



用户指南

AWS License Manager



AWS License Manager: 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 AWS License Manager?	1
托管权限	1
License Manager 使用案例	2
相关服务	2
License Manager 的工作原理	4
开始使用	6
使用 License Manager	7
自我管理许可证	8
参数和规则	9
通过供应商许可证构建规则	10
创建自我管理许可证	12
共享自我管理许可证	13
编辑自我管理许可证	17
停用自我管理许可证	18
删除自我管理许可证	18
许可证规则	19
关联自行管理的许可证和 AMIs	20
取消关联自行管理的许可证和 AMIs	21
使用情况报告	21
创建使用情况报告	22
编辑使用情况报告	23
删除使用情况报告	23
许可证类型转换	24
符合条件的许可证类型	25
先决条件	33
转换许可证类型	35
租赁转换	44
问题排查	45
主机资源组	46
创建主机资源组	47
共享主机资源组	48
将专用主机添加到主机资源组	48
在主机资源组中启动实例	49
修改主机资源组	49

从主机资源组中移除专用主机	50
删除主机资源组	50
库存搜索	51
使用库存搜索	51
自动发现清单	57
已授予的许可证	59
查看已授予的许可证	59
管理已授予的许可证	60
分配权限	63
授予接受和激活	64
许可证状态	66
买家账户指标	67
卖家颁发的许可证	68
权限	69
许可证使用	69
所需的权限	70
创建卖家颁发的许可证	71
授予卖家颁发的许可证	73
ISV客户的临时证书	73
查看卖家颁发的许可证	74
删除卖家颁发的许可证	75
基于用户的订阅	75
注意事项	76
基于用户的订阅先决条件	77
支持的软件订阅	82
其他软件	84
开始使用	84
GPO为更多会话进行配置	91
使用随附的许可证启动实例 AMI	92
连接到实例	93
修改微软 Office 的防火墙设置	94
管理订阅用户	94
取消注册活动目录	96
故障排除	97
管理 Linux 订阅	98
配置发现	100

查看实例数据	105
账单信息	107
管理 CloudWatch 警报	109
设置	111
编辑 License Manager 设置	112
托管许可证设置	113
Linux 订阅设置	114
基于用户的订阅设置	117
委派管理员设置	117
控制面板	121
监控 License Manager	124
使用监控 CloudWatch	124
创建 CloudWatch 警报	126
CloudTrail 日志	126
中的 License Manager 信息 CloudTrail	126
了解 License Manager 日志文件条目	127
安全性	129
数据保护	129
静态加密	130
身份和访问管理	130
创建用户、组和角色	131
IAM策略结构	131
为 License Manager 创建IAM策略	132
向用户、组和角色授予权限	133
服务相关角色	134
核心角色	134
管理账户角色	137
成员账户角色	138
基于用户的订阅角色	140
Linux 订阅角色	142
AWS 托管策略	144
AWSLicenseManagerServiceRolePolicy	144
AWSLicenseManagerMasterAccountRolePolicy	146
AWSLicenseManagerMemberAccountRolePolicy	150
AWSLicenseManagerConsumptionPolicy	151
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	151

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	153
策略更新	154
许可证签名	157
合规性验证	158
弹性	159
基础设施安全性	160
VPC端点带有 AWS PrivateLink	160
为 License Manager 创建接口VPC端点	160
为 License Manager 创建VPC端点策略	161
故障排除	162
跨账户发现错误	162
管理账户无法解除资源与自行管理许可证的关联	162
Systems Manager 清单过期	162
注销的明显持续存在 AMI	162
新子账户实例在资源清单中缓慢出现	163
在启用跨账户模式后，子账户实例会缓慢出现	163
无法禁用跨账户发现	163
子账户用户无法将共享自管理许可证与实例关联	163
链接 AWS Organizations 账户失败	163
文档历史记录	164
.....	clxix

什么是 AWS License Manager?

AWS License Manager 是一项服务，可让您更轻松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 以及您的本地环境。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。

当您在 AWS 上构建云基础架构时，您可以使用“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 通过直接关联的库存跟踪降低了许可超额和处罚的风险 AWS 服务的支持。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 (vCPUs)、物理内核、插槽或计算机数量获得许可的任何软件。这包括来自微软、SAP、甲骨文和其他供应商的各种软件产品。

与 AWS License Manager，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。可以将这些时间序列数据追踪到所有 CloudWatch 指标和事件。ISVs 可以将这些数据用于分析、审计和其他类似目的。

AWS License Manager 已与集成 [AWS Marketplace](#) 和 [AWS Data Exchange](#)，以及以下内容 AWS 服务：[AWS Identity and Access Management \(IAM\)](#)、[AWS Organizations](#)、Service Quotas、[AWS CloudFormation](#)、AWS 资源标记，以及 [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 (ISVs) 可以使用 AWS License Manager 通过托管授权管理软件许可证和数据并将其分发给最终用户。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。ISVs 通过销售 AWS Marketplace 受益于作为交易工作流程一部分的自动许可证创建和分发。ISVs 也可以使用 License Manager 为没有 License Manager 的客户创建许可证密钥并激活许可证 AWS account。

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身份或通过由生成的数字签名令牌将其分发给最终用户 AWS License Manager。最终用户使用 AWS 可以进一步将许可证权利重新分配给 AWS 各自组织中的身份。拥有分布式授权的最终用户可以通过与您的软件集成，从该许可证中签出并签入所需的授权 AWS License Manager。每次许可证签出都指定权利、关联数量和签出时间段，例如在 1 小时内签出 10 **admin-users**。可以根据分布式许可证的底层IAM身份或由生成的长期令牌来执行此签出 AWS License Manager 通过 AWS License Manager 服务。

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 处理消耗这些许可证的命令。
- [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](#)— 用于管理从中获得的许可证的使用 AWS Marketplace, AWS Data Exchange，或者直接来自将软件与托管权利集成的卖家。
- [License Manager 中的许可证类型转换](#)— 用于在两者之间更改您的许可证类型 AWS 提供了许可和自带许可模式 (BYOL)，无需重新部署您的工作负载。
- [License Manager 中的库存搜索](#)— 用于使用发现和跟踪本地应用程序 AWS Systems Manager 库存和许可规则。
- [使用基于用户的 License Manager 订阅来购买支持的软件产品](#) — 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。
- [在许可证管理器中管理 Linux 订阅](#)— 用于查看和管理您拥有并运行的商业 Linux 订阅 AWS。

相关服务

License Manager 已与亚马逊EC2、亚马逊RDS、 AWS Marketplace, AWS Systems Manager，以及 AWS Organizations.

Amazon EC2 集成允许您跟踪以下资源的许可并在整个资源生命周期中强制执行许可规则：

- [亚马逊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](#)

当你同时使用 License Manager 与 AWS Systems Manager 时，您可以管理托管在外部的物理或虚拟服务器上的许可证 AWS。你可以将 License Manager 与 AWS Organizations 集中管理您的所有组织帐户。

此外，您还可以管理从以下地址购买的许可证的使用 AWS Marketplace, AWS Data Exchange，或者直接来自将软件与集成在一起的卖家 AWS License Manager。你可以用 AWS License Manager 将使用权（称为权利）分配给特定的 AWS 账户。

License Manager 与 Amazon RDS 集成，CPU 基于 RDS 的 Db2 v 的 BYOL 许可证与亚马逊集成。通过这种集成，您可以了解适用于 Oracle 和 Db2 数据库实例 RDS 的 v CPU 使用情况。RDS 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。

- [RDS 适用于 Oracle 许可选项](#)
- [RDS 适用于 Db2 许可选项](#)

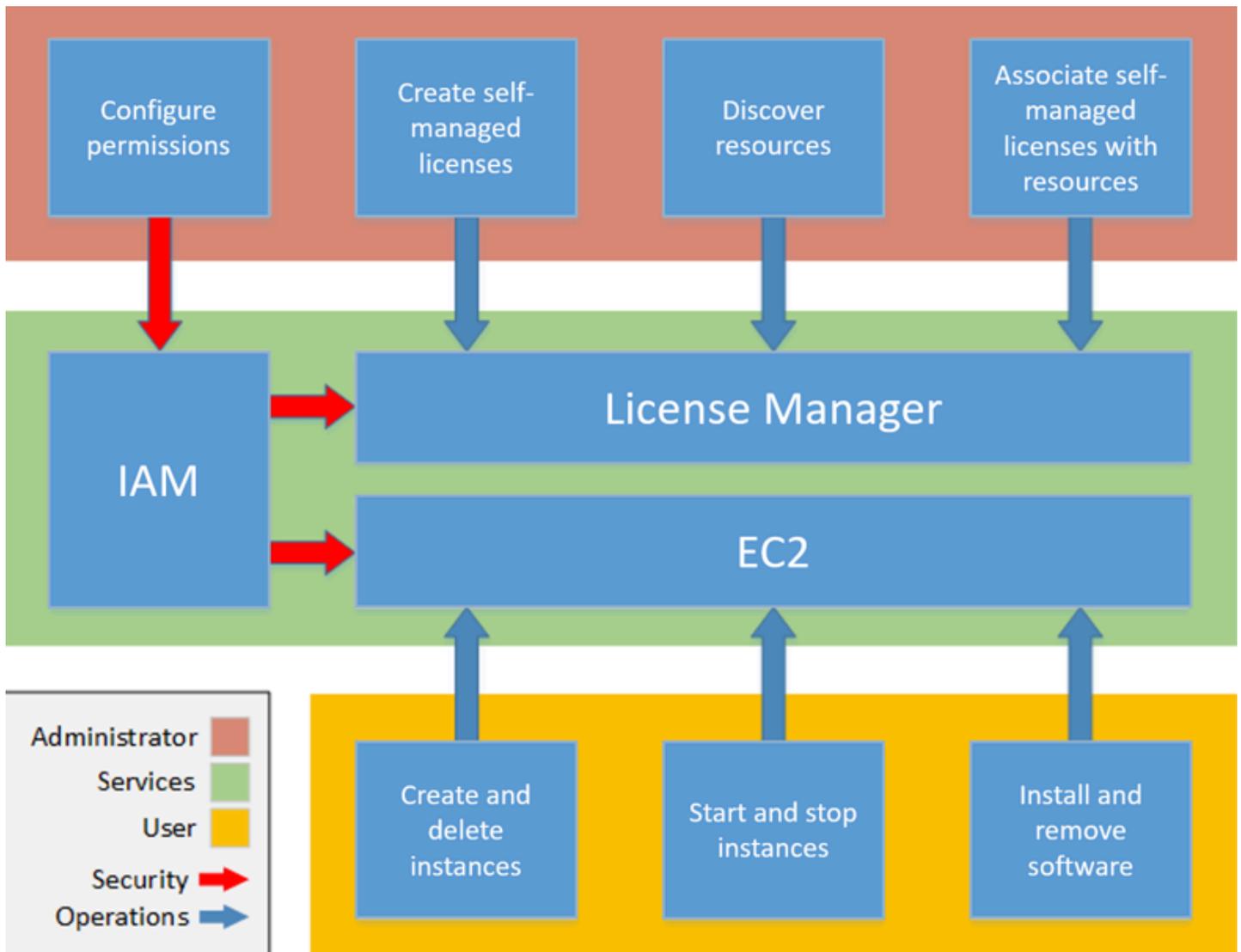
License Manager 的工作原理

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，它还原生集成了 AWS 服务 — 例如，使用 Amazon EC2 控制平面创建和删除实例。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。

下图说明了管理权限和配置 License Manager 的许可证管理员和通过亚马逊 EC2 控制台创建、管理和删除资源的用户的不同但协调的职责。



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，创建自我管理许可证，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，这可能意味着将自我管理许可证与 IT 部门用作所有 Amazon EC2 实例部署模板的经批准的 Amazon 系统映像 (AMI) 相关联。

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。

开始使用 License Manager

要将 AWS License Manager，您必须先完成入职步骤。以下过程将引导您完成中的入职步骤 AWS Management Console.

开始使用 License Manager

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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](#)。

有关管理用户、群组和角色在关注时使用 License Manager 的权限的更多信息 AWS 最佳实践，请参阅[License Manager 的身份和访问管理](#)。有关设置与 License Manager 集成的亚马逊EC2资源的更多信息，请参阅[亚马逊弹性计算云用户指南EC2中的设置使用亚马逊](#)。

使用 License Manager

License Manager 可以应用于具有以下混合基础架构的企业标准场景 AWS 资源和本地资源。您可以创建自我管理许可证，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。

许可 AWS Marketplace 产品

使用 License Manager，您现在可以将许可规则关联到 AWS Marketplace BYOLAMI 通过 Amazon EC2 发布模板发布的商品，AWS CloudFormation 模板或 Service Catalog 产品。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 不会更改您 BYOLAMIs 从 Marketplace 获取和激活的方式。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

使用 License Manager，您可以发现外部运行的应用程序 AWS 使用 [Systems Manager 清单](#)，然后为其附加许可规则。附加许可规则后，您可以跟踪本地服务器以及 AWS License Manager 控制台中的资源。

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。这使您能够准确报告 BYOL 许可证的使用情况。此过滤器需要 SSM 版本 2.3.722.0 或更高版本。

你的 License Manager AWS 账户

License Manager 使您能够管理您的所有许可证 AWS 账户。您只需在自己的版本中创建一次许可证配置 AWS Organizations 管理账户并使用在您的账户中共享 AWS Resource Access Manager 或者通过链接 AWS Organizations 使用 License Manager 设置的帐户。这也使您能够执行跨账户发现，以搜索您的所有库存 AWS 账户。

内容

- [License Manager 中的自我管理许可证](#)
- [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](#)
- [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](#)
- [使用基于用户的 License Manager 订阅来购买支持的软件产品](#)
- [在许可证管理器中管理 Linux 订阅](#)
- [License Manager 中的设置](#)
- [License Manager 中的控制面板](#)

License Manager 中的自我管理许可证

自我管理许可证（以前称为许可证配置）是 License Manager 的核心。自我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。在创建自我管理许可证时，请与组织的合规性团队密切合作以审核您的企业协议。

AWS 服务 例如 License Manager 的服务配额定义了每个区域可供你使用的最大资源或操作数 AWS 账户 为了那项服务。例如，使用 License Manager，每种资源最多可以拥有10自我管理许可证，在任何给定资源中，自行管理的许可证总数不得超过25自行管理的许可总数 AWS 区域。要了解有关 License Manager 配额的更多信息，请参阅 [AWS License Manager](#) 中的服务配额 AWS 一般参考。

Note

Systems Manager 托管实例必须与 v CPU 和实例类型的自我管理许可证相关联。

内容

- [License Manager 中的自我管理许可证参数和规则](#)
- [通过供应商许可证构建 License Manager 规则](#)
- [在 License Manager 中创建自行管理的许可证](#)
- [在 License Manager 中共享自行管理的许可证](#)
- [在 License Manager 中编辑自行管理的许可证](#)
- [在 License Manager 中停用自行管理的许可证](#)
- [在 License Manager 中删除自行管理的许可证](#)

License Manager 中的自我管理许可证参数和规则

自我管理许可证包括基本参数和根据参数值变化的规则。您还可以为自我管理许可证添加标签。创建自我管理许可证后，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：

- 自我管理许可证名称 — 自我管理许可证的名称。
- (可选) 描述 — 自我管理许可证的描述。
- 许可证类型 — 用于对许可证计数的指标。支持的值为“内核”vCPUs、“插槽”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。支持的产品有 Windows Server、Ser SQL ver、RDS适用于 Oracle 的亚马逊和RDS适用于 Db2 的亚马逊。
- (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。
 - 最大值 vCPUs-资源的最大计数 vCPUs 。
 - 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。
 - 最小值 vCPUs-资源的最小数量 vCPUs 。
 - 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vCPUs，则支持共享租赁、专用主机和专用实例。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)
 - v CPU 优化 — License Manager 与 Amazon EC2 中的[CPU优化](#)支持集成，使您可以自定义实例 vCPUs 上的数量。如果此规则设置为 True，则 License Manager 将 vCPUs 根据自定义的核心和线程数进行计数。否则，License Manager 会计算该实例类型的默认数量。vCPUs

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名字	内核	实例	套接字	vCPUs
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		✓	✓	
最大值 vCPUs	maximumVcpus		✓		✓
最小内核数	minimumCores	✓	✓		
最小套接字数	minimumSockets		✓	✓	
最低限度 vCPUs	minimumVcpus		✓		✓
租赁	allowedTenancy	✓	✓	✓	✓
v CPU 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。您的选择还取决于您计划将资源迁移到的详细信息 AWS。

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之互动 AWS 要求和限制。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CPU核心类型、租赁和每台服务器的最低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 。
最小值/最大值 vCPUs 或内核	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**。

在 License Manager 中创建自行管理的许可证

自我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。您的自行管理许可证指定了您的许可证应如何计数（例如，按实例数vCPUs 或实例数）。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 RDS 的 Amazon 和 Db2 数据库RDS的亚马逊注意事项

当您添加产品信息以配置自动发现适用RDS于 Oracle 的 Amazon 或 Amazon RDS for Db2 数据库时，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。
- 每个自我管理许可证可以跟踪一个产品版本。
- 您无法使用相同的自我管理许可证追踪亚马逊RDS数据库和其他产品。

使用控制台创建自我管理许可证

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在左侧导航窗格中，选择自我管理许可证。
3. 选择创建自我管理许可证。
4. 在 Configuration details (配置详细信息) 面板中提供以下信息：
 - 自我管理许可证名称 — 自我管理许可证的名称。
 - 描述 — 自我管理许可证的可选描述。
 - 许可证类型-此许可证的计数模型（内核vCPUs、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，AWS 支持账户IDs 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我管理许可证配置。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。

使用命令行创建自我管理许可证配置

- [create-license-configuration](#) (AWS CLI)
- [新-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

在 License Manager 中共享自行管理的许可证

您可以使用 ... AWS Resource Access Manager 与任何人共享您的自行管理许可证 AWS 账户或通过 AWS Organizations。有关更多信息，请参阅[共享您的 AWS](#)中的资源 AWS RAM 用户指南。

支持的账户配额

如果您在中启用了许可证共享 AWS License Manager 在 2023 年 10 月 14 日之前，您的组织中 License Manager 支持的最大账户数量的配额将低于新的默认最大值。您可以通过使用以下 API 操作来增加此配额 AWS RAM 将在下一节中提供。有关 License Manager 中默认配额的更多信息，请参阅 License Manager 中[使用许可证的配额](#) AWS 一般参考 指南。

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 命令使用以下操作ARN来确定您的组织：

```
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 命令使用以下操作ARN来确定您的组织：

```
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 用于启用资源共享的命令 AWS RAM:

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

{
  "returnValue": true
}
```

你可以使用 [list-aws-service-access-for-organization](#) AWS CLI 命令以验证 Organizations 列表是否已为 License Manager 启用服务主体和 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

最多可能需要六个小时 AWS RAM 为您的组织完成此操作。必须先完成此过程，然后才能继续。

- 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
    }
  ]
}
```

在 License Manager 中编辑自行管理的许可证

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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)
- [更新-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

在 License Manager 中停用自行管理的许可证

停用自行管理的许可证后，使用该许可证的现有资源不会受到影响，并且仍然可以启动AMIs使用该许可证。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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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)
- [更新-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

在 License Manager 中删除自行管理的许可证

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。

使用控制台删除自我管理许可证

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在左侧导航窗格中，选择自我管理许可证。
3. 选择自我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）。

使用命令行删除自我管理许可证

- [delete-license-configuration](#) (AWS CLI)
- [删除-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

License Manager 中的许可证规则

在创建自我管理许可证规则后，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。组织中的用户可以无缝启动指定EC2实例AMIs，管理员可以通过内置的 License Manager 控制面板跟踪许可证库存。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：

- 手动关联自行管理的许可证 AMIs-要跟踪操作系统或其他软件的许可证，可以在发布许可规则AMIs之前将其附加到以供组织中更广泛地使用。然后，License Manager 会自动跟踪AMIs这些部署中的任何部署，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的AMI构建机制，例如 Systems Manager Automation、VM Import/Export 和 Packer。](#)

- Amazon EC2 发布模板和 AWS CloudFormation— 如果将许可规则附加到AMIs不是首选选项，则可以在[EC2启动模板中将其指定为可选参数](#)，或者 [AWS CloudFormation 模板](#)。将使用 License Manager 跟踪使用这些模板进行的部署。您可以对EC2启动模板强制执行规则，或者 AWS CloudFormation 通过在自我管理许可证字段IDs中指定一个或多个自行管理许可证来创建模板。

AWS 将许可证跟踪数据视为敏感的客户数据，只能通过以下方式访问 AWS 拥有它的账户。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。

关联自行管理的许可证和 AMIs

以下过程演示如何将自行管理的许可证与AMIs使用 License Manager 控制台相关联。该过程假设您至少有一个现有的自管理许可证。您可以将自行管理的许可证与任何您有权访问AMI的许可证相关联，无论是拥有的还是共享的。如果AMI已与您共享，则可以将其与当前账户中的自我管理许可证相关联。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。

如果您在所有账户中将AMI与自行管理的许可证相关联，则可以跟踪AMI跨账户的实例启动情况。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。

如果您复制同一区域AMI内的，并且该许可证配置关联AMI了，则这些许可证配置将自动与新的许可证配置相关联AMI。当您从新AMI版本启动实例时，License Manager 会对其进行跟踪。同样，如果您AMI从具有关联许可证配置的正在运行的实例创建新实例，则这些许可证配置将自动与新实例关联AMI，而 License Manager 会跟踪您从新实例启动的实例AMI。

Warning

License Manager 不支持跨区域实例跟踪。如果您将关联许可证配置AMI的复制到其他区域，License Manager 会阻止从新的区域启动所有实例AMI。

关联自行管理的许可证和 AMI

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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AMIs，请选择“关联”AMIs。

4. 选择 AssociateAMI。
5. 在“可用”中AMIs，选择一个或多个AMIs，然后选择“关联”。
 - 如果您的账户至少拥有其中一个AMIs，则系统会提示您为自己拥有的AMIs账户选择AMI关联范围。AMIs任何从其他账户共享的内容仅与您的账户关联。选择确认。
 - 如果AMIs是从其他账户与您共享的，则它们仅与您的账户关联。

AMIs现在，新关联的用户将显示在许可证详细信息页面的关联AMIs选项卡上。

取消关联自行管理的许可证和 AMIs

以下过程演示如何AMIs使用License Manager控制台取消自行管理许可证的关联。您无法取消与已取消注册的关联。AMILicense Manager AMIs 每 8 小时检查一次是否已取消注册，并自动将其解除关联。

解除自行管理的许可证和的关联 AMI

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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“关联”AMIs。
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 您可以通过安排许可证使用情况的定期快照来跟踪自行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。

在 License Manager 中创建使用情况报告

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。使用指定的自我管理许可证类型的每个跟踪资源都列出了详细信息，例如许可证 ID、资源状态和 AWS 拥有资源的账户 ID。

创建使用情况报告

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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
```

在 License Manager 中编辑使用情况报告

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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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。

在 License Manager 中删除使用情况报告

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

如果自我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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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 (AmazonEC2) 并使用 AWS 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 许可类型转换在提供的许可证之间切换 BYOL 或切换 BYOS 到 AWS 提供的许可证。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 或时 BYOS，这些选项可能需要长期承诺。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

- [在 License Manager 中进行许可类型转换的符合条件的许可证类型](#)
- [License Manager 许可类型的转换先决条件](#)
- [在 License Manager 中转换许可证类型](#)
- [License Manager 中的租约转换](#)
- [在 License Manager 中对许可证类型转换进行故障排除](#)

在 License Manager 中进行许可类型转换的符合条件的许可证类型

您可以将 License Manager 许可类型转换与 Windows Server 和 Microsoft SQL Server 许可证的支持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

- [License Manager 中适用于 Windows 和 SQL Server 的合格许可证类型](#)
 - [SQL 服务器版本](#)
 - [SQL 服务器版本](#)
 - [使用操作值](#)
 - [媒体兼容性](#)
 - [转换路径](#)
- [License Manager 中符合条件的 Linux 订阅类型](#)

License Manager 中适用于 Windows 和 SQL Server 的合格许可证类型

Important

最初从亚马逊提供的亚马逊系统映像 (AMI) 启动的实例不符合将许可类型转换为 BYOL。

Windows 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

- [SQL 服务器版本](#)
- [SQL 服务器版本](#)

- [使用操作值](#)
- [媒体兼容性](#)
- [转换路径](#)

SQL服务器版本

License Manager 支持以下SQL服务器版本：

- SQL服务器标准版
- SQL服务器企业版
- SQL服务器 Web 版

SQL服务器版本

License Manager 支持以下SQL服务器版本：

- SQL2005 年服务器
- SQL2008 年服务器
- SQL服务器 2012
- SQL2014 年服务器
- SQL2016 年服务器
- SQL2017 年服务器
- SQL2019 年服务器
- SQL服务器 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账单信息字段](#)。

操作系统详细信息	使用情况操作
Windows 服务器作为 BYOL	RunInstances:0800

操作系统详细信息	使用情况操作
Windows 服务器作为 BYOL SQL服务器 (任何版本) 为 BYOL	RunInstances:0800
Windows Server 使用随附许可证	RunInstances:0002
Windows Server 使用随附许可证 SQL服务器 (任何版本) 为 BYOL	RunInstances:0002
Windows Server 使用随附许可证 SQL包含许可的服务器 Web	RunInstances:0202
Windows Server 使用随附许可证 SQL服务器标准, 因为包括许可证	RunInstances:0006
Windows Server 使用随附许可证 SQL企业服务器 (包含许可证)	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

来源	目标	
AWS 提供的SQL服务器镜像	否	是
您的 Windows Server 媒体 ¹	是	是
你的SQL服务器媒体 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服务器安装媒体 (.iso、.exe)。

转换路径

下表确认了源许可模式是否可以在包含许可证BYOL之间转换为另一种模式。有关更多信息，请参阅 [在 License Manager 中转换许可证类型](#)。

Important

- Windows Server BYOL 和包含SQL服务器作为许可证的配置是不支持的。
- 指定为“不需要”的转换不会更改使用操作值。

来源	目标				
Windows 服务器作为 BYOL	Windows Server 使用随附许可证	Windows 服务器作为 BYOL	Windows Server 使用随附许可证	Windows 服务器作为 BYOL	Windows Server 使用随附许可证
		SQL服务器为 BYOL	SQL服务器为 BYOL	SQL包括服务器即许可证	SQL包括服务器即许可证

来源	目标	是	不需要	是 ¹	不支持	是 ¹
Windows 服务器作为 BYOL (你的媒体)	不需要	是	不需要	是 ¹	不支持	是 ¹
Windows Server 使用随附许可证 (您的媒体)	是 ²	不需要	是的 ^{1、2}	不需要 ³	不支持	是 ¹
包含许可的 Windows 服务器 (AWS 提供的图片)	不是 x	不需要	不是 x	不需要 ³	不支持	是 ¹
Windows 服务器作为 BYOL (你的媒体)	不需要 ⁴	是	不需要	是	不支持	是
SQL 服务器作为 BYOL (您的媒体)						

来源	目标					
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服务器作为BYOL (您的媒体)	不是 x	不需要 ⁴	不是 x	不需要	不支持	是
包含许可的Windows服务器 (AWS提供的图片)	不是 x	不需要 ⁴	不是 x	不需要	不支持	是
SQL服务器作为BYOL (您的媒体)	不是 x	不需要 ⁴	不是 x	不需要	不支持	是
Windows服务器作为BYOL (你的媒体)	不支持	不支持	不支持	不支持	不支持	不支持
SQL包括服务器即许可证	不支持	不支持	不支持	不支持	不支持	不支持

来源	目标					
包含许可的 Windows 服务器 (AWS 提供的图像或您的媒体)	不是 x	不是 x	不是 x	不是 x	不支持	不需要
SQL 包括服务器作为许可证 (AWS 提供的图片)						
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 包括服务器即许可证 (您的媒体)						

来源	目标					
	不是 x	是 ⁵	不是 x	是	不支持	不需要
包含许可的 Windows 服务器 (AWS 提供的图片)						
SQL 包括服务器即许可证 (您的媒体)						

x 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 在转换为 fo SQL r 服务器之前，BYOL 必须先安装 SQL 服务器。

² 必须先修改 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 从不带 SQL 服务器的源转换为带 SQL 服务器的目标时，必须先安装 SQL 服务器 (无论 SQL 服务器许可证类型如何)。

⁴ 从带 SQL 服务器的源转换为不带 SQL 服务器的目标时，必须先卸载 SQL 服务器 (无论 SQL 服务器许可证类型如何)。

⁵ 在转换为包含许可证 SQL 的 SQL 服务器之前，必须先卸载服务器。

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包含许可证的 Windows Server，然后再次将许可证类型转换为 Windows Server BYOL。

License Manager 中符合条件的 Linux 订阅类型

受支持的 Ubuntu 版本可以进行许可证类型转换。支持的版本包括诸如 Ubuntu 18.04.1 之类的更新。LTS 当您订阅转换为 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

Ubuntu

您可以将任何支持的 Ubuntu 版本转换为 Ubuntu LTS 专业版。如果您需要从 Ubuntu Pro 转换为 Ubuntu LTS，则需要向提出请求。AWS Support 有关更多信息，请参阅[创建支持案例](#)。

License Manager 许可类型的转换先决条件

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 [开始使用 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 [在 License Manager 中对许可证类型转换进行故障排除](#)。
- 目标实例必须使用 S AWS systems 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 实例和 AWS Systems Manager 清单设置 Systems Manager](#)。
- 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：

- 最初从亚马逊提供的亚马逊系统映像 (AMI) 启动的实例不符合将许可类型转换为 BYOL。必须从您自己的虚拟机 (VM) 映像启动原始 Amazon EC2 实例。有关将虚拟机转换为 Amazon 的更多信息，请参阅 [虚拟机导入/导出](#)。

- 要将SQL服务器许可证更改为BYOL，必须使用您自己的媒体安装SQL服务器。

Linux

Linux 实例必须满足以下先决条件：

- 实例必须正在运行 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。您必须允许您的实例通过 TCP 端口 443 的出站流量到达以下终端节点：
 - 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下载 ()。CDNs
 - 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](#)。

在 License Manager 中转换许可证类型

您可以使用 License Manager 控制台或，转换 Windows 许可证、微软 SQL 服务器许可证和 Ubuntu Linux 订阅。AWS CLI 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我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 的任何自我管理许可证，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，如果您的自我管理许可证包含两条自动发现规则，并且每条规则都不包括包含许可证的 Windows Server，则从 BYOL 许可证类型转换为包含许可证的 Windows Server 会导致该实例与自行管理的许可证解除关联。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，AMI 用于启动实例的计费产品信息不会发生变化。要检索准确的账单信息，请使用 Amazon EC2 [DescribeInstances](#) API。此外，如果您有从中搜索账单信息的现有工作流程 AMIs，请更新这些工作流程以供使用 `DescribeInstances`。

目录

- [在许可证管理器中转换适用于 Windows 和 SQL Server 的许可证类型](#)
 - [许可证类型转换限制](#)
 - [使用 License Manager 控制台转换许可证类型](#)
 - [使用转换许可证类型 AWS CLI](#)
- [在许可证管理器中转换适用于 Linux 的许可证类型](#)
 - [许可证类型转换注意事项](#)
 - [使用 License Manager 控制台转换许可证类型](#)
 - [使用转换许可证类型 AWS CLI](#)
 - [移除 Ubuntu Pro 订阅](#)

在许可证管理器中转换适用于 Windows 和 SQL Server 的许可证类型

您可以使用 License Manager 控制台或转换符合条件的 Windows 和 SQL Server 实例的许可证类型。

AWS CLI

主题

- [许可证类型转换限制](#)
- [使用 License Manager 控制台转换许可证类型](#)
- [使用转换许可证类型 AWS CLI](#)

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。

- Amazon EC2 实例必须从您自己的虚拟机 (VM) 映像启动。
- 包含许可证的 SQL 服务器无法在专用主机上运行。
- 包含许可证的 SQL 服务器实例必须至少有 4 个 vCPUs

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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。

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：
 - Ubuntu LTS
 - 窗户 BYOL
 - 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

如果你将 Windows Server 从随附的许可证转换为 BYOL，则必须根据微软许可协议激活 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. 确认您有权运行该 `create-license-conversion-task-for-resource` AWS CLI 命令。如需帮助，请参阅 [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 [DescribeInstances](#) 在 Amazon EC2 API 参考资料中。

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

Note

带有 Server Enterprise SQL e BYOL 的 Windows 服务器的使用操作与 Windows 的使用操作相同，BYOL 因为它们的计费方式相同。

将 Windows 服务器从随附的许可证转换为 BYOL

当你将 Windows Server 从随附的许可证转换为 BYOL，许可证管理器不会自动激活 Windows。您必须将实例的 KMS 服务器从 AWS KMS 服务器切换到您自己的 KMS 服务器。

Important

要从随附的许可证转换为 BYOL，必须从您自己的虚拟机 (VM) 映像启动原始 Amazon EC2 实例。有关将虚拟机转换为 Amazon 的更多信息 EC2，请参阅 [虚拟机导入/导出](#)。最初从 Amazon 系统映像 (AMI) 启动的实例不符合将许可证转换为 BYOL 的资格。

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 ARN 的实例的许可类型：

```
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 KMS 服务器指向自己的 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 服务器从 BYOL 转换为包含许可证

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 转换为包含的许可证，请运行以下命令，将 `<instance_arn>` 替换为您要转换 ARN 的实例的许可类型：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 服务器和 SQL 服务器从 BYOL 转换为包含许可证

您可以同时切换多款产品。例如，您可以在一次许可证类型转换中同时转换 Windows SQL 服务器和服务。

要将 Windows Server 实例的许可证类型从 BYOL 包含许可证转换为“包含许可证”，将“SQL 服务器标准”从许可证 BYOL 转换为包含许可证，请运行以下命令，将 `<instance_arn>` 替换为要转换 ARN 的实例：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
```

在许可证管理器中转换适用于 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 实例的许可类型。AWS CLI

主题

- [许可证类型转换注意事项](#)
- [使用 License Manager 控制台转换许可证类型](#)
- [使用转换许可证类型 AWS CLI](#)
- [移除 Ubuntu Pro 订阅](#)

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。

Ubuntu 转换

- 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 Savings 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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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：
 - Ubuntu LTS
 - 窗户 BYOL
 - 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[License Manager 中符合条件的 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。确认您有权运行该 `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 [DescribeInstances](#) 在 Amazon EC2 API 参考中。

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

转换为 Ubuntu Pro

在将您的实例从 Ubuntu 转换为 Ubuntu LTS u Pro 之前，您的实例必须配置出站互联网访问权限，以便从规范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 [License Manager 许可类型的转换先决条件](#)。

要将 Ubuntu 转换为 Ubuntu LTS u Pro，请按照以下步骤操作：

1. 在指定您的实例的 AWS CLI 同时运行以下命令ARN：

```
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 转换为 Ubuntu P LTS ro。如果您需要从 Ubuntu Pro 转换为 Ubuntu LTS，则需要向提出请求。AWS Support 有关更多信息，请参阅[创建支持案例](#)。

License Manager 中的租约转换

您可以更改实例的租赁，使其最适合您的使用案例。您可以使用[modify-instance-placement](#) AWS CLI 命令在以下租户之间切换：

- 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[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在共享租赁和专用实例上使用所有支持的 SQL 服务器版本和 SUSE (SLES) 许可证包含的账单代码。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>
```

在 License Manager 中对许可证类型转换进行故障排除

故障排除主题

- [Windows 激活](#)
- [实例 \[实例\] 从 Amazon 拥有的用户启动AMI。提供最初从中启动的实例BYOLAMI。](#)
- [无法验证实例 \[实例\] 是从启动的BYOLAMI。确保SSM代理已在您的实例上运行。](#)
- [调用CreateLicenseConversionTaskForResource操作时出错 \(InvalidParameterValueException\) : 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。确保您拥有以下权限 EC2 StopInstances.](#)

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转换为包含许可证时，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。

要修复此问题，请按照[为什么 Windows 实例上的 Windows 激活 Windows 失败？](#)中的步骤进行操作 EC2 要么使用 Systems Manager 激活 Windows [AWSSupport-ActivateWindowsWithAmazonLicense](#) 自动化运行手册，或者登录实例并手动切换到 AWS KMS服务器。

实例 [实例] 从 Amazon 拥有的用户启动AMI。提供最初从中启动的实例BYOLAMI。

您必须从已导入的启动您AMI的 Amazon EC2 Windows 实例，才能将许可类型转换为“自带许可模式”(BYOL)。最初由亚马逊拥有的实例AMI不符合将许可证类型转换为。BYOL有关更多信息，请参阅[License Manager 许可类型的转换先决条件](#)。

无法验证实例 [实例] 是从启动的BYOLAMI。确保SSM代理已在您的实例上运行。

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。代 AWS Systems Manager 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代理状态和启动SSM代理和故障排除代理](#)。

调用**CreateLicenseConversionTaskForResource**操作时出错 (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[License Manager 许可类型的转换先决条件](#)和[排查实例的停止问题](#)。

EC2实例 [实例] 未能停止。确保您拥有以下权限 **EC2 StopInstances**。

您必须拥有对目标实例执行StopInstancesEC2API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](#)。

License Manager 中的主机资源组

Amazon EC2 专用主机是物理服务器，其EC2实例容量完全专供您使用。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[专用主机](#)。

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**-表示如果在此主机资源组中启动实例会超出其可用容量，Amazon 是否 EC2 可以代表您分配新主机。
- **自动释放主机**-指示 Amazon 是否 EC2 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**-指示 Amazon 是否 EC2 可以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。

内容

- [在 License Manager 中创建主机资源组](#)
- [在 License Manager 中共享主机资源组](#)
- [在 License Manager 中将专用主机添加到主机资源组](#)
- [在 License Manager 的主机资源组中启动实例](#)
- [在 License Manager 中修改主机资源组](#)
- [在 License Manager 中从主机资源组中移除专用主机](#)
- [在 License Manager 中删除主机资源组](#)

在 License Manager 中创建主机资源组

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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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 专用主机管理设置，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. 对于自我管理许可证，请选择一个或多个基于内核或套接字的自我管理许可证。
8. （可选）对于标签，请添加一个或多个标签。
9. 选择创建。

在 License Manager 中共享主机资源组

您可以使用 ... AWS Resource Access Manager 通过共享您的房东资源组 AWS Organizations。共享主机资源组和自我管理许可证后，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](#)。

在 License Manager 中将专用主机添加到主机资源组

您可以从中将现有主机添加到主机资源组 AWS Management Console, AWS CLI，或 AWS API。要添加您的房东，您必须是 AWS 您在其中创建专用主机和主机资源组的账户所有者。如果您的主机资源组列出了允许的自我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

如果您停止实例并想要重启实例，则必须执行以下两项任务：

- [修改](#)实例以指向主机资源组。
- [关联](#)自我管理许可证以匹配主机资源组。

有关 Resource Groups 的更多信息，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. 登录到 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 License Manager 的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。您必须将基于核心或套接字的自我管理许可证与相关联。AMI

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

您也可以使用 Amazon EC2 控制台。有关更多信息，请参阅 Amazon EC2 用户指南中的 [将实例启动到主机资源组](#)。

在 License Manager 中修改主机资源组

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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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 Save changes (保存更改)。

在 License Manager 中从主机资源组中移除专用主机

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。如果您与其他人共享主机资源组 AWS 帐户，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上移出。要使用已从主机资源组中移除的专用主机，请参阅 Amazon EC2 用户指南中的使用[专用主机](#)。

使用以下步骤将专属主机移至主机资源组：

1. 登录到 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。

在 License Manager 中删除主机资源组

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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 [在 License Manager 中使用服务相关角色](#)。

如果您的组织不限制 AWS 用户创建AMI派生实例或在正在运行的实例上安装其他软件，则资源清单跟踪也很有用。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已发现的资源，并像从托管创建的实例一样跟踪和验证它们AMIs。

内容

- [在 License Manager 中使用库存搜索](#)
- [在 License Manager 中自动发现库存](#)

在 License Manager 中使用库存搜索

License Manager 使用 [Systems Manager 清单](#) 来发现本地软件使用情况。将自我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

- [为库存搜索进行设置](#)
- [使用库存搜索](#)
- [向自行管理的许可证添加自动发现规则](#)

- [将自行管理的许可证与库存搜索相关联](#)
- [解除自行管理许可证和资源的关联](#)

为库存搜索进行设置

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 [License Manager 中的设置](#)。
- 为要管理的服务器和应用程序创建自我管理许可证。例如，创建一个自我管理许可证，以反映你与 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服务器”开头的名称）和包含的许可证类型（例如，不适用于“SQLServer Web”的许可证）搜索应用程序。

搜索您的资源清单

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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	

筛选条件名称	描述	逻辑运算符	支持的值
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	<ul style="list-style-type: none"> • SQL Server Enterprise • SQL Server Standard • SQL Server Web • Windows Server Datacenter
标签	<p>分配给资源的元数据标签键和可选值。</p> <p>请注意，仅当启用跨账户发现时，Not equals逻辑运算符才可用。</p>	Equals, Not equals	

亚马逊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	<ul style="list-style-type: none">oracle-eeoracle-seoracle-se1oracle-se2db2-sedb2-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 for Oracle 许可证关联 RDS的管理包。	Equals	<ul style="list-style-type: none"> • Spatial and Graph • Active Data Guard • Label Security • Oracle On-Line Analytical Processing (OLAP) • Diagnostic Pack and Tuning Pack

有关亚马逊RDS数据库产品许可证的更多信息，[RDS请参阅 Oracle 许可选项](#)或RDS亚马逊RDS用户指南中的 [Db2 许可选项](#)。

向自行管理的许可证添加自动发现规则

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 [在 License Manager 中自动发现库存](#)。

向自管理许可证添加自动化发现规则

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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（RDS例如 Oracle 和 RDS Db2）。

- 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。

将自行管理的许可证与库存搜索相关联

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

将自我管理许可证与资源相关联

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

解除自行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，然后删除自我管理许可证。

解除自我管理许可证和资源的关联

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。

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。

在 License Manager 中自动发现库存

License Manager 使用 [Systems Manager 库存](#) 来发现亚马逊 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 账户的实例 IDs 或与资源标签关联的实例排除在自动发现范围之外。

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。通过 CLI 使用 [UpdateLicenseConfiguration](#) API 命令，可以随时编辑自动发现规则。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 [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 [在 License Manager 中创建自行管理的许可证](#)。

向现有自我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我管理许可证，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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在左侧导航窗格中，选择自我管理许可证。
3. 选择自我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。

Note

以下限制适用于亚马逊RDS数据库产品（例如 Oracle 版的亚马逊和适用RDS于 Db2 RDS 的亚马逊）：

- 最多支持一条指定 Amazon RDS 数据库产品的规则。
- 每个 Amazon RDS 数据库产品只允许使用一种许可配置。

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 RDS 的亚马逊和适用于 Db2 RDS 的亚马逊）。
- 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

授予的许可证是指您的组织从中购买的产品的许可证 [AWS Marketplace](#), [AWS Data Exchange](#) , 或者直接来自将软件与托管权利集成的卖家。管理员可以使用的许可证 AWS License Manager 管理这些许可证的使用, 并将使用权 (称为权利) 分配给特定的 AWS 账户。

数据许可证已分发给 AWS Data Exchange 产品可用于 AWS 账户通过 AWS Data Exchange。在您可以从中分发许可证之前 AWS Marketplace , 则必须启用订阅共享。有关更多信息, 请参阅[在组织中共享订阅](#)。

许可证管理员分发来自的授权后 AWS Marketplace 许可给 AWS 帐户, 并且接收者接受并激活授予的许可证, 则订阅可供使用 AWS 账户通过 AWS Marketplace。该账户还可以访问该产品。例如, 如果许可管理员从中购买了 Amazon 系统映像 (AMI) AWS Marketplace 并将权利分配给您的 AWS 账户, 您可以AMI使用启动 Amazon EC2 实例 AWS Marketplace 还有亚马逊EC2。

主题

- [查看已授予的许可证](#)
- [在 License Manager 中管理您已授予的许可](#)
- [分发 License Manager 权利](#)
- [在 License Manager 中接受和激活授权](#)
- [License Manager 中授权的许可状态](#)
- [CloudWatch License Manager 中买家账户的指标](#)

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。

在 License Manager 中管理您已授予的许可

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许可证是否来自 AWS Marketplace，如果您的账户是组织中的成员账户 AWS Organizations，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许可证 AWS 区域。这使您能够集中查看向您授予许可证的所有区域。

来自的许可证 AWS Marketplace 以及 AWS Data Exchange

- 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授予的许可证 AWS 账户。

管理账户中已授予的许可证

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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可能存在于多个产品中ISVs。
 - 收件人-许可证接收者的接收者。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以下实体以外的实体 AWS Marketplace，初始拨款状态为“等待接受”。请执行以下操作之一：
 - 选择接受并激活许可证。生成的授予状态为活跃。
 - 选择接受许可证。生成的授予状态为已禁用。准备好使用许可证后，选择激活许可证。
 - 选择拒绝许可证。生成的授予状态为已拒绝。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，必须先进行链接 AWS Organizations 使用 AWS License Manager 控制台设置。有关更多信息，请参阅 [License Manager 中的设置](#)。

要管理您账户中已授予的许可证 AWS Organizations

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。

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可能存在于多个产品中ISVs。
 - “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以下实体以外的实体 AWS Marketplace，请执行以下任一操作：
 - 选择激活许可证。生成的授予状态为活跃。
 - 选择停用许可证。生成的授予状态为已停用。

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 使用您授予的许可证进行工作。

要管理您授予的许可证，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](#)

分发 License Manager 权利

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，则可以通过创建授予将已授予的许可证中的权限分配给您的组织。有关 AWS Organizations，请参阅 [AWS Organizations 术语和概念](#)。

您可以将授予的收件人指定为下列选项之一：

- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 AWS 账户，其中仅包括指定的账户。
- 组织根，包括您组织中的所有账户。
- 一种组织单位 (OU) (未嵌套)，包括指定 OU 中以及嵌套在指定 OU OUs 下的所有帐户。

Note

您最多可以为每个许可证创建两千个授予。

您可以使用任一 AWS License Manager 控制台或 AWS CLI 分配您的应享权利。在控制台中创建授权 ARN 时，您可以指定组织 ID 或组织，但该 ARN 格式必须与 AWS CLI。例如，ARNs 将类似于以下内容：

组织标识 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

创建授予 (控制台)

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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. 从授予部分选择创建授予。
5. 在详细信息面板上，执行以下操作：
 - a. 输入授予的名称，以帮助您标识授予的用途或收件人。
 - b. 输入 AWS 账户 同义词，AWS Organizations OU ID 或 ARN，或 AWS Organizations 补助金接受者的身份证或 ARN 身份。
 - c. 选择创建授予。
6. 在许可证概览页面上，您将在授予面板中看到授予条目。授予的初始状态是待接受。当收件人接受授予时，状态将更改为活跃，当收件人拒绝授予时，将更改为已拒绝。

AWS CLI

您可以使用 AWS CLI 分配权利。使用时，必须使用指定组织 ID 或 OU 的 ARN 格式 AWS License Manager API。

要创建和列出您的补助金，请使用 AWS CLI:

- [create-grant](#)
- [list-distributed-grants](#)

授予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。

在 License Manager 中接受和激活授权

为已授予的许可证创建授予时，该授予将分配给收件人。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。授权激活过程可以包括来自以下来源的已授予许可证的其他选项 AWS Marketplace。

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 授予。已接受但尚未激活的授予的状态为 Disabled。已接受且已激活的授予的状态为 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，已授予许可证的授予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予的状态为已禁用。已接受且已激活的授予的状态均为活跃。

i Tip

您可以自动接受来自组织管理账户的授予。要启用自动接受授权，请在[设置](#)页面上关联您的组织账户 AWS License Manager 来自管理账户的控制台。

您无法从中为同一产品激活两个许可证 AWS Marketplace 同时。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），则可以以下操作之一：

1. 禁用同一产品的现有授予，然后激活新的授予。
2. 激活新的授予，并指定要禁用的现有活跃授予，并用新授予替换现有的活跃授予。您可以使用 License Manager 控制台或 AWS CLI:
 - a. 使用 License Manager 控制台激活新授予，同时选择是以替换活跃授予。
 - b. 使用 `CreateGrantVersionAPI`，通过 `ALL_GRANTS_PERMITTED_BY_ISSUER` 为指定为来激活新的授 Status 权 `Active`。 `ActivationOverrideBehavior`

Console

您可以使用 License Manager 控制台来激活授予。当您激活来自的赠款时 AWS Marketplace，您可能会看到是否替换有效授权的选项：

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

激活授予（控制台）

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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. 选择授予名称以打开授予概览页面。

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予：
 - a. 否 — 此选项将激活授予，而不会替换收件人（被授予者）的任何现有活跃授予。
 - b. 是 — 此选项将禁用对同一产品的授予，并为定义的收件人（被授予者）激活新的授予：
 - i. 已指定 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）给出激活授予的原因。
7. 在输入框中输入 **activate**，然后选择激活。

AWS CLI

您可以使用 AWS CLI 使用您授予的许可证进行工作。

要使用分布式赠款，请使用 AWS CLI:

- [accept-grant](#)
- [create-grant-version](#)
- [list-received-grants](#)
- [list-received-grants-for-organization](#)
- [reject-grant](#)

License Manager 中授权的许可状态

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：

Status	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。

Status	描述
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。

下表显示了授予的不同状态：

Status	描述
PENDING_WORKFLOW	该授予正在分配过程中。
PENDING_ACCEPT	已创建授予，但授予收件人尚未接受。
REJECTED	该授予已被授予收件人拒绝。
ACTIVE	该授予已被接受并激活，供授予收件人使用。可以使用许可的资源。
FAILED_WORKFLOW	分配授予失败。
DELETED	该授予已被授予人删除。
PENDING_DELETE	正在删除分配的授予。
DISABLED	该授予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予。授予详细信息显示组织中每个账户的子授予状态。

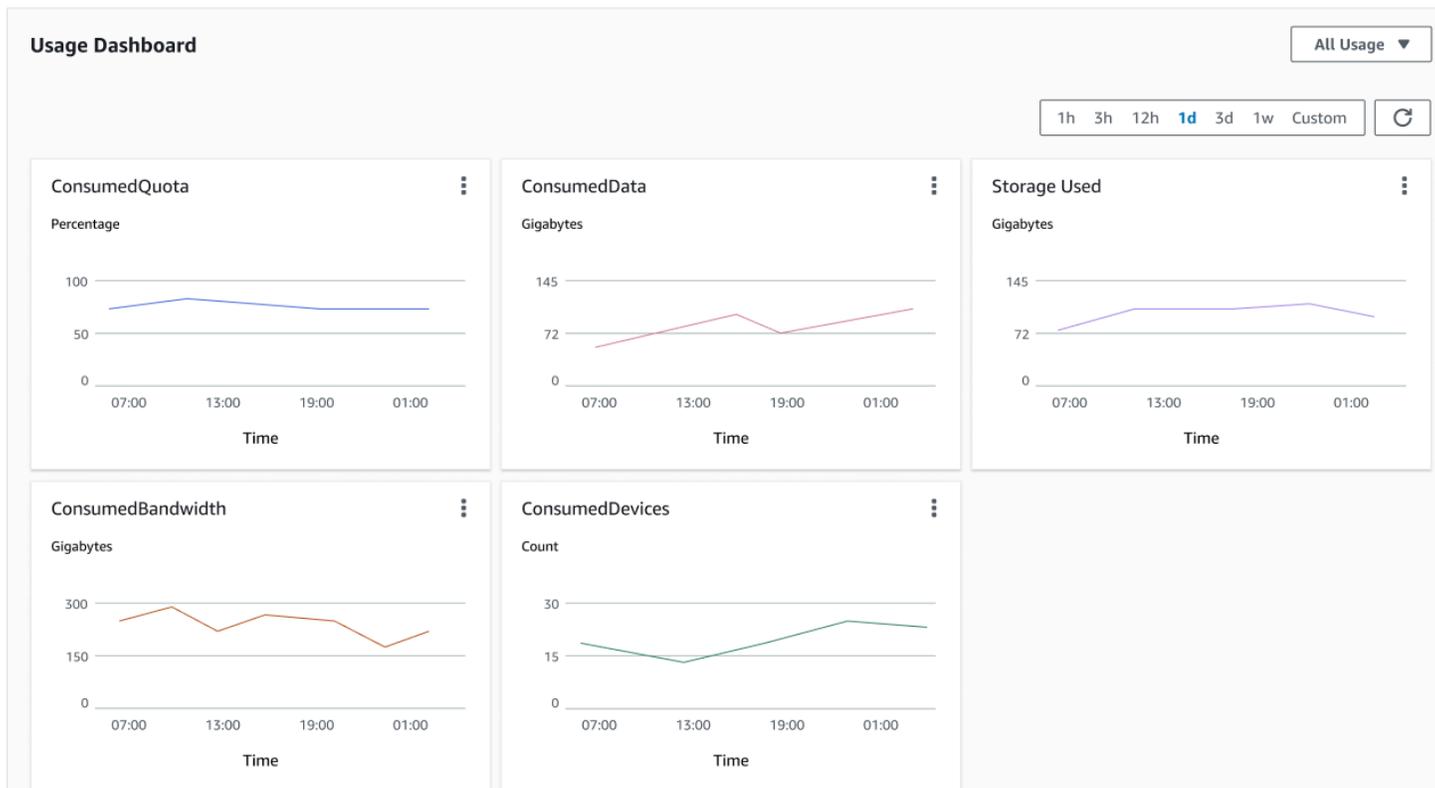
CloudWatch License Manager 中买家账户的指标

当卖家颁发的许可证的授予配置为允许提交选定的使用记录时，License Manager 会向卖家账户、root 买家账户和记录使用情况的账户发出一个 CloudWatch 指标。买家账户是 AWS 账户 购买或获得卖方颁发的许可证的人。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买家账户将在 License Manager 控制台的“使用情况”控制面板页面上看到一个带有使用记录 CloudWatch 的小部件。买家还可以在中查看他们已向其分配许可证的账户的指标 AWS Organizations。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 (ISVs) 可以使用 AWS License Manager 管理软件许可证并将其分发给最终用户。作为发放者，您可以使用 License Manager 控制面板集中跟踪您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。因为 ISV，你拥有非对称的 AWS KMS 密钥并将其存储在您的帐户中。

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 — 具有基于使用情况的特定条款的许可证，例如API请求数量、交易数量或存储容量。

您可以在 License Manager 中创建许可证，然后通过以下方式将其分发给客户 AWS IAM身份或通过 License Manager 生成的不记名令牌。ISV有以下内容的客户 AWS 账户可以将许可证权利重新分配给 AWS 各自组织中的身份。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。

卖家在 License Manager 中颁发的许可证权利

License Manager 将卖方颁发的许可功能作为授权记录在许可证中。权限的特征是数量有限或不限数量。例如，“40GB 数据传输”就是一个有限权限。“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。

要签出或签入有限的权限，ISV应用程序必须指定每个有限容量的数量。要获得无限制的权限，ISV应用程序只需指定相关权利即可再次退房或办理登机手续。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 会跟踪并向其报告使用情况以及任何超额费用。ISV

卖家在 License Manager 中颁发的许可证使用情况

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 事件”跟踪此时间序列数据。

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。

在 License Manager 中跟踪卖家颁发的许可证使用情况所需的权限

要开始使用此功能，您需要获得调用以下 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": "*"
    }
  ]
}
```

如果你要与 License Manager 集成，这样客户就没有 AWS 账户可以使用在以外的地方出售的许可证 AWS Marketplace，您必须创建一个允许您的软件应用程序调用 License Manager 的 IAM 角色 API。

如果您将 AWS Management Console 为没有 AWS 账户，License Manager 将自动创建 `AWSLicenseManagerConsumptionRole` 代表你创建。有关更多信息，请参阅 [为没有证书的 ISV 客户获取临时证书 AWS account](#)。要从中创建此角色 AWS CLI，使用 AWS IAM `create-role` 命令，如下示例所示。

```
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
```

提供的trust-policy-document.json文件应与以下示例类似，其中包含您自己的文件 AWS 账户 ID 被替换为代币发行者账户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "openid-license-manager.amazonaws.com"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "ForAnyValue:StringLike": {
          "openid-license-manager.amazonaws.com:amr": "aws:license-
manager:token-issuer-account-id:123456789012"
        }
      }
    }
  ]
}
```

接下来，使用[attach-role-policy](#)命令添加 AWSLicenseManagerConsumptionPolicy AWS AWSLicenseManagerConsumptionRole角色的托管策略。

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

在 License Manager 中创建卖家颁发的许可证

使用以下步骤创建要向客户授予的许可证块 AWS Management Console。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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。

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）。
 - 家乡地区 — The AWS 许可证的区域。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 [在 License Manager 中对许可证进行加密签名](#)。
 - 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URL的内容。
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。

Grant License Manager 卖家向ISV买家颁发了许可

添加新许可证后，您可以通过以下方式将许可证授予客户 AWS 账户使用 AWS Management Console。在使用许可证之前，接收者必须接受授权。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 帐户，您可以使用 License Manager 让客户API能够[使用许可证](#)。

使用控制台向客户授予许可证

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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，请选择创建授予。
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 — AWS 许可证接收者的账号。
 - 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利分配给其他人，请选择“分配”AWS 账户。
 - 选择“允许本地生成令牌”，无需使用即可对共享许可证进行身份验证 AWS 身份或凭证。
 - 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。
 - 家乡地区 — The AWS 区域 获取许可证。
6. 选择创建授予。

为没有证书的ISV客户获取临时证书 AWS account

对于没有 AWS 帐户，您可以像使用客户一样使用权利 AWS account。使用以下步骤获取临时信息 AWS 您的客户无需凭证 AWS account。必须在本地区API拨打电话。

获取用于调用 License Manager 的临时证书 API

1. 调用[CreateToken](#)API操作以获取编码为令牌的刷新JWT令牌。
2. 调用[GetAccessToken](#)API操作，指定您在上一步CreateToken中收到的刷新令牌，以接收临时访问令牌。

3. 调用该[AssumeRoleWithWebIdentity](#) API操作，指定您在上一步GetAccessToken中收到的访问令牌以及您创建的AWSLicenseManagerConsumptionRole角色，以获取临时权限 AWS 证书。

要从中创建令牌 AWS License Manager Console

1. 在 [License Manager 控制台](#) 中，导航到许可详细信息页面，查看您要在不使用 License Manager 的情况下使用的特定许可权利 AWS account。
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](#)。

在 License Manager 中查看卖家颁发的许可证

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。召集[CheckoutLicense](#) API行动。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可能存在于多个产品中ISVs。因此，可信密钥指纹起着重要作用。

示例：1a2b3c4d2f5e69f440bae30eaec9570bbaec9570bb1fb7358824f9ddfa1aa5a0da EXAMPLE

- 权限 — 可签出的功能。如果您指定无限功能，则数量为零。例如：

```
"Entitlements": [
  {
```

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

- 受益人 — 软件即服务 (SaaS) ISVs 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

在 License Manager 中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。

使用以下步骤删除您使用创建的许可证 AWS Management Console。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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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 Delete (删除)。

使用基于用户的 License Manager 订阅来购买支持的软件产品

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。亚马逊 EC2 为预配置的亚马逊系统映像 (AMIs) 提供支持的软件，以及包含许可证的 Windows Server 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) 或您的自我管理（本地）域的用户与提供软件的EC2实例相关联。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AMIs配置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。

每个关联的用户和包含许可证CPU的实例的 [v](#) 都需要付费。Amazon EC2 预留实例和 Savings Plan 定价模式可以帮助优化您的亚马逊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。

主题

- [在 License Manager 中使用基于用户的订阅的注意事项](#)
- [在 License Manager 中创建基于用户的订阅的先决条件](#)
- [License Manager 中支持基于用户的订阅的软件产品](#)
- [其他软件](#)
- [在 License Manager 中开始使用基于用户的订阅](#)
- [GPO为更活跃的远程用户会话配置活动目录](#)
- [使用随附的许可证启动实例 AMI](#)
- [使用 Connect 连接到基于用户的订阅实例 RDP](#)
- [修改微软 Office 订阅的防火墙设置](#)
- [管理 License Manager 基于用户的订阅的订阅用户](#)
- [从 License Manager 设置中取消注册活动目录](#)
- [对 License Manager 中基于用户的订阅进行故障排除](#)

在 License Manager 中使用基于用户的订阅的注意事项

在 License Manager 中使用基于用户的订阅时，需要考虑以下注意事项：

- 包含许可证的 Microsoft 远程桌面服务 (Win Remote Desktop Services SAL) 的 AWS Marketplace 订阅按用户每月收费，不按比例分配。
- 默认情况下，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。要启用两个以上的活动用户会话，可以配置 Active Directory 组策略对象 (GPO)，并将 Microsoft RDS 许可模式设置为 Per User。有关更多信息，请参阅的先决条件[GPO为更活跃的远程用户会话配置活动目录](#)。

- 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健康。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](#)。
- 使用 Microsoft Office 产品配置 Active Directory 时，VPC 必须至少在一个子网中配置 [VPC 终端](#)。如果要移除由 License Manager 创建的所有 VPC 端点资源，则必须从许可证管理器设置中删除配置的任何 Active Directory。有关更多信息，请参阅 [从 License Manager 设置中取消注册活动目录](#)。
- 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。
- 为了使服务按预期运行，不得更改或删除为 License Manager 创建的两个网络接口。
- 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[对 License Manager 中基于用户的订阅进行故障排除](#)章节。
- 要停止向用户收取订阅费用，您必须取消该用户与其关联的所有实例的关联。有关更多信息，请参阅[取消用户与提供基于用户的订阅的实例的关联](#)。

在 License Manager 中创建基于用户的订阅的先决条件

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。

目录

- [IAM 角色和权限](#)
- [Active Directory](#)
- [安全组](#)
- [网络配置](#)
- [提供基于用户的订阅产品的实例](#)
- [微软远程桌面服务](#)
 - [管理凭证机密](#)

IAM 角色和权限

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。在 License Manager 控制台中，如果角色尚未创建，则在基于用户的订阅中会显示一条提示。在您响应

提示并同意允许 License Manager 创建角色后，选择“创建”继续。有关更多信息，请参阅 [在 License Manager 中使用服务相关角色](#)。

- 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`

Active Directory

要使用基于 License Manager 用户的订阅，必须创建一个包含订阅产品用户的用户信息的活动目录 (AD)。根据您的配置，您可以使用自管理 A AWS Managed Microsoft AD D 或自管理 AD。

如果您同时使用 AWS 托管和自行管理的 Active 目录，则必须在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

Note

为您的目录配置的子网必须全部来自相同的VPC子网。AWS 账户

AWS 托管活动目录具有以下限制。

- 不支持与您共享的目录。
- 不支持多因素身份验证

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](#)。

安全组

安全组控制允许进出您网络上资源的网络流量。为确保基于用户的订阅环境中的资源可以通信，您的安全组必须满足以下标准。

VPC终端节点的安全组

识别或创建允许入站TCP端口1688连接的安全组。配置VPC设置时，您需要指定此安全组。有关更多信息，请参阅[使用安全组](#)。

License Manager 将此安全组与它在配置时代表您创建的VPC端点相关联VPC。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](#)。

活动目录域控制器的安全组

确保用于 AD 域控制器的安全组允许每个域控制器的网络接口IPv4地址的出站流量。

基于用户的订阅实例的安全组

确定或创建一个允许以下用户访问和访问您的实例的安全组。有关更多信息，请参阅[使用安全组](#)。

- 来自您批准的3389连接源的@@ 入站TCP端口连接。
- 出站TCP端口1688连接，用于到达VPC端点并与之通信 AWS Systems Manager。

网络配置

License Manager 会创建两个网络接口，它们使用您的 AWS Managed Microsoft AD 配置VPC所在的默认安全组。这些接口用于服务与您的目录进行交互。有关更多信息，请参阅 AWS Directory Service 管理指南中的[第 2 步：在 License Manager 中注册您的活动目录](#) 和[创建的内容](#)。

配置过程完成后，您可以将不同的安全组关联到 License Manager 创建的接口。

DNS分辨率

您为基于用户的订阅注册的 Active Directory 必须可以从您在 License Manager 设置中配置的任何子网进行访问。为确保 Active Directory 节点可以访问，请按以下方式配置DNS分辨率：

- 针对基于用户的订阅，在 License Manager 设置中配置的活动目录VPCs和活动目录之间配置DNS转发。您可以使用 Amazon Route 53 或其他DNS服务进行转发。DNS有关更多信息，请参阅博客文章“[将您的目录服务的解析与 Amazon Route 53 解析器集成](#)”。
- 为您的VPC启用DNS主机名和DNS分辨率。有关更多信息，请参阅[查看和更新您的DNS属性VPC](#)。

提供基于用户的订阅产品的实例

要使基于用户的订阅实例按预期运行，您必须满足以下先决条件：

- 如中所述，为您的实例设置安全组[安全组](#)。
- 确保为通过 Microsoft Office 提供基于用户的订阅而启动的实例具有通往配置VPC终端节点的子网的路由。
- 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，以便在许可证激活后保持合规性。

Note

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[对 License Manager 中基于用户的订阅进行故障排除](#)章节。

- 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 IAM Systems Manager 创建实例配置文件](#)”。
- 在终止实例[取消用户与实例的关联](#)之前，您必须这样做。

微软远程桌面服务

Microsoft 远程桌面服务许可证服务器需要在关联的 Active Directory 中定义的管理用户。该用户必须能够执行以下任务：

- 在活动目录域下创建 OU
- 在创建的 OU 中加入域名实例 (创建计算机)
- 将计算机对象添加到 Active Directory 域内的终端服务器组
- 委托控制 Active Directory 域中的用户对象，以读取和写入终端服务器许可证服务器，以便生成许可证服务器报告。

要了解有关委派的更多信息，请参阅 [Active Directory 域服务中的控制授权](#)。

管理凭证机密

License Manager 用于 AWS Secrets Manager 管理在 Microsoft 远程桌面服务许可证服务器上执行用户管理任务所需的凭据。在设置许可证服务器之前，必须在 Secrets Manager 中创建一个密钥，其中包含在许可证服务器上执行用户管理任务的用户的凭据。配置许可证服务器设置时，必须提供您创建的密钥的 ID。

Note

该用户必须与您为生成 RDS 许可证服务器报告所定义的用户相同。

要创建密钥，请按照 [Secrets Manager 用户指南中创建 AWS Secrets Manager 密钥](#) 页面上的详细说明进行操作，并使用以下特定于 License Manager 的设置。

Important

要使用该密钥，License Manager 取决于以下列表中指定的确切密钥名称、用户名值和加密密钥。密钥名称必须以以下前缀开头：`license-manager-user-`。

在“选择密钥类型”页面上：

- 密钥类型-选择其他类型的密钥。
- 密钥/值对-指定要存储在密钥中的以下密钥对。

用户名

- 键：`username`
- 值：`Administrator`

密码

- 键 : password
 - 值 : *The password*
- 加密密钥-确保所选选项是 aws/secretsmanager.

在“配置密钥”页面上：

- 密钥名称 — 为您的密钥指定一个名称，该名称以 License Manager 用来识别许可证服务器凭据密钥的前缀开头。例如：

```
license-manager-user-admin-credentials
```

这些说明假设您正在 AWS Management Console 使用创建您的密钥。Secrets Manager 用户指南还包括其他方法的详细说明。有关 Secrets Manager 的更多信息，请参阅[什么是 Secrets Manager](#)。有关成本的具体信息，请参阅 S ecrets Manager 用户指南 [AWS Secrets Manager 中的定价](#)。

License Manager 中支持基于用户的订阅的软件产品

AWS License Manager 支持微软 Visual Studio 和微软 Office 的基于用户的订阅。License Manager 会跟踪支持的软件利用率。每位用户都需要单独订阅 Windows Server 远程桌面服务订阅者访问许可证 (RDSSAL)，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。有关更多信息，请参阅 [在 License Manager 中开始使用基于用户的订阅](#)。

支持的 Windows 操作系统 (OS) 平台

你可以找到AMIs包含以下 Windows 操作系统平台RDSSAL许可证所涵盖产品的 Windows：

- 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 Office](#)

Microsoft Visual Studio

Microsoft Visual Studio 是一个集成开发环境 (IDE)，它使开发人员能够创建、编辑、调试和发布应用程序。提供的微软 Visual Studio AMIs 包括[AWS 工具包](#)、[NET 重构](#)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基于 License Manager 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
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

- 2021 年办公LTSC专业人士增强版

下表详细说明了用于基于 License Manager 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
2021 年办公LTSC专业人士增强版	OFFICE_PROFESSIONAL_PLUS

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。这些安装必须使用您的 Active Directory 的管理帐户执行。如果您使用 AWS Managed Microsoft AD，则默认情况下，将在您的目录中创建管理员帐户（管理员）。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 Active Directory 管理帐户安装其他软件，您必须：

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

有关更多信息，请参阅 [在 License Manager 中开始使用基于用户的订阅](#)。

在 License Manager 中开始使用基于用户的订阅

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 [在 License Manager 中创建基于用户的订阅的先决条件](#)。

步骤

- [第 1 步：订阅产品](#)
- [第 2 步：在 License Manager 中注册您的活动目录](#)
- [步骤 3：配置 RDS 许可证服务器](#)
- [步骤 4：启动实例以提供基于用户的订阅](#)
- [步骤 5：将用户关联到基于用户的订阅实例](#)

第 1 步：订阅产品

像 Office 或 Visual Studio 这样的微软产品需要有效的订阅，然后才能将 Active Directory 用户关联到包含这些产品的实例。Marketplace 订阅状态显示为“不可售”的订阅产品尚未订阅。

当你从中订阅基于用户的 Microsoft 订阅产品时 AWS Marketplace，如果你还没有 Microsoft 远程桌面服务 (RDS)，License Manager 会自动为你的账户添加订阅 Microsoft 远程桌面服务 ()。RDS 需要在从附带许可证 AMIs 启动的 EC2 实例上远程访问图形桌面和基于订阅的 Windows 应用程序。

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](#)
- [2021 年办公 LTSC 专业人士增强版](#)
- [Win 远程桌面服务 SAL](#)

通过 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. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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“在”中查看 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已激活订阅，您就可以继续为 Active Directory 用户订阅这些产品了。

Note

对于尚未结束的账单周期（标记为“待定账单状态”），您的用户数量费用和相关费用的预计账单需要 48 小时才能显示 AWS Billing。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](#)。

第 2 步：在 License Manager 中注册您的活动目录

License Manager 要求在 Active Directory 中定义订阅用户，以便将用户与基于用户的订阅关联起来。这可以是活动目录，也可以是自行管理的 Active Directory。AWS Managed Microsoft AD

配置目录时，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。当您注册 Active Directory 时，License Manager 将创建两个网络接口，以便服务可以与您的目录通信。网络接口的描述将类似于为 AWS 创建的网络接口 LicenseManager `<directory_id>`。

您必须为基于用户的订阅注册VPCs的任何其他内容配置DNS转发。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的Active Directory，其DNS转发配置如下。

要将Microsoft Office与基于用户的订阅一起使用，必须授予许可证管理器更新VPC配置的权限。在您配置时VPC，License Manager会代表您创建[VPC端点](#)。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。

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[在License Manager中创建基于用户的订阅的先决条件](#)。

控制台中的注册步骤略有不同，具体取决于您使用的Active Directory类型。

控制台注册：AWS Managed Microsoft AD

要注册AWS Managed Microsoft AD为基于用户的订阅的Active Directory，请按照以下步骤操作：

1. 打开License Manager控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 导航到左侧导航窗格中“设置”下的“基于用户的订阅”。
3. 在基于用户的订阅页面上，选择注册Active Directory。
4. 选择AWS托管目录名称和ID，用于存储基于用户的订阅的用户信息。
5. 选择“添加”以注册您的活动目录。

控制台注册：自行管理的活动目录

要为基于用户的订阅注册自行管理的Active Directory，请执行以下步骤：

1. 打开License Manager控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 导航到左侧导航窗格中“设置”下的“基于用户的订阅”。
3. 在基于用户的订阅页面上，选择注册Active Directory。
4. 选择AWS托管目录名称和ID，用于存储基于用户的订阅的用户信息。

从注册活动目录AWS CLI

您可以将您的Active Directory注册为基于用户的订阅的身份提供商 [RegisterIdentityProvider](#)操作。

```
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 Active Directory 和你VPC的 ()AWS CLI

您可以将您的 Active Directory 注册为身份提供商，并使用配置您的用户订阅以VPC进行基于用户的订阅 [RegisterIdentityProvider](#)操作。

```
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-1234567890abcde>
```

有关可用软件产品的更多信息，请参阅[License Manager 中支持基于用户的订阅的软件产品](#)。

步骤 3：配置RDS许可证服务器

当 Active Directory 用户访问提供基于用户的订阅 Microsoft 产品的EC2实例时，Microsoft 远程桌面服务 (RDSSALs) 许可证服务器会向他们颁发订阅者访问许可证 ()。完成步骤 1 和步骤 2 后，您可以按如下方式配置许可证服务器。

在开始RDS之前，请确保您已经完成了 for。 [基于用户的订阅先决条件](#)此过程假设您已经设置了活动目录。

为基于用户的订阅配置RDS许可证服务器 (控制台)

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 导航到左侧导航窗格中“设置”下的“基于用户的订阅”页面。
3. 在远程桌面服务 (RDS) 选项卡上，您应该会在列表中看到个或多个活动目录。可能会显示一条提示，告知您需要为 Active Directory RDS 进行配置。
4. 从提示符或“操作”菜单中选择“配置RDS许可证服务器”。
5. 在“配置RDS许可证服务器”对话框中，您可以配置以下设置：

Active Directory

本节包含连接到您配置的RDS许可证服务器的目录的关键详细信息。

密钥

您必须为许可证服务器上用于用户管理任务的凭据选择现有密钥或创建新密钥。机密名称的第一部分必须遵循的“管理凭证”机密部分中描述的模式[基于用户的订阅先决条件](#)。

标签

您可以选择为许可证服务器资源输入标签。

6. 选择“配置”以保存您的设置。

步骤 4：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，让您的用户可以从包含 AWS Marketplace AMI 该产品的进行连接。启动实例后，AWS Systems Manager 尝试将该实例加入 Active Directory 域并对该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。

要启动具有基于用户的订阅的实例，请参[使用随附的许可证启动实例 AMI](#)。

步骤 5：将用户关联到基于用户的订阅实例

一旦您订阅了所需的产品 AWS Marketplace AMI，就可以为用户订阅产品并将他们与提供该产品的实例关联起来。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 远程桌面服务订阅者访问许可证 (RDSSAL) 和他们将要使用的产品。当您的账户 RDSSAL 按中所述进行订阅后[第 1 步：订阅产品](#)，您的用户将在订阅基于用户的订阅产品时代表他们进行订阅。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 Active Directory 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。

每位用户都必须订阅两者RDSSAL以及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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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

为用户订阅产品 (AWS CLI)

您可以通过以下方式为用户订阅在您的身份提供商处注册的产品 [StartProductSubscription](#) 操作。

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

使用自行管理的 Active Directory 为用户订阅产品 ()AWS CLI

您可以使用以下命令为自己管理的 Active Directory 中的用户订阅已在您的 AWS Managed Microsoft AD 目录中注册的产品 [StartProductSubscription](#) 操作。

```
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[License Manager 中支持基于用户的订阅的软件产品](#)。

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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，该实例为基于用户的订阅提供了 [AssociateUser](#) 操作。

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

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

您可以将自己管理的 Active Directory 中的用户与启动的实例关联起来，该实例为基于用户的订阅提供了 [AssociateUser](#) 操作。

```
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 [License Manager 中支持基于用户的订阅的软件产品](#)。

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。

GPO为更活跃的远程用户会话配置活动目录

默认情况下，在提供基于用户的订阅产品的 EC2 Windows 实例上，Microsoft 最多RDS允许同时进行两个用户会话。配置许可证服务器端点后，可以将 Microsoft 配置RDS为允许同时使用 Active Directory 组策略对象 (GPO) 进行两个以上的用户会话，如下所示。

先决条件

您必须已在自己的环境中创建了许可证服务器。要创建许可证服务器，请参阅 [步骤 3：配置RDS许可证服务器](#)。

1. 用于配置的工具GPO取决于您从何处运行它，如下所示：

通过您的域控制器进行中央配置

以管理员身份登录您的 Active Directory 域控制器，然后打开 Windows 组策略管理控制台。

在会话主机上配置组策略

以管理员身份登录您的许可证服务器，然后打开本地组策略编辑器。

2. 在管理控制台或策略编辑器中，编辑组策略以指定通过 Microsoft 连接的会话主机RDS。您可以在 License Manager 产品详细信息页面中找到RDS许可证服务器的端点地址，也可以使用中的[list-license-server-endpoints](#)命令找到 AWS CLI。
3. 将远程桌面会话主机的许可模式设置为Per User，然后保存。

有关为 License Manager 配置RDS许可证服务器的更多信息，请参阅“入门”主题[???](#)中的。有关 Microsoft RDS 会话主机配置的更多信息，请参阅[许可远程桌面会话主机](#)。

使用随附的许可证启动实例 AMI

订阅产品后，您必须启动实例，让您的用户可以从包含 AWS Marketplace AMI该产品的进行连接。启动实例后，AWS Systems Manager 尝试将该实例加入 Active Directory 域并对该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 [在 License Manager 中创建基于用户的订阅的先决条件](#) 和 [对 License Manager 中基于用户的订阅进行故障排除](#)。

使用基于用户的订阅启动实例

1. 访问亚马逊EC2控制台，网址为<https://console.aws.amazon.com/ec2/>。
2. 在“图片”下，选择“AMI目录”。
3. 选择AWS Marketplace AMIs。
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“使用启动实例”AMI。

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，您的实例可以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 Active Directory 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。

当你有来自的正在运行的实例时 AWS Marketplace AMI，你必须为用户订阅产品并将他们与提供产品的实例关联起来，这样他们才能使用产品。

从特定操作系统版本启动实例 AMI

当你从支持Office LTSC Professional Plus或 Microsoft Visual Studio 的中启动实例时，启动时默认为最新的 Windows 操作系统版本的AMI（例如 Windows Server 2022）。AMI要使用特定的操作系统版本启动AMI，请按照以下步骤操作。

1. 在 <https://console.aws.amazon.com/marketplace> 上打开控制台。
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AMI的 Windows 操作系统平台启动实例，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。

使用 Connect 连接到基于用户的订阅实例 RDP

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。用户需要使用域名的用户凭据进行连接，才能使用带有其关联身份的产品。

⚠ Important

创建EC2实例并为用户准备实例的过程可能需要大约 20 分钟。实例的关联状态必须为 `Active` 才能访问和使用产品。

使用基于用户的订阅连接到实例

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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 [Connect to 您的 Windows 实例中列出的步骤进行操作](#)，RDP同时确保指定关联用户的完全限定用户名。

修改微软 Office 订阅的防火墙设置

防火墙可保护您的网络资源免受未经授权的入站或出站流量的侵害。你为安全组定义的规则充当资源的防火墙，这些VPC资源协同工作以在 EC2 Windows 实例上提供基于用户的订阅 Microsoft Office。

您可以使用以下步骤来编辑子网和安全组。License Manager 使用你的设置为微软 Office 配置端点 AWS PrivateLink。有关VPC终端节点的更多信息，请参阅 [什么是 AWS PrivateLink ?](#) 在亚马逊 Virtual Private Cloud 文档中。

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
2. 导航到左侧导航窗格中“设置”下的“基于用户的订阅”页面。
3. 要编辑防火墙设置，请选择 Microsoft Office 订阅产品选项卡，然后从“防火墙”部分的顶部选择“编辑”。这将打开“编辑防火墙”对话框。
4. 更改设置后，选择“保存”进行更新，或选择“取消”以保留当前设置。

License Manager 可能需要几分钟才能完成对这些设置的更改。

管理 License Manager 基于用户的订阅的订阅用户

为了确保产品订阅的计费 and 报告的准确性，并防止未经授权访问订阅资源，您可以按如下方式管理基于 License Manager 用户的订阅的用户访问权限。

取消用户与实例的关联

取消用户与托管 License Manager 基于用户的订阅的实例的关联以移除对该资源的访问权限。

取消订阅用户

取消订阅用户基于用户的订阅，AWS License Manager 以停止向这些个人收取订阅费用。

Note

从 Active Directory 中删除用户不会改变用户关联或订阅。您必须在 License Manager 中取消用户与订阅产品详情页面的关联，才能删除他们与实例的关联。然后，您必须取消订阅该用户。

本主题不包括活动目录管理。

订阅费用

对于 Microsoft Office 和 Visual Studio 订阅，一旦你取消了用户与提供订阅产品的所有实例的关联，并取消了他们对该产品的订阅，计费就会停止。

Micro RDS soft 按每位用户每月计费，部分月份不按比例计费。要在当月结束后停止计费，还必须将该用户从为许可证服务器配置的 Active Directory 中删除。如果用户在月底之后继续登录，他们将自动重新注册，直到其许可令牌到期。

取消用户与提供基于用户的订阅的实例的关联

要删除用户对提供基于用户的 License Manager 订阅的实例的访问权限，您可以取消订阅用户与该实例的关联。此更改不会影响用户的订阅状态。要取消订阅用户并停止向该用户收取订阅费用，请参阅在 [License Manager 中取消用户订阅基于用户的订阅](#)。

取消订阅用户与实例的关联

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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。

在 License Manager 中取消用户订阅基于用户的订阅

您必须取消用户对基于用户的订阅产品的订阅，才能停止为其收取费用。

Important

必须先取消用户与当前关联的所有实例的关联，然后才能取消订阅。

从基于用户的订阅中取消用户订阅

1. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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。

从 License Manager 设置中取消注册活动目录

如果您不想再使用您的 Active Directory 进行基于用户的订阅，则可以从 License Manager 设置中取消注册。从 License Manager 设置中取消注册目录配置不会删除该目录。从设置中注销目录后，您无法再在 License Manager 中将该目录中的用户关联到基于用户的订阅。

先决条件

在从 License Manager 设置中取消注册目录之前，必须执行以下任务：

1. [取消用户与实例的关联](#)来自每个引用您要取消注册的目录的实例。
2. 取消所有订阅用户与实例的关联后，终止该实例。重复此操作，直到所有引用 Active Directory 的实例都终止。
3. 您还需要属于要取消注册[取消订阅用户](#)的 Active Directory 的内容，才能停止对其进行更改。

取消注册

从 License Manager 设置中取消注册活动目录

完成所有必备任务后，打开位于的 License Manager 控制台 <https://console.aws.amazon.com/license-manager/>。

1. 在左侧导航窗格中，选择 设置。
2. 在“设置”页面的 AWS Managed Microsoft AD 部分下，选择“删除”。
3. 输入所需的文本以确认您要删除该目录，然后选择删除。

选择“删除”后，“设置”页面上的AWS Managed Microsoft AD部分将显示您的目录 ID，状态为“配置”。配置过程完成后，该目录将从该AWS Managed Microsoft AD部分中删除。

对 License Manager 中基于用户的订阅进行故障排除

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

- [排除实例合规性故障](#)
- [排除许可证合规性故障](#)
- [排除实例连接故障](#)
- [解决加入域名失败的问题](#)
- [Systems Manager 连接故障排除](#)
- [Systems Manager 运行命令疑难解答](#)

排除实例合规性故障

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 [在 License Manager 中创建基于用户的订阅的先决条件](#)。

排除许可证合规性故障

如果您将 Active Directory 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许可证管理器创建的VPC端点。端点需要端口TCP口 1688 上来自提供基于用户的订阅的实例的入站流量。

您可以使用 [Reachability Analyzer](#) 来帮助确认您的实例中提供基于用户的订阅和终端节点的网络配置是否配置正VPC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 作为源，将为

Microsoft Office 产品配置的VPC终端节点指定为目标。TCP为要分析的路径指定为协议，指定为目标端口 1688。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？](#)。

排除实例连接故障

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《亚马逊EC2用户指南》中的[Windows 实例连接疑难解答](#)。

解决加入域名失败的问题

用户必须能够从 License Manager 设置中配置的 Active Directory 连接到为基于用户的订阅产品提供用户身份的实例。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](#)。

Systems Manager 连接故障排除

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[SSM代理故障排除和托管节点可用性疑难解答](#)。

Systems Manager 运行命令疑难解答

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](#)。

在许可证管理器中管理 Linux 订阅

随着 AWS License Manager，您可以查看和管理您的 Amazon EC2 实例使用的商业 Linux 订阅。您可以跟踪您的 Linux 订阅的使用情况 AWS 区域 还有账号在 AWS Organizations 你在设置中定义的。License Manager 可让您全面了解使用 Linux 订阅的正在运行的实例。它还会指示实例何时定义了多个订阅。

License Manager 发现的数据会汇总并显示在许可证管理器控制台和亚马逊控制 CloudWatch 面板中。您也可以通过以下方式访问您的订阅数据 AWS CLI 以及 License Manager Linux 订阅API或相关SDKs 的。

Linux 许可证订阅可以来自以下来源：

包含订阅 AMIs

- 红帽企业 Linux (RHEL)
- RHEL使用红帽云访问计划自带订阅模式 (BYOS)
- SUSELinux 企业服务器
- 包含 Ubuntu Pro 订阅 AMI

第三方订阅提供商

- RHEL从红帽订阅管理器订阅 (RHSM)

Linux 订阅发现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 可确保您的资源定期更新您的 Linux 订阅数据。如果在这些时间间隔内没有摄取某些数据，则会在下一个公制排放时提供这些信息。这种行为可能会延迟资源（例如新推出的 EC2 商用 Linux 实例）在 Linux 订阅控制面板中显示。

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。发现您的资源后，系统会每小时发布一次 Linux 订阅数据的亚马逊 CloudWatch 指标。

如果你的账户在 AWS Organizations，您可以将成员账号注册为委托管理员。有关更多信息，请参阅 [License Manager 中的委托管理员设置](#)。

检测到重复的订阅

当 License Manager 在同一个 EC2 实例上检测到两个 Linux 订阅时，它会设置重复订阅警报。您可以从 License Manager 控制台的“实例”页面查看和筛选 Linux 订阅数据。

Red Hat Enterprise Linux RHEL 7 扩展生命周期支持 (7ELS) 实例：当您从包含订阅 AMI 的 RHEL 7 实例启动实例时 ELS，您仍应向红帽注册您的实例并使用授权。在本例中，License Manager 会报告重复订阅，但这是预期的行为。

其他红帽 Linux 实例：我们建议您在 [红帽混合云控制台](#) 中搜索订阅清单，以了解您的实例消耗了哪些订阅。

其他主题

- [在 License Manager 中配置 Linux 订阅发现](#)
- [在 License Manager 中查看发现的实例数据](#)
- [License Manager 中有关 Linux 订阅的账单信息](#)
- [在 License Manager 中管理 Linux 订阅的亚马逊 CloudWatch 警报](#)

在 License Manager 中配置 Linux 订阅发现

您可以通过 License Manager 控制台配置 Linux 订阅的发现，AWS CLI、License Manager Linux 订阅API或相关的SDKs。当你激活 Linux 订阅的发现功能时 AWS 区域 你指定，你可以选择将发现范围扩展到你的账户 AWS Organizations。如果您不想再跟踪订阅使用情况，也可以停用发现。

Note

每个账户最多可以发现和显示 5,000 个资源 AWS 区域 默认情况下。要申请上调限制，请使用[限制上调表](#)。

主题

- [配置 Linux 订阅发现](#)
- [激活红帽订阅管理器订阅发现](#)
- [资源发现状态原因](#)
- [停用对 Linux 订阅的发现](#)

配置 Linux 订阅发现

要从 License Manager 控制台的“设置”页面配置 Linux 订阅发现，请执行以下步骤：

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在导航窗格中，选择 Settings (设置)。这将打开“设置”页面。
3. 打开 Linux 订阅选项卡，然后选择配置。这将打开“配置 Linux 订阅设置”面板。
4. 选择来源 AWS 区域Linux 订阅发现应该在哪里运行。
5. 要汇总您账户中的订阅数据 AWS Organizations，选择“链接”AWS Organizations。此选项仅在以下情况下才会出现 AWS Organizations 是为你的账户配置的。
6. 查看并确认授予的选项 AWS License Manager 为 Linux 订阅创建服务相关角色的权限。

7. 选择 Save configuration。

激活红帽订阅管理器订阅发现

要代表您从红帽订阅管理器 (RHSM) 检索订阅信息，License Manager 必须提供您的红帽客户账户API凭证。

先决条件

在激活订阅发现之前，请确保满足以下先决条件。

- 必须为您激活 Linux 订阅的默认发现功能 AWS 账户 然后才能配置RHSM订阅发现。如果默认发现设置为“未激活”，请参见[配置 Linux 订阅发现](#)。
- 如果您使用组织管理员提供的企业红帽登录信息，请确保您的登录 ID 已分配以下角色和权限：
 - 角色：管理您的订阅
 - 权限：View All，或 View/Edit All

如果您的登录 ID 没有所需的角色和权限，请联系您的红帽门户组织管理员并请求将其添加到您的登录名中。有关红帽角色和权限的更多信息，请参阅[红帽客户门户的角色和权限](#)。有关如何联系您的红帽门户组织管理员的更多信息，请参阅[如何知道我的组织管理员是谁？](#) 在红帽客户门户知识库中。

- 要激活RHSM订阅发现，您必须提供红帽客户账户API离线令牌，或者 AWS Secrets Manager 包含离线令牌的密钥。要获取离线令牌，请按照红帽文档网站上[生成新的离线令牌](#)中所述的步骤进行操作。

Important

您的安全对我们很重要。您的红帽离线访问令牌安全地存储在 Secrets Manager 中。每次向红帽请求订阅详细信息时，License Manager 都会使用您的密钥生成临时访问令牌。

激活

要从 License Manager 控制台的“设置”页面激活RHSM发现，请执行以下步骤：

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在导航窗格中，选择 Settings (设置)。
3. 在“设置”页面上，打开 Linux 订阅选项卡。
4. 选择“编辑”以更新您的 Linux 订阅设置。这将打开配置 Linux 订阅发现页面。

5. 要开始激活过程，请选中“激活红帽订阅管理器 (RHSM) 发现”复选框。这将显示关联RHSM账户面板。
6. 选择适用于您的密钥的 Secret (Token) 选项，然后按照其余步骤进行操作，具体取决于您选择的选项。
7. 选项：创建新密钥 — 推荐

提供红帽离线访问令牌，然后让 License Manager 代表你在 Secrets Manager 中创建访问密钥。

- a. 在密钥名称中输入您的密钥的名称。
- b. 将您的红帽离线访问令牌粘贴到离线令牌框中。确保代币值前后没有多余的空格或换行符。您可以在[红帽订阅管理器令牌页面上生成您的红帽离线访问API令牌](#)。

选项：选择一个密钥

在 Secrets Manager 中选择一个包含您的红帽离线访问令牌的现有密钥。

8. (可选) 为您的密钥添加标签。
9. 选中页面底部的复选框以确认激活红帽订阅管理器发现即表示您授予访问权限 AWS License Manager 服务，用于收集与 Amazon EC2 实例上使用的红帽订阅相关的数据。
10. 选择激活。

资源发现状态原因

AWS License Manager 将显示每个状态和相应的状态原因 AWS 区域 您选择为 Linux 订阅启用发现。如果您将 Linux 订阅与关联了，则状态原因会有所不同 AWS Organizations:

- 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。

状态原因操作	描述
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 `UpdateServiceSettingsAPI` 然后再调用 `GetServiceSettingsAPI` 以监控启用 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：

Status	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。
	"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。

Status	状态原因	描述
	"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。
	"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。

停用对 Linux 订阅的发现

您可以从中停用对 Linux 订阅的发现 AWS License Manager 设置页面。但是，如果您已激活发现

Warning

如果您禁用发现，则之前为 Linux 订阅发现的所有数据都将从中删除 AWS License Manager。

禁用 Linux 订阅的发现功能

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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 以及 AWS Organizations](#)。

在 License Manager 中查看发现的实例数据

在 License Manager 完成所选资源中的初始资源发现过程之后 AWS 区域，您可以在控制台中查看结果。如果你选择链接 AWS Organizations，License Manager 会汇总来自组织内账户的数据。要查看订阅符合筛选条件的实例列表，请导航至 Instances 部分 AWS License Manager console。列表显示以下关键字段。

- 实例 ID — 实例的 ID。
- 状态 — 实例的状态。
- 实例类型 — 实例的类型。
- 订阅-实例使用的许可证订阅的名称。
- 重复警报-表示您的实例上同一软件有两种不同的许可证订阅。
- 账户 ID — 拥有实例的账户的 ID。
- 地区 — AWS 区域 实例所在的位置。
- AMIID — AMI 用于启动实例的 ID。
- 使用操作-实例的操作以及与关联的账单代码AMI。有关更多信息，请参阅 [使用操作值](#)。
- 产品代码 — 与关联的产品代码，AMI用于启动实例。有关更多信息，请参阅[AMI产品代码](#)。
- LastUpdatedTime— 上次发现更新实例详细信息的时间。

主题

- [查看所有实例的数据](#)
- [通过订阅查看实例的数据](#)

查看所有实例的数据

您可以查看和筛选 License Manager 为账户中的实例发现的 Linux 订阅数据，或者 AWS Organizations，如下所示。

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在左侧导航窗格中的“Linux 订阅”下，选择实例。这将显示包含 Linux 订阅数据的实例列表。
3. （可选）您可以使用以下筛选器来简化结果：
 - 帐户
 - AMI身份证
 - 重复订阅
 - 实例 ID
 - 区域
 - 产品代码
 - 使用情况操作
4. （可选）选择将视图导出CSV到，将所有实例的数据导出为逗号分隔值文件（.csv）CSV。

通过订阅查看实例的数据

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。

查看使用特定订阅的实例的已发现数据

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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
 - 帐户
 - 区域
 - AMI身份证
 - 使用情况操作
 - 产品代码

5. (可选) 选择“将视图导出CSV到”，将使用此订阅的实例的数据导出为逗号分隔值文件 () CSV。

License Manager 中有关 Linux 订阅的账单信息

在亚马逊上运行的每个商业 Linux 订阅EC2都有与亚马逊系统映像 (AMI) 关联的账单信息。商用 Linux 订阅具有亚马逊EC2使用操作功能，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 弹性计算云用户指南中的[AMI账单信息字段](#)和中的[AMI产品代码](#) AWS Marketplace 卖家指南。

订阅名称	亚马逊EC2使用操作	AWS Marketplace 产品代码	订阅类型
红帽企业 Linux 服务器 BYOS	RunInstances:00g0	x	自带订阅模式 (BYOS)
Red Hat Enterprise Linux Server	RunInstances00:10	x	EC2包含订阅
具有高可用性附加组件的 Red Hat Enterprise Linux	RunInstances:1010	x	EC2包含订阅
具有SQL服务器标准和高可用性的红帽企业 Linux	RunInstances:1014	x	EC2包含订阅
具有企业SQL服务器和高可用性的红帽企业 Linux	RunInstances:1110	x	EC2包含订阅
采用SQL服务器标准的红帽企业 Linux	RunInstances00:14	x	EC2包含订阅
搭载 Web SQL 服务器的红帽企业 Linux	RunInstances:0210	x	EC2包含订阅

订阅名称	亚马逊EC2使用操作	AWS Marketplace 产品代码	订阅类型
搭载企业SQL服务器的红帽企业 Linux	RunInstances:0110	✗	EC2包含订阅
SUSELinux 企业服务器	RunInstances:000g	✗	EC2包含订阅
SAP具有高可用性和更新服务的红帽企业 Linux	RunInstances00:10	✓	AWS Marketplace 订阅 ¹
SUSE带有 Linux 企业服务器的 SAP	✗	✓	AWS Marketplace 订阅
Ubuntu Pro	RunInstances:0g00	✓	AWS Marketplace 订阅
Red Hat Enterprise Linux 工作站	✗	✓	AWS Marketplace 订阅

¹ 此订阅既有 Amazon EC2 使用操作，又有 AWS Marketplace 产品代码。

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	<p>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。</p> <p>单位：计数</p> <p>维度：</p> <p>SubscriptionName：订阅的名称。</p> <p>Region：发现使用商业 Linux 订阅的资源的区域。</p>

在 License Manager 中管理 Linux 订阅的亚马逊 CloudWatch 警报

License Manager 控制台中的 Linux 订阅列表页面显示了以下关键细节，包括您为许可证管理器在您的实例上找到的每个 Linux 订阅配置的亚马逊 CloudWatch 警报。

- 订阅名称
- 订阅类型
- 每次订阅的运行实例数
- 已配置的亚马逊 CloudWatch 警报

当您从列表页面选择 Linux 订阅时，使用情况指标和警报选项卡会显示该订阅的数据。在此选项卡中，License Manager 控制台中显示所选订阅的 Amazon 控制 CloudWatch 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，其中包含以下详细信息：

- 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 以及已定义的实例类型。
- 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提醒。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。

以下是可能的 CloudWatch 警报状态：

- 正常 — 指标或表达式在定义的阈值范围内。
- ALARM— 指标或表达式超出了定义的阈值。
- INSUFFICIENT_DATA — 警报刚刚开始，指标不可用，或者指标可用数据不足，无法确定警报状态。

主题

- [为 Linux 订阅创建 CloudWatch 警报](#)
- [修改 Linux 订阅的 CloudWatch 警报](#)

- [删除 Linux 订阅的 CloudWatch 警报](#)

为 Linux 订阅创建 CloudWatch 警报

您可以为在正在运行的EC2实例上发现的每个商用 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。

从控制台为 Linux 订阅创建 CloudWatch 警报

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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 CloudWatch 警报

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

从控制台修改 Linux 订阅的 CloudWatch 警报

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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 CloudWatch 警报

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

从控制台删除 Linux 订阅的 CloudWatch 警报

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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。

License Manager 中的设置

的“设置”部分 AWS License Manager 控制台显示当前账户的设置。必须配置设置才能启用相关功能。

Managed licenses

托管许可证可配置以下设置：

- 向您的组织分发托管授权和自我管理许可证
- 跨账户资源查找
- 亚马逊SNS通知

有关更多信息，请参阅 [License Manager 中的托管许可设置](#)。

Linux subscriptions

可以为 Linux 订阅配置以下设置：

- 发现和汇总商用 Linux 许可证订阅数据
- 红帽订阅管理器 (RHSM) 发现 Linux 订阅

有关更多信息，请参阅 [License Manager 中的 Linux 订阅设置](#)。

User-based subscriptions

以下设置可针对基于用户的订阅进行配置：

- AWS Managed Microsoft AD
- 虚拟私有云 (VPC)

有关更多信息，请参阅 [License Manager 中基于用户的订阅设置](#)。

Delegated administration

如果您的账户拥有组织的管理权限，则会显示此选项卡。作为管理员，您可以从中注册委托管理员 AWS CLI 或者 AWS Management Console。有关更多信息，请参阅[License Manager 中的委托管理员设置](#)。

设置主题

- [编辑 License Manager 设置](#)
- [License Manager 中的托管许可设置](#)
 - [账户详细信息](#)
 - [跨账户资源查找](#)
 - [简单通知服务 \(SNS\)](#)
- [License Manager 中的 Linux 订阅设置](#)
 - [Linux 订阅设置](#)
 - [红帽订阅管理器发现](#)
- [License Manager 中基于用户的订阅设置](#)
 - [AWS Managed Microsoft AD](#)
 - [虚拟私有云](#)
- [License Manager 中的委托管理员设置](#)
 - [授权的 License Manager 管理员支持的区域](#)
 - [注册委派的 License Manager 管理员](#)
 - [取消注册委派的 License Manager 管理员](#)

编辑 License Manager 设置

要编辑您的 License Manager 设置，请执行以下步骤：

1. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在左侧导航窗格中，选择 设置。
3. 选择包含要配置的设置选项卡。例如，选择托管许可证以配置账户详细信息。
4. 配置完设置后，选择“保存”，或者选择“取消”进行退出。

License Manager 中的托管许可设置

以下设置适用于托管许可证。

账户详细信息

您可以查看您的账户详细信息以查看诸如账户类型、账户是否属于 AWS Organizations 已关联，账户的 License Manager S3 存储段ARN以及 AWS Resource Access Manager 分享ARN。本部分还允许您链接您的 AWS Organizations 账户。

要在组织内分发托管授权或自行管理许可证，请选择链接 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予。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

要启用此选项，您必须登录自己的管理账户，并且必须启用所有功能 AWS Organizations。有关更多信息，请参阅中的[启用组织中的所有功能](#) AWS Organizations 用户指南。

此选择还会创建一个 AWS Resource Access Manager 管理账户中的资源共享，允许您无缝共享自行管理的许可证。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[UpdateServiceSettingsAPI](#)。

跨账户资源查找

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

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 将自动关联以在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](#) 汇总您账户中的库存数据 AWS Organizations.
- [AWS Glue](#) 提供快速的查询体验。

Note

以下 AWS 区域 不需要 Amazon Athena 或者 AWS Glue 要查询或汇总 Systems Manager 清单的库存数据以发现软件使用情况，请执行以下操作：

- 亚太地区 (雅加达)
- 以色列 (特拉维夫)

简单通知服务 (SNS)

您可以将 Amazon 配置 SNS 为接收来自许可证管理器的通知和提醒。

配置 Amazon SNS 主题

1. 选择简单通知服务 (SNS) 旁边的编辑。
2. 按以下格式指定 SNS 主题 ARN：

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

3. 选择 Save changes (保存更改)。

License Manager 中的 Linux 订阅设置

在发现过程中，License Manager 会搜索在您的下运行的 EC2 实例 AWS 账户 适用于 Linux 订阅。它会检测您是否为任何实例定义了多个 Linux 订阅，并汇总数据。

Linux 订阅设置

您可以配置 Linux 订阅的设置，以控制 License Manager 处理发现和聚合的方式。默认发现设置适用于所有类型的 Linux 订阅。

以下操作可用于配置 Linux 订阅发现。

编辑

更改 Linux 订阅发现的设置。

停用

停用与您的EC2实例关联的 Linux 订阅的发现和聚合。如果您还为红帽订阅管理器激活了发现，License Manager 会先停用您的RHSM注册提供商，然后继续停用 Linux 订阅发现。

Note

停用不会影响您对红帽订阅管理器的访问密钥 (RHSM)。为了避免向您收费 AWS 为不再需要的关联密钥开具账单，请参阅[删除 AWS Secrets Manager 秘密](#)在 AWS Secrets Manager 用户指南。

License Manager 控制台中显示了以下设置，用于 Linux 订阅发现。

Linux 订阅发现设置

Linux 订阅发现

表示您是否已为自己的账户激活 Linux 订阅发现。

来源 AWS 区域

AWS 区域 您希望 License Manager 在其中发现订阅数据。

AWS Organizations

(可选) 在您的账户中汇总订阅数据 AWS Organizations.

有关更多信息，请参阅 [在许可证管理器中管理 Linux 订阅](#)。

红帽订阅管理器发现

如果您已激活 Linux 订阅发现，则可以配置许可证管理器的访问权限，以检索通过红帽RHEL订阅管理器 (RHSM) 管理的订阅的其他数据。

以下操作可用于配置您的RHSM订阅发现。

编辑标签

更改与您的访问密钥关联的标签。

Note

如果您需要对RHSM订阅进行其他更改，则必须先停用当前的注册，然后再设置新的注册。

停用

停用您的RHSM注册提供商。

Note

停用不会影响您对红帽订阅管理器的访问密钥 (RHSM)。为了避免向您收费 AWS 为不再需要的关联密钥开具账单，请参阅[删除 AWS Secrets Manager 秘密](#)在 AWS Secrets Manager 用户指南。

以下设置显示在 License Manager 控制台中以供RHSM发现。

红帽订阅管理器发现设置

发现状态

表示您是否已激活RHSM订阅发现功能。

机密名称

指向RHSM访问密钥的链接 AWS Secrets Manager 其中包含您的红帽离线令牌。License Manager 使用此密钥生成新的临时访问令牌，以便向红帽订阅管理器 (RHSM) 请求订阅数据。

您可以通过 Secrets Manager 对现有密钥进行更改。要更新密钥的标签或其他元数据，请参阅[修改 AWS Secrets Manager 秘密](#)在 AWS Secrets Manager 用户指南。要更新密钥值，请参阅[更新密钥的值 AWS Secrets Manager 秘密](#)。

上次同步数据的时间为

上次成功更新已注册红帽订阅管理器 (RHSM) 账户的订阅数据的时间戳。

标签

你可以为许可证管理器在 Secrets Manager 中分配给你的RHSM访问密钥的标签定义密钥值对。要检索和解密您的RHSM访问密钥，License Manager 服务相关角色策略需要该密钥以及任何关联的密钥 AWS KMS key，以分配以下标签：

```
"LicenseManagerLinuxSubscriptions": "enabled"
```

如果 License Manager 在注册过程中创建了您的密钥，则会自动分配该标签。如果您为离线令牌创建自己的密钥，请确保将该标签分配给密钥和关联的密钥（如果密KMS钥已加密）。要添加标签，请参阅[修改 AWS Secrets Manager 秘密](#)在 AWS Secrets Manager 用户指南。

License Manager 中基于用户的订阅设置

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 需要 AWS Managed Microsoft AD 需要先进行配置，然后才能使用基于用户的订阅。有关更多信息，请参阅[使用基于用户的 License Manager 订阅来购买支持的软件产品](#)。

虚拟私有云

除了你的 VPC License Manager 之外，还需要对你进行配置 AWS Managed Microsoft AD，当你在 Microsoft Office 上使用基于用户的订阅时。有关更多信息，请参阅[使用基于用户的 License Manager 订阅来购买支持的软件产品](#)。

License Manager 中的委托管理员设置

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。使用这种方法时，您的组织中将有有一个授权管理员来管理许可管理器。

使用 AWS CLI 或者 SDKs，您可以将组织中的不同成员帐户注册为 License Manager 每项支持的功能的委托管理员。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 账户以加入您的组织并启用可信访问权限 AWS Organizations](#)。

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我管理许可证、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，例如查看和管理您拥有并运行的商业 Linux 订阅 AWS 区域 还有你的账号在 AWS Organizations。您还可以为您的 Linux 订阅创建和管理亚马逊 CloudWatch 警报。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，委派的管理员可以查看您组织中账户拥有的EC2实例。

您可以使用注册和取消注册委派的管理员 [AWS License Manager 控制台](#)，[AWS CLI](#)，或者 [AWS SDKs](#)。

授权的 License Manager 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)
- 美国东部 (弗吉尼亚州北部)
- 美国西部 (加利福尼亚北部)
- 美国西部 (俄勒冈州)
- 亚太地区 (孟买)
- 亚太地区 (首尔)
- 亚太地区 (新加坡)
- 亚太地区 (悉尼)
- 亚太地区 (东京)
- 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)
- 欧洲地区 (伦敦)
- 欧洲地区 (巴黎)
- Europe (Stockholm)
- 欧洲地区 (米兰)
- 非洲 (开普敦)
- 南美洲 (圣保罗)

注册委派的 License Manager 管理员

您可以使用注册委派管理员 AWS CLI 或者 AWS Management Console.

Console

要使用注册委派管理员 AWS License Manager 控制台，请执行以下步骤：

1. 登录到 AWS 作为管理账户的管理员。
2. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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

要注册托管许可证的委派管理员，请使用 AWS CLI，请执行以下步骤：

1. 在命令行中运行以下命令 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 Linux 订阅注册委派管理员 AWS CLI，请执行以下步骤：

1. 在命令行中运行以下命令 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
```

取消注册委派的 License Manager 管理员

您可以使用取消注册委派的管理员 AWS CLI 或者 AWS Management Console。

Console

要取消注册委派管理员，请使用 AWS License Manager 控制台，请执行以下步骤：

1. 登录到 AWS 作为管理账户的管理员。
2. 打开 License Manager 控制台，网址为 <https://console.aws.amazon.com/license-manager/>。
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

要取消托管许可证的委托管理员的注册，请使用 AWS CLI，请执行以下步骤：

1. 在命令行中运行以下命令 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
```

要取消注册 Linux 订阅的委派管理员，请使用 AWS CLI，请执行以下步骤：

1. 在命令行中运行以下命令 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。

License Manager 中的控制面板

License Manager 控制台的“控制面板”部分提供了使用细节，您可以使用这些详细信息来跟踪与以下内容相关的许可证使用情况：

- 自管理许可证
- 已授予的许可证权限
- 基于用户的订阅的订阅用户
- 正在运行的实例

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。

权利

授权的名称。

使用量

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。

权利

授权的名称。

使用量

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

在您的所有账户中汇总的正在运行的实例总量 AWS Organizations 在这个地区。此图表仅对管理账户和委托管理员账户可见。

监控 License Manager

您可以监控中跟踪的许可证和订阅的使用情况 AWS License Manager 使用亚马逊 CloudWatch。CloudWatch 收集原始数据并将其处理成可读的、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 [通过亚马逊监控 License Manager 许可证的使用情况 CloudWatch](#)。

您可以捕捉由您或其代表API拨打的电话和相关事件 AWS 账户 使用 AWS CloudTrail。事件被捕获为日志文件并传送到您指定的 Amazon S3 存储桶。您可以识别哪些用户和账户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 [日志记录 AWS License Manager API 使用呼叫 AWS CloudTrail](#)。

目录

- [通过亚马逊监控 License Manager 许可证的使用情况 CloudWatch](#)
 - [创建警报来监控 License Manager 指标](#)
- [日志记录 AWS License Manager API使用呼叫 AWS CloudTrail](#)
 - [中的 License Manager 信息 CloudTrail](#)
 - [了解 License Manager 日志文件条目](#)

通过亚马逊监控 License Manager 许可证的使用情况 CloudWatch

您可以使用亚马逊监控许可证管理器的指标统计数据 CloudWatch。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	<p>在您的所有账户中运行的实例总数 AWS Organizations 在当前 AWS 区域。</p> <p>单位：计数</p> <p>维度：</p> <p>SubscriptionName : 订阅的名称。</p>
TotalLicenseConfigurationUsageCount	<p>可用的许可证配置总数。</p> <p>单位：计数</p> <p>维度：</p> <ul style="list-style-type: none"> LicenseConfigurationArn : 许可配置 Amazon 资源名称 (ARN)。 LicenseConfigurationType : 许可证配置类型。
LicenseConfigurationUsageCount	<p>此配置中已使用的许可证总数。</p> <p>单位：计数</p> <p>维度：</p> <ul style="list-style-type: none"> LicenseConfigurationArn : 许可证配置ARN。 LicenseConfigurationType : 许可证配置类型。
LicenseConfigurationUsagePercentage	<p>该许可证配置的已用许可证百分比。</p> <p>单位：百分比</p> <p>维度：</p> <ul style="list-style-type: none"> 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

您可以创建一个 CloudWatch 警报，当指标值发生变化并导致警报状态发生变化时，该警报会发送亚马逊简单通知服务 (AmazonSNS) 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。警报仅针对持续的状态变化调用操作。CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关更多信息，请参阅[使用 CloudWatch 警报](#)。

日志记录 AWS License Manager API 使用呼叫 AWS CloudTrail

AWS License Manager 已与集成 AWS CloudTrail，一项提供用户、角色或用户所执行操作记录的服务。AWS 在 License Manager 中提供服务。CloudTrail 将所有对 License Manager 的 API 调用捕获为事件。捕获的调用包括来自许可证管理器控制台的调用和对许可证管理器 API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括许可管理器的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的“事件历史记录”中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 License Manager 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅[AWS CloudTrail 用户指南](#)。

主题

- [中的 License Manager 信息 CloudTrail](#)
- [了解 License Manager 日志文件条目](#)

中的 License Manager 信息 CloudTrail

CloudTrail 已在您的设备上启用 AWS 账户 当您创建账户时。在 License Manager 中发生活动时，该活动会与其他 CloudTrail 活动一起记录在事件中 AWS 事件历史记录中的服务事件。您可以查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅[使用事件历史记录查看 CloudTrail 事件](#)。

如需持续记录您的事件 AWS 账户（包括 License Manager 的事件），创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有跟踪 AWS 区域。该跟踪记录了来自所有区域的事件 AWS 对日志文件进行分区并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您还可以配置其他 AWS 服务，用于进一步分析 CloudTrail 日志中收集的事件数据并据此采取行动。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](#)
- [为以下各项配置亚马逊SNS通知 CloudTrail](#)
- [接收来自多个区域的 CloudTrail 日志文件](#)和[接收来自多个账户的 CloudTrail 日志文件](#)

所有 License Manager 操作都由记录 CloudTrail 并记录在 [AWS License Manager API参考](#)。例如，对调用的调用ListResourceInventory和DeleteLicenseConfiguration操作会在 CloudTrail 日志文件中生成条目。CreateLicenseConfiguration

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用 root 还是通过 root 发出 AWS Identity and Access Management (IAM) 用户凭证。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他人提出 AWS 服务。

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，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。CloudTrail 日志文件不是公共API调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该DeleteLicenseConfiguration操作的 CloudTrail 日志条目。

```
{
  "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"
}
```

License Manager 中的安全性

云安全位于 AWS 是最高优先级。作为 AWS 客户，您将受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方的共同责任 AWS 还有你。[责任共担模式](#)将此描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护运行的基础架构 AWS 中的服务 AWS 云。AWS 还为您提供可以安全使用的服务。作为安全措施的一部分，第三方审计师会定期测试和验证我们安全的有效性 [AWS 合规计划](#)。要了解适用于 License Manager 的合规计划，请参阅 [AWS 按合规计划划分的范围内的服务](#)。
- 云端安全 — 您的责任由以下因素决定 AWS 您使用的服务。您还需要对其他因素负责，包括您的数据的敏感性、您的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。你还会学习如何使用其他 AWS 可帮助您监控和保护您的 License Manager 资源的服务。

内容

- [License Manager 中的数据保护](#)
- [License Manager 的身份和访问管理](#)
- [在 License Manager 中使用服务相关角色](#)
- [AWS License Manager 的托管策略](#)
- [在 License Manager 中对许可证进行加密签名](#)
- [License Manager 的合规性验证](#)
- [License Manager 中的弹性](#)
- [License Manager 中的基础架构安全](#)
- [License Manager 和接口VPC端点与 AWS PrivateLink](#)

License Manager 中的数据保护

这些区域有：AWS [分担责任模型](#)适用于以下领域的的数据保护 AWS License Manager。如本模型所述，AWS 负责保护运行所有内容的全球基础设施 AWS Cloud。您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信

息，请参阅[数据隐私FAQ](#)。有关欧洲数据保护的信息，请参阅 [AWS 责任共担模型和GDPR](#) 博客文章 [AWS 安全博客](#)。

出于数据保护的目，我们建议您进行保护 AWS 账户凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。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与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。有关使用 CloudTrail 轨迹捕获的信息 AWS 活动，请参阅[使用中的 CloudTrail 轨迹](#) AWS CloudTrail 用户指南。
- 使用 AWS 加密解决方案，以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅[联邦信息处理标准 \(FIPS\) 140-3](#)。

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）。这包括当你使用 License Manager 或其他软件时 AWS 服务使用控制台，API，AWS CLI，或 AWS SDKs。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URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

静态加密

License Manager 将数据存储于管理账户的 Amazon S3 存储桶中。存储桶是使用 Amazon S3 托管加密密钥 (SSE-S3) 配置的。

License Manager 的身份和访问管理

AWS Identity and Access Management (IAM) 是一项可帮助管理员安全地控制对 AWS 资源的访问的 AWS 服务。IAM管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 AWS 资源。IAM您可以使用您的 AWS 账户创建用户和群组。您可以控制用户使用 AWS 资源执行任务所拥有的权限。您无需IAM支付额外费用即可使用。

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，必须创建一个明确授予他们权限的IAM策略。

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》指南中的[策略和权限](#)。

创建用户、组和角色

您可以为自己 AWS 账户 创建用户和群组，然后为他们分配所需的权限。作为最佳实践，用户应通过担任IAM角色来获得权限。有关如何为 AWS 账户设置用户和组的更多信息，请参阅 [开始使用 License Manager](#)。

[IAM角色](#)是您可以在自己的账户中创建的具有特定权限的IAM身份。IAM角色与IAM用户的相似之处在于，它是一个 AWS 身份，其权限策略决定了该身份可以做什么和不能做什么 AWS。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。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策略是由一个或多个声明组成的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，用户无权使用资源和API操作，因此所有请求都将被拒绝。显式允许将覆盖默认规则。显式拒绝将覆盖任何允许。
- **操作**：API操作是您授予或拒绝权限的特定操作。
- **资源**：受操作影响的资源。某些 License Manager API 操作允许您在策略中加入可由操作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[由定义的操作 AWS License Manager](#)。

- 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策略声明中，您可以指定任何支持的服务中的任何API操作IAM。License Manager 使用以下前缀作为API操作名称：

- `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 的更多信息APIs，请参阅以下API参考资料：

- [AWS License Manager API参考](#)
- [AWS License Manager 用户订阅API参考](#)
- [AWS License Manager Linux 订阅API指南](#)

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，您可以按如下方式指定名称以“列表”一词开头的
所有 License Manager API 操作：

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

要指定所有 License Manager API 操作，请按如下方式使用* 通配符：

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

ISV使用 License Manager 的策略示例

ISVs通过 License Manager 分发许可证需要以下权限：

```
{
  "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、群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：

- 中的用户和群组 AWS IAM Identity Center：

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。

- IAM通过身份提供商管理的用户：

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）](#)中的说明进行操作。

- IAM用户：
 - 创建您的用户可以担任的角色。按照《用户指南》中[为IAM用户创建角色](#)中的IAM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《用户指南》中[向用户\(控制台\)添加权限](#)中的IAM说明进行操作。

在 License Manager 中使用服务相关角色

AWS License Manager uses AWS Identity and Access Management (IAM) [服务相关角色](#)。服务相关角色是一种独特的角色类型，直接链接到 License Manager。IAM服务相关角色由 License Manager 预定义，包括该服务调用其他角色所需的所有权限 AWS 代表您提供服务。

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，并且该权限策略不能附加到任何其他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

名为的服务相关角色AWSServiceRoleForAWSLicenseManagerRole允许 License Manager 访问 AWS 代表您管理许可证的资源。

`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](#)。要详细了解如何为服务相关角色配置权限，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 IAMAPI，或者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”中出现了一个新角色](#)。

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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 所需的权限，然后选择继续。

您还可以使用IAM控制台在 License Manager 用例中创建服务相关角色。或者，在 AWS CLI 或者 AWS API，IAM用于创建具有服务名称的`license-manager.amazonaws.com`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](#)。

如果您删除此服务相关角色，则可以使用相同的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，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。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功能或服务，我们建议您删除该角色。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

在使用IAM删除服务相关角色之前，必须先删除该角色使用的所有资源。这意味着要取消任何自我管理许可证与关联实例的关联AMIs，然后删除自行管理的许可证。

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 在导航窗格中，选择自我管理许可证。
3. 选择您作为所有者的自行管理许可证，并取消关联AMIs和资源选项卡中所有条目的关联。对每个许可证配置重复此过程。
4. 仍在自我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，直到删除所有自我管理许可证。

手动删除服务相关角色

使用IAM控制台，AWS CLI，或者AWS API删除`AWSServiceRoleForAWSLicenseManagerRole`服务相关角色。如果你也在使用 [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) 并且 [AWSLicenseManagerMemberAccountRole](#)，请先删除这些角色。有关更多信息，请参阅IAM用户指南中的[删除服务相关角色](#)。

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

名为的服务相关角色 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 允许 License Manager 访问 AWS 用于代表您管理中央管理账户的许可证管理操作的资源。

`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 托管策略：AWSLicenseManagerMasterAccountRolePolicy](#)。要详细了解如何为服务相关角色配置权限，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。当您在中配置跨账户许可证管理时 AWS Management Console，License Manager 会为您创建服务相关角色。

Note

要在 License Manager 中使用跨账户支持，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。

你也可以使用 IAM 控制台，AWS CLI IAM API，或者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”中出现了一个新角色](#)。

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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
2. 选择 Settings (设置) 和 Edit (编辑)。
3. 选择“链接”AWS Organizations 账户。
4. 选择 应用。

您还可以使用IAM控制台在“许可证管理器-管理帐户”用例中创建服务相关角色。或者，在 AWS CLI 或者 AWS API，IAM用于创建具有服务名称的license-manager.master-account.amazonaws.com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](#)。

如果您删除此服务相关角色，则可以使用相同的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，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。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功能或服务，我们建议您删除该角色。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

使用控制IAM台，AWS CLI，或 AWS API删除AWSServiceRoleForAWSLicenseManagerMasterAccountRole服务相关角色。有关更多信息，请参阅IAM用户指南中的[删除服务相关角色](#)。

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

名为的服务相关角色 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 允许 License Manager 进行访问 AWS 代表您使用配置的管理账户执行许可证管理操作的资源。

`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 托管策略：AWSLicenseManagerMemberAccountRolePolicy](#)。要详细了解如何为服务相关角色配置权限，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。您可以启用与的集成 AWS Organizations 从 License Manager 控制台的“设置”页面上的管理帐户中获取。您也可以使用 AWS CLI（运行 `update-service-settings`）或者 AWS API（呼叫 `UpdateServiceSettings`）。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。

你也可以使用 IAM 控制台，AWS CLI，或者 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”中出现了一个新角色](#)。

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. 登录到你的 AWS Organizations 管理账户。

2. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
3. 在左侧导航栏上，选择设置，然后选择编辑。
4. 选择“链接”AWS Organizations 账户。
5. 选择应用。这将创建角色 [AWSServiceRoleForAWSLicenseManagerRole](#) 和 [AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) 在所有儿童账户中。

您还可以使用IAM控制台创建包含该License Manager - Member account用例的服务相关角色。或者，在AWS CLI 或者 AWS API，使用服务名称创建服务相关角色。license-manager.member-account.amazonaws.com有关更多信息，请参阅IAM用户指南中的[创建服务相关角色](#)。

如果您删除此服务相关角色，则可以使用相同的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，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。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功能或服务，我们建议您删除该角色。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

使用控制IAM台，AWS CLI，或 AWS API删

除[AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#)服务相关角色。有关更多信息，请参阅IAM用户指南中的[删除服务相关角色](#)。

License Manager — 基于用户的订阅角色

License Manager 需要服务相关角色才能进行管理 AWS 将提供基于用户的订阅的资源。

基于用户的订阅角色的权限

名为的服务相关角色[AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService](#)允许 License Manager 使用 AWS Systems Manager 并管理提供基于用户的订阅的 Amazon EC2 资源，以及描述 AWS Directory Service 资源的费用。

要查看的权限 `AWSLicenseManagerUserSubscriptionsServiceRolePolicy`，请参阅[AWS 托管策略：AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。要详细了解如何为服务相关角色配置权限，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 IAMAPI，或者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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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。

您还可以使用IAM控制台创建包含该License Manager - User-based subscriptions用例的服务相关角色。或者，在 AWS CLI 或者 AWS API，使用服务名称创建服务相关角色。`license-manager-user-subscriptions.amazonaws.com`有关更多信息，请参阅IAM用户指南中的[创建服务相关角色](#)。

如果您删除此服务相关角色，则可以使用相同的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，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。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功能或服务，我们建议您删除该角色。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

使用控制IAM台，AWS CLI，或 AWS API删

除AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService服务相关角色。有关更多信息，请参阅IAM用户指南中的[删除服务相关角色](#)。

License Manager — Linux 订阅角色

License Manager 需要服务相关角色才能管理 AWS 提供 Linux 订阅的资源。

Linux 订阅角色的权限

名为的服务相关角

色AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService允许 License Manager 对 Linux 订阅执行以下操作。

- 探索 Amazon 弹性计算云和 AWS Organizations 资源的费用。
- 检索标有 from "LicenseManagerLinuxSubscriptions": "enabled" 的机密 AWS Secrets Manager 访问第三方 Linux 订阅提供商以获取订阅信息。
- 使用标有标签的KMS密钥"LicenseManagerLinuxSubscriptions": "enabled"来解密机密。

要查看的权限 AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy，请参阅[AWS 托管策略：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。要详细了解如何为服务相关角色配置权限，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 IAMAPI，或者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. 打开 License Manager 控制台，网址为<https://console.aws.amazon.com/license-manager/>。
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。

您还可以使用IAM控制台创建包含该License Manager - Linux subscriptions用例的服务相关角色。或者，在 AWS CLI 或者 AWS API，使用服务名称创建服务相关角色。license-manager-linux-subscriptions.amazonaws.com有关更多信息，请参阅IAM用户指南中的[创建服务相关角色](#)。

如果您删除此服务相关角色，则可以使用相同的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，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。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功能或服务，我们建议您删除该角色。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

使用控制IAM台，AWS CLI，或 AWS API删

除AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService服务相关角色。有关更多信息，请参阅IAM用户指南中的[删除服务相关角色](#)。

AWS License Manager 的托管策略

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。[创建IAM客户托管策略](#)以仅向您的团队提供他们所需的权限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。这些政策涵盖常见用例，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 托管策略](#)。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 管理型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，服务最有可能更新 AWS 管理型策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时，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[工作职能AWS 托管策略](#)。

AWS 托管策略：AWSLicenseManagerServiceRolePolicy

此策略附加AWSServiceRoleForAWSLicenseManagerRole到名为的服务相关角色，允许 License Manager 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
<code>iam:CreateServiceLinkedRole</code>	<code>arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement</code>
<code>iam:CreateServiceLinkedRole</code>	<code>arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com</code>

操作	资源 ARN
	/AWSServiceRoleFor AWSLicenseManagerM emberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license- manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license- manager-service-*
s3:ListAllMyBuckets	*
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:ListAWSServiceAccessFo rOrganization	*
organizations:DescribeOrganization	*

操作	资源 ARN
<code>organizations:ListDelegatedAdministrators</code>	*
<code>license-manager:GetServiceSettings</code>	*
<code>license-manager:GetLicense*</code>	*
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*
<code>license-manager:List*</code>	*

要在中查看此策略的权限 AWS Management Console，请参阅 [AWSLicenseManagerServiceRolePolicy](#)。

AWS 托管策略：AWSLicenseManagerMasterAccountRolePolicy

此策略附加AWSServiceRoleForAWSLicenseManagerMasterAccountRole到名为的服务相关角色，允许 License Manager 代表您调用对中央管理帐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
<code>s3:GetBucketLocation</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:ListBucket</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:GetLifecycleConfiguration</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>
<code>s3:PutLifecycleConfiguration</code>	<code>arn:aws:s3:::aws-license-manager-service-*</code>

操作	资源 ARN
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-*
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

操作	资源 ARN
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	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram>DeleteResourceShare	*

操作	资源 ARN
<code>resource-groups:PutGroupPolicy</code>	*
<code>iam:GetRole</code>	*
<code>iam:PassRole</code>	<code>arn:aws:iam::*:role/LicenseManagerServiceResourceDataSyncRole*</code>
<code>cloudformation:UpdateStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation>CreateStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation>DeleteStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>

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 托管策略：AWSLicenseManagerMemberAccountRolePolicy

此策略附加AWSServiceRoleForAWSLicenseManagerMemberAccountRole到名为的服务相关角色，允许 License Manager 代表您从已配置的管理账户调用许可证管理API操作。有关更多信息，请参阅 [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
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*
<code>license-manager:GetLicenseConfiguration</code>	*
<code>ssm:ListInventoryEntries</code>	*
<code>ssm:GetInventory</code>	*
<code>ssm:CreateAssociation</code>	*
<code>ssm:CreateResourceDataSync</code>	*
<code>ssm>DeleteResourceDataSync</code>	*
<code>ssm:ListResourceDataSync</code>	*

操作	资源 ARN
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策略附加到您的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，请参阅 [卖家在 License Manager 中颁发的许可证使用情况](#)。

要查看此策略的权限，请参阅 [AWSLicenseManagerConsumptionPolicy](#)在 AWS Management Console。

AWS 托管策略：AWSLicenseManagerUserSubscriptionsServiceRolePolicy

此策略附加到名为策略的服务相关角色，允许 L

AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService icense Manager 调用 API操作来管理基于用户的订阅资源。有关更多信息，请参阅 [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	*

操作	资源 ARN
ec2: DescribeNetworkInterfaces	*
ec2: DescribeSecurityGroupRules	*
ec2: DescribeSubnets	*
ec2: DescribeVpcPeeringConnections	*
ec2: TerminateInstances	arn:aws:ec2:*:*:instance/* ¹
53 号公路 : GetHostedZone	*
53 号公路 : ListResourceRecordSets	*
秘密管理器 : GetSecretValue	arn:aws:secretsmanager:*:*:secret:* license-manager-user
ssm : DescribeInstanceInformation	*
ssm : GetCommandInvocation	*
ssm : GetInventory	*
ssm : ListCommandInvocations	*
ssm : SendCommand	arn:aws:ssm:*::document/- ² AWS RunPowerShellScript 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、值为的实例上使用AWS-RunPowerShellScript文档执行SSM运行命令UserSubscriptions。

要在中查看此策略的权限 AWS Management Console，请参阅 [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。

AWS 托管策略：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

此策略附加到名为策略的服务相关角色中，允许 L

AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService icense Manager 调用API操作来管理 Linux 订阅资源。有关更多信息，请参阅 [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	Conditions	资源
ec2:DescribeInstances	不适用	*
ec2:DescribeRegions	不适用	*
organizations:DescribeOrganization	不适用	*
organizations:ListAccounts	不适用	*
organizations:DescribeAccount	不适用	*
organizations:ListChildren	不适用	*
organizations:ListParents	不适用	*
organizations:ListAccountsForParent	不适用	*
organizations:ListRoots	不适用	*
organizations:ListAWSServiceAccessForOrganization	不适用	*

操作	Conditions	资源
organizations:ListDelegatedAdministrators	不适用	*
秘密管理器 : GetSecretValue	StringEquals: “aws:ResourceTag/”: LicenseManagerLinuxSubscriptions “已启用” “aws:ResourceAccount “: “\${aws:PrincipalAccount}”	arn:aws:secretsmanager:*:*:secret:*
kms:Decrypt	StringEquals: “aws:ResourceTag/”: LicenseManagerLinuxSubscriptions “已启用”, “aws:ResourceAccount “: “\${aws:PrincipalAccount}” StringLike: “kms:”: [ViaService“secretmanager.*.amazonaws.com”]	arn:aws:kms:*:*:key/*

要在中查看此策略的权限 AWS Management Console，请参阅 [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

License Manager 更新 AWS 了托管策略

查看自该服务开始跟踪这些更改以来，License Manager AWS 托管策略更新的详细信息。

更改	描述	日期
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – 对现有策略的更新	License Manager 添加了以下权限来管理许可和 Active Directory 数据：从 Route 53 获取路线信息，从亚马逊获取网络信息和安全组规则EC2，以及从 Secrets Manager 获取机密。	2024 年 11 月 7 日
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy – 更新现有策略	License Manager 增加了存储和检索密钥的权限 AWS Secrets Manager，以及使用 AWS KMS 密钥解密自带许可证 (BYOL) 订阅的访问令牌密钥的权限。	2024 年 5 月 22 日
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy : 新策略	License Manager 添加了创建名为 AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService 的服务相关角色的权限。此角色提供 License Manager 列出 AWS Organizations 和亚马逊EC2资源的权限。	2022 年 12 月 21 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – 更新现有策略	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。此角色为 License Manager 提供了列出	2022 年 7 月 18 日

更改	描述	日期
	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 – 更新现有策略	License Manager 为管理的资源组添加了 <code>resource-groups:PutGroupPolicy</code> 权限 AWS Resource Access Manager。	2022 年 6 月 27 日
AWSLicenseManagerMasterAccountRolePolicy – 更新现有策略	License Manager 将的 AWS 托管策略AWSLicenseManagerMasterAccountRolePolicy 条件密钥 AWS Resource Access Manager 从使用 <code>ram:ResourceTag</code> 更改为 <code>aws:ResourceTag</code> 。	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 – 更新现有策略	License Manager 添加了列出委托管理员的权限和创建名为 <code>AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code> 的服务相关角色的权限。	2021 年 6 月 16 日
AWSLicenseManagerServiceRolePolicy – 更新现有策略	License Manager 添加了列出所有 License Manager 资源 (例如许可证配置、许可证和授予) 的权限。	2021 年 6 月 15 日

更改	描述	日期
AWSLicenseManagerServiceRolePolicy – 更新现有策略	License Manager 添加了创建名为 <code>AWSServiceRoleForMarketplaceLicenseManagement</code> 的服务相关角色的权限。此角色 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 开始跟踪其 AWS 托管策略的更改。	2021 年 3 月 9 日

在 License Manager 中对许可证进行加密签名

License Manager 可以用加密方式签署由 ISV 或通过颁发的许可证 AWS Marketplace 代表 ISV。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。

要签署许可证，License Manager 使用非对称的 AWS KMS key 属于 ISV 并受保护 AWS Key Management Service (AWS KMS)。该客户管理的 CMK 由数学上相关的公钥和私钥 pair 组成。当用户申请许可时，License Manager 会生成一个列出许可权利的对象，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，请参阅 AWS KMS，请参阅[使用对称和非对称密钥](#)。

Note

License Manager 称之为 AWS KMS [Sign](#) 以及签署和验证许可证时的 [Verify](#) API 操作。的密钥使用值 CMK 必须为 [SIGN](#) 才能 VERIFY 用于这些操作。这种类型 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，或者SDK，许可证管理员创建非对称客户托管CMK。CMK必须具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CMKs](#)和[如何选择CMK配置](#)。
2. 在 License Manager 中，许可管理员创建的使用配置包括 AWS KMS ARN或身份证。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，同时还会返回列出授权的JSON对象。明文JSON类似于以下内容：

```
{
  "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:1-6585590917ad46858328ff02dEXAMPLE",
  "licenseConsumptionToken":"306eb19afd354ba79c3687b9bEXAMPLE",
  "nodeId":"100.20.15.10",
  "checkoutMetadata":{
    "Mac":"ABCDEFGHI"
  }
}
```

License Manager 的合规性验证

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：

- [Security Compliance & Governance](#)：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- [在 Amazon Web Services 上进行HIPAA安全与合规架构](#) — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

Note

并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《[HIPAA符合条件的服务参考](#)》。

- [AWS 合规资源AWS](#) — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- [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 提供了您内部安全状态的全面视图 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 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- [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。

License Manager 中的弹性

这些区域有：AWS 全球基础设施是围绕着建立的 AWS 地区和可用区。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 地区和可用区，请参阅 [AWS 全球基础设施](#)。

License Manager 中的基础架构安全

作为一项托管服务，AWS License Manager 受保护 AWS 全球网络安全。有关信息 AWS 安全服务及其方式 AWS 保护基础架构，请参阅 [AWS 云安全](#)。设计你的 AWS 使用基础设施安全最佳实践的环境，请参阅安全支柱中的 [基础设施保护](#) AWS 架构精良的框架。

你用 AWS 已发布通过网络访问 License Manager 的API呼叫。客户端必须支持以下内容：

- 传输层安全 (TLS)。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 具有完美前向保密性的密码套件 ()，例如 (Ephemeral Diffie-HellmanPFS) 或 (Elliptic C DHE urve Ephemeral Diffie-Hellman)。ECDHE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委托人关联的私有访问密钥对请求进行签名。或者你可以使用 [AWS Security Token Service](#) (AWS STS) 生成用于签署请求的临时安全证书。

License Manager 和接口VPC端点与 AWS PrivateLink

您可以在虚拟私有云 (VPC) 和之间建立私有连接 AWS License Manager 通过创建接口VPC端点。接口端点由 [AWS PrivateLink](#)，一种API无需互联网网关、NAT设备、VPN连接即可私密访问 License Manager 的技术 AWS Direct Connect 连接。您中的实例VPC不需要公有 IP 地址即可与 License Manager 通信。您VPC和 License Manager 之间的流量不会离开亚马逊网络。

每个接口端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[接口VPC终端节点 \(AWS PrivateLink\)](#) 在《亚马逊VPC用户指南》中。

为 License Manager 创建接口VPC端点

使用以下服务名称之一为 License Manager 创建接口终端节点：

- com.amazonaws.**region**.许可证管理器
- com.amazonaws.**region**.license-manager-fips

如果您DNS为终端节点启用私有功能，则可以使用该区域的默认DNS名称向 License Manager API 发出请求。例如，`license-manager.region.amazonaws.com`。

有关更多信息，请参阅 Amazon VPC 用户指南中的[创建接口终端节点](#)。

为 License Manager 创建VPC端点策略

您可以将策略附加到VPC终端以控制对 License Manager 的访问。该策略指定以下信息：

- 可执行操作的主体
- 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](#)。

对许可证管理器进行故障排除

以下信息可以帮助您在使用时解决问题 AWS License Manager。在开始之前，请确认您的 License Manager 设置满足中所述的要求[License Manager 中的设置](#)。

跨账户发现错误

在设置跨账户发现时，您可能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 管理的数据目录而不是 AWS Glue Data Catalog。有关升级说明，请参阅[升级到 AWS Glue 数据目录分步进行](#)。

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了其账户中的 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服务关联角色 (SLR)，并且有成员拥有的资源与自我管理的许可证相关联，则该管理账户将无法解除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关联资源，请恢复 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。

注销的明显持续存在 AMI

License Manager 每隔几个小时就会清除一次资源和自我管理许可证之间的过时关联。如果通过亚马逊注销了与自我管理许可证 AMI 相关的许可，则在清除之前 EC2，AMI 可能会短暂地继续出现在 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。您可以通过编辑更新脚本来更改更新脚本 `LicenseManagerResourceSynDataProcessJobTrigger` 的运行频率。AWS Glue 管理账户的控制台。

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我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我管理许可证。

链接 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。

License Manager 的文档历史记录

下表描述了的版本 AWS License Manager。

更改	描述	日期
增加了对 Microsoft 远程桌面服务订阅者访问许可证 (RDSSAL) 基于用户的订阅的支持	License Manager 增加了对管理和配置RDSSAL基于用户的订阅的支持，包括能够一次配置两个以上的远程桌面连接。	2024 年 11 月 14 日
更新了基于用户的订阅SLR托管策略以获取路线和网络信息	License Manager 添加了以下权限来管理许可和 Active Directory 数据：从 Route 53 获取路线信息，从亚马逊获取网络信息和安全组规则EC2，以及从 Secrets Manager 获取机密。有关更多信息，请参阅 AWS 托管策略：AWSLicenseManagerUserSubscriptionsServiceRolePolicy 。	2024 年 11 月 7 日
从红帽BYOL订阅管理器检索订阅信息 (RHSM)	License Manager 增加了从中 RHSM检索红帽企业 Linux 实例上BYOL许可证的订阅信息的支持。这包括对以下内容的更新 AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 。	2024 年 7 月 10 日
为CPU基BYOL于 Db2 v RDS 的许可证增加了对 Amazon 的支持	License Manager 增加了对亚马逊RDS对CPU基于 Db2 v 的BYOL许可证的支持。	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 通过亚马逊提供的亚马逊微软 Office Profession LTSC al Plus 2021 许可证，在亚马	2023 年 12 月 4 日

更改	描述	日期
	逊机器映像 (AMIs) 中增加了对 Windows Server 2019 的支持。EC2	
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
Ubun LTS tu 订阅的许可证类型转换	License Manager 增加了对 Ubuntu LTS 实例的支持, 即使用许可证类型转换来添加 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
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

更改	描述	日期
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 License Manager 控制台，在 AWS 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)	在 AWS 提供的许可和自带许可模式 (BYOL) 之间更改许可证类型，AWS CLI 无需重新部署现有工作负载。	2021 年 9 月 22 日
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 IDs 和标签从 License Manager 自动发现中排除实例。	2021 年 3 月 5 日

更改	描述	日期
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	将您的自行管理的许可证和与您的 AWS 账户 AMIs 共享的许可证相关联。	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 Oracle 在亚马逊上的部署 RDS	跟踪 Amazon 上的 Oracle 数据库引擎版本和许可包的许可证使用情况RDS。	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
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，并将相应的自我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

更改	描述	日期
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。