails	*
ec2:CreateTags	arn:aws:ec2:*:*:instance/* [1]
ec2:DescribeInstances	*
ec2:DescribeVpcPeeringConnections	*
ec2:TerminateInstances	arn:aws:ec2:*:*:instance/* [1]
ssm:DescribeInstanceInformation	*
ssm:GetCommandInvocation	*
ssm:GetInventory	*
ssm:ListCommandInvocations	*
ssm:SendCommand	arn: aws: ssm: *:: document/aws-[2] RunPowerShellScript

操作	资源 ARN
	arn:aws:ec2:*:*:instance/* [2]

[1] License Manager 只能在产品代码为 bz0vcy31ooqlzk5tsash4r1ik、77yzkpa7kvee1y1tt7wnsdwoc 或 d44g89hc0gp9jdzm99rznthpw 的实例上创建标签并终止这些实例。

[2] License Manager 只能在标签名称为 `AWSLicenseManager`、值为 `UserSubscriptions` 的实例上使用 `AWS-RunPowerShellScript` 文档执行 SSM Run Command。

要在中查看此策略的权限AWS Management Console，请参阅AWSLicenseManagerUserSubscriptionsServiceRolePolicy。

AWS 托管式策略：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

此策略将附加到名为 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 策略的服务相关角色，这样 License Manager 可以调用 API 操作来管理 Linux 订阅资源。有关更多信息，请参见 License Manager — Linux 订阅角色。

角色权限策略允许 License Manager 对指定的资源完成以下操作。

操作	资源 ARN
`ec2:DescribeInstances`	*
`ec2:DescribeRegions`	*
`organizations:DescribeOrganization`	*
`organizations:ListAccounts`	*
`organizations:DescribeAccount`	*
`organizations:ListChildren`	*
`organizations:ListParents`	*
`organizations:ListAccountsForParent`	*

操作	资源 ARN
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:ListDelegatedAdministrators	*

要在中查看此策略的权限AWS Management Console，请参阅AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy。

License Manager 更新到 AWS 托管策略

查看有关 License Manager 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。

更改	描述	日期
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy - 新策略	License Manager 添加了创建名为 AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService 的服务相关角色的权限。此角色向 License Manager 提供列出 AWS Organizations 和 Amazon EC2 资源的权限。	2022 年 12 月 21 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – 更新了现有策略	License Manager 已添加 ec2:DescribeVpcPeeringConnections 权限。	2022 年 11 月 28 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy - 新策略	License Manager 添加了创建名为 AWSLicenseManagerUserSubscriptionsServiceRolePolicy 的服务相关角色的权限。该角色向	2022 年 7 月 18 日

更改	描述	日期
	License Manager 提供了列出 AWS Directory Service 资源、使用 Systems Manager 功能和管理为基于用户的订阅创建的 Amazon EC2 资源的权限。	
AWSLicenseManagerMasterAccountRolePolicy – 更新了现有策略	License Manager 为由 AWS Resource Access Manager 管理的资源组添加了 `resource-groups:PutGroupPolicy` 权限。	2022 年 6 月 27 日
AWSLicenseManagerMasterAccountRolePolicy – 更新了现有策略	License Manager 将用于 AWS 托管策略 `AWSLicenseManagerMasterAccountRolePolicy` 的 AWS Resource Access Manager 条件键从使用 `ram:ResourceTag` 变为 `aws:ResourceTag` 。	2021 年 11 月 16 日
AWSLicenseManagerConsumptionPolicy - 新策略	License Manager 添加了一项新策略，该策略授予使用许可证的权限。	2021 年 8 月 11 日
AWSLicenseManagerServiceRolePolicy – 更新了现有策略	License Manager 添加了列出委托管理员的权限和创建名为 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 的服务相关角色的权限。	2021 年 6 月 16 日
AWSLicenseManagerServiceRolePolicy – 更新了现有策略	License Manager 添加了列出所有 License Manager 资源（例如许可证配置、许可证和授权）的权限。	2021 年 6 月 15 日

更改	描述	日期
AWSLicenseManagerServiceRolePolicy – 更新了现有策略	License Manager 添加了创建名为 AWSServiceRoleForMarketplaceLicenseManagement 的服务相关角色的权限。此角色给 AWS Marketplace 提供在 License Manager 中创建和管理许可证的权限。有关更多信息，请参阅《AWS Marketplace 买家指南》中的 AWS Marketplace 的服务相关角色。	2021 年 3 月 9 日
License Manager 开始跟踪更改	License Manager 为其 AWS 托管策略开始跟踪更改。	2021 年 3 月 9 日

许可证的加密签名

License Manager 可以对独立软件供应商或代表 ISV 颁发的许可证 AWS Marketplace 进行加密签名。即使在离线环境下，签名也允许供应商在应用程序内验证许可证的完整性和来源。

为了签署许可证，License Manager 使用 AWS KMS key 属于独立软件供应商并在 AWS Key Management Service ()AWS KMS中保护的非对称数据。此客户托管 CMK 由数学上相关的公钥和私钥对组成。当用户申请许可证时，License Manager 会生成一个列出许可证权限的 JSON 对象，并使用私钥对该对象进行签名。签名和纯文本 JSON 对象将返回给用户。提供这些对象的任何一方都可以使用公钥来验证许可证文本是否未被更改，并且许可证是否由私钥的所有者签名。key pair 的私密部分永远不会离开 AWS KMS。有关非对称加密的更多信息 AWS KMS，请参阅使用对称和非对称密钥。

> **Note**
>
> 在签署 AWS KMS Sign和验证许可证时，License Manager 会调用和 VerifyAPI 操作。CMK 的密钥用法值必须为 SIGN_VERIFY，才能用于这些操作。此类 CMK 不能用于加密和解密。

以下工作流程描述了加密签名许可证的颁发：

1. 在 AWS KMS 控制台、API 或 SDK 中，许可证管理员创建一个非对称的客户托管 CMK。CMK 必须有签名和验证的密钥用法，并支持 RSASSA-PSS SHA-256 签名算法。有关更多信息，请参阅创建非对称 CMK 和如何选择 CMK 配置。
2. 在 License Manager 中，许可管理员创建包含 AWS KMS ARN 或 ID 的使用配置。该配置可以指定借用和/或临时选项。有关更多信息，请参阅创建卖家颁发的许可证块。
3. 最终用户使用 `CheckoutLicense` 或 `CheckoutBorrowLicense` API 操作获取许可证。仅允许在配置了借用的许可证上执行 `CheckoutBorrowLicense` 操作。它会返回一个数字签名作为其响应的一部分，同时还会返回列出权限的 JSON 对象。纯文本 JSON 与以下内容类似：

```
{
   "entitlementsAllowed":[
      {
         "name":"EntitlementCount",
         "unit":"Count",
         "value":"1"
      }
   ],
   "expiration":"2020-12-01T00:47:35",
   "issuedAt":"2020-11-30T23:47:35",
   "licenseArn":"arn:aws:license-
manager::123456789012:license:l-6585590917ad46858328ff02dEXAMPLE",
   "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
   "nodeId":"100.20.15.10",
   "checkoutMetadata":{
      "Mac":"ABCDEFGHI"
   }
}
```

合规性验证 AWS License Manager

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

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

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS License Manager 中的故障恢复能力

AWS全球基础设施围绕AWS区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关AWS区域和可用区的更多信息，请参阅AWS全球基础设施。

AWS License Manager 中的基础设施安全性

作为一项托管式服务，AWS License Manager 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 License Manager。客户端必须支持以下内容：

- 传输层安全性协议（TLS）我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（Ephemeral Diffie-Hellman）或 ECDHE（Elliptic Curve Ephemeral Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

AWS License Manager 和接口 VPC 终端节点 (AWS PrivateLink)

您可以通过创建接口 VPC 终端节点来在 Virtual Private Cloud (VPC) 与 AWS License Manager 之间建立专用连接。接口终端节点由 AWS PrivateLink 提供支持，该技术支持您通过私有连接访问 License Manager API，而无需采用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与 License Manager 进行通信。您的 VPC 与 License Manager 之间的流量不会离开 Amazon 网络。

每个接口终端节点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 Amazon VPC 用户指南中的接口 VPC 终端节点 (AWS PrivateLink)。

为 License Manager 创建接口 VPC 终端节点

使用以下服务名称之一为 License Manager 创建接口终端节点：

- com.amazonaws.*region*.license-manager
- com.amazonaws.*region*.license-manager-fips

如果为终端节点启用私有 DNS，则可以使用其原定设置的 DNS 名称用作区域名，向 License Manager 发送 API 请求。例如，`license-manager.region.amazonaws.com`。

有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口端点。

为 License Manager 创建 VPC 终端节点

您可以向 VPC 终端节点附加策略来控制对 License Manager 的访问。该策略指定以下信息：

- 可执行操作的委托人
- 可执行的操作
- 可对其执行操作的资源

下面是用于 License Manager 的终端节点策略示例。当附加到终端节点时，此策略会向所有资源上的所有主体授予对指定的 License Manager 操作的访问权限。

```
{
   "Statement": [
        {
            "Principal": "*",
            "Effect": "Allow",
            "Action": [
              "license-manager:*"
            ],
            "Resource": "*"
        }
    ]
}
```

有关更多信息，请参阅 Amazon VPC 用户指南中的使用 VPC 终端节点控制对服务的访问。

故障排除 AWS License Manager

以下信息可以帮助您解决使用 AWS License Manager时的问题。在开始之前，请确认您的 License Manager 设置满足 AWS License Manager 中的设置中所述的要求。

跨账户发现错误

在设置跨账户发现时，您可能会在库存搜索页面上看到以下错误消息：

Athena 异常：Athena 查询失败，因为权限不足，无法执行该查询。请迁移您的目录以允许访问此数据库。

如果您的 Athena 服务使用 Athena 托管数据目录而不是 AWS Glue Data Catalog，则会出现此情况。有关升级说明，请参阅逐步升级到 AWS Glue 数据目录。

管理账户无法解除资源与自行管理许可证的关联

如果组织的成员账户删除其账户中的 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服务相关角色 (SLR)，并且存在与自管理许可证关联的成员拥有的资源，则将阻止管理账户取消许可证与这些成员账户资源的关联。这意味着成员账户资源将继续使用管理账户池中的许可证。要允许管理账户取消资源的关联，请还原 SLR。

当客户不希望管理账户执行一些影响成员账户资源的操作时，此行为可以解释这种情况。

Systems Manager 清单过期

Systems Manager 将数据存储为清单数据 30 天。在此期间，License Manager 会将托管实例计为活动实例，即使无法对该实例进行 Ping 操作也是如此。在从 Systems Manager 中清除清单数据后，License Manager 会将实例标记为非活动状态并更新本地清单数据。为了确保托管实例计数准确，我们建议在 Systems Manager 中手动取消注册实例，以便 License Manager 能够运行清理操作。

已取消注册的 AMI 的明显持久性

License Manager 每隔几个小时就会清除一次资源和自管理许可证之间的过时关联。如果已通过 Amazon EC2 取消注册与自管理许可证关联的 AMI，则此 AMI 可能会在清除之前短暂地继续显示在 License Manager 资源清单中。

新子账户实例在资源清单中缓慢出现

在启用跨账户支持时，默认情况下，License Manager 每天下午 1 点更新一次客户账户。当天晚些时候添加的实例会在第二天显示在管理账户资源清单中。您可以通过在 AWS Glue 控制台`LicenseManagerResourceSynDataProcessJobTrigger`中编辑管理账户更新脚本来更改更新脚本的运行频率。

在启用跨账户模式后，子账户实例会缓慢出现

在 License Manager 中启用跨账户模式后，子账户中的实例可能需要几分钟到几小时才能显示在资源清单中。时间取决于子账户的数量和每个子账户中的实例数。

无法禁用跨账户发现

在为跨账户发现配置账户后，无法还原为单账户发现。

子账户用户无法将共享自管理许可证与实例关联

如果发生此情况并且已启用跨账户发现，请检查：

- 已从组织中删除子账户。
- 已从在管理账户中创建的资源共享中删除子账户。
- 已从资源共享中删除自管理许可证。

关联 AWS Organizations 账户失败

如果 Settings (设置) 页面报告此错误，则意味着账户不是组织的成员，原因如下：

- 已从组织中删除子账户。
- 客户已禁止从管理账户的组织控制台访问 License Manager。

的文档历史记录 AWS License Manager

下表描述了的版本 AWS License Manager。

更改	描述	日期
增加了对基于 Db2 vCPU 的 Amazon RDS 自带设备许可证的支持	License Manager 增加了对基于 Db2 vCPU 的 BYOL 许可证的 Amazon RDS 的支持。	2024年3月20日
增加了 Windows Server 2019 对 Microsoft Office 基于用户的订阅的支持	AWS 在亚马逊系统映像 (AMI) 中增加了对 Windows Server 2019 的支持，亚马逊为亚马逊 EC2 上的 Microsoft Office LTSC Professional Plus 2021 提供了许可证。	2023 年 12 月 4 日
自管理（本地）域用户可以使用基于用户的订阅	License Manager 增加了对自我管理的活动目录域中的用户在与您的 AWS Managed Microsoft AD 目录建立信任关系后使用基于用户的订阅的支持。	2023 年 9 月 6 日
Ubuntu LTS 订阅的许可证类型转换	License Manager 增加了对 Ubuntu LTS 实例的支持，以使用许可证类型转换功能来添加 Ubuntu Pro 订阅。	2023 年 4 月 20 日
替换有效授予	License Manager 增加了一些功能，可以在授予激活期间选择替换已授予许可证的有效授予。	2023 年 3 月 31 日
对 Linux 订阅进行委托管理	License Manager 增加针对 Linux 订阅的委托管理员的支持。	2023 年 3 月 3 日

更改	描述	日期
Linux 订阅	License Manager 增加了对商业 Linux 订阅的跟踪。	2022 年 12 月 21 日
亚马逊 CloudWatch 指标	License Manager 现在会发布许可证配置使用情况和订阅的 CloudWatch 指标。	2022 年 12 月 21 日
用于基于用户的订阅的 Microsoft Office	License Manager 添加了 Microsoft Office 作为基于用户的订阅的受支持软件。	2022 年 11 月 28 日
向组织单位分配权限	将权限分配给组织中的特定组织单位。	2022 年 11 月 17 日
组织范围视图（控制台）	AWS Organizations 使用 License Manager 控制台管理所有账户中已授予的许可证。	2022 年 11 月 11 日
基于用户的订阅	在 Amazon EC2 上使用受支持的基于用户的订阅产品。	2022 年 8 月 2 日
记录并提交许可证使用情况数据（控制台）	使用 License Manager 控制台记录和提交许可证使用情况数据。	2022 年 3 月 28 日
许可证类型转换（控制台）	使用 Licen AWS se Manager 控制台在提供的许可和自带许可模式 (BYOL) 之间更改许可类型，无需重新部署现有工作负载。	2021 年 11 月 9 日
许可证类型转换 (CLI)	AWS CLI 无需重新部署现有工作负 AWS载，即可在提供的许可和自带许可模式 (BYOL) 之间更改许可证类型。	2021 年 9 月 22 日

更改	描述	日期
共享权限	只需一次申请，即可与整个组织共享托管许可证权限。	2021 年 7 月 16 日
使用情况报告	使用 License Manager 使用情况报告跟踪许可证类型配置的历史记录。使用情况报告以前称为报告生成器和许可证报告。	2021 年 5 月 18 日
自动化发现排除规则	根据 AWS 账户 ID 和标签，从 License Manager 自动发现中排除实例。	2021 年 3 月 5 日
托管权限	跟踪和分发从购买的产品 AWS Marketplace 和使用 License Manager 分发许可证的卖家的许可权利。	2020 年 12 月 3 日
对已卸载软件进行自动化会计	配置自动化发现功能，以在卸载软件时停止跟踪实例。	2020 年 12 月 3 日
基于标签的筛选	使用标签搜索资源清单。	2020 年 12 月 3 日
AMI 关联范围	将您的自管理许可证和与您的 AWS 账户共享的 AMI 相关联	2020 年 11 月 23 日
许可证关联到主机	在特定天数内强制向专用硬件分配许可证。	2020 年 8 月 12 日
跟踪 Amazon RDS 上的 Oracle 部署	在 Amazon RDS 上跟踪 Oracle 数据库引擎版本和许可包的许可证使用情况。	2020 年 3 月 23 日
主机资源组	配置主机资源组以允许 License Manager 管理您的专属主机。	2019 年 12 月 1 日

更改	描述	日期
自动化软件发现	配置 License Manager 来搜索新安装的操作系统或应用程序，并将相应的自管理许可证附加到实例。	2019 年 12 月 1 日
区分随附许可证和自带许可证	根据您使用的是 Amazon 提供的许可证还是您自己的许可证来筛选搜索结果。	2019 年 11 月 8 日
将许可证附加到本地资源	将许可证附加到本地实例后，License Manager 会定期收集软件清单、更新许可信息并报告使用情况。	2019 年 3 月 8 日
AWS License Manager 初始版本	首次服务发布	2018 年 11 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。