



使用者指南

# AWS License Manager



# AWS License Manager: 使用者指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 AWS License Manager ? .....	1
受管權利 .....	1
License Manager 使用案例 .....	2
相關服務 .....	2
License Manager 的運作方式 .....	4
授權管理工作流程中的授權資產群組 .....	6
與現有 License Manager 功能的關係 .....	6
授權資產群組使用案例 .....	6
開始使用 .....	7
使用 License Manager .....	8
授權資產群組 .....	9
了解 AWS License Manager 授權資產群組 .....	9
授權資產群組入門 .....	10
使用授權資產群組 .....	11
使用授權資產規則集 .....	16
自我管理的授權 .....	23
參數和規則 .....	24
從廠商授權建置規則 .....	26
建立自我管理的授權 .....	27
共用自我管理的授權 .....	29
編輯自我管理的授權 .....	33
檢視自我管理的授權 .....	34
停用自我管理的授權 .....	35
刪除自我管理的授權 .....	36
自我管理授權規則 .....	36
授予的授權 .....	38
檢視您授予的授權 .....	39
管理您授予的授權 .....	40
分佈權利 .....	42
授予接受和啟用 .....	44
授權狀態 .....	46
買方帳戶的指標 .....	47
授權分析 .....	48
主要儀表板檢視 .....	48

個別授權資產群組檢視 .....	49
建立用量報告 .....	50
庫存搜尋 .....	52
使用庫存搜尋 .....	53
自動化探索庫存 .....	59
授權類型轉換 .....	61
合格授權類型 .....	62
先決條件 .....	70
轉換授權類型 .....	73
租用轉換 .....	85
疑難排解 .....	87
主機資源群組 .....	88
建立主機資源群組 .....	89
共用主機資源群組 .....	90
將專用主機新增至主機資源群組 .....	90
在主機資源群組中啟動執行個體 .....	91
修改主機資源群組 .....	91
從主機資源群組移除專用主機 .....	91
刪除主機資源群組 .....	92
以使用者為基礎的訂閱 .....	92
考量事項 .....	93
License Manager 中的訂閱費用 .....	94
以使用者為基礎的訂閱先決條件 .....	98
支援的軟體訂閱 .....	106
Active Directory .....	108
其他軟體 .....	108
開始使用 .....	109
為更多工作階段設定 GPO .....	117
跨帳戶授權管理員 .....	118
從包含的授權 AMI 啟動執行個體 .....	124
連接至執行個體 .....	126
修改 Microsoft Office 的防火牆設定 .....	126
管理訂閱使用者 .....	127
取消註冊 Active Directory .....	129
疑難排解 .....	129
管理 Linux 訂閱 .....	140

設定探索 .....	141
檢視執行個體資料 .....	146
帳單資訊 .....	148
管理 CloudWatch 警示 .....	150
賣方發行的授權 .....	153
權利 .....	153
授權用量 .....	154
所需的許可 .....	154
建立賣方發行的授權 .....	156
授予賣方發行的授權 .....	157
ISV 客戶的臨時登入資料 .....	158
查看賣方發行的授權 .....	159
刪除賣方發行的授權 .....	160
設定 .....	160
編輯 License Manager 設定 .....	162
受管授權設定 .....	162
Linux 訂閱設定 .....	164
以使用者為基礎的訂閱設定 .....	166
委派管理員設定 .....	167
監控 License Manager .....	172
使用 CloudWatch 進行監控 .....	172
建立 CloudWatch 警示 .....	174
CloudTrail 日誌 .....	174
CloudTrail 中的 License Manager 資訊 .....	175
了解 License Manager 日誌檔案項目 .....	176
安全 .....	177
資料保護 .....	177
靜態加密 .....	178
身分與存取管理 .....	178
建立使用者、群組和角色 .....	179
IAM 政策結構 .....	179
建立 License Manager 的 IAM 政策 .....	180
向使用者、群組和角色授予許可 .....	181
服務連結角色 .....	182
核心角色 .....	182
管理帳戶角色 .....	185

成員帳戶角色 .....	186
以使用者為基礎的訂閱角色 .....	188
Linux 訂閱角色 .....	190
AWS 受管政策 .....	191
AWSLicenseManagerServiceRolePolicy .....	192
AWSLicenseManagerMasterAccountRolePolicy .....	194
AWSLicenseManagerMemberAccountRolePolicy .....	198
AWSLicenseManagerConsumptionPolicy .....	199
AWSLicenseManagerUserSubscriptionsServiceRolePolicy .....	199
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy .....	201
政策更新 .....	202
授權簽署 .....	205
法規遵循驗證 .....	207
恢復能力 .....	207
基礎架構安全 .....	207
使用的 VPC 端點 AWS PrivateLink .....	207
建立 License Manager 的介面 VPC 端點 .....	208
建立 License Manager 的 VPC 端點政策 .....	208
疑難排解 .....	210
跨帳戶探索錯誤 .....	210
管理帳戶無法取消資源與自我管理授權的關聯 .....	210
Systems Manager 庫存已過期 .....	210
取消註冊 AMI 的明顯持久性 .....	210
新的子帳戶執行個體在資源庫存中顯示的速度很慢 .....	211
啟用跨帳戶模式後，子帳戶執行個體的顯示速度會變慢 .....	211
無法停用跨帳戶探索 .....	211
子帳戶使用者無法將共用自我管理授權與執行個體建立關聯 .....	211
連結 AWS Organizations 帳戶失敗 .....	211
文件歷史紀錄 .....	212
.....	ccxvii

# 什麼是 AWS License Manager ？

AWS License Manager 可讓您更輕鬆地管理組織中多個 AWS 區域和帳戶的軟體廠商（例如 Microsoft、SAP、Oracle 和 IBM）的軟體授權，提供整合的可見性和全方位的報告，以實現大規模的軟體授權合規。這可讓您限制授權超額，並降低不合規和報告錯誤的風險。

在建置雲端基礎設施時 AWS，您可以使用自有授權模型 (BYOL) 機會來節省成本。也就是說，您可以重新利用現有的授權庫存，以與雲端資源搭配使用。

License Manager 透過直接繫結至 AWS 服務的庫存追蹤，降低授權超額和懲罰的風險。透過以規則為基礎的授權使用控制，管理員可以對新的和現有的雲端部署設定硬性或軟性限制。根據這些限制，License Manager 會在不合規的伺服器使用發生之前協助停止。

License Manager 的內建儀表板可讓您持續查看授權用量，並協助進行廠商稽核。

License Manager 支援追蹤根據虛擬核心 (vCPUs)、實體核心、通訊端或機器數量授權的任何軟體。這包括 Microsoft、IBM、SAP、Oracle 和其他廠商的各類軟體產品。

使用 AWS License Manager，您可以透過維護所有已簽出權利的計數，集中追蹤授權並強制執行跨多個區域的限制。License Manager 也會追蹤最終使用者身分和基礎資源識別符，如果可用的話，與每次簽出相關聯，以及簽出時間。此時間序列資料可透過 CloudWatch 指標和事件追蹤至 ISV。ISVs 可以將此資料用於分析、稽核和其他類似用途。

AWS License Manager 已與 [AWS Marketplace](#) 和 [AWS Data Exchange](#) 整合，並與下列 AWS 服務整合：[AWS Identity and Access Management \(IAM\)](#)、[AWS Organizations](#)、Service Quotas、[CloudFormation](#) AWS 資源標記和 [AWS X-Ray](#)。

## 受管權利

透過 License Manager，授權管理員可以跨帳戶和整個組織分發、啟用和追蹤軟體授權。

獨立軟體廠商 (ISVs) 可以透過受管權利，使用 AWS License Manager 來管理和分發軟體授權和資料給最終使用者。身為發行者，您可以使用 License Manager 儀表板集中追蹤賣方發行的授權使用情況。透過銷售 ISVs AWS Marketplace 受益於交易工作流程中的自動授權建立和分發。ISVs 也可以使用 License Manager 來建立授權金鑰，並為沒有 AWS 帳戶的客戶啟用授權。

License Manager 使用開放、安全、業界標準來代表授權，並允許客戶以密碼編譯方式驗證其真實性。License Manager 支援各種不同的授權模式，包括永久授權、浮動授權、訂閱授權和用量型授權。如果您有必須鎖定節點的授權，License Manager 會提供以這種方式取用授權的機制。

您可以在 中建立授權 AWS License Manager ，並使用 IAM 身分或透過 產生的數位簽章權杖將授權分發給最終使用者 AWS License Manager。使用的最終使用者可以 AWS 進一步將授權權利重新分配到其各自組織中的 AWS 身分。具有分散式權利的最終使用者可以透過與 的軟體整合，從該授權簽出和簽入所需的權利 AWS License Manager。每個授權簽出都會指定權利、相關數量和簽出期間，例如 10 個 1 小時 `admin-users` 的簽出時間。此簽出可以根據分散式授權的基礎 IAM 身分，或根據 AWS License Manager 服務產生的長期字串來執行 AWS License Manager 。

## License Manager 使用案例

以下是 License Manager 為各種使用案例提供的 功能範例：

- [License Manager 中的自我管理授權](#) – 用來根據企業協議的條款，定義單一 AWS 帳戶中自我管理授權的授權規則。對於多帳戶案例，請考慮使用授權資產群組進行集中式控管。
- [授權資產群組](#) – 用於集中管理和追蹤組織中多個 AWS 區域和帳戶的授權。
- [賣方在 License Manager 中發行的授權](#) – 用來管理和分發軟體授權給最終使用者。
- [License Manager 中授予的授權](#) – 用來控管使用從 取得的授權 AWS Marketplace AWS Data Exchange，或直接從整合其軟體與受管權利的賣方取得的授權。可以使用授權資產群組，在單一帳戶內或集中管理多個帳戶。
- [License Manager 中的授權類型轉換](#) – 用於在 AWS 提供的授權和自攜授權模型 (BYOL) 之間變更授權類型，而無需重新部署工作負載。
- [License Manager 中的庫存搜尋](#) – 用於使用 AWS Systems Manager 庫存和授權規則來探索和追蹤內部部署應用程式。
- [針對支援的軟體產品使用 License Manager 使用者型訂閱](#) – 用來為支援的軟體購買完全相容的 Amazon 提供的授權，每個使用者需支付 訂閱費。
- [在 License Manager 中管理 Linux 訂閱](#) – 用來檢視和管理您擁有並執行的商業 Linux 訂閱 AWS。

## 相關服務

License Manager 已與 Amazon EC2 AWS Marketplace AWS Systems Manager、Amazon RDS 和 整合 AWS Organizations。

Amazon EC2 整合可讓您追蹤下列資源的授權，並在整個資源生命週期強制執行授權規則：

- [Amazon EC2 執行個體](#)
- [專用執行個體](#)

- [專用主機](#)
- [Spot 執行個體和 Spot 機群](#)
- [受管節點](#)

搭配使用 License Manager 與 時 AWS Systems Manager，您可以在外部託管的實體或虛擬伺服器上管理授權 AWS。您可以使用 License Manager 搭配 AWS Organizations 集中管理所有組織帳戶。

此外，您可以控管從 購買授權 AWS Marketplace 的使用 AWS Data Exchange，或直接從與其軟體整合的賣方購買授權 AWS License Manager。您可以使用 AWS License Manager 將稱為權利的使用權分發給特定 AWS 帳戶。

License Manager 與 Amazon RDS for Oracle 和 Amazon RDS for Db2 vCPU 型 BYOL 授權整合。透過此整合，您可以了解 RDS for Oracle 和 RDS for Db2 資料庫執行個體的 vCPU 用量。您可以使用此資料，根據您與資料庫管理系統廠商的授權條款來計算耗用的授權數量。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的下列相關連結。

- [RDS for Oracle 授權選項](#)
- [RDS for Db2 授權選項](#)

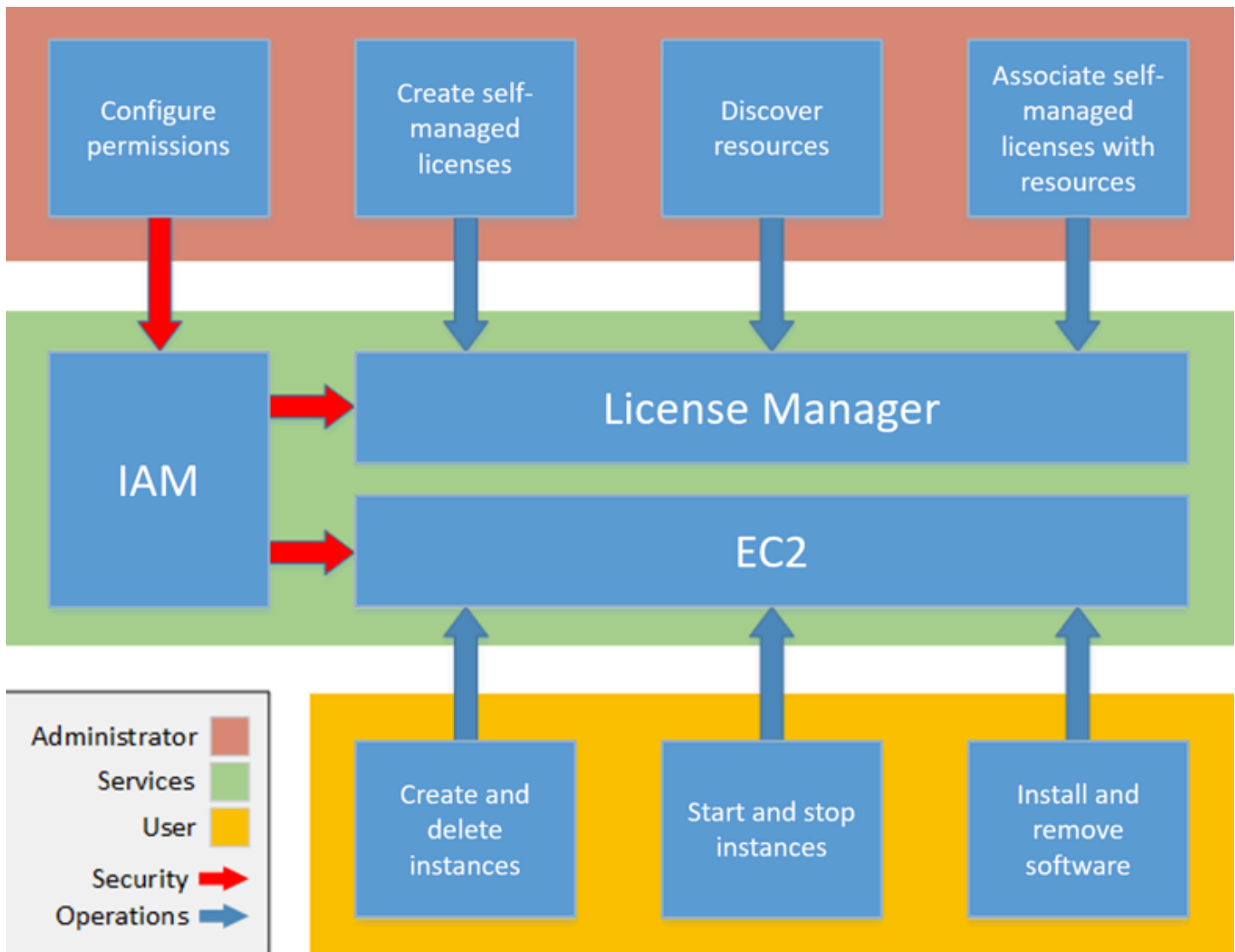
# License Manager 的運作方式

有效的軟體授權管理需仰賴以下要素：

- 精通企業授權協議語言的專家
- 應適當限制會使用授權的操作存取權限
- 準確追蹤授權庫存

企業可能會設立專門人員或團隊負責處理上述各項領域。然後，它會成為有效通訊的問題，特別是授權專家和系統管理員之間。License Manager 提供從各種網域集區知識的方法。重要的是，它還原生整合了 AWS 服務，例如，與建立和刪除執行個體的 Amazon EC2 控制平面。這表示 License Manager 規則和限制會擷取業務和操作知識，也會轉換為執行個體建立和應用程式部署的自動化控制。

下圖說明透過 Amazon EC2 主控台管理許可和設定 License Manager 以及建立、管理和刪除資源之使用者之授權管理員的不同但協調職責。



如果您負責管理組織中的授權，您可以使用 License Manager 來設定授權規則、將其連接至您的啟動，以及追蹤用量。如此一來，組織內的使用者即可直接新增或移除使用授權的資源，無需進行其他操作。

授權資產群組透過提供跨多個 AWS 區域和帳戶的全組織授權管理來擴展此功能。授權資產群組不會在每個區域和帳戶中個別管理授權，而是將授權資訊合併為統一檢視，從而在整個 AWS Organizations 中實現集中式監督和自動化合規監控。

一般來說，授權專家需負責管理整個組織的全部授權、判斷資源庫存需求、監督授權採購作業，同時推動所有人員使用合規授權。在使用 License Manager 的企業中，此工作是透過 License Manager 主控台合併。如下圖所示，這涉及設定服務許可、建立自我管理的授權、清查內部部署和雲端中的運算資源，以及將自我管理的授權與探索的資源建立關聯。透過授權資產群組，授權專家也可以建立集中式授權群組，自動探索和追蹤跨區域和帳戶的軟體，從而降低大規模管理授權的管理開銷。實際上，這

可能意味著將自我管理授權與 IT 用作所有 Amazon EC2 執行個體部署範本的已核准 Amazon Machine Image (AMI) 建立關聯。

License Manager 可節省因違反授權而遺失的成本。雖然內部稽核只會在事實發生之後才顯示違規，但當無法避免因不合規而受到懲罰時，License Manager 會防止發生昂貴的事件。License Manager 使用內建儀表板來簡化報告，顯示追蹤的授權耗用量和資源。

## 授權管理工作流程中的授權資產群組

授權資產群組為授權管理工作流程提供額外的組織層和自動化層。雖然傳統授權組態在個別授權層級運作，但授權資產群組在組織層級運作，提供跨多個區域和帳戶的合併檢視和自動化管理。

### 與現有 License Manager 功能的關係

授權資產群組補充和增強現有的 License Manager 功能：

- 授權組態 - 授權資產群組可以整合自我管理的授權組態和授予的授權，無論最初建立或取得授權的方式為何，都能提供統一的檢視。
- 庫存搜尋 - 授權資產群組使用與庫存搜尋相同的探索機制，但會根據規則集自動分組和持續監控探索的資源。
- 用量報告 - 授權資產群組會產生涵蓋多個區域和帳戶的全面報告，提供個別授權報告無法實現的全組織可見性。
- 跨帳戶管理 - 授權資產群組專為多帳戶案例而設計，與 AWS Organizations 無縫合作，提供集中式授權控管。

### 授權資產群組使用案例

在下列案例中，授權資產群組特別有價值：

- 多區域部署 - 當您的組織跨多個 AWS 區域執行工作負載，並且需要合併的授權追蹤，而無需單獨管理每個區域。
- 多帳戶組織 - 使用具有多個帳戶的 AWS Organizations 時，需要管理或委派管理員帳戶的集中授權監督。
- 自動化合規監控 - 當您需要在整個 AWS 環境中主動授權過期通知和自動化合規追蹤時。
- 稽核準備 - 當您需要完整、全組織的授權用量報告，以進行廠商稽核或內部合規審查時。

# License Manager 入門

若要使用 AWS License Manager，您必須先完成加入步驟。下列程序會逐步引導您完成 中的加入步驟 AWS 管理主控台。

## License Manager 入門

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 系統會提示您設定 License Manager 及其支援服務的許可。依照指示設定必要的許可。
3. 完成初始設定後，您就可以針對所需的 繼續使用 License Manager [License Manager 使用案例](#)。

如需在遵循 AWS 最佳實務時，管理使用者、群組和角色使用 License Manager 許可的詳細資訊，請參閱 [License Manager 的身分和存取管理](#)。如需設定與 License Manager 整合之 Amazon EC2 資源的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [設定以使用 Amazon EC2](#)。

# 使用 License Manager

License Manager 可以套用到具有混合 AWS 資源基礎設施和內部部署資源的企業的標準案例。您可以建立自我管理的授權、清查耗用授權的資源、將自我管理的授權與資源建立關聯，以及追蹤清查和合規。

## AWS Marketplace 產品的授權

使用 License Manager，您現在可以透過 Amazon EC2 啟動範本、AWS CloudFormation 範本或 Service Catalog 產品，將授權規則與 AWS Marketplace BYOL AMI 產品建立關聯。在每個案例中，您將享有集中化授權追蹤和合規強制執行的優勢。

### Note

License Manager 不會變更您從 Marketplace 取得和啟用 BYOL AMIs 的方式。在啟動後，您必須提供直接從賣方取得的授權金鑰以啟用任何第三方軟體。

## 追蹤現場部署資料中心資源的授權

使用 License Manager，您可以探索在外部 AWS 使用 [Systems Manager 庫存](#) 執行的應用程式，然後將授權規則連接到這些應用程式。連接授權規則後，您可以在 License Manager 主控台中追蹤內部部署伺服器以及 AWS 資源。

## 區分包含的授權和 BYOL

使用 License Manager，您可以識別哪些資源具有包含在產品中的授權，以及哪些資源使用您擁有的授權。這可讓您準確報告如何使用 BYOL 授權。此篩選條件需要 SSM 2.3.722.0 版或更新版本。

## 您 AWS 帳戶間的 License Manager

License Manager 可讓您跨 AWS 帳戶管理授權。您可以在 AWS Organizations 管理帳戶中建立一次授權組態，並使用 AWS Resource Access Manager 或使用 License Manager 設定連結 AWS Organizations 帳戶，在帳戶中共用這些組態。這也可讓您執行跨帳戶探索，以跨 AWS 帳戶搜尋庫存。

## 目錄

- [授權資產群組](#)
- [License Manager 中的自我管理授權](#)

- [License Manager 中授予的授權](#)
- [授權分析](#)
- [License Manager 中的庫存搜尋](#)
- [License Manager 中的授權類型轉換](#)
- [License Manager 中的主機資源群組](#)
- [針對支援的軟體產品使用 License Manager 使用者型訂閱](#)
- [在 License Manager 中管理 Linux 訂閱](#)
- [賣方在 License Manager 中發行的授權](#)
- [License Manager 中的設定](#)

## 授權資產群組

授權資產群組提供集中式方法來管理和監控您 AWS 環境中的授權用量。您可以分組相關資產、套用授權規則，以及從管理帳戶或委派管理員帳戶追蹤合規性。

### 目錄

- [了解 AWS License Manager 授權資產群組](#)
- [授權資產群組入門](#)
- [使用授權資產群組](#)
- [使用授權資產規則集](#)

## 了解 AWS License Manager 授權資產群組

中的授權資產群組 AWS License Manager 提供組織內跨 AWS 區域和帳戶的集中授權管理，提供合併可見性、自動化通知，以及軟體授權合規的完整報告。

### 什麼是授權資產群組

授權資產群組是內的容器 AWS License Manager，會根據使用者定義的規則來合併授權及其相關聯的 EC2 執行個體。這些群組提供整個 AWS Organizations 軟體授權狀態的統一檢視，無論授權和執行個體所在的區域或帳戶為何。

授權資產群組的運作方式是套用規則集，定義哪些授權和執行個體屬於一起。例如，您可以建立「Windows Server」授權資產群組，追蹤所有 Windows Server 授權，以及整個組織中執行 Windows Server 的 EC2 執行個體。群組會根據您設定的規則，自動探索並包含相關資源。

系統支援 Microsoft Windows Server、SQL Server、Red Hat Enterprise Linux、Ubuntu Pro 和 SUSE Enterprise Linux 等常見軟體產品的兩種 AWS 受管規則集，以及您可以為特定授權需求建立的自訂規則集。

## 主要功能和元件

### 集中授權可見性

授權資產群組會將多個 AWS 區域的授權資訊彙總為單一檢視。這種跨區域可見性無需個別檢查每個區域，即可了解組織的軟體授權狀態。群組會使用 AWS Systems Manager 代理程式自動探索工作負載上執行的軟體產品，並合併此資訊，以取得整個組織的可見性。

### 彈性的規則型組織

授權資產群組使用規則集來定義其追蹤和維護的授權和執行個體。群組和規則集之間的這種彈性關係可讓您根據業務需求來組織授權。您可以針對廣泛採用的產品使用 AWS 受管規則集，或為專用軟體建立自訂規則。

### 自動化合規監控

授權資產群組會透過 Amazon SNS 提供自動授權過期通知，協助您主動管理授權續約。授權使用會根據 vCPU、通訊端、執行個體或核心指標等定義的用量維度進行追蹤，以確保您持續了解授權義務。

## 與現有 AWS 服務整合

授權資產群組以現有 AWS License Manager 功能為基礎，並與數個 AWS 服務整合，以提供全方位的授權管理。此功能可與您可能已經在使用的授權組態和自動探索功能搭配使用。

若要啟用軟體探索，請在 EC2 執行個體上安裝 AWS Systems Manager 代理程式。對於多帳戶案例，您需要設定跨帳戶探索，並確保整個組織中 License Manager 操作的適當 IAM 許可。

## 授權資產群組入門

本節可協助您開始使用 中的授權資產群組 AWS License Manager。您將了解如何設定先決條件、設定來源區域，以及建立第一個授權資產群組。

### 先決條件

開始使用授權資產群組之前，請確定您有下列先決條件：

- AWS Systems Manager 安裝在 EC2 執行個體上的 (SSM) 代理程式
- 如果跨多個帳戶管理授權，則會設定跨帳戶探索

- 如果您是第一次加入，請遵循 [License Manager 入門指南](#) 來設定所有必要的許可

## 設定授權資產群組

### 設定來源區域

授權資產群組可在 AWS License Manager 提供的所有 AWS 商業區域中使用。跨區域探索需要在設定期間選取來源 AWS 區域。這可讓 License Manager 探索所選區域中的所有軟體。

### 使用主控台設定來源區域

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇設定，然後選擇授權資產探索和規則集。
3. 在授權資產探索區段中，選擇編輯。
4. 在區域探索下，選取您要從中探索產品的區域。
5. 如果您是組織擁有者，並想要探索所有組織帳戶，請選擇啟用。
6. 選擇儲存變更。

## 使用授權資產群組

本節說明如何在 中建立、更新、刪除和管理授權資產群組 AWS License Manager。授權資產群組可協助追蹤和管理跨 AWS 資源的授權。

### 建立授權資產群組

授權資產群組會追蹤和管理整個 AWS 資源的授權。您可以建立多個資產群組來組織不同的軟體產品，並隨時修改其設定，以適應您的授權需求。

#### Note

您可以使用一鍵式範本快速建立授權資產群組，或依照下列步驟，根據您的特定需求新增各種授權規則集，以手動建立授權資產群組。

### 使用主控台建立授權資產群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權資產探索和規則集。

3. 在授權資產探索區段中，確保區域探索填入區域。
4. 在授權資產規則集區段中，選取 AWS 受管規則集（針對特定受管產品設定的預設規則）AWS 或自訂規則集。請參閱 [???](#)。
5. 選擇使用規則集建立授權資產群組。
6. 針對授權資產群組名稱，輸入易記的名稱來記住如何分組資產。
7. （選用）針對授權資產群組描述，輸入如何分組資產的詳細說明。
8. 針對用量維度，選擇下列其中一個選項：vCPU、通訊端、執行個體或核心。此欄位決定資產的用量計算。
9. 選取一或多個授權資產規則集，建立新的規則集或從現有的 AWS 受管或自訂規則集新增。請參閱 [???](#)。
10. （選用）針對標籤，新增一或多個標籤。
11. 選擇建立授權資產群組。

#### Note

建立授權資產群組後，探索會自動開始，通常在 24 小時內完成。在此期間，License Manager 會掃描您設定的區域和帳戶，以識別符合您規則集條件的所有執行個體。

### 使用 CLI 建立授權資產群組

- 使用 `create-license-asset-group` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager create-license-asset-group \
  --name "Windows Server Group" \
  --description "License asset group for Windows Server instances" \
  --license-asset-group-configurations UsageDimension=vCPU \
  --associated-license-asset-ruleset-arns arn:aws:license-
manager:region:account:ruleset/ruleset-id \
  --client-token unique-token
```

### 更新授權資產群組

您可以更新授權資產群組來修改其組態、新增或移除規則集，以及更新標籤。

## 使用主控台更新授權資產群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權。
3. 在授權資產群組區段中，確保一或多個授權資產群組可用。
4. 若要選取要編輯的授權資產群組，請選取核取方塊，然後選擇動作、編輯。或者，選擇項目本身。
5. 選擇授權資產群組頁面上的編輯按鈕。從這裡，您可以：
  - 編輯授權資產群組名稱
  - 編輯授權資產群組描述
  - 新增或移除授權資產規則集
  - 新增或移除授權資產群組標籤
6. 當您完成變更時，請選擇儲存變更。

## 使用 CLI 更新授權資產群組

- 使用 `update-license-asset-group` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager update-license-asset-group \  
  --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-  
group/group-id \  
  --name "Updated Windows Server Group" \  
  --description "Updated description for Windows Server instances"
```

## 刪除授權資產群組

您可以刪除不再需要的授權資產群組。請注意，此動作無法復原，且不會刪除與授權資產群組相關聯的規則集。

### 使用主控台刪除授權資產群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權。
3. 在授權資產群組區段中，確保一或多個授權資產群組可用。

- 若要選取要刪除的授權資產群組，請選取核取方塊，然後選擇動作、刪除。或者，選擇項目本身，然後從授權資產群組的頁面中選擇刪除按鈕。
- 若要永久刪除授權資產群組，請在文字方塊 **confirm** 中輸入 `confirm`，然後選擇刪除。

### Important

這個操作無法復原。與此授權資產群組相關聯的規則集將不會刪除。

## 使用 CLI 刪除授權資產群組

- 使用 `delete-license-asset-group` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager delete-license-asset-group \  
  --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-  
  group/group-id
```

## 檢視授權資產群組詳細資訊

您可以檢視授權資產群組的詳細資訊，包括相關聯的規則集、執行個體和授權。

### 使用主控台檢視授權資產群組詳細資訊

- 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
- 在導覽窗格中，選擇授權。
- 在授權資產群組區段中，確保一或多個授權資產群組可用。
- 若要檢視授權資產群組的詳細資訊，請選取核取方塊，然後選擇動作、檢視詳細資訊。或者，選擇項目本身。

### 使用 CLI 檢視授權資產群組

- 使用 `get-license-asset-group` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager get-license-asset-group \  
  --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-  
  group/group-id
```

```
--license-asset-group-arn arn:aws:license-manager:region:account:license-asset-  
group/group-id
```

## 列出授權資產群組

您可以列出帳戶中的所有授權資產群組，以檢視其狀態和組態。

### 使用主控台列出授權資產群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇授權資產群組。
3. 檢視具有其名稱、狀態和相關聯規則集的授權資產群組清單。

### 使用 CLI 列出授權資產群組

- 使用 `list-license-asset-groups` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager list-license-asset-groups \  
  --max-results 50 \  
  --next-token token-from-previous-call
```

## 列出授權資產群組的探索資產

檢視授權資產群組內相關聯的所有執行個體、授予的授權和自我管理授權，最多需要 24 小時的時間。執行個體、授予的授權和自我管理的授權的任何變更都會在 24 小時內反映。

### 使用主控台列出授權資產群組的資產

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權。
3. 選取核取方塊並選擇動作、檢視詳細資訊，以檢視授權資產群組的詳細資訊。或者，選擇項目本身。
4. 從授權資產群組的頁面，您可以檢視與授權資產群組相關聯的所有執行個體、授予的授權和自我管理的授權。

## 使用 CLI 列出授權資產群組的資產

- 使用 `list-assets-for-license-asset-group` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager list-assets-for-license-asset-group \
  --license-asset-group-arn arn:aws:license-manager:region:account:license-asset-
  group/group-id
```

## 使用授權資產規則集

本節說明如何在 中建立、更新、刪除和管理授權資產規則集 AWS License Manager。授權資產規則集會定義授權資產群組的資源探索條件。

### 了解規則集

規則集是 License Manager 中的資源，可定義產品的資源探索條件。它可作為相關規則的邏輯分組，可用於產品探索，而規則集可用於不同的產品。

規則集有兩種不同類型：

- AWS 受管規則集 - 由 License Manager 服務建立和維護
- 自訂規則集 - 由客戶建立和管理

規則集的主要優點是可將新規則新增至規則集，而這些變更會使用自動用來探索產品的相同規則集，自動反映在所有授權資產群組中。

### 規則集類型

#### 授權型

適用於自我管理或授予的授權，包括 AWS Marketplace 產品

#### 執行個體型

根據特定屬性探索執行個體

每個規則集包含最多 5 個規則，定義如何探索和追蹤您的軟體。您可以建立規則來識別授權、執行個體或兩者，並使用 AND、OR 或完全相符的邏輯結合多個條件，以精確鎖定您要管理的資源。

下表顯示您可以在建立授權資產規則集規則時使用的可用金鑰：

### 授權資產規則集規則金鑰

規則類型	金鑰	運算子	值類型	接受的值
自我管理授權	授權組態 ARN	等於、不等於	清單	有效 ARN
	AWS 帳戶 ID	等於、不等於	清單	String
授予的授權	授權 ARN	等於、不等於	清單	有效 ARN
	產品 SKU	等於、不等於	清單	String
	發行者	等於、不等於	清單	String
	受益人	等於、不等於	清單	String
	授權狀態	等於、不等於	清單	有效授權狀態
	主區域	等於、不等於	清單	有效 AWS 區域
執行個體	平台	等於、不等於	清單	Windows , Linux
	EC2 帳單產品	等於、不等於	清單	windows-server-enterprise、windows-byol、sql-server-standard、sql-server-enterprise、rhel、rhe

規則類型	金鑰	運算子	值類型	接受的值
				l-byol、rhel-high-availability、ubuntu-pro、suse-linux
	Marketplace 產品程式碼	等於、不等於	清單	String
	AMI ID	等於、不等於	清單	String
	執行個體類型	等於、不等於	清單	String
	執行個體 ID	等於、不等於	清單	String
	主機 ID	等於、不等於	清單	String
	AWS 帳戶 ID	等於、不等於	清單	String

## 使用 AWS 受管規則集

AWS 提供常見軟體產品的預先設定規則集。這些受管規則集會由自動更新和維護 AWS。

### 使用 AWS 受管規則集

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權資產探索和規則集。
3. 在授權資產規則集區段中，選取 AWS 受管規則集。
4. 瀏覽可用的受管規則集，然後選取符合您軟體產品的規則集。

可用的 AWS 受管規則集包括：

- Microsoft Windows Server Datacenter

- Microsoft SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition
- Red Hat Enterprise Linux
- Ubuntu Pro
- SUSE Enterprise Linux

## 建立自訂規則集

您可以建立自己的規則集，以定義環境和需求特有的授權和執行個體追蹤規則。

### 使用主控台建立規則集

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權資產探索和規則集。
3. 在授權資產規則集區段中，選擇建立規則集。
4. 針對規則集名稱，輸入規則集的易記名稱。
5. 針對規則集描述，提供規則集的用途描述。
6. （選用）新增規則集的標籤，然後選擇下一步。
7. 在步驟 2（設定授權的探索）中，您可以新增與授權相關的規則。這可確保系統可以使用授權來計算產品所安裝執行個體的授權用量。雖然設定探索授權是選用的，但如果您想要授權用量計算，建議您新增它。
  - 您可以新增自我管理的授權，並提供 ARN 或帳戶 ID
  - 您也可以新增授予的授權（從 AWS Marketplace 取得的授權）ARN、ProductSKU 等。
  - 您可以選擇新增規則來新增多個規則
8. 在步驟 3（設定執行個體的探索）中，您可以新增如何探索各種執行個體的規則。這可確保根據選擇條件找到執行個體，而且這些執行個體會計入您正在設定授權資產群組的產品。您可以選取下列欄位來新增一或多個規則：
  - 平台 (Windows 或 Linux)
  - EC2 帳單產品代碼
  - Marketplace 產品代碼
  - AMI ID、主機 ID、執行個體 ID 等。
9. 檢閱您的組態，然後選擇提交。

10. 您可以在我的規則集下查看最近建立的規則集。

### 使用 CLI 建立規則集

- 使用 `create-license-asset-ruleset` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager create-license-asset-ruleset \
  --name "Custom Windows Ruleset" \
  --description "Custom ruleset for Windows Server tracking" \
  --rules '[
    {
      "RuleStatement": {
        "InstanceRuleStatement": {
          "MatchingRuleStatement": {
            "Attribute": "Platform",
            "Values": ["Windows"]
          }
        }
      }
    }
  ]' \
  --client-token unique-token
```

### 更新規則集

您可以更新自訂規則集來修改其組態、新增或移除規則，以及更新標籤。

#### 使用主控台更新規則集

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權資產探索和規則集。
3. 在授權資產規則集區段中，導覽至我的規則集。
4. 若要選取規則集，請選取相關聯的核取方塊，然後選擇動作、編輯。或者，選擇規則集名稱，然後選擇規則集頁面上的編輯按鈕。
5. 從這裡，您可以進行下列更新：
  - 編輯規則集名稱

- 編輯規則集描述
  - 新增或移除與資源相關聯的標籤
6. 當您完成變更時，請選擇下一步。在下一個畫面中，您可以：
    - 新增或移除規則
    - 更新現有規則的授權類型
    - 更新現有規則的條件
  7. 當您完成變更時，請選擇下一步。在下一個畫面中，您可以：
    - 新增或移除包含規則，以指定條件來識別您要包含的執行個體
  8. 檢閱和編輯先前畫面上所做的變更。選擇提交以完成變更。

### 使用 CLI 更新規則集

- 使用 `update-license-asset-ruleset` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager update-license-asset-ruleset \  
  --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/  
ruleset-id \  
  --name "Updated Custom Windows Ruleset" \  
  --description "Updated description for Windows Server tracking"
```

### 刪除規則集

您可以刪除不再需要的自訂規則集。請注意，規則集必須先從所有授權資產群組中移除，才能將其刪除。

### 使用主控台刪除規則集

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授權資產探索和規則集。
3. 在授權資產規則集區段中，導覽至我的規則集。
4. 若要選取要刪除的規則集，請選取相關聯的核取方塊，然後選擇動作、刪除。或者，選擇規則集名稱，然後選擇規則集頁面上的刪除按鈕。

5. 若要永久刪除規則集，請在文字方塊**confirm**中輸入 `confirm`，然後選擇刪除。

#### Important

這個操作無法復原。除非已從所有授權資產群組中移除規則集，否則無法刪除規則集。

### 使用 CLI 刪除規則集

- 使用 `delete-license-asset-ruleset` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager delete-license-asset-ruleset \  
  --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/  
ruleset-id
```

### 取得規則集詳細資訊

您可以擷取特定規則集的詳細資訊，包括其組態和規則。

### 使用 CLI 取得規則集

- 使用 `get-license-asset-ruleset` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager get-license-asset-ruleset \  
  --license-asset-ruleset-arn arn:aws:license-manager:region:account:ruleset/  
ruleset-id
```

### 列出規則集

您可以列出帳戶中的所有規則集，以取得可用規則集的概觀。

### 使用 CLI 列出規則集

- 使用 `list-license-asset-rulesets` 命令。如需詳細資訊，請參閱 [AWS CLI 指令參考](#)。

```
aws license-manager list-license-asset-rulesets \  
  --max-results 50 \  
  --next-token token-from-previous-call
```

## License Manager 中的自我管理授權

自我管理的授權（先前稱為授權組態）是 License Manager 的核心。自我管理的授權包含根據您企業協議條款的授權規則。您建立的規則會決定 AWS 如何處理使用授權的命令。在建立自我管理授權時，會與您組織的合規團隊緊密合作，以檢閱您的企業協議。

自我管理的授權可以在單一 AWS 帳戶或跨內獨立使用，AWS 帳戶或與授權資產群組整合，以跨組織多個 AWS 帳戶和區域集中管理 AWS。此整合可為企業環境提供增強的控管和合規追蹤。

AWS 服務例如 License Manager 具有服務配額，可定義每個區域可供您 AWS 帳戶用於該服務的資源或操作數目上限。例如，使用 License Manager，每個資源最多可以有 10 個自我管理的授權，任何指定的授權總計不超過 25 個自我管理授權 AWS 區域。若要進一步了解 License Manager 配額，請參閱《》中的 [AWS License Manager 服務配額](#) AWS 一般參考。

### Note

Systems Manager 受管執行個體必須與 vCPU 和執行個體類型自我管理授權相關聯。

## 目錄

- [License Manager 中的自我管理授權參數和規則](#)
- [從廠商授權建置 License Manager 規則](#)
- [在 License Manager 中建立自我管理的授權](#)
- [在 License Manager 中共用自我管理的授權](#)
- [在 License Manager 中編輯自我管理的授權](#)
- [在 License Manager 中檢視自我管理的授權](#)
- [在 License Manager 中停用自我管理的授權](#)
- [在 License Manager 中刪除自我管理的授權](#)
- [License Manager 中的自我管理授權規則](#)

## License Manager 中的自我管理授權參數和規則

自我管理授權由基本參數和規則組成，這些參數和規則會根據參數值而有所不同。您也可以將標籤新增至自我管理的授權。建立自我管理授權之後，管理員可以修改授權數量和用量限制，以反映不斷變化的資源需求。

對於跨多個 AWS 帳戶管理授權的組織，請考慮使用提供集中管理和政策強制執行的授權資產群組。自我管理的授權可在個別帳戶中運作，並且可以與授權資產群組整合，以實現整個組織的可見性。

其中包括下列可用的參數和規則：

- 自我管理授權名稱 – 自我管理授權的名稱。
- (選用) 描述 – 自我管理授權的描述。
- 授權類型 – 用於計算授權數量的指標。支援的值為 vCPUs、Cores、Sockets 和執行個體。
- (選用) <option> 的數量 – 資源使用的授權數量。
- 狀態 – 指出組態是否處於作用中狀態。
- (選用) 過期日期 – 指出此授權組態何時過期。客戶可根據其 BYOL 授權的條款，根據過期日期輸入此日期。
- 產品資訊 – 用於[自動探索](#)的產品名稱和版本。支援的產品包括 Windows Server、SQL Server、Amazon RDS for Oracle 和 Amazon RDS for Db2。
- (選用) 規則 – 其中包括下列項目。可用的規則會因計數類型而有所不同。
  - 主機的授權親和性 (以天為單位) – 在指定的天數內限制主機的授權使用。範圍為 1 到 180。計數類型必須是 Cores 或 Sockets。親和期過後，授權將在 24 小時內重複使用。
  - 最大核心 — 資源的最大計數核心。
  - 最大通訊端 – 資源的最大計數通訊端。
  - vCPUs 上限 – 資源的 vCPUs 計數上限。
  - 最小核心 – 資源的最小計數核心。
  - 最小通訊端 – 資源的最小計數通訊端。
  - 最小 vCPUs – 資源的最小計數 vCPUs。
  - 租用 – 將授權用量限制為指定的 EC2 租用。如果計數類型為 Cores 或 Sockets，則需要專用主機。如果計數類型為執行個體或 vCPUs，則支援共用租用、專用主機和專用執行個體。主控台 (和 API) 名稱如下所示：
    - 共用 (EC2-Default)
    - 專用執行個體 (EC2-DedicatedInstance)

- 專用主機 (EC2-DedicatedHost)
- vCPU 最佳化 – License Manager 與 Amazon EC2 中的 [CPU 最佳化](#) 支援整合，可讓您自訂執行個體上的 vCPUs 數量。如果此規則設定為 True，則 License Manager 會根據自訂的核心和執行緒計數來計算 vCPUs。否則，License Manager 會計算執行個體類型的預設 vCPUs 數量。
- 包含已停止的執行個體 – 當此規則設為 True 時，License Manager 會追蹤已停止的執行個體，並將其計為授權用量。預設值為 False。設為 False 時，停止的執行個體不會計入授權用量，而且其授權會釋出回可用的授權集區。

下表說明適用於每個計數類型的授權規則。

主控台名稱	API 名稱	核心	執行個體	通訊埠	vCPUs
主機的授權親和性 (以天為單位)	licenseAffinityToHost	✓		✓	
核心上限	maximumCores	✓	✓		
通訊端上限	maximumSockets		✓	✓	
vCPUs 上限	maximumVcpus		✓		✓
最小核心	minimumCores	✓	✓		
最小通訊端	minimumSockets		✓	✓	
最低 vCPUs	minimumVcpus		✓		✓
租用	allowedTenancy	✓	✓	✓	✓
vCPU 最佳化	honorVcpuOptimization				✓
包含已停止的執行個體	includedStoppedInstances	✓	✓	✓	✓

## 從廠商授權建置 License Manager 規則

您可以根據軟體廠商授權的語言來建立 License Manager 規則集。下列範例並非實際使用案例的藍圖。在授權協議的任何實際應用中，您可以根據特定現場部署伺服器環境的架構和授權歷史記錄在競爭選項中進行選擇。您的選項也取決於您計畫將資源遷移至 AWS 的詳細資訊。

這些範例盡可能與特定廠商無關，置重點在廣泛適用的硬體和軟體分配問題。廠商授權規定也會與 AWS 需求和限制互動。應用程式所需的授權數會隨著所選的執行個體類型和其他因素而異。

### Important

AWS 不會參與軟體廠商的稽核程序。客戶負責合規，並承擔根據其授權合約仔細了解規則並將其擷取到 License Manager 的責任。

### 範例：實作作業系統授權

此範例將包含伺服器作業系統授權。授權語言會對 CPU 核心類型、租用和每個伺服器的最少授權數量強加限制。

在此範例中，授權條款包含下列條文：

- 實體處理器核心決定了授權計數。
- 授權數量必須等於核心數量。
- 一個伺服器必須執行至少 8 個核心。
- 作業系統必須在非虛擬主機上運作。
- 即使執行個體停止，授權仍必須保持配置狀態。

此外，客戶也做出以下決定：

- 已購買適用於 96 個核心的授權。
- 硬性限制授權使用量不得逾越購買數量。
- 每個伺服器最多需要 16 個核心。

下表將 License Manager 規則制定參數與其擷取和自動化的廠商授權要求建立關聯。範例值僅用於說明目的；您可以在自己的自我管理授權中指定所需的值。

License Manager 規則	設定
授權計數類型	授權類型設定為 <b>Cores</b> 。
授權計數	核心數量設定為 <b>96</b> 。
最小/最大 vCPUs或核心	最小核心設定為 <b>8</b> 。 最大核心設定為 <b>16</b> 。
授權計數硬性限制	已選擇 Enforce license limit (強制授權限制)。
允許租用	租用設定為 <b>Dedicated Host</b> 。
包含已停止的執行個體	包含已停止的執行個體會設定為 <b>True</b> 。已停止的執行個體會繼續耗用授權。

## 在 License Manager 中建立自我管理的授權

自我管理授權代表與軟體廠商簽訂協議中的授權條款。您的自我管理授權指定應如何計算授權（例如，依 vCPUs或執行個體數量）。它也會指定用量限制，以便防止用量超過已配置的授權數量。此外，它也可以指定授權的其他限制條件，例如租用類型。

### Note

在建立自我管理授權之前，請考慮您的組織結構：

- 單一帳戶用量：直接在您的帳戶中建立自我管理的授權
- 多帳戶用量：請考慮先建立授權資產群組，然後建立自我管理授權的關聯以進行集中式管理

## Amazon RDS for Oracle 和 Amazon RDS for Db2 資料庫的考量

當您新增產品資訊以設定自動探索 Amazon RDS for Oracle 或 Amazon RDS for Db2 資料庫時，適用下列要求：

- 支援的授權計數類型為 vCPU。
- 不支援規則。
- 不支援硬授權限制。
- 您可以追蹤每個自我管理授權的一個產品版本。
- 您無法使用相同的自我管理授權來追蹤 Amazon RDS 資料庫和其他產品。

### 使用主控台建立自我管理授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理的授權。
3. 選擇建立自我管理授權。
4. 在 Configuration details (組態詳細資訊) 面板中，提供以下資訊：
  - 自我管理授權名稱 – 自我管理授權的名稱。
  - 描述 – 自我管理授權的選用描述。
  - 過期日期 – 自我管理授權的選用過期日期。
  - 授權類型 – 此授權的計數模型 (vCPUs、Core、Sockets 或執行個體)。
  - <option> 的數量 – 顯示的選項取決於授權類型。超過授權限制時，License Manager 會通知您 (軟性限制) 或防止資源部署 (硬性限制)。
  - 強制執行授權限制 – 如果選取，則授權限制為硬性限制。
  - 規則 – 一或多個規則。對於每個規則，選取一種規則類型、提供規則值，然後選擇 Add rule (新增規則)。顯示的規則類型將依授權類型而有不同。例如，最小值、最大值和租用。如果您未指定租用類型，則所有類型都會獲准。
5. (選用) 在自動探索規則面板中，執行下列動作：
  - a. 選擇每個產品的產品名稱、產品類型和資源類型，以使用 [自動探索](#) 來探索和追蹤。
  - b. 選取在軟體解除安裝時停止追蹤執行個體，以在 License Manager 偵測到軟體已解除安裝且任何授權親和性期間已過之後，讓授權可供重複使用。
  - c. (選用) 如果您的帳戶是 Organizations 的授權管理員管理帳戶，您可以選擇定義要從自動探索中排除的資源。若要這樣做，請選取新增排除規則，選擇要篩選的屬性，支援 AWS 帳戶 IDs 和資源標籤，然後輸入資訊以識別該屬性。
6. (選用) 展開標籤面板，將一或多個標籤新增至您的自我管理授權。標籤均為金鑰值對。為每個標籤提供下列資訊：

- 金鑰 – 金鑰的可搜尋名稱。
- 值 – 金鑰的值。

## 7. 選擇提交。

### Note

設定授權過期日期後，授權管理員可以在 120 天、90 天、60 天、30 天、0 天向中設定的 Amazon SNS 主題傳送通知 [License Manager 中的受管授權設定](#)。

使用命令列建立自我管理授權

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

## 在 License Manager 中共用自我管理的授權

您可以使用與任何 AWS 帳戶或透過 AWS Resource Access Manager 共用自我管理的授權 AWS Organizations。如需詳細資訊，請參閱 AWS RAM 《使用者指南》中的 [共用您的 AWS 資源](#)。

## 與 AWS Organization 共用自我管理的授權

先決條件

若要完成此程序，您必須將 AWS Organization 與 License Manager 連結。如需詳細資訊，請參閱 [License Manager 中的受管授權設定](#)。

共用您的授權

若要與 AWS Organization 共用自我管理授權，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選取自我管理的授權。
4. 從動作功能表中選擇與 AWS 組織帳戶共用。

## 支援的帳戶配額

如果您在 2023 年 10 月 14 日 AWS License Manager 日之前在 中啟用授權共用，則授權管理員在組織內支援的最大帳戶數量配額將小於新的預設上限。您可以使用下一節提供的 的 API 操作 AWS RAM 來增加此配額。如需 License Manager 預設配額的詳細資訊，請參閱 AWS 一般參考 指南中的 [使用授權的配額](#)。

### 先決條件

若要完成下列程序，您必須以具有下列許可的組織管理帳戶中的委託人身分登入：

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

### 增加支援的帳戶配額

下列程序會將 的目前配額增加 `Number of accounts per organization for License Manager` 為目前的預設最大值。

### 增加 License Manager 支援的帳戶配額

1. 使用 [describe-organization](#) AWS CLI 命令，透過 操作來判斷組織的 ARN：

```
aws organizations describe-organization

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

```
    }  
  ]  
}  
}
```

2. 使用 [get-resource-shares](#) AWS CLI 命令，透過 操作來判斷組織的 ARN：

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

3. 使用 [enable-sharing-with-aws-organization](#) AWS CLI 命令來啟用資源共用 AWS RAM：

```
aws ram enable-sharing-with-aws-organization  
  
{  
  "returnValue": true  
}
```

您可以使用 [list-aws-service-access-for-organization](#) AWS CLI 命令來驗證已為 License Manager 啟用 Organizations 列出服務主體，以及 AWS RAM：

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

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

#### Important

最多可能需要六個小時，AWS RAM 才能為您的組織完成此操作。此程序必須先完成，您才能繼續。

4. 使用 [associate-resource-share](#) AWS CLI 命令將 License Manager 資源共用與組織建立關聯：

```
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 命令來驗證資源共享關聯的 status 是 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 中編輯自我管理的授權

您可以在自我管理授權中編輯下列欄位的值：

- 自我管理的授權名稱
- Description
- 過期日期
- <option> 的數量
- 強制執行授權類型限制
- 包含已停止的執行個體

## 編輯自我管理的授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理的授權。
3. 選取自我管理的授權。
4. 選擇 Actions (動作)、Edit (編輯)。
5. 視需要編輯詳細資訊，然後選擇更新。

### Note

設定授權過期日期後，授權管理員可以在 120 天、90 天、60 天、30 天、0 天向中設定的 Amazon SNS 主題傳送通知 [License Manager 中的受管授權設定](#)。

## 使用命令列編輯自我管理的授權

- [update-license-configuration](#) (AWS CLI)
- [Update-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

## 在 License Manager 中檢視自我管理的授權

您可以透過 License Manager 主控台檢視自我管理的授權，以監控整個 AWS 環境的使用情況、合規性和分佈。

### 在單一帳戶中檢視授權

若要檢視目前帳戶中的自我管理授權：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇 **Self-managed licenses**。
3. 檢閱授權清單、其狀態和目前用量。
4. 選擇授權名稱以檢視詳細資訊，包括相關聯的資源和合規狀態。

## 檢視彙總授權（適用於組織管理員或委派管理員）

組織管理員和委派管理員可以從集中位置檢視組織中所有 AWS 帳戶的自我管理授權。這可提供整個組織的可見度和管理功能，以實現授權合規。

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 確保您以組織管理員或委派管理員的身分登入。
3. 在左側導覽窗格中，選擇 **Self-managed licenses**。
4. 選擇 **Organization license configuration** 索引標籤以檢視彙總的授權檢視。
5. 檢閱組織帳戶中所有自我管理授權的彙總檢視。

此彙總檢視可讓您集中管理授權，並協助確保整個 AWS 組織的合規性。

使用命令列檢視彙總的授權

- [list-license-configurations-for-organization](#) (AWS CLI)

## 在 License Manager 中停用自我管理的授權

當您停用自我管理授權時，使用該授權的現有資源不會受到影響，而且仍可啟動使用該授權的 AMIs。不過，將不再追蹤授權使用數。

停用自我管理授權時，不得連接到任何執行中的執行個體。停用後，無法使用自我管理的授權執行啟動。

停用自我管理的授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理的授權。
3. 選取自我管理的授權。
4. 選擇動作、停用。出現確認提示時，請選取 Deactivate (停用)。

使用命令列停用自我管理授權

- [update-license-configuration](#) (AWS CLI)
- [Update-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

## 在 License Manager 中刪除自我管理的授權

您必須先取消任何資源的關聯，才能刪除自我管理的授權。如果您需要從新的授權規則重新開始，可以刪除自我管理的授權。如果軟體廠商的授權條款有所變更，您可以取消現有資源的關聯、刪除自我管理的授權、建立新的自我管理授權，以反映更新後的條款，並將其與現有資源建立關聯。

### 使用主控台刪除自我管理的授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選擇自我管理授權的名稱，以開啟授權詳細資訊頁面。
4. 選取每個資源（個別或大量），然後選擇取消關聯資源。重複此操作直到清單為空。
5. 選擇 Actions (動作)、Delete (刪除)。出現確認提示時，請選擇 Delete (刪除)。

### 使用命令列刪除自我管理的授權

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

## License Manager 中的自我管理授權規則

建立自我管理的授權規則後，即可連接至相關的啟動機制，直接防止部署不合規的新資源。組織中的使用者可以從指定的 AMIs 無縫啟動 EC2 執行個體，管理員可以透過內建的 License Manager 儀表板追蹤授權庫存。啟動控制和儀表板提醒可讓您更輕鬆地強制執行合規。

### Important

AWS 不會參與軟體廠商的稽核程序。客戶負責合規，並承擔根據其授權合約仔細了解規則並將其擷取到 License Manager 的責任。

授權追蹤將依連接到執行個體的時間規則運作，直到其終止為止。您可以定義用量限制和授權規則，而 License Manager 會追蹤部署，同時提醒您違反規則。如果您已設定硬性限制，License Manager 可以防止資源啟動。

追蹤伺服器終止時，會釋出其授權並傳回至可用授權的集區。根據預設，當追蹤伺服器停止時，也會釋出其授權並傳回至集區。不過，如果包含已停止的執行個體規則 (`includedStoppedInstances`) 設

定為 True，則會繼續追蹤已停止的執行個體，並計為授權用量。當您的授權條款要求無論執行個體的執行狀態為何，授權仍配置給執行個體時，這會很有用。

由於組織有不同的操作和合規方法，因此 License Manager 支援多種啟動機制：

- 手動將自我管理授權與 AMIs 建立關聯 – 對於追蹤作業系統或其他軟體的授權，您可以在發佈授權規則以供組織廣泛使用之前，將授權規則連接到 AMIs。然後，這些 AMIs 中的任何部署都會使用 License Manager 自動追蹤，而不需要使用者進行任何額外的動作。您也可以將授權規則連接至目前的 AMI 建置機制，例如 [Systems Manager Automation](#)、[VM Import/Export](#) 和 [Packer](#)。
- Amazon EC2 啟動範本和 AWS CloudFormation – 如果將授權規則連接至 AMIs 不是偏好的選項，您可以在 [EC2 啟動範本](#) 或 [CloudFormation 範本](#) 中將其指定為選用參數。使用這些範本的部署會使用 License Manager 進行追蹤。您可以在自我管理的授權欄位中指定一或多個自我管理的授權 IDs，以強制執行 EC2 啟動 CloudFormation 範本的規則。

AWS 將授權追蹤資料視為敏感的客戶資料，只能透過擁有該資料的 AWS 帳戶存取。AWS 無法存取您的授權追蹤資料。您可以控制您的授權追蹤的資料，也可以隨時將其刪除。

## 關聯自我管理的授權和 AMIs

下列程序示範如何使用 License Manager 主控台將自我管理的授權與 AMIs 建立關聯。此程序假設您至少有一個現有的自我管理授權。您可以將自我管理的授權與您有權存取的任何 AMI 建立關聯，無論是擁有還是共用。如果與您共用 AMI，您可以將其與目前帳戶中的自我管理授權建立關聯。否則，您可以指定 AMI 是否與所有帳戶的自我管理授權相關聯，或僅與目前帳戶相關聯。

如果您將 AMI 與所有帳戶的自我管理授權建立關聯，則可以跨帳戶追蹤從 AMI 啟動的執行個體。達到硬性限制時，License Manager 會封鎖其他執行個體啟動。達到軟性限制時，License Manager 會通知您額外的執行個體啟動。

如果您在相同區域內複製 AMI，且 AMI 具有相關聯的授權組態，則這些授權組態會自動與新的 AMI 建立關聯。當您從新的 AMI 啟動執行個體時，License Manager 會追蹤它。同樣地，如果您從具有相關聯授權組態的執行中執行個體建立新的 AMI，這些授權組態會自動與新 AMI 建立關聯，而 License Manager 會追蹤您從新 AMI 啟動的執行個體。

### Warning

License Manager 不支援跨區域執行個體追蹤。如果您將具有相關聯授權組態的 AMI 複製到不同的區域，則 License Manager 會封鎖從新 AMI 啟動的所有執行個體。

## 建立自我管理授權和 AMI 的關聯

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選擇自我管理授權的名稱，以開啟授權詳細資訊頁面。若要檢視目前關聯的 AMIs，請選擇關聯的 AMIs。
4. 選擇關聯 AMI。
5. 針對可用的 AMIs，選取一或多個 AMIs，然後選擇關聯。
  - 如果您的帳戶擁有至少一個 AMIs，系統會提示您為擁有的 AMI 選擇 AMIs 關聯範圍。從另一個帳戶共用的任何 AMIs 只會與您的帳戶相關聯。選擇確認。
  - 如果 AMIs 是從另一個帳戶與您共用，它們只會與您的帳戶相關聯。

新關聯的 AMIs 現在會出現在授權詳細資訊頁面上 AMIs 索引標籤上。

## 取消自我管理授權和 AMIs 關聯

下列程序示範如何使用 License Manager 主控台取消自我管理授權與 AMIs 的關聯。您無法取消已取消註冊 AMI 的關聯。License Manager 每 8 小時檢查一次已取消註冊 AMIs，並自動取消它們的關聯。

### 取消自我管理授權與 AMI 的關聯

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選擇自我管理授權的名稱，以開啟授權詳細資訊頁面。
4. 選擇 Associated AMIs (關聯的 AMI)。
5. 選取 AMI，然後選擇取消關聯 AMI。

## License Manager 中授予的授權

授予的授權是您組織從 [AWS Marketplace](#)、[AWS Data Exchange](#) 或直接從整合其軟體與受管權利的賣方購買的產品的授權。授權管理員可以使用 AWS License Manager 來控管這些授權的使用，以及將稱為權利的使用權分發給特定 AWS 帳戶。

分發給 AWS Data Exchange 產品的資料授權可透過 AWS Data Exchange 提供給帳戶 AWS。您必須先啟用訂閱共用 AWS Marketplace，才能從分發授權。如需詳細資訊，請參閱 [在組織中共用訂閱](#)。

授權管理員從 AWS Marketplace 授權將權利分發至 AWS 帳戶，且收件人接受並啟用授予的授權後，帳戶即可 AWS 透過 取得訂閱 AWS Marketplace。帳戶也可以存取 產品。例如，如果授權管理員從購買 Amazon Machine Image (AMI) AWS Marketplace 並將權利分配給 AWS 您的帳戶，您可以使用 AWS Marketplace 和 Amazon EC2 從 AMI 啟動 Amazon EC2 執行個體。

## 主題

- [檢視您授予的授權](#)
- [在 License Manager 中管理您授予的授權](#)
- [分佈 License Manager 權限](#)
- [在 License Manager 中授予接受和啟用](#)
- [License Manager 中授予的授權狀態](#)
- [License Manager 中買方帳戶的 CloudWatch 指標](#)

## 檢視您授予的授權

License Manager 會顯示索引標籤，根據您經過身分驗證的許可來檢視和管理授予的授權。授予的授權頁面可以顯示下列標籤：

### 我的授權

此標籤可供有權在 License Manager 中檢視授予授權的任何使用者使用。標籤具有我的授權區段，其中包含每個授權的相關資訊，例如授權 ID 和產品名稱。在此頁面上，您可以檢視每個授權的其他資訊。

### 授權摘要（適用於組織管理員）

此索引標籤僅適用於組織管理員。標籤具有總計區段，其中列出組織中所有帳戶的產品總數和授予的授權。它也會顯示產品區段，其中包含詳細說明每個產品屬性的資料表，例如產品名稱和授予的授權數量。

### 彙總授權（適用於組織管理員）

此索引標籤僅適用於組織管理員。此索引標籤有一個區段，詳細說明我的組織授予的授權，其中包含每個授權的相關資訊，例如授權 ID 和產品名稱。在此頁面上，您可以檢視每個授權的其他資訊。

## 在 License Manager 中管理您授予的授權

已授予您的授權會顯示在 License Manager 主控台中。收件人必須先接受並啟用授予的授權，才能使用該產品。接受和啟用授權的方式取決於授權是否來自 AWS Marketplace、您的帳戶是否為組織中的成員帳戶 AWS Organizations，以及是否為您的組織啟用所有功能。

授予的授權需要跨區域複寫授權中繼資料。License Manager 會自動將每個授予的授權及其相關資訊複寫到其他 AWS 區域。這可讓您集中檢視授予授權的所有區域。

### 來自 AWS Marketplace 和 AWS Data Exchange 的授權

- 您購買的訂閱授權會自動接受並啟用。
- 如果已啟用所有功能的組織的管理帳戶購買訂閱並將授權分發給成員帳戶，則成員帳戶中會自動接受授權。管理帳戶或成員帳戶稍後可以啟用授權。
- 如果只啟用合併帳單功能的組織的管理帳戶購買訂閱並將授權分發給成員帳戶，則每個成員帳戶都必須接受並啟用授權。

### 賣方的授權

- 您必須接受並啟用使用 License Manager 分發授權之產品的授權。
- 如果已啟用所有功能的組織的管理帳戶購買產品並將授權分發給成員帳戶，則成員帳戶中會自動接受授權。管理帳戶或成員帳戶稍後可以啟用授權。
- 如果只啟用合併帳單功能的組織的管理帳戶購買產品並將授權分發給成員帳戶，則每個成員帳戶都必須接受並啟用授權。

### Console (My licenses)

您可以檢視和管理單一 的授予授權 AWS 帳戶。

#### 在帳戶中管理授予的授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授予的授權。
3. 如果不是目前的選擇，請選擇我的授權索引標籤。
4. (選用) 使用如下所示的篩選條件選項，來限制顯示的授權清單。

- 產品 SKU – 此授權的產品識別符，由授權發行者在建立授權時定義。相同的產品 SKU 可能存在於多個 ISVs。
  - 收件人 – 授權收件人的 ARN。
  - 狀態 – 授權的狀態。例如，可用。
5. 若要檢視授權的其他資訊，請選擇授權 ID 以開啟授權概觀頁面。
  6. 如果授權發行者是 以外的實體 AWS Marketplace，則初始授予狀態為待接受。執行以下任意一項：
    - 選擇接受並啟用授權。產生的授予狀態為作用中。
    - 選擇接受授權。產生的授予狀態為已停用。當您準備好要使用授權時，請選擇啟用授權。
    - 選擇拒絕授權。產生的授予狀態為拒絕。拒絕授權之後，就無法啟用授權。

如果您不想繼續使用已啟用的授權，您可以返回授權概觀頁面，然後選擇停用授權。如果您想要繼續使用已停用的授權，請返回授權概觀頁面，然後選擇啟用授權。

## Console (Aggregated licenses)

您可以檢視已從組織中的所有帳戶彙總的已授予授權。

### Important

若要針對您授予的授權使用全組織檢視，您必須先 AWS Organizations 使用 AWS License Manager 主控台設定進行連結。如需詳細資訊，請參閱[License Manager 中的設定](#)。

在 中跨您的帳戶管理授予的授權 AWS Organizations

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授予的授權。
3. 如果不是目前選擇，請選擇彙總授權索引標籤。
4. (選用) 使用如下所示的篩選條件選項，來限制顯示的授權清單。
  - 產品 SKU – 此授權的產品識別符，由授權發行者在建立授權時定義。相同的產品 SKU 可能存在於多個 ISVs。
  - 受益人 – 組織中授予授權的帳戶。

5. 若要檢視授權的其他資訊，請選擇授權 ID 以開啟授權詳細資訊頁面。
6. 如果授權發行者是 以外的實體 AWS Marketplace，請執行下列其中一項操作：
  - 選擇啟用授權。產生的授予狀態為作用中。
  - 選擇停用授權。產生的授予狀態為已停用。

如果您不想繼續使用已啟用的授權，您可以返回授權概觀頁面，然後選擇停用授權。如果您想要繼續使用已停用的授權，請返回授權概觀頁面，然後選擇啟用授權。

## AWS CLI

您可以使用 AWS CLI 來使用已授予的授權。

若要使用 管理授予的授權 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](#)

## 分佈 License Manager 權限

如果您是在組織管理帳戶中操作的授權管理員，且已啟用[所有功能](#)，您可以透過建立授予的授權，將權利分配到組織。如需的詳細資訊 AWS Organizations，請參閱[AWS Organizations 術語和概念](#)。

您可以將授予的收件人指定為下列其中一項：

- AWS 帳戶，只包含指定的帳戶。
- 組織根目錄，其中包含整個組織的所有帳戶。
- 組織單位 (OU) ( 未巢狀 )，其中包含指定 OU 和指定 OUs 下巢狀 OU 中的所有帳戶。

**Note**

每個授權最多可以建立 2,000 個授權。

您可以使用 AWS License Manager 主控台或 AWS CLI 來分配您的權利。您可以在主控台中建立授予時指定組織 ID 或組織 ARN，但 ARN 格式必須與 搭配使用 AWS CLI。例如，ARNs 類似以下內容：

**組織 ID ARN**

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

**Organization OU ARN**

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

**Console****建立授予（主控台）**

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授予的授權。
3. 選擇授權 ID 以開啟授權概觀頁面。
4. 從授予區段中，選擇建立授予。
5. 在授予詳細資訊面板上，執行下列動作：
  - a. 輸入授予的名稱，以協助您識別授予的目的或收件人。
  - b. 輸入授予收件人的 AWS 帳戶 ID、AWS Organizations OU ID 或 ARN，或 AWS Organizations ID 或 ARN。
  - c. 選擇建立授予。
6. 在授權概觀頁面上，您會在授權面板中看到授予的項目。授予的初始狀態為待接受。當收件人接受授予或收件人拒絕授予時，狀態會變更為作用中。

## AWS CLI

您可以使用 AWS CLI 來分發權利。使用 AWS License Manager API 時，您必須使用 ARN 格式的指定組織 ID 或 OU。

若要使用 建立和列出您的授予 AWS CLI：

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

授予詳細資訊頁面會顯示您已授予權利存取權的帳戶清單。將授權分發給組織後，您可以個別停用或啟用每個帳戶上的授權。

## 在 License Manager 中授予接受和啟用

為授予的授權建立授予時，會分發給收件人。必須先接受並啟用授予的授權，才能讓授予收件人使用。授予啟用程序可以包含從 取得的授予授權的其他選項 AWS Marketplace。

根據預設，授予授權的授予概觀頁面的狀態為 Pending Acceptance。您可以選擇 Accept、Accept and Activate 或 Reject 授予。已接受但尚未啟用的授予狀態為 Disabled。已接受和已啟用的授予狀態為 Active。

必須先接受並啟用授予的授權，才能讓授予收件人使用。根據預設，授予授權的授予詳細資訊頁面狀態為待接受。您可以選擇接受、接受和啟用或拒絕授權。已接受但尚未啟用的授予狀態為已停用。已接受和已啟用的授予狀態為作用中。

### Tip

您可以自動接受來自組織管理帳戶的授予。若要啟用授予自動接受，請從 管理帳戶在 AWS License Manager 主控台的 [設定](#) 頁面上連結您的組織帳戶。

您無法 AWS Marketplace 同時為來自的相同產品啟用兩個授權。如果您有兩個訂閱（例如，產品的公開優惠和私有優惠，或產品的訂閱授權和相同產品的授予授權），您可以採取下列其中一個動作：

1. 停用相同產品的現有授予，然後啟用新的授予。
2. 啟用新的授予，並指定您要停用，並以新的授取代現有的作用中授予。您可以使用 License Manager 主控台或 AWS CLI：

- a. 使用 License Manager 主控台，在選取您要取代作用中授予的是時，啟用新的授予。
- b. 使用 CreateGrantVersion API，透過 ActivationOverrideBehavior 使用 Status 的 ALL\_GRANTS\_PERMITTED\_BY\_ISSUER 指定 來啟用新的授予 Active。

## Console

您可以使用 License Manager 主控台來啟用授予。當您啟用來自的授予時 AWS Marketplace，您可能看到是否取代作用中授予的選項：

- 身為授權管理員，您必須在啟用授予時指定是否要取代作用中授予。
- 身為授予者，您可以選擇性地指定在組織中另一個帳戶啟用授予時，是否要取代作用中授予。
- 身為承授者，如果建立分散式授予的承授者未指定是否取代作用中授予，您必須在啟用授予時進行選擇。

### 啟用授予（主控台）

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇授予的授權。
3. 選擇授權 ID 以開啟授權概觀頁面。
4. 選擇授予名稱以開啟授予概觀頁面。
5. 如果顯示，請針對是否要取代作用中授予選取啟用選項：
  - a. 否 – 此選項將啟用授予，而不會取代收件人（承授者）的任何現有作用中授予。
  - b. 是 – 此選項會停用相同產品的授予，並為定義的收件人（承授者）啟用新的授予：
    - i. 指定的 AWS 帳戶。
    - ii. 指定組織 OU 的成員帳戶。
    - iii. 組織的所有成員帳戶。
6. （選用）提供啟用授予的原因。
7. 在輸入方塊中輸入 **activate**，然後選擇啟用。

## AWS CLI

您可以使用 AWS CLI 來使用已授予的授權。

若要使用 處理分散式授予 AWS CLI：

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

## License Manager 中授予的授權狀態

授權有兩種狀態：授權狀態，其顯示授權的整體可用性和可分割性，以及授予狀態，其顯示使用授權的能力。

下表顯示已授予授權的各種狀態：

狀態	Description
AVAILABLE	授權可供 使用和共用。
PENDING_AVAILABLE	由於授權仍在處理中，因此無法使用。
已停用	由於授權發行者已停用授權，因此無法使用該授權。
SUSPENDED	授權暫停時無法使用。
已過期	由於授權已到期，因此無法使用。
PENDING_DELETE	由於授權正在進行刪除，因此無法使用。
DELETED	授權無法使用，因為授權合約已取消。

下表顯示授予的各種狀態：

狀態	Description
PENDING_WORKFLOW	授予正在進行分發。

狀態	Description
PENDING_ACCEPT	授予已建立，且授予收件人尚未接受。
REJECTED	授予收件人已拒絕授予。
ACTIVE	授予接受並啟用以供授予收件人使用。您可以使用授權資源。
FAILED_WORKFLOW	授予無法分配。
DELETED	授予者已刪除授予。
PENDING_DELETE	分發的授予正在進行刪除。
DISABLED	授予收件人已接受授予，但尚未啟用以供使用。
WORKFLOW_COMPLETE	已分發或回收對組織的授予。授予詳細資訊會顯示組織中每個帳戶子授予的狀態。

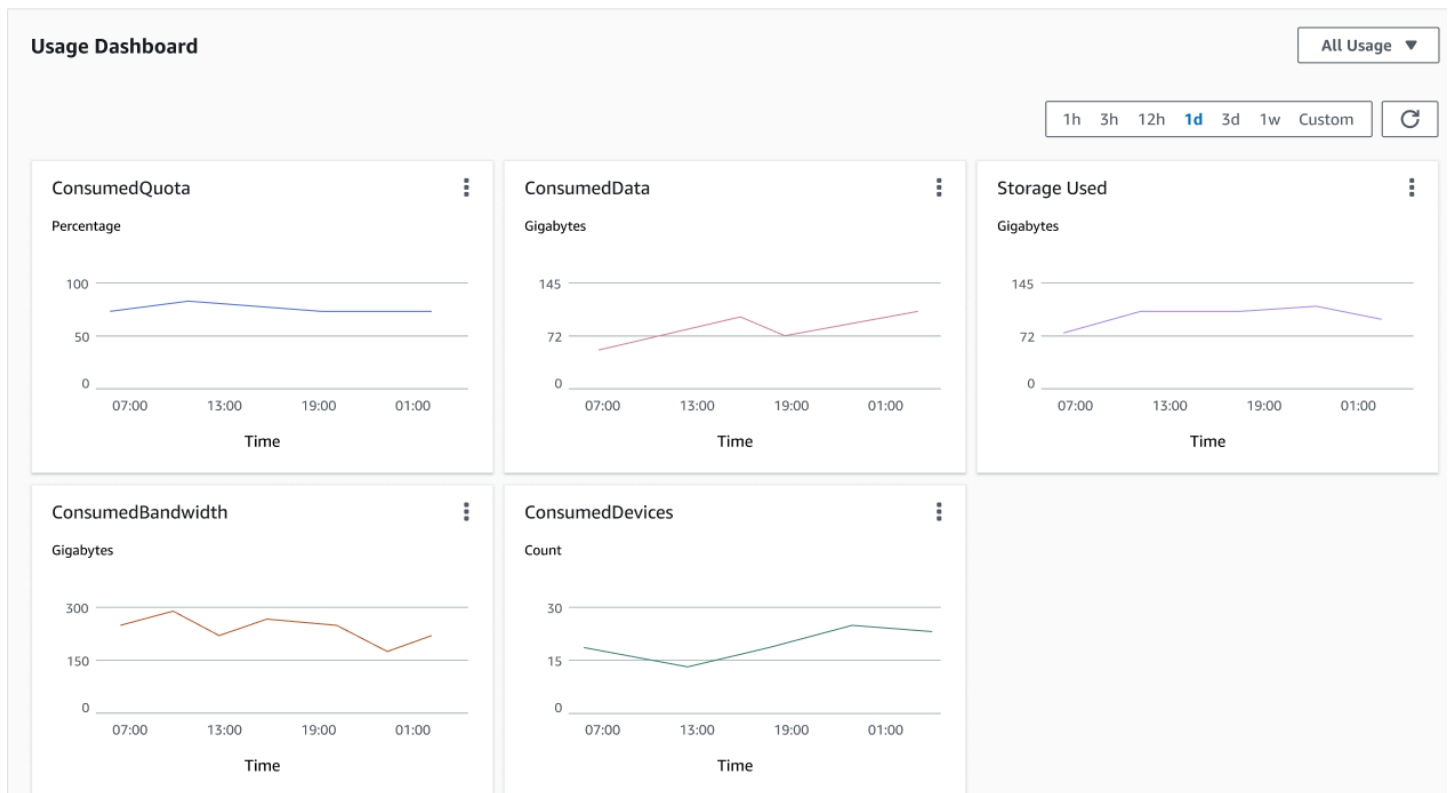
## License Manager 中買方帳戶的 CloudWatch 指標

當賣方發行的授權授予設定為允許提交選取的用量記錄時，License Manager 會向賣方帳戶、根買方帳戶和記錄用量的帳戶發出 CloudWatch 指標。買方帳戶是已購買或獲授予賣方發行授權 AWS 帳戶的。如需詳細資訊，請參閱[授予授權給客戶](#)。

### 用量儀表板

當賣方或獨立軟體廠商 (ISV) 應用程式針對買方帳戶的授權記錄用量時，記錄用量的帳戶和根買方帳戶會在 License Manager 主控台的用量儀表板頁面上看到含有用量記錄的 CloudWatch 小工具。買方也可以查看其擁有分散式授權的帳戶指標 AWS Organizations。用量儀表板頁面上的圖形適用於已傳送用量記錄的每個授權。

下圖是用量儀表板的範例：



## 授權分析

授權資產群組提供全方位的儀表板和視覺化功能，可讓您了解組織中所有 AWS 區域和帳戶的軟體授權產品組合。

### 目錄

- [主要儀表板檢視](#)
- [個別授權資產群組檢視](#)
- [建立用量報告](#)

## 主要儀表板檢視

授權資產群組儀表板會根據具有即時耗用量追蹤的執行個體計數，顯示前 5 個授權資產群組。

### 時間範圍選擇

- 從中選擇：過去 1、3、6 或 12 個月，或自訂日期範圍
- 使用彈性日期範圍來識別季節性模式並追蹤成長趨勢

## 互動式視覺化

- 將滑鼠游標暫留在圖形上，以檢視詳細的執行個體計數
- 檢視跨授權類型的用量趨勢：
  - 自我管理授權 - 軟體供應商的 BYOL
  - 授予的授權 - AWS Marketplace 或第三方採購和 AWS 提供的授權

## 個別授權資產群組檢視

從下拉式選單中選取授權資產群組，以檢視詳細資訊

### 摘要索引標籤

#### 詳細資訊

- 在授權資產群組中追蹤的執行個體總數
- 在授權資產群組中追蹤的授予授權
- 在授權資產群組中追蹤的自我管理授權

### 即將續約

在未來 7、30 或 100 天內，在授權資產群組中追蹤的續約授權清單

#### Note

您必須設定授權過期日期，才能檢視即將進行的續約。請參閱 [在 License Manager 中編輯自我管理的授權](#)。

### 用量趨勢

執行個體和授權趨勢會在授權資產群組內追蹤的所選期間內，顯示自我管理和授予授權的授權使用模式

若要了解授權資產群組所提供指標的詳細資訊，請參閱 [使用 Amazon CloudWatch 監控 License Manager](#)。

## 建立用量報告

AWS License Manager 為自我管理的授權和授權資產群組提供全面的用量報告功能。您可以為自我管理的授權產生定期報告，或為授權資產群組產生隨需報告，以追蹤整個組織的授權用量、合規性和資源庫存。

### 自我管理的授權報告

自我管理的授權報告會提供授權用量的定期快照。您可以設定多個用量報告，透過自動發佈到 Amazon S3 儲存貯體來追蹤環境中的不同授權類型。

#### 自我管理的授權摘要報告

包含有關耗用授權數量的資訊，以及有關自我管理授權組態的詳細資訊，包括授權計數、授權規則和跨資源類型的分佈。

#### 資源用量報告

提供追蹤資源及其授權耗用的詳細資訊，列出每個資源的授權 ID、狀態和 AWS 帳戶 ID 資訊。

### 建立自我管理的授權用量報告

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從導覽面板選擇用量報告（在授權分析下）。
3. 選擇建立用量報告，然後定義參數：
  - a. 輸入用量報告的名稱和選用的描述。
  - b. 從下拉式清單中選取自我管理的授權類型。
  - c. 選擇要產生的報告類型。
  - d. 選擇頻率：每 24 小時一次、每 7 天一次或每 30 天一次。
  - e. （選用）新增標籤以追蹤用量報告資源。
4. 選取建立用量報告。

### 使用 CLI 建立自我管理的授權報告

- 使用 `create-license-manager-report-generator` 命令：

```
aws license-manager create-license-manager-report-generator \
```

```
--report-generator-name "Daily License Usage Report" \  
--type LicenseUsageReport \  
--report-context '{  
  "licenseConfigurationArns": [  
    "arn:aws:license-manager:region:account:license-configuration/lic-config-  
id"  
  ]  
' \  
--report-frequency '{  
  "value": 1,  
  "period": "DAY"  
' \  
--client-token unique-token
```

## 授權資產群組報告

授權資產群組報告提供隨需、全面的報告，以涵蓋組織內多個 AWS 區域和帳戶的軟體授權合規。這些報告提供探索並映射至授權資產群組之所有資源的詳細清查。

### 建立授權資產群組報告

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從導覽面板選擇用量報告（在授權分析下）。
3. 選擇建立授權資產群組報告，然後定義參數：
  - a. 輸入報告的名稱和選用的描述。
  - b. 從下拉式清單中選取授權資產群組。
  - c. 選擇日期範圍，列出該範圍內的所有資源。
  - d. （選用）新增標籤以追蹤用量報告資源。
4. 選取建立用量報告。

### 使用 CLI 建立授權資產群組報告

- 針對具有特定時間範圍的隨需報告使用 `create-license-manager-report-generator` 命令：

```
aws license-manager create-license-manager-report-generator \  
--report-generator-name "License asset group Report" \  

```

```
--type LicenseAssetGroupReport \  
--report-context '{  
  "licenseAssetGroupArns": [  
    "arn:aws:license-manager:region:account:license-asset-group/group-id"  
  ],  
  "startTime": "2024-01-01T00:00:00Z",  
  "endTime": "2024-01-31T23:59:59Z"  
}' \  
--client-token unique-token
```

### Note

授權資產群組報告是針對指定的時間範圍隨需產生，不支援定期排程。省略 `--report-frequency` 參數。

## 報告儲存

用量報告會在 60 分鐘內開始發佈。如果您還沒有與帳戶相關聯的 Amazon S3 儲存貯體，License Manager 會在您建立用量報告時建立新的 Amazon S3 儲存貯體。報告會以下列 Amazon S3 URI 模式儲存：

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

如需 CLI 命令的詳細資訊，請參閱 [create-license-manager-report-generator](#) (AWS CLI)。

### Note

AWS License Manager 不會存放您的報告。報告會直接發佈到您的 Amazon S3 儲存貯體。刪除用量報告後，報告將不再發佈到您的 Amazon S3 儲存貯體。

## License Manager 中的庫存搜尋

License Manager 可讓您使用 [Systems Manager 庫存](#) 探索內部部署應用程式，然後將授權規則連接至這些應用程式。將授權規則連接到這些伺服器後，您可以在 License Manager 儀表板中追蹤它們與您的 AWS 伺服器。

對於使用授權資產群組的組織，庫存搜尋結果可以合併到 AWS 組織內的多個 AWS 區域和帳戶，提供探索到資源的統一檢視，無論他們位於哪個區域或帳戶。

不過，License Manager 無法在啟動或終止時驗證這些伺服器的授權規則。若要讓非 AWS 伺服器的資訊保持 up-to-date，您必須使用 License Manager 主控台的庫存搜尋區段定期重新整理庫存資訊。

Systems Manager 會將資料存放在其庫存資料中 30 天。在此期間，License Manager 會將受管執行個體視為作用中，即使無法 ping。從 Systems Manager 清除庫存資料後，License Manager 會將執行個體標記為非作用中，並更新本機庫存資料。為了保持受管執行個體計數的準確性，我們建議在 Systems Manager 中手動取消註冊執行個體，以便 License Manager 可以執行清除操作。

查詢 Systems Manager 清查需要資源資料同步，才能將清查存放在 Amazon S3 儲存貯體，Amazon Athena 會彙總組織帳戶的清查資料，並提供 AWS Glue 快速查詢體驗。如需詳細資訊，請參閱 [使用 License Manager 的服務連結角色](#)。

如果您的組織不限制 AWS 使用者建立 AMI 衍生的執行個體或在執行中的執行個體上安裝其他軟體，資源庫存追蹤也很有用。License Manager 為您提供一種機制，讓您使用庫存搜尋輕鬆探索這些執行個體和應用程式。您可以將規則連接到這些發現到的資源，並以受管 AMI 中建立的執行個體相同的方式來追蹤和驗證它們。

## 目錄

- [在 License Manager 中使用庫存搜尋](#)
- [在 License Manager 中自動探索庫存](#)

## 在 License Manager 中使用庫存搜尋

License Manager 使用 [Systems Manager 庫存](#) 來探索內部部署的軟體用量。將自我管理授權與內部部署伺服器建立關聯後，License Manager 會定期收集軟體庫存、更新授權資訊，並重新整理其儀表板以報告用量。

### 任務

- [設定庫存搜尋](#)
- [使用庫存搜尋](#)
- [將自動探索規則新增至自我管理的授權](#)
- [建立自我管理授權與庫存搜尋的關聯](#)
- [取消自我管理授權和資源的關聯](#)

## 設定庫存搜尋

使用資源庫存搜尋之前，請先完成下列要求：

- 將 License Manager 與您的 AWS Organizations 帳戶整合，以啟用跨帳戶庫存探索。如需詳細資訊，請參閱 [License Manager 中的設定](#)。
- 為要管理的伺服器 and 應用程式建立自我管理的授權。例如，建立可反映您與 Microsoft for SQL Server Enterprise 授權合約條款的自我管理授權。

## 使用庫存搜尋

完成以下步驟來搜尋您的資源庫存。您可以依名稱（例如以「SQL Server」開頭的名稱）和包含的授權類型（例如，不是「SQL Server Web」的授權）來搜尋應用程式。

搜尋您的資源庫存

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇庫存搜尋。
3. （選用）您可以指定篩選條件選項，以簡化搜尋結果，如下所示。

### Amazon EC2 資源

篩選器名稱	Description	邏輯運算子	支援的值
Resource ID (資源 ID)	資源的 ID。	Equals, Not equals	
帳戶 ID	擁有資源 AWS 的帳戶 ID。	Equals, Not equals	
平台名稱	資源的作業系統平台。	Equals, Not equals, Begins with, Contains	
Application name (應用程式名稱)	應用程式名稱。	Equals, Begins with	

篩選器名稱	Description	邏輯運算子	支援的值
包含授權的名稱	包含的授權類型。	Equals, Not equals	<ul style="list-style-type: none"> <li>SQL Server Enterprise</li> <li>SQL Server Standard</li> <li>SQL Server Web</li> <li>Windows Server Datacenter</li> </ul>
Tag	<p>指派給資源的中繼資料標籤索引鍵和選用值。</p> <p>請注意，只有在啟用跨帳戶探索時，才能使用Not equals邏輯運算子。</p>	Equals, Not equals	

## Amazon RDS 資源

篩選器名稱	Description	邏輯運算子	支援的值
引擎版本	資料庫引擎版本。	Equals	<ul style="list-style-type: none"><li>oracle-ee</li><li>oracle-se</li><li>oracle-se1</li><li>oracle-se2</li><li>db2-se</li><li>db2-ae</li></ul>

篩選器名稱	Description	邏輯運算子	支援的值
授權套件 ( 僅限 Oracle)	與 Amazon RDS for Oracle 授權相關聯的管理套件。	Equals	<ul style="list-style-type: none"> <li>Spatial and Graph</li> <li>Active Data Guard</li> <li>Label Security</li> <li>Oracle On-Line Analytical Processing (OLAP)</li> <li>Diagnostic Pack and Tuning Pack</li> </ul>

如需 Amazon RDS 資料庫產品授權的詳細資訊，請參閱《Amazon RDS 使用者指南》中的 [RDS for Oracle 授權選項](#) 或 [RDS for Db2 授權選項](#)。


## 將自動探索規則新增至自我管理的授權

將產品資訊新增至自我管理授權後，License Manager 可以追蹤已安裝這些產品的執行個體的授權用量。如需詳細資訊，請參閱 [在 License Manager 中自動探索庫存](#)。

### 將自動探索規則新增至自我管理的授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 開啟庫存搜尋頁面。
3. 選取資源，然後選擇新增自動探索規則。
4. 針對自我管理授權，選取自我管理授權。

5. 指定要探索和追蹤的產品。
6. (選用) 選取在解除安裝軟體時停止追蹤執行個體，以在 License Manager 偵測到軟體已解除安裝且任何授權親和性期間已過之後，讓授權可供重複使用。
7. (選用) 若要從自動探索中排除資源，請選取新增排除規則。

 Note

排除規則不適用於 Amazon RDS 產品 (例如 RDS for Oracle 和 RDS for Db2)。

- a. 選擇要篩選的屬性，目前支援帳戶 ID 和標籤。
  - b. 輸入資訊以識別該屬性。針對帳戶 ID，指定 12 位數 AWS 的帳戶 ID 做為值。對於標籤，輸入鍵/值對。
  - c. 重複步驟 7 以新增其他規則。
8. 選擇新增。

## 建立自我管理授權與庫存搜尋的關聯

識別您需要管理的未受管資源之後，您可以手動將資源與自我管理的授權建立關聯，而不是使用自動探索。

### 建立自我管理授權與資源的關聯

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 開啟庫存搜尋頁面。
3. 選取資源，然後選擇關聯自我管理授權。
4. 針對自我管理的授權名稱，選取自我管理的授權。
5. (選用) 選取與我的所有成員帳戶共用自我管理授權。
6. 選擇關聯。

## 取消自我管理授權和資源的關聯

如果軟體廠商的授權條款變更，您可以取消手動關聯的資源關聯，然後刪除自我管理的授權。

## 取消自我管理授權和資源的關聯

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選擇自我管理授權的名稱。
4. 選擇資源。
5. 選取要與自我管理授權取消關聯的每個資源，然後選擇取消關聯資源。

## 在 License Manager 中自動探索庫存

License Manager 使用 [Systems Manager 庫存](#) 來探索 Amazon EC2 執行個體和內部部署執行個體上的軟體使用量。您可以將產品資訊新增至自我管理的授權，而 License Manager 會追蹤已安裝這些產品的執行個體。此外，您可以根據您的授權合約指定排除規則，以決定要排除哪些執行個體。您可以排除屬於 AWS 帳戶 IDs 或與資源標籤相關聯的執行個體，以免被考慮進行自動探索

自動化探索可以新增到新的授權集、現有的自我管理授權或庫存中的資源。您可以隨時使用 [UpdateLicenseConfiguration](#) API 命令，透過 CLI 編輯自動探索規則。若要在主控台中編輯規則，您必須刪除現有的自我管理授權，並建立新的授權。

若要使用自動探索，您必須將產品資訊新增至自我管理的授權。您可以在使用庫存搜尋建立自我管理授權時執行此操作。

您無法手動取消自動探索追蹤的執行個體關聯。根據預設，在解除安裝軟體之後，自動探索不會取消追蹤執行個體的關聯。您可以設定自動探索，在解除安裝軟體時停止追蹤執行個體。

設定自動探索之後，您可以透過 License Manager 儀表板追蹤授權用量。

### 先決條件

- 將 License Manager 與您的 AWS Organizations 帳戶整合，以啟用跨帳戶庫存搜尋。如需詳細資訊，請參閱 [License Manager 中的設定](#)。

#### Note

單一帳戶可以設定自動探索，但無法新增排除規則。

- 在執行個體上安裝 Systems Manager 庫存。


### 在建立自我管理授權時設定自動探索

您可以在建立自我管理授權時設定自動探索規則和排除規則。如需詳細資訊，請參閱在 [License Manager](#) 中建立自我管理的授權。

將自動探索規則新增至現有的自我管理授權

使用以下程序，透過主控台將自動探索規則新增至現有的自我管理授權，您也可以從庫存搜尋窗格選取資源 ID 並選取新增自動探索規則來執行此操作。


1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選擇自我管理授權的名稱，以開啟授權詳細資訊頁面。
4. 在自動探索規則索引標籤上，選擇新增自動探索規則。
5. 指定要探索和追蹤的產品。

 Note

下列限制適用於 Amazon RDS 資料庫產品（例如 Amazon RDS for Oracle 和 Amazon RDS for Db2）：

- 最多支援一個指定 Amazon RDS 資料庫產品的規則。
- 每個 Amazon RDS 資料庫產品僅允許一個授權組態。

6. （選用）選取在解除安裝軟體時停止追蹤執行個體，以便在 License Manager 偵測到軟體已解除安裝且已過任何授權親和性期間後，讓授權可供重複使用。
7. （選用）若要定義要從自動探索中排除的資源，請選取新增排除規則。

 Note

- 排除規則不適用於 RDS 資料庫產品（例如 Amazon RDS for Oracle 和 Amazon RDS for Db2）。
- 排除規則只有在 [Cross-account resource discovery \(跨帳戶資源探索\)](#) 已啟用時才能使用。

- a. 選擇要篩選的屬性，目前支援帳戶 ID 和標籤。
- b. 輸入資訊以識別該屬性。針對帳戶 ID，指定 12 位數 AWS 的帳戶 ID 做為值。對於標籤，輸入鍵/值對。

- c. 重複步驟 7 以新增其他規則。
8. 完成後，請選擇新增以套用您的自動探索規則。

## License Manager 中的授權類型轉換

使用 License Manager，您可以隨著業務需求變更，在 AWS 提供的授權和自帶授權模型 (BYOL) 之間變更授權類型。您可以變更授權類型，而無需重新部署現有的工作負載。

您可以使用授權類型轉換，針對下列案例最佳化授權庫存：

### 將內部部署工作負載遷移至 Amazon EC2

在遷移期間，您可以將工作負載部署到 Amazon Elastic Compute Cloud (Amazon EC2)，並使用 AWS 提供的授權。遷移完成時，請使用 License Manager 授權類型轉換來變更執行個體的授權類型。您可以變更為 BYOL，以便使用遷移期間發行的授權。

### 使用即將到期的授權合約繼續執行工作負載

您可以使用 License Manager 授權類型轉換，從 BYOL 切換到 AWS 提供的授權。此切換可讓您使用提供的完全合規軟體授權繼續執行工作負載，AWS 並提供靈活的 pay-as-you 授權模型。如果您與作業系統的軟體廠商，例如 Microsoft 或 Canonical 的授權合約即將到期，而且您未計劃續約，您可以選擇這麼做。

### 最佳化成本

對於小型或不規則的工作負載，AWS 提供的授權（包含授權）執行個體可能更具成本效益。當您選擇使用 BYOL 時，這些選項可能需要更長期的承諾。在這種情況下，您可以使用 License Manager 授權類型轉換，將執行個體切換為包含的授權，以最佳化授權相關成本。如果您的執行個體是從您自己的虛擬機器 (VM) 映像啟動，您可以切換回 BYOL。當工作負載更穩定或可預測時，您可以選擇這樣做。

### 延伸維護

如果您的 Ubuntu 作業系統已達到標準支援結束，您可以新增 Ubuntu Pro 的付費訂閱。在 Pro 上將訂閱新增至 Ubuntu 可延長安全性更新期間。如需詳細資訊，請參閱正式文件中的 [Ubuntu Pro](#)。

### 主題

- [License Manager 中授權類型轉換的合格授權類型](#)
- [License Manager 授權類型的轉換先決條件](#)
- [在 License Manager 中轉換授權類型](#)

- [License Manager 中的租用轉換](#)
- [對 License Manager 中的授權類型轉換進行故障診斷](#)

## License Manager 中授權類型轉換的合格授權類型

您可以使用 License Manager 授權類型轉換搭配 Windows Server 和 Microsoft SQL Server 授權的支援版本和組合。您也可以搭配 Ubuntu Linux 訂閱使用授權類型轉換。

### 內容

- [License Manager 中 Windows 和 SQL Server 的合格授權類型](#)
  - [SQL Server 版本](#)
  - [SQL Server 版本](#)
  - [用量操作值](#)
  - [媒體相容性](#)
  - [轉換路徑](#)
- [License Manager 中 Linux 的合格訂閱類型](#)
  - [授權類型轉換考量事項](#)

## License Manager 中 Windows 和 SQL Server 的合格授權類型

### Important

最初從 Amazon 提供的 Amazon Machine Image (AMI) 啟動的執行個體不符合將授權類型轉換為 BYOL 的資格。

Windows 和 SQL Server 必須符合特定需求，才有資格進行授權類型轉換。

### 主題

- [SQL Server 版本](#)
- [SQL Server 版本](#)
- [用量操作值](#)
- [媒體相容性](#)
- [轉換路徑](#)

## SQL Server 版本

License Manager 支援下列 SQL Server 版本：

- SQL Server Standard 版
- SQL Server Enterprise Edition
- SQL Server Web 版本

## SQL Server 版本

License Manager 支援下列 SQL Server 版本：

- SQL Server 2005
- SQL Server 2008
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

## 用量操作值

授權類型轉換會變更與執行個體相關聯的用量操作值。下表提供每個支援作業系統的使用操作值。如需詳細資訊，請參閱 [AMI 帳單資訊欄位](#)。

作業系統詳細資訊	使用操作
將 Windows Server 做為 BYOL	RunInstances:0800
將 Windows Server 做為 BYOL 作為 BYOL 的 SQL Server (任何版本)	RunInstances:0800
包含 Windows Server 做為授權	RunInstances:0002

作業系統詳細資訊	使用操作
包含 Windows Server 做為授權 作為 BYOL 的 SQL Server ( 任何版本 )	RunInstances:0002
包含 Windows Server 做為授權 包含授權的 SQL Server Web	RunInstances:0202
包含 Windows Server 做為授權 包含授權的 SQL Server Standard	RunInstances:0006
包含 Windows Server 做為授權 包含授權的 SQL Server Enterprise	RunInstances:0102

## 媒體相容性

下表確認哪些媒體可用於哪些執行個體授權模型。

來源	Target	包含授權
	BYOL	包含授權
AWS 提供的 Windows Server 映像	否	是
AWS 提供的 SQL Server 映像	否	是
您的 Windows Server 媒體 <sup>1</sup>	是	是

來源 Target  
您的 SQL Server 媒體<sup>2</sup> 是 是

<sup>1</sup> 表示執行個體最初是從您自己的匯入虛擬機器 (VM) 啟動。您可以使用 VM Import/Export 或 等服務來匯入 [VMAWS Application Migration Service](#)。

<sup>2</sup> 表示您已取得自己的 SQL Server 安裝媒體 (.iso、.exe)。

### 轉換路徑

下表確認來源授權模型是否可以在 BYOL 和包含的授權之間轉換為另一個。如需詳細資訊，請參閱 [在 License Manager 中轉換授權類型](#)。

#### Important

- Windows Server as BYOL with SQL Server as included license 是不支援的組態。
- 指定為「不需要」的轉換不會變更改用量操作值。

來源	Target		Target		Target	
	將 Windows Server 做為 BYOL	包含 Windows Server 做為授權	將 Windows Server 做為 BYOL	包含 Windows Server 做為授權	將 Windows Server 做為 BYOL	包含 Windows Server 做為授權
Windows Server as BYOL ( 您的媒體 )	Not needed	Yes	Not needed	Yes <sup>1</sup>	Unsupported	Yes <sup>1</sup>

來源	Target					
包含授權的 Windows Server (您的媒體)	Yes <sup>2</sup>	Not needed	Yes <sup>1, 2</sup>	Not needed <sup>3</sup>	Unsupported	Yes <sup>1</sup>
包含授權的 Windows Server AWS (提供的映像)	NoX	Not needed	NoX	Not needed <sup>3</sup>	Unsupported	Yes <sup>3</sup>
Windows Server as BYOL (您的媒體)	Not needed <sup>4</sup>	Yes	Not needed	Yes	Unsupported	Yes
SQL Server as BYOL (您的媒體)						
包含授權的 Windows Server (您的媒體)	Yes <sup>2</sup>	Not needed <sup>4</sup>	Yes <sup>2</sup>	Not needed	Unsupported	Yes
SQL Server as BYOL (您的媒體)						

來源	Target					
包含授權的 Windows Server AWS (提供的映像)	NoX	Not needed <sup>4</sup>	NoX	Not needed	Unsupported	Yes
SQL Server as BYOL (您的媒體)						
Windows Server as BYOL (您的媒體)	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
包含授權的 SQL Server						
包含授權的 Windows Server (AWS 提供映像或媒體)	NoX	NoX	NoX	NoX	Unsupported	Not needed
包含授權的 SQL Server AWS (提供的影像)						

來源	Target					
包含授權的 Windows Server (您的媒體)	Yes <sup>2、5、6</sup>	Yes <sup>5</sup>	Yes <sup>2</sup>	Yes	Unsupported	Not needed
包含授權的 SQL Server (您的媒體)						
包含授權的 Windows Server AWS (提供的影像)	NoX	Yes <sup>5</sup>	NoX	Yes	Unsupported	Not needed
包含授權的 SQL Server (您的媒體)						

X 您必須使用替代組態部署新的執行個體，因為不支援轉換為目標授權類型 (s)。如需詳細資訊，請參閱 [媒體相容性](#)。

對於其他轉換案例，您可能需要採取下列步驟來執行授權轉換：

<sup>1</sup> 您必須先安裝 SQL Server，才能轉換為 BYOL for SQL Server。

<sup>2</sup> 您必須先修改 Windows 組態，以使用您自己的 KMS 伺服器來啟用授權。如需詳細資訊，請參閱 [Convert Windows Server from license included to BYOL](#)。

- <sup>3</sup> 當您從沒有 SQL Server 的來源轉換為具有 SQL Server 的目標（無論 SQL Server 授權類型為何）時，您必須先安裝 SQL Server。
- <sup>4</sup> 當您從具有 SQL Server 的來源轉換為沒有 SQL Server 的目標（無論 SQL Server 授權類型為何）時，您必須先解除安裝 SQL Server。
- <sup>5</sup> 您必須先解除安裝 SQL Server，才能轉換為包含授權的 SQL Server。
- <sup>6</sup> 您必須先執行 <sup>2</sup> 和 <sup>5</sup> 的步驟。完成這些步驟後，您必須將授權類型轉換為包含授權的 Windows Server，然後再次將授權類型轉換為 BYOL 的 Windows Server。

## License Manager 中 Linux 的合格訂閱類型

授權類型轉換適用於支援的 Ubuntu 版本。支援的版本包括 Ubuntu 18.04.1 LTS 等更新。當您將訂閱轉換為 Ubuntu Pro 時，安全更新會額外提供五年。如需詳細資訊，請參閱正式文件中的 [Ubuntu Pro](#)。

您可以使用授權類型轉換來長期支援 (LTS) 版本的 Ubuntu、RHEL 和 RHEL for SAP。您可以在 AWS 提供的選項與 Red Hat 提供的選項之間切換訂閱 AWS Marketplace。

### 授權類型轉換考量事項

授權類型轉換受制的一些考量事項如下。這並非完整清單，可能會有所變更。

#### 用於 SAP 轉換的 RHEL 和 RHEL

- 如果您要轉換到 Red Hat 銷售的訂閱做為上的 AMI 清單 AWS Marketplace，您必須先訂閱 Marketplace AMI 清單，才能啟動授權轉換。
- 若要轉換至上的 Red Hat 訂閱 SaaS 清單 AWS Marketplace，您需要在轉換之前從 Red Hat 購買訂閱。
- 如果您有來自的年度 Red Hat 合約 AWS Marketplace，則在轉換為其他訂閱類型時，將不會收到未使用月份的退款。
- 若要從 Red Hat 在中銷售的 RHEL for SAP AWS Marketplace 轉換為由在 AWS 中銷售的 RHEL for SAP，請將請求 AWS Marketplace 傳送至支援。如需詳細資訊，請參閱[建立支援案例](#)。

#### Ubuntu 轉換

- 執行個體必須執行 Ubuntu LTS，才能將授權類型轉換為 Ubuntu Pro。
- 您無法將授權類型轉換用於 Ubuntu Pro 訂閱。若要移除 Ubuntu Pro 訂閱，請參閱[移除 Ubuntu Pro 訂閱](#)。

- Ubuntu Pro 不可作為預留執行個體使用。為了節省隨需執行個體定價，我們建議您將 Ubuntu Pro 與 Savings Plans 搭配使用。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[預留執行個體](#)和《[Savings Plans 使用者指南](#)》中的[什麼是 Savings Plans ?](#)。Savings Plans
- 若要從 Ubuntu Pro 轉換為 Ubuntu LTS，請將請求傳送至支援。如需詳細資訊，請參閱[建立支援案例](#)。

## License Manager 授權類型的轉換先決條件

若要使用 License Manager 轉換授權類型，有一般和作業系統特定的先決條件。

### 主題

- [一般](#)
- [Windows](#)
- [Linux](#)

### 一般

您必須先符合下列一般先決條件，才能執行授權類型轉換：

- 您的 AWS 帳戶 必須加入 License Manager。請參閱 [License Manager 入門](#)。
- 目標執行個體必須在其上執行 AWS。不支援現場部署執行個體。
- 在您轉換授權類型之前，目標執行個體必須處於停止狀態。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[停止及啟動您的執行個體](#)。
- 如果已在目標執行個體上啟用停止保護，轉換程序將會失敗。如需詳細資訊，請參閱[對 License Manager 中的授權類型轉換進行故障診斷](#)。
- 目標執行個體必須使用 AWS Systems Manager 庫存設定。如需詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的[為 EC2 執行個體和庫存設定 Systems Manager](#)。 [AWS Systems Manager](#)
- 您的使用者或角色必須具有下列許可：
  - 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`

如需 Systems Manager 庫存的詳細資訊，請參閱 [AWS Systems Manager 庫存](#)。

## Windows

Windows 執行個體必須符合下列先決條件：

- 最初從 Amazon 提供的 Amazon Machine Image (AMI) 啟動的執行個體不符合轉換為 BYOL 的授權類型資格。原始 Amazon EC2 執行個體必須從您自己的虛擬機器 (VM) 映像啟動。如需將 VM 轉換為 Amazon EC2 的詳細資訊，請參閱 [VM Import/Export](#)。
- 若要將 SQL Server 授權變更為 BYOL，必須使用您自己的媒體安裝 SQL Server。

## Linux

Linux 執行個體必須符合下列先決條件：

### RHEL

- 如果從 AWS 提供的訂閱轉換為 Red Hat 以 AMI 清單形式銷售的訂閱 AWS Marketplace，您必須先從 Red Hat 訂閱 Marketplace AMI 清單，才能啟動授權轉換。
- 若要從 AWS 提供的訂閱轉換到上的 Red Hat 訂閱 SaaS 清單 AWS Marketplace，您需要在轉換之前從 Red Hat 購買訂閱。

## RHEL for SAP

- 對於 RHEL for SAP 和更新服務轉換，必須使用 AWS Marketplace RunInstance : 0010 用量操作和連接 AWS Marketplace 的產品程式碼從 啟動執行個體。
- 如果從 AWS 提供的訂閱轉換為 Red Hat 以 AMI 清單形式銷售的訂閱 AWS Marketplace，您必須先從 Red Hat 訂閱 Marketplace AMI 清單，才能啟動授權轉換。
- 若要從 AWS 提供的訂閱轉換到 上的 Red Hat 訂閱 SaaS 清單 AWS Marketplace，您需要在轉換之前從 Red Hat 購買訂閱。

## Ubuntu

- 執行個體必須執行 Ubuntu LTS。
- Ubuntu Pro Client 必須安裝在 Ubuntu 作業系統中。
  - 執行下列命令以確認是否已安裝 Ubuntu Pro Client：

```
pro --version
```

- 如果找不到 命令，或需要更新版本，請執行下列命令來安裝 Ubuntu Pro 用戶端：

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

- 執行個體必須能夠連接多個端點，以啟用其 Ubuntu Pro 訂閱並接收更新。您必須允許透過 TCP 連接埠 443 從執行個體傳出流量到達下列端點：
  - contracts.canonical.com – 用於 Ubuntu Pro 啟用。
  - esm.ubuntu.com : // – 用於大多數服務的 APT 儲存庫存取。
  - api.snapcraft.io – 用於安裝和執行 Snaps。
  - dashboard.snapcraft.io – 用於安裝和執行 Snaps。
  - login.ubuntu.com – 用於安裝和執行快照。
  - cloudfront.cdn.snapcraftcontent.com – 用於從內容開發網路 (CDNs) 下載。
  - livepatch.canonical.com – 用於從 Livepatch 伺服器下載修補程式。

如需詳細資訊，請參閱 [Ubuntu Pro Client 文件中的 Ubuntu Pro Client 網路需求](#)，以及 Canonical Snapcraft 文件中的 [網路需求](#)。

## 在 License Manager 中轉換授權類型

您可以使用 License Manager 主控台或轉換 Windows 授權、Microsoft SQL Server 授權和 Ubuntu Linux 訂閱 AWS CLI。您可能需要完成其他步驟，才能在執行個體的作業系統中轉換授權或訂閱。

您可以使用 License Manager 主控台或轉換授權類型 AWS CLI。當您建立授權類型轉換時，License Manager 會驗證執行個體上的帳單產品。如果這些初步驗證成功，License Manager 會建立授權類型轉換。您可以使用 `list-license-conversion-tasks` 和 `get-license-conversion-task` AWS CLI 命令來檢查授權類型轉換的狀態。

License Manager 可能會更新與自我管理授權相關聯的資源，作為授權類型轉換的一部分。具體而言，對於任何自動探索規則類型為 `自我管理授權License Included`，如果 `license included` 自動探索規則明確排除資源，則 License Manager 會取消授權類型轉換中的資源與授權的關聯。

例如，如果您的自我管理授權包含兩個自動探索規則，而且每個規則排除了包含授權的 Windows Server，則從 BYOL 轉換為授權的授權類型會讓包含 Windows Server 取消執行個體與自我管理授權的關聯。不過，如果兩個自動探索規則中只有一個包含 `License Included` 規則，則執行個體不會取消關聯。

當授權類型轉換正在進行時，您不應該啟動或停止執行個體。當授權類型轉換成功時，其狀態會從變更為 `IN_PROGRESS SUCCEEDED`。如果 License Manager 在工作流程期間遇到問題，它會更新授權類型轉換為的狀態 `FAILED`，並使用錯誤訊息更新狀態訊息。

### Note

當您轉換授權類型時，用於啟動執行個體的 AMI 上的帳單產品資訊不會變更。若要擷取準確的帳單資訊，請使用 Amazon EC2 [DescribeInstances](#) API。此外，如果您現有的工作流程從 AMIs 搜尋帳單資訊，請更新這些工作流程以使用 `DescribeInstances`。

### 內容

- [在 License Manager 中轉換 Windows 和 SQL Server 的授權類型](#)
  - [授權類型轉換限制](#)
  - [使用 License Manager 主控台轉換授權類型](#)
  - [使用轉換授權類型 AWS CLI](#)
- [在 License Manager 中轉換 Linux 的授權類型](#)
  - [使用 License Manager 主控台轉換授權類型](#)
  - [使用轉換授權類型 AWS CLI](#)

- [Red Hat 支援的轉換](#)
  - [從 RHEL for SAP with HA and Update Services \(由 AWS 銷售 AWS Marketplace\) 轉換為 RHEL for SAP with HA and Update Services \(由 Red Hat 在 銷售 AWS Marketplace\)](#)
  - [從具有 HA 和更新服務的 RHEL for SAP \(由 AWS 銷售 AWS Marketplace\) 轉換為 Red Hat 訂閱 \(由 Red Hat 銷售 AWS Marketplace\)](#)
  - [從 Red Hat License-Included \(LI\) 轉換為 RHEL \(由 Red Hat 在 銷售 AWS Marketplace\)](#)
  - [從的 Red Hat Enterprise Linux \(RHEL\) AWS 轉換為 Red Hat License-Included \(LI\)](#)
- [從 Red Hat 訂閱 \(由 Red Hat 於 中販售 AWS Marketplace\) 轉換為 Red Hat License-Included \(LI\)](#)
- [其他使用要求](#)
- [轉換為 Ubuntu Pro](#)
- [移除 Ubuntu Pro 訂閱](#)

## 在 License Manager 中轉換 Windows 和 SQL Server 的授權類型

您可以使用 License Manager 主控台或 AWS CLI 來轉換合格 Windows 和 SQL Server 執行個體的授權類型。

### 主題

- [授權類型轉換限制](#)
- [使用 License Manager 主控台轉換授權類型](#)
- [使用 轉換授權類型 AWS CLI](#)

### 授權類型轉換限制

#### Important

Microsoft 軟體的使用受 Microsoft 授權條款的約束。您有責任遵守 Microsoft 授權條款。本文件是為了方便起見而提供，您無權依賴其描述。本文件並不構成法律建議。如果您對 Microsoft 軟體的授權權利有任何疑問，請洽詢您的法務團隊、Microsoft 或 Microsoft 經銷商。

License Manager 會限制您可以根據 Microsoft Service Provider License Agreement (SPLA) 建立的授權轉換類型。授權類型轉換受制的一些限制如下所示。這並非完整清單，可能會有所變更。

- Amazon EC2 執行個體必須從您自己的虛擬機器 (VM) 映像啟動。
- 包含授權的 SQL Server 無法在專用主機上執行。
- 包含授權的 SQL Server 執行個體必須至少有 4 vCPUs。

## 使用 License Manager 主控台轉換授權類型

您可以使用 License Manager 主控台來轉換授權類型。

### Note

只會顯示處於已停止狀態且已與 AWS Systems Manager 庫存建立關聯的執行個體。

## 在主控台中開始授權類型轉換

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從左側導覽窗格中，選擇授權類型轉換，然後選擇建立授權類型轉換。
3. 針對來源作業系統，選擇您要轉換的執行個體平台：
  - RHEL
  - 適用於 SAP 的 RHEL
  - Ubuntu LTS
  - Windows BYOL
  - 包含 Windows 授權
4. (選用) 透過指定執行個體 ID 或用量操作值的值來篩選可用的執行個體。
5. 選取您要轉換其授權的執行個體，然後選擇下一步。
6. 輸入授權類型的用量操作值，選取您要轉換到的授權，然後選擇下一步。
7. 驗證您對授權類型轉換組態是否滿意，然後選擇開始轉換。

您可以從授權類型轉換面板檢視授權類型轉換的狀態。轉換狀態欄會將轉換狀態顯示為進行中、已完成或失敗。

**⚠ Important**

如果您將 Windows Server 從包含的授權轉換為 BYOL，則必須根據您的 Microsoft 授權合約啟用 Windows。如需詳細資訊，請參閱[Convert Windows Server from license included to BYOL](#)。

## 使用 轉換授權類型 AWS CLI

若要在 中開始授權類型轉換 AWS CLI：

### 判斷執行個體的授權類型

1. 確認您已安裝並設定 AWS CLI。如需詳細資訊，請參閱[安裝、更新和解除安裝 AWS CLI](#)和[設定 AWS CLI](#)。

**⚠ Important**

您可能需要更新 AWS CLI 來執行特定命令，並在下列步驟中接收所有必要的輸出。

2. 確認您具有執行 `create-license-conversion-task-for-resource` AWS CLI 命令的許可。如需此方面的協助，請參閱 [建立 License Manager 的 IAM 政策](#)。
3. 若要判斷目前與執行個體相關聯的授權類型，請執行下列 AWS CLI 命令。將執行個體 ID 取代為您要決定授權類型的執行個體 ID。

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

4. 以下是 `describe-instances` 命令的範例回應。請注意，`UsageOperation` 值是與授權相關聯的帳單資訊代碼。`UsageOperationUpdateTime` 是帳單代碼更新的時間。如需詳細資訊，請參閱《Amazon EC2 API 參考 [DescribeInstances](#)》中的。

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

**Note**

使用 SQL Server Enterprise BYOL 的 Windows Server 用量操作與 Windows BYOL 的用量操作相同，因為它們的費用相同。

## 將 Windows Server 從包含的授權轉換為 BYOL

當您將 Windows Server 從包含的授權轉換為 BYOL 時，License Manager 不會自動啟用 Windows。您必須將執行個體的 KMS 伺服器從 AWS KMS 伺服器切換到您自己的 KMS 伺服器。

**Important**

若要從包含的授權轉換為 BYOL，必須從您自己的虛擬機器 (VM) 映像啟動原始 Amazon EC2 執行個體。如需將 VM 轉換為 Amazon EC2 的詳細資訊，請參閱 [VM Import/Export](#)。最初從 Amazon Machine Image (AMI) 啟動的執行個體不符合授權轉換為 BYOL 的資格。

請檢查您的 Microsoft 授權合約，以判斷您可以使用哪些方法來啟用 Microsoft Windows Server。例如，如果您使用的是 KMS 伺服器，您必須從執行個體的原始 BYOL 組態取得 KMS 伺服器的地址。

1. 若要轉換執行個體的授權類型，請執行下列命令，將 ARN 取代為您要轉換之執行個體的 ARN：

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

2. 若要在轉換授權後啟用 Windows，您必須將作業系統的 Windows Server KMS 伺服器指向您自己的 KMS 伺服器。登入 Windows 執行個體並執行下列命令：

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

## 將 Windows Server 從 BYOL 轉換為包含的授權

當您將 Windows Server 從 BYOL 轉換為包含授權時，License Manager 會自動將執行個體的 KMS 伺服器切換到 AWS KMS 伺服器。

若要將執行個體的授權類型從 BYOL 轉換為包含的授權，請執行下列命令，以您要轉換之執行個體的 ARN 取代 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
```

從 BYOL 將 Windows Server 和 SQL Server 轉換為包含的授權

您可以同時切換多個產品。例如，您可以在一個授權類型轉換中同時轉換 Windows Server 和 SQL Server。

若要將 Windows Server 執行個體的授權類型從 BYOL 轉換為包含授權，以及將 SQL Server Standard 從 BYOL 轉換為包含授權，請執行下列命令，以您要轉換之執行個體的 ARN 取代 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 License Manager 中轉換 Linux 的授權類型

您可以使用 License Manager 主控台或 AWS CLI 來轉換合格 Ubuntu LTS、RHEL 和 RHEL for SAP 執行個體的授權類型。

主題

- [使用 License Manager 主控台轉換授權類型](#)
- [使用 轉換授權類型 AWS CLI](#)
- [移除 Ubuntu Pro 訂閱](#)

使用 License Manager 主控台轉換授權類型

您可以使用 License Manager 主控台來轉換授權類型。

#### Note

只會顯示處於已停止狀態且已與 AWS Systems Manager 庫存建立關聯的執行個體。

## 在主控台中開始授權類型轉換

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從左側導覽窗格中，選擇授權類型轉換，然後選擇建立授權類型轉換。
3. 針對來源作業系統，選擇您要轉換的執行個體平台：
  - RHEL
  - 適用於 SAP 的 RHEL
  - Ubuntu LTS
  - Windows BYOL
  - 包含 Windows 授權
4. (選用) 透過指定執行個體 ID 或用量操作值的值來篩選可用的執行個體。
5. 選取您要轉換其授權的執行個體，然後選擇下一步。
6. 輸入授權類型的用量操作值，選取您要轉換到的授權，然後選擇下一步。
7. 驗證您對授權類型轉換組態是否滿意，然後選擇開始轉換。

您可以從授權類型轉換面板檢視授權類型轉換的狀態。轉換狀態欄會將轉換狀態顯示為進行中、已完成或失敗。

## 使用 轉換授權類型 AWS CLI

若要在 中開始授權類型轉換 AWS CLI，您應該確認執行個體的授權類型符合資格，然後執行授權類型轉換以變更為必要的訂閱。如需合格訂閱類型的詳細資訊，請參閱 [License Manager 中 Linux 的合格訂閱類型](#)。

## 判斷執行個體的授權類型

確認您已安裝並設定 AWS CLI。如需詳細資訊，請參閱安裝、更新和解除安裝 AWS CLI 和設定 AWS CLI。

### Important

您可能需要更新 AWS CLI 來執行特定命令，並在下列步驟中接收所有必要的輸出。確認您具有執行 `create-license-conversion-task-for-resource` AWS CLI 命令的許可。如需詳細資訊，請參閱 [建立 License Manager 的 IAM 政策](#)。

若要判斷目前與執行個體相關聯的授權類型，請執行下列 AWS CLI 命令。將執行個體 ID 取代為您要決定授權類型的執行個體 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 命令的範例回應。UsageOperation 值是與授權相關聯的帳單資訊代碼。用量操作值 RunInstances 表示執行個體正在使用 AWS 提供的授權。UsageOperationUpdateTime 是帳單代碼更新的時間。如需詳細資訊，請參閱《Amazon EC2 API 參考 [DescribeInstances](#)》中的。

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

## Red Hat 支援的轉換

Red Hat Enterprise Linux (RHEL) 產品支援下列轉換。每個轉換都需要特定的來源和目的地授權內容，並且可能會有其他要求。

從 RHEL for SAP with HA and Update Services (由 AWS 銷售 AWS Marketplace) 轉換為 RHEL for SAP with HA and Update Services (由 Red Hat in 銷售 AWS Marketplace)

範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \
--resource-arn <instance_arn> \
--source-license-context
"UsageOperation=RunInstances:0010,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<so
\
--destination-license-context
"UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<de
```

備註：

- 具有 HA 和更新服務的 RHEL for SAP (由 AWS 銷售 AWS Marketplace) 有許多不同的產品代碼 IDs (a.k.a. Marketplace 代碼)，視您的 AWS Marketplace 產品訂閱而定。請檢查 EC2 describe-instances 回應，以取得執行個體上的正確產品代碼 ID。

- RHEL for SAP with HA and Update Services (由 Red Hat 在銷售 AWS Marketplace) 有兩個不同的產品代碼 IDs：du6111oq9lwrc996awt04qyql (NA & Global) 和 952qwcsxkm430zxhpy32i7w8g (EMEA)。您應該使用哪些取決於您的區域。請查看您的 RHEL for SAP with HA and Update Services subscription in Marketplace，了解它是什麼。

轉換後，您無法將執行個體轉換回具有 HA 和更新服務的 RHEL for SAP (由 AWS 銷售 AWS Marketplace)，除非您被允許列出此私有功能，這需要支援請求。如需詳細資訊，請參閱[建立支援案例](#)。

從具有 HA 和更新服務的 RHEL for SAP (由 AWS 銷售 AWS Marketplace) 轉換為 Red Hat 訂閱 (由 Red Hat 銷售 AWS Marketplace)

Red Hat 訂閱 (由 Red Hat 在中販售 AWS Marketplace) 是指客戶可以從中購買的 SaaS 訂閱 AWS Marketplace。目前還有兩個清單。

範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \  
  --resource-arn <instance_arn> \  
  --source-license-context  
  "UsageOperation=RunInstances:0010,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<source_product_code_id>}" \  
  --destination-license-context "UsageOperation=RunInstances:00g0"
```

備註：

- 具有 HA 和更新服務的 RHEL for SAP (由 AWS 銷售 AWS Marketplace) 有許多不同的產品代碼 IDs(a.k.a. Marketplace 代碼)，取決於您的 AWS Marketplace 產品訂閱。請檢查 EC2 describe-instances 回應，以取得執行個體上的正確產品代碼 ID。
- Red Hat 訂閱 (由 Red Hat 於中販售 AWS Marketplace) 沒有產品代碼可新增至執行個體。
  - 說明：SaaS 產品代碼未連接至 EC2 執行個體，因此客戶在叫用 create-license-conversion-task-for-resource CLI 命令時，預期不會包含目的地產品代碼。

轉換後，您無法將執行個體轉換回具有 HA 和更新服務的 RHEL for SAP (由 AWS 銷售 AWS Marketplace)，除非您被允許列出此私有功能，這需要支援請求。如需詳細資訊，請參閱[建立支援案例](#)。

## 從 Red Hat License-Included (LI) 轉換為 RHEL (由 Red Hat in 銷售 AWS Marketplace)

### 範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context "UsageOperation=RunInstances:0010" \
  --destination-license-context
  "UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<de
```

### 備註：

- RHEL (由 Red Hat in 銷售 AWS Marketplace) 有兩個不同的產品代碼 IDs：6cd5fxzrad0cu2j23p692xytz (NA & Global) 和 6t1yup6mik9ng3ge36n33xqhw (EMEA)。您應該使用哪些取決於您的區域。請查看您的 RHEL for SAP with HA and Update Services subscription in Marketplace，了解它是什麼。

## 從的 Red Hat Enterprise Linux (RHEL) AWS 轉換為 Red Hat License-Included (LI)

### 範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
  "UsageOperation=RunInstances,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<source_
  \
  --destination-license-context "UsageOperation=RunInstances:0010"
```

### 或者，這個：

```
aws license-manager create-license-conversion-task-for-resource \
  --resource-arn <instance_arn> \
  --source-license-context
  "UsageOperation=RunInstances:00g0,ProductCodes=[{ProductCodeType=marketplace,ProductCodeId=<so
  \
  --destination-license-context "UsageOperation=RunInstances:0010"
```

### 備註：

- 的 Red Hat Enterprise Linux (RHEL) AWS 有兩個不同的產品代碼 IDs：6cd5fxzrad0cu2j23p692xytz (NA & Global) 和 6t1yup6mik9ng3ge36n33xqhw (EMEA)。您應該使

用哪些 取決於您的區域。請檢查 EC2 describe-instances 回應，以取得執行個體上的正確產品代碼 ID。

- AWS 執行個體的 Red Hat Enterprise Linux (RHEL) 可能有用量操作 RunInstances 或 RunInstances : 00g0。這取決於執行個體最初是從 AWS 產品 AMI 的 Red Hat Enterprise Linux (RHEL) 啟動，還是稍後轉換為此訂閱。請檢查 EC2 describe-instances 回應，了解執行個體上的正確用量操作。

範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \  
  --resource-arn <instance_arn> \  
  --source-license-context "UsageOperation=RunInstances:0010" \  
  --destination-license-context "UsageOperation=RunInstances:00g0"
```

備註：

- Red Hat 訂閱（由 Red Hat 於中販售 AWS Marketplace）沒有產品代碼可新增至執行個體。
  - 說明：SaaS 產品代碼未連接至 EC2 執行個體，因此客戶在叫用 create-license-conversion-task-for-resource CLI 命令時，預期不會包含目的地產品代碼。
- Red Hat 訂閱（由 Red Hat 於中販售 AWS Marketplace）必須由 CLI 命令的發起人訂閱。目前尚不支援相同組織中其他帳戶中的訂閱。

從 Red Hat 訂閱（由 Red Hat 於中販售 AWS Marketplace）轉換為 Red Hat License-Included (LI)

範例 CLI 命令：

```
aws license-manager create-license-conversion-task-for-resource \  
  --resource-arn <instance_arn> \  
  --source-license-context "UsageOperation=RunInstances:00g0" \  
  --destination-license-context "UsageOperation=RunInstances:0010"
```

備註：

- Red Hat 訂閱（由 Red Hat 於中販售 AWS Marketplace）沒有新增至執行個體的產品代碼。

## 其他使用要求

執行個體在建立其授權轉換任務之前，必須處於停止狀態。在授權轉換任務完成或失敗之前，客戶不應嘗試啟動或終止執行個體。這與所有授權類型轉換的要求相同。

如果目的地是下列其中一個 Marketplace 產品：

- RHEL for SAP 搭配 HA 和更新服務（由 Red Hat 在中販售 AWS Marketplace)
- RHEL（由 Red Hat 在中販售 AWS Marketplace)
- Red Hat 訂閱（由 Red Hat 在中販售 AWS Marketplace)

然後，客戶在 Marketplace 中必須擁有作用中的訂閱，才能叫用 CLI 命令。否則，轉換請求可能會被拒絕或失敗。與主控台不同，從 CLI 建立授權轉換任務時，License Manager 不會嘗試自動將客戶訂閱到目的地產品。

## 轉換為 Ubuntu Pro

將執行個體從 Ubuntu LTS 轉換為 Ubuntu Pro 之前，您的執行個體必須設定傳出網際網路存取，以從正式伺服器擷取授權字符並安裝 Ubuntu Pro 用戶端。如需詳細資訊，請參閱[License Manager 授權類型的轉換先決條件](#)。

若要將 Ubuntu LTS 轉換為 Ubuntu Pro，請遵循下列步驟：

1. 從執行下列命令，AWS CLI 同時指定執行個體的 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. 從執行個體內執行下列命令，以擷取 Ubuntu Pro 訂閱狀態的詳細資訊：

```
pro status
```

3. 確認您的輸出表示執行個體具有有效的 Ubuntu Pro 訂閱：

```

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 訂閱

授權類型轉換只能用來從 Ubuntu LTS 轉換為 Ubuntu Pro。如果您需要從 Ubuntu Pro 轉換為 Ubuntu LTS，您將需要向 [提出請求](#) 支援。如需詳細資訊，請參閱[建立支援案例](#)。

## License Manager 中的租用轉換

您可以變更執行個體的租用，以最適合您的使用案例。您可以使用 [modify-instance-placement](#) AWS CLI 命令來切換下列租用：

- 共同
- Dedicated Instance
- Dedicated Host
- 主機資源群組

您的帳戶必須具有可用容量的專用主機，才能啟動執行個體，以切換到專用主機租用類型。如需使用專用主機的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[使用專用主機](#)。

若要移至主機資源群組租用類型，您的帳戶中必須至少有一個主機資源群組。若要在主機資源群組中啟動執行個體，執行個體必須具有與主機資源群組相關聯的相同授權集。如需詳細資訊，請參閱[License Manager 中的主機資源群組](#)。

### 租用轉換限制

下列限制適用於租用轉換：

- 所有租用類型都允許使用 Linux 帳單代碼。
- 共用租用不允許使用 Windows BYOL 帳單代碼。

- 所有租用類型皆允許包含 Windows Server 授權的帳單代碼。
- 共用租用和專用執行個體上允許所有支援的 SQL Server 版本和包含 SUSE (SLES) 授權的帳單代碼。不過，專用主機和主機資源群組上不允許這些帳單代碼。
- 專用主機和主機資源群組上不允許包含 Windows Server 以外的授權帳單代碼。

使用 變更執行個體的租用 AWS CLI

執行個體必須處於 stopped 狀態，才能變更其租用。

若要停止執行個體，請執行下列命令：

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

若要將執行個體從任何租用變更為 default 或 dedicated 租用，請執行下列命令：

default

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

dedicated

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

若要使用自動配置將執行個體從任何租用變更為 host 租用，請執行下列命令：

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

若要將執行個體從任何租用變更為 host 租用，以特定專用主機為目標，請執行下列命令：

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

若要使用主機資源群組將執行個體從任何租用變更為 host 租用，請執行下列命令：

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

```
--tenancy host --host-resource-group-arn <host_resource_group_arn>
```

## 對 License Manager 中的授權類型轉換進行故障診斷

### 故障診斷主題

- [Windows 啟用](#)
- [執行個體【執行個體】是從 Amazon 擁有的 AMI 啟動。提供最初從 BYOL AMI 啟動的執行個體。](#)
- [無法驗證該執行個體【執行個體】是從 BYOL AMI 啟動。確保 SSM Agent 在您的執行個體上執行。](#)
- [呼叫 CreateLicenseConversionTaskForResource 操作時發生錯誤 \(InvalidParameterValueException\) : ResourceId - 【instance】處於變更授權類型的無效狀態。](#)
- [EC2 執行個體【執行個體】無法停止。確保您具有 EC2 的許可 StopInstances。](#)

### Windows 啟用

授權類型轉換包含多個步驟。在某些情況下，當您將 Windows Server 執行個體從 BYOL 轉換為包含授權時，執行個體上的帳單產品會成功更新。不過，KMS 伺服器可能不會切換到 AWS KMS 伺服器。

若要修復此問題，請依照[為什麼我的 EC2 Windows 執行個體上的 Windows 啟用失敗？](#)中的步驟，使用 Systems Manager [AWSSupport-ActivateWindowsWithAmazonLicense](#) Automation Runbook 啟用 Windows，或登入執行個體並手動切換到 AWS KMS 伺服器。

**執行個體【執行個體】** 是從 Amazon 擁有的 AMI 啟動。提供最初從 BYOL AMI 啟動的執行個體。

您必須從已匯入的 AMI 啟動 Amazon EC2 Windows 執行個體，才能執行授權類型轉換為自有授權模型 (BYOL)。最初從 Amazon 擁有的 AMI 啟動的執行個體不符合將授權類型轉換為 BYOL 的資格。如需詳細資訊，請參閱[License Manager 授權類型的轉換先決條件](#)。

**無法驗證該執行個體【執行個體】** 是從 BYOL AMI 啟動。確保 SSM Agent 在您的執行個體上執行。

為了讓授權類型轉換成功，您的執行個體必須先上線並由 Systems Manager 管理，才能收集其庫存。AWS Systems Manager 代理程式 (SSM 代理程式) 將從執行個體收集庫存，其中包含作業系統的詳細資訊。如需詳細資訊，請參閱 AWS Systems Manager 《使用者指南》中的[檢查 SSM 代理程式狀態和啟動代理程式](#)和[對 SSM 代理程式進行故障診斷](#)。

呼叫 **CreateLicenseConversionTaskForResource** 操作時發生錯誤 (InvalidParameterValueException) : ResourceId - **【instance】** 處於變更授權類型的無效狀態。

若要執行授權類型轉換，目標執行個體必須處於停止狀態。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [License Manager 授權類型的轉換先決條件](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesStopping.html) 和 停用執行個體的故障診斷。 <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/TroubleshootingInstancesStopping.html>

EC2 執行個體 **【執行個體】** 無法停止。確保您具有 EC2 的許可 **StopInstances**。

您必須擁有許可，才能在目標執行個體上執行 StopInstances EC2 API 動作。此外，如果在目標執行個體上啟用停止保護，轉換程序將會失敗。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [停用執行中或已停止執行個體的停止保護](#)。

## License Manager 中的主機資源群組

Amazon EC2 專用主機是實體伺服器，具有完全專用於您的 EC2 執行個體容量。主機資源群組是您可以做為單一實體管理的專用主機集合。啟動執行個體時，License Manager 會根據您設定的設定，配置主機並啟動執行個體。您可以將現有的專用主機新增至主機資源群組，並透過 License Manager 利用自動化主機管理。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [專用主機](#)。

您可以使用主機資源群組，依用途分隔主機，例如開發測試主機與生產、組織單位或授權限制條件。將專用主機新增至主機資源群組後，您無法直接在專用主機上啟動執行個體，您必須使用主機資源群組來啟動執行個體。

### 設定

您可以為主機資源群組設定下列設定：

- 自動配置主機 – 指出如果在此主機資源群組中啟動執行個體會超過其可用容量，Amazon EC2 是否可以代表您配置新的主機。
- 自動釋出主機 – 指出 Amazon EC2 是否可以代表您釋出未使用的主機。未使用的主機沒有執行中的執行個體。
- 自動復原主機 – 指出 Amazon EC2 是否可以將執行個體從意外失敗的主機移至新的主機。
- 關聯的自我管理授權 – 可用來啟動此主機資源群組中執行個體的自我管理授權。
- (選用) 執行個體系列 – 您可以啟動的執行個體類型。根據預設，您可以啟動專用主機上支援的任何執行個體類型。如果您啟動 [Nitro 型](#) 執行個體，則可以在相同的主機資源群組中啟動具有不同執行

個體類型的執行個體。否則，您只能在相同的主機資源群組中啟動具有相同執行個體類型的執行個體。

## 目錄

- [在 License Manager 中建立主機資源群組](#)
- [在 License Manager 中共用主機資源群組](#)
- [在 License Manager 中將專用主機新增至主機資源群組](#)
- [在 License Manager 中的主機資源群組中啟動執行個體](#)
- [在 License Manager 中修改主機資源群組](#)
- [從 License Manager 中的主機資源群組移除專用主機](#)
- [在 License Manager 中刪除主機資源群組](#)

## 在 License Manager 中建立主機資源群組

設定主機資源群組，讓 License Manager 管理您的專用主機。為了充分利用最昂貴的授權，您可以將一個或多個核心或通訊端型自我管理授權與主機資源群組建立關聯。若要最佳化主機使用率，您可以使用主機資源群組來允許所有核心型或通訊端型自我管理授權。

### 建立主機資源群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇主機資源群組。
3. 選擇建立主機資源群組。
4. 如需主機資源群組詳細資訊，請指定主機資源群組的名稱和描述。
5. 對於 EC2 專用主機管理設定，請視需要啟用或停用下列設定：
  - 自動配置主機
  - 自動發行主機
  - 自動復原主機
6. (選用) 針對其他設定，選取您可以在主機資源群組中啟動的執行個體系列。
7. 針對自我管理的授權，選取一或多個核心型或通訊端型自我管理的授權。
8. (選用) 針對標籤，新增一或多個標籤。
9. 選擇 Create (建立)。

## 在 License Manager 中共用主機資源群組

您可以使用 AWS Resource Access Manager 透過 共用主機資源群組 AWS Organizations。在您共用主機資源群組和自我管理授權之後，成員帳戶可以在共用主機資源群組中啟動執行個體。新主機配置在擁有主機資源群組的帳戶中。成員帳戶擁有執行個體。如需詳細資訊，請參閱《AWS RAM 使用者指南》<https://docs.aws.amazon.com/ram/latest/userguide/>。

## 在 License Manager 中將專用主機新增至主機資源群組

您可以從 AWS 管理主控台 AWS CLI 或 AWS API 將現有主機新增至主機資源群組。若要新增主機，您必須是建立專用主機和主機資源群組 AWS 的帳戶擁有者。如果您的主機資源群組列出允許的自我管理授權和執行個體類型，您新增的主機必須符合這些要求。

### Note

如果您停止執行個體並想要重新啟動執行個體，則必須執行下列兩個任務：

- [修改](#)執行個體以指向主機資源群組。
- [關聯](#)自我管理的授權以符合主機資源群組。

您可以新增至主機資源群組的專用主機數量沒有限制。如需資源群組的詳細資訊，請參閱 [AWS Resource Groups 使用者指南](#)。

使用下列步驟將一或多個專用主機新增至資源群組：

1. 登入位於 <https://console.aws.amazon.com/license-manager/> 的 License Manager 主控台。
2. 選擇主機資源群組。
3. 從主機資源群組名稱清單中，按一下您要新增專用主機的主機資源群組名稱。
4. 選擇專用主機。
5. 選擇新增。
6. 選擇要新增至主機資源群組的一或多個專用主機。
7. 選擇新增。

新增主機可能需要 1 - 2 分鐘，然後會出現在專用主機清單中。

## 在 License Manager 中的主機資源群組中啟動執行個體

啟動執行個體時，您可以指定主機資源群組。例如，您可以使用下列 [run-instances](#) 命令。您必須將核心或通訊端型自我管理授權與 AMI 建立關聯。

```
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 主控台。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[在主機資源群組中啟動執行個體](#)。

## 在 License Manager 中修改主機資源群組

您可以隨時修改主機資源群組的設定。您無法將主機限制設定為低於主機資源群組中現有主機的數量。如果主機資源群組中執行該類型的執行個體，則無法移除執行個體類型。

### 修改主機資源群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇主機資源群組。
3. 選取主機資源群組，然後選擇動作、編輯。
4. 視需要修改設定。
5. 選擇 Save changes (儲存變更)。

## 從 License Manager 中的主機資源群組移除專用主機

當您從主機資源群組中移除主機時，主機上執行的執行個體會保留在主機上。連接至主機資源群組的執行個體會保持與該群組的關聯，而透過親和性直接連接至主機的執行個體會維護相同的屬性。如果您與其他 AWS 帳戶共用主機資源群組，License Manager 會自動移除共用主機，而消費者會收到移出通知，在 15 天內從主機移動其執行個體。若要使用已從主機資源群組移除的專用主機，請參閱《Amazon EC2 使用者指南》中的[使用專用主機](#)。

使用下列步驟將專用主機移除至主機資源群組：

1. 登入位於 <https://console.aws.amazon.com/license-manager/> 的 License Manager 主控台。

2. 選擇主機資源群組。
3. 按一下您要移除專用主機的主機資源名稱。
4. 選擇專用主機。
5. 選擇要從主機資源群組刪除的專用主機。或者，您可以依主機 ID、主機類型、主機狀態或可用區域來搜尋專用主機。
6. 選擇移除。
7. 再次選擇移除以確認。

## 在 License Manager 中刪除主機資源群組

如果主機資源群組沒有主機，您可以將其刪除。

### 刪除主機資源群組

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇主機資源群組。
3. 選取主機資源群組，然後選擇動作、刪除。
4. 出現確認提示時，請選擇 Delete (刪除)。

## 針對支援的軟體產品使用 License Manager 使用者型訂閱

透過 中的使用者型訂閱 AWS License Manager，您可以購買完全相容的授權軟體訂閱。授權由 Amazon 提供，並收取每位使用者的訂閱費用。Amazon EC2 提供預先設定的 Amazon Machine Image (AMIs) 與支援的軟體，以及包含授權的 Windows Server 授權。這些授權可以在沒有長期授權承諾的情況下使用。

若要使用使用者型訂閱，請將來自 [AWS Directory Service for Microsoft Active Directory](#)(AWS Managed Microsoft AD) 或來自自我管理（內部部署）網域的使用者與提供軟體的 EC2 執行個體建立關聯。若要提供授權軟體，您必須建立以使用者為基礎的訂閱，並將其與從預先設定的 AMIs 執行個體建立關聯。[AWS Systems Manager](#) 會設定並強化您啟動的授權包含執行個體。使用者必須與遠端桌面軟體連線，才能存取提供軟體的執行個體。

包含授權之執行個體的每個相關聯使用者和 [vCPU](#) 都會產生費用。Amazon EC2 預留執行個體和 Savings Plan 定價模型有助於最佳化 Amazon EC2 成本。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的 [預留執行個體](#)。以使用者為基礎的訂閱會從上半月開始計費，直到月底為止。

## 主題

- [在 License Manager 中使用使用者型訂閱的考量事項](#)
- [License Manager 中的訂閱費用](#)
- [在 License Manager 中建立使用者型訂閱的先決條件](#)
- [License Manager 中使用者型訂閱支援的軟體產品](#)
- [Active Directory](#)
- [其他軟體](#)
- [License Manager 中的使用者型訂閱入門](#)
- [為更活躍的遠端使用者工作階段設定 Active Directory GPO](#)
- [AWS License Manager 使用共用的跨帳戶入門 AWS Managed Microsoft AD](#)
- [從包含的授權 AMI 啟動執行個體](#)
- [使用 RDP 連線至以使用者為基礎的訂閱執行個體](#)
- [修改 Microsoft Office 訂閱的防火牆設定](#)
- [管理 License Manager 使用者型訂閱的訂閱使用者](#)
- [從 License Manager 設定取消註冊 Active Directory](#)
- [對 License Manager 中的使用者型訂閱進行故障診斷](#)

## 在 License Manager 中使用使用者型訂閱的考量事項

搭配 License Manager 使用使用者型訂閱時，適用下列考量：

- 包含授權的 Microsoft 遠端桌面服務 (Win Remote Desktop Services SAL) AWS Marketplace 訂閱需支付每位使用者的每月費用，不按比例分配。
- 根據預設，提供以使用者為基礎的訂閱的執行個體一次最多支援兩個作用中的使用者工作階段。若要啟用兩個以上的作用中使用者工作階段，您可以設定 Active Directory 群組政策物件 (GPO)，並將 Microsoft RDS 授權模式設定為 Per User。如需詳細資訊，請參閱 [先決條件為更活躍的遠端使用者工作階段設定 Active Directory GPO](#)。
- 當您在提供以使用者為基礎的訂閱的執行個體上建立具有管理員權限的本機使用者時，執行個體運作狀態可能會變更為運作狀態不佳。License Manager 可以終止不合規運作狀態不佳的執行個體。如需詳細資訊，請參閱 [對執行個體合規進行故障診斷](#)。
- 當您使用 Microsoft Office 產品設定 Active Directory 時，VPC 必須在至少一個子網路中佈建 [VPC 端點](#)。如果您想要移除 License Manager 建立的所有 VPC 端點資源，您必須從 License Manager 設

定中移除任何已設定的 Active Directory。如需詳細資訊，請參閱[從 License Manager 設定取消註冊 Active Directory](#)。

- AWSLicenseManager 具有 License Manager UserSubscriptions 指派給執行個體之值的標籤索引鍵不得變更或刪除。
- 為了讓服務如預期運作，為 License Manager 建立的兩個網路介面不得變更或刪除。
- License Manager 在 AWS Managed Microsoft AD 目錄AWS 的預留組織單位 (OU) 中建立的物件不得變更或刪除。
- 針對使用者型訂閱部署的執行個體必須是具有的受管節點，AWS Systems Manager 並加入相同的網域。如需由 Systems Manager 管理執行個體的相關資訊，請參閱本指南的[對 License Manager 中的使用者型訂閱進行故障診斷](#)一節。
- 若要停止使用者產生 Microsoft Office 或 Visual Studio 訂閱費用，您必須取消使用者與其關聯之所有執行個體的關聯。如需詳細資訊，請參閱[取消使用者與提供 License Manager 使用者型訂閱之執行個體的關聯](#)。

## License Manager 中的訂閱費用

License Manager 中的訂閱和計費會根據使用的訂閱產品而有所不同。

### Microsoft Office 和 Visual Studio 訂閱

對於 Microsoft Office 和 Visual Studio 訂閱，一旦您將使用者與提供訂閱產品的所有執行個體取消關聯，並從產品取消訂閱，帳單就會停止。

### Microsoft 遠端桌面服務 (RDS) 訂閱

Microsoft RDS 會根據使用者訂閱和使用者連線到提供訂閱產品的執行個體時，從授權伺服器發出的用戶端存取授權 (CAL) 字符的組合，按每位使用者每月計費。

## License Manager 中的 Microsoft RDS 帳單

Microsoft RDS 計費從 Active Directory 使用者透過 License Manager 訂閱時開始，並在用戶端存取授權 (CAL) 字符過期後結束，從發出之日起 60 天，不按比例分配部分月份。即使您取消訂閱使用者，帳單仍會持續到字符過期為止。

如果取消訂閱的使用者在授權字符過期後繼續登入，則會自動重新訂閱使用者，計費會持續進行，直到再次取消訂閱且其字符過期為止。

同樣地，如果使用者從未訂閱，但登入與授權伺服器相關聯的執行個體，則 License Manager 會自動訂閱他們並開始 RDS 計費。帳單會持續進行，直到取消訂閱且其字符過期為止。

若要在當月結束時停止使用者計費，您必須在取消訂閱之前，將該使用者從為授權伺服器設定的 Active Directory 中移除。

### Warning

如果您移除仍擁有作用中 Microsoft Office 或 Visual Studio 訂閱的 Active Directory 使用者，則該使用者將無法再存取與其相關聯的執行個體。

下列範例案例示範 RDS 帳單的運作方式。

#### 案例 1：標準訂閱和計費

下列案例顯示一組標準動作，這些動作會影響在 12/15/2024 訂閱但從未存取訂閱執行個體的 Active Directory (AD) 使用者的帳單。

動作：如果使用者從未取消訂閱，則帳單會無限期繼續。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除使用者	帳單結束
12/15/2024	12/15/2024	--	N/A	--	--	--

動作：使用者已於 1/15/2025 取消訂閱。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除使用者	帳單結束
12/15/2024	12/15/2024	--	N/A	1/15/2025	No	1/31/2025

#### 案例 2：授權字符如何影響使用者訂閱和計費

下列案例顯示授權字符過期如何影響在 9/15/2024 訂閱的 Active Directory (AD) 使用者的使用者訂閱，並在同一天登入加入網域的訂閱產品執行個體。

動作：AD 使用者的初始訂閱和登入。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除使用者	帳單結束
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

動作：相同的 AD 使用者已於 10/19/2024 取消訂閱。不過，由於使用者並未從目錄中移除，因此計費會持續到授權字符到期的月底為止。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除使用者	帳單結束
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

替代動作：AD 管理員會在 10/20/2024 從目錄移除使用者，然後在第二天取消訂閱使用者。在此情況下，計費會在使用者從目錄移除的月底停止。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除的使用者	帳單結束
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/21/2024	10/20/2024	10/31/2024

案例 3：已取消訂閱的使用者已重新訂閱

下列案例顯示，在存取加入網域的訂閱產品執行個體時，授權字符已過期的已取消訂閱 Active Directory (AD) 使用者如何自動重新訂閱。

動作：AD 使用者的初始訂閱和登入。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除的使用者	帳單結束
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

動作：相同的 AD 使用者已於 10/19/2024 取消訂閱。不過，由於使用者並未從目錄中移除，因此計費會持續到授權字符到期的月底為止。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除的使用者	帳單結束
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

動作：相同的 AD 使用者會在其先前的授權字符過期後但在帳單結束之前存取加入網域的訂閱產品執行個體。帳單會持續進行，直到使用者再次取消訂閱且其新字符過期為止。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除的使用者	帳單結束
11/20/2024 (re-subscribed)	billing continues	11/20/2024 4	1/20/2025	--	--	--

#### 案例 4：執行個體存取時自動訂閱

下列案例顯示從未訂閱 RDS SAL 的 Active Directory (AD) 使用者如何在登入加入網域的訂閱產品執行個體時自動訂閱。

動作：從未在 9/15/2024 訂閱 RDS SAL 的 AD 使用者登入加入網域的訂閱產品執行個體，並自動訂閱。帳單開始，並持續到使用者取消訂閱且其新字符過期為止。

已訂閱 AD 使用者	帳單開始	發行的 CAL	CAL 過期	使用者已取消訂閱	從 AD 移除的使用者	帳單結束
9/15/2024 (自動訂閱)	9/15/2024	9/15/2024	11/15/2024	--	--	--

如需每個使用者 CALs 的 Microsoft RDS 運作方式的詳細資訊，請參閱 Microsoft Learn 網站上的授權遠端桌面部署文章中的每個使用者 CALs 一節。<https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license>

## 在 License Manager 中建立使用者型訂閱的先決條件

您必須先在環境中實作下列先決條件，才能建立以使用者為基礎的訂閱。

### 內容

- [IAM 角色和許可](#)
  - [AWS KMS License Server 登入資料的金鑰政策](#)
- [Active Directory](#)
- [Security groups \(安全群組\)](#)
- [網路組態](#)
- [提供以使用者為基礎的訂閱產品的執行個體](#)
- [Microsoft 遠端桌面服務](#)
  - [管理登入資料秘密](#)

## IAM 角色和許可

您必須允許 License Manager 建立服務連結角色，才能讓加入 AWS 帳戶以使用者為基礎的訂閱。在 License Manager 主控台中，如果尚未建立角色，則以使用者為基礎的訂閱中會出現提示。在您回應提示並同意允許 License Manager 建立角色之後，請選擇建立以繼續。如需詳細資訊，請參閱[使用 License Manager 的服務連結角色](#)。

若要建立以使用者為基礎的訂閱，您的使用者或角色必須具有下列許可：

- Amazon EC2 – 使用網路介面和子網路。

- ec2:CreateNetworkInterface
- ec2>DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:CreateNetworkInterfacePermission
- ec2:DescribeSubnets
- Directory Service – 管理 Active Directory。
  - ds:DescribeDirectories
  - ds:AuthorizeApplication
  - ds:UnauthorizeApplication
  - ds:GetAuthorizedApplicationDetails
  - ds:DescribeDomainControllers
- Route 53 – 設定路由。
  - route53>DeleteHealthCheck
  - route53:ChangeResourceRecordSets
  - route53:GetHostedZone
  - route53>ListHostedZonesByName
  - route53>ListHostedZones
  - route53>ListHostedZonesByVPC
  - route53>CreateHostedZone
  - route53>DeleteHostedZone
  - route53>ListResourceRecordSets
  - route53:GetHealthCheckCount
  - route53:AssociateVPCWithHostedZone

若要為 Microsoft Office 產品建立使用者型訂閱，您的使用者或角色也必須具有下列額外許可：

- ec2:CreateVpcEndpoint
- ec2>DeleteVpcEndpoints
- ec2:DescribeVpcEndpoints
- ec2:ModifyVpcEndpoint
- ec2:DescribeSecurityGroups

## AWS KMS License Server 登入資料的金鑰政策

若要使用您自己的 KMS 金鑰來加密和解密 Microsoft RDS License Server 的管理登入資料秘密，您必須將政策連接至您用來存取 License Manager 操作的角色。下列範例顯示的政策會授予 Secrets Manager 存取 KMS 金鑰的許可，以加密和解密 Microsoft RDS License Server 登入資料秘密。

### JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/RoLeName"
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com"
        }
      }
    },
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/aws-  
service-role/license-manager-user-subscriptions.amazonaws.com/  
AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService"
      },
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:us-  
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "secretsmanager.*.amazonaws.com"
        }
      }
    }
  ]
}
```

```
    }  
  }  
}  
]  
}
```

## Active Directory

若要使用 License Manager 使用者型訂閱，您必須建立 Active Directory (AD)，其中包含訂閱產品使用者的使用者資訊。根據您的組態，您可以使用 AWS Managed Microsoft AD 或自我管理 AD。

如果您同時使用 AWS 受管和自我管理的 Active Directory，則必須在目錄之間建立雙向樹系信任。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的[教學課程：在 AWS Managed Microsoft AD 與自我管理的 Active Directory 網域之間建立信任關係](#)。

### Note

為您的目錄設定的子網路都必須來自您的相同 VPC AWS 帳戶。不支援共用子網路。

AWS 受管 Active Directory 有下列限制。

- 只有在目錄先加入主要帳戶時，才支援與您共用的目錄，然後您可以在共用帳戶中加入該目錄。
- 不支援多重要素驗證

### 標籤型篩選條件的先決條件

如果您將為 Active Directory 使用標籤型篩選條件，您必須先加入 AWS 資源總管 服務，如下所示：

1. 在 [https://https://resource-explorer.console.aws.amazon.com/resource-explorer](https://resource-explorer.console.aws.amazon.com/resource-explorer) 開啟 Resource Explorer 主控台。
2. 選擇開啟資源總管。
3. 在設定資源總管頁面中，選擇設定選項，如下所示。

### 快速設定

針對基本組態選取此選項。

## 進階設定

針對自訂組態選取此選項。請確定您至少為 Active Directory 所在的區域建立索引。

4. 選取彙總器索引區域的區域。
5. 選擇開啟資源總管以儲存您的設定。
6. 在導覽窗格中，選取檢視，然後選擇建立檢視。

### Note

若要顯示隱藏的導覽窗格，請選擇選單圖示（三個水平長條）。

7.
  - a. 在建立檢視頁面中，**license-manager-user-subscriptions-view**輸入名稱。
  - b. 確認資源篩選條件設定為包含所有資源。
  - c. 在其他資源屬性區段中，確認已選取標籤核取方塊。
8. 選擇建立檢視以完成。

如需建立 AWS Managed Microsoft AD 目錄的詳細資訊，請參閱 AWS Directory Service 《使用者指南》中的[AWS Managed Microsoft AD 先決條件](#)和[建立 AWS Managed Microsoft AD 目錄](#)。

若要將使用者與建立關聯 AWS Managed Microsoft AD，您必須在 AWS Managed Microsoft AD 目錄中佈建使用者。如需詳細資訊，請參閱《[管理指南](#)》中的[管理中的使用者和群組 AWS Managed Microsoft AD](#)。AWS Directory Service

## Security groups (安全群組)

安全群組會控制允許進出您網路上資源的網路流量。為了確保以使用者為基礎的訂閱環境中的資源可以通訊，您的安全群組必須符合下列條件。

### VPC 端點的安全群組

識別或建立允許傳入 TCP 連接埠1688連線的安全群組。設定 VPC 設定時，您將指定此安全群組。如需詳細資訊，請參閱[使用安全群組](#)。

License Manager 會將此安全群組與其在設定 VPC 時代表您建立的 VPC 端點建立關聯。如需 VPC 端點的詳細資訊，請參閱《[AWS PrivateLink 指南](#)》中的[使用介面 VPC 端點存取 AWS 服務](#)。

### Active Directory 網域控制站的安全群組

請確定您用於 AD 網域控制站的安全群組允許傳出流量到每個網域控制站的網路介面 IP 地址。此外，網域控制站安全群組應允許在所有 Active Directory 相關連接埠上進行通訊，包括 TCP 9389。Active Directory Web Services (ADWS) 需要連接埠 9389，Active Directory PowerShell 模組和其他管理工具會使用此連接埠與網域控制站通訊。

### "Register your Active Directory" 步驟的安全群組需求

在將您的 Active Directory 加入 License Manager 期間，我們會在您提供的子網路中建立網路介面，並使用 VPC 的預設安全群組進行標記。請確定允許此安全群組存取您的 Active Directory 網域控制站。這可以在加入完成後替換成您選擇的群組，但仍需要網域控制站的網路存取權。

#### 「設定 RDS 授權伺服器」步驟的安全群組需求

在授權伺服器組態期間，License Manager 會在您提供的子網路中建立兩個網路介面。這些網路介面會自動標記新建立的安全群組，其中包含所有必要的連接埠組態。確保您的 Active Directory 網域控制器安全群組允許來自所有 Active Directory 相關連接埠上子網路 CIDRs 雙向流量，包括 TCP 連接埠 9389。Active Directory Web Services (ADWS) 需要連接埠 9389，Active Directory PowerShell 模組和其他管理工具會使用此連接埠與網域控制站通訊。

### 使用者型訂閱執行個體的安全群組

識別或建立安全群組，允許下列存取您執行個體的 `和`。如需詳細資訊，請參閱[使用安全群組](#)。

- 從核准的連線來源傳入 TCP 連接埠連線。 3389
- 傳出 TCP 連接埠 1688 連線，以到達 VPC 端點並與之通訊 AWS Systems Manager。

## 網路組態

License Manager 會建立兩個網路介面，使用 AWS Managed Microsoft AD 佈建您之 VPC 的預設安全群組。這些界面用於服務與您的目錄互動。如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的[步驟 2：在 License Manager 中註冊 Active Directory](#) 和 [建立的內容](#)。

佈建程序完成後，您可以將不同的安全群組與 License Manager 建立的介面建立關聯。

## DNS 解析

您註冊以使用者為基礎的訂閱的 Active Directory 必須可從您在 License Manager 設定中設定的任何 VPCs 和子網路存取。若要確保 Active Directory 節點可存取，請設定 DNS 解析，如下所示：

- 針對以使用者為基礎的訂閱，在 License Manager 設定中設定的 VPCs 和 Active Directory 之間設定 DNS 轉送。您可以使用 Amazon Route 53 或其他 DNS 服務進行 DNS 轉送。如需詳細資訊，請參閱部落格文章[將 Directory Service 的 DNS 解析與 Amazon Route 53 解析程式整合](#)。
- 為您的 VPC 啟用 DNS 主機名稱和 DNS 解析。如需詳細資訊，請參閱[檢視和更新 VPC 的 DNS 屬性](#)。

## 提供以使用者為基礎的訂閱產品的執行個體

若要讓以使用者為基礎的訂閱執行個體如預期運作，您必須符合下列先決條件：

- 設定執行個體的安全群組，如中所述[Security groups \(安全群組\)](#)。
- 確保啟動以使用 Microsoft Office 提供使用者型訂閱的執行個體具有路由到佈建 VPC 端點的子網路。
- 提供以使用者為基礎的訂閱的執行個體必須由 AWS Systems Manager 管理，才能擁有良好狀態。此外，您的執行個體必須能夠啟用其使用者型訂閱授權，以便在授權啟用後保持合規。

### Note

License Manager 會嘗試復原運作狀態不佳的執行個體，但無法恢復運作狀態的執行個體將會終止。如需透過 Systems Manager 管理執行個體以及執行個體合規的疑難排解資訊，請參閱本指南的[對 License Manager 中的使用者型訂閱進行故障診斷](#)一節。

- 您必須將執行個體描述檔角色連接到提供使用者型訂閱產品的執行個體，以允許資源由管理 AWS Systems Manager。如需詳細資訊，請參閱《AWS Systems Manager 使用者指南》中的[建立 Systems Manager 的 IAM 執行個體設定檔](#)。
- 您必須先[取消使用者與執行個體的關聯](#)終止執行個體。

## Microsoft 遠端桌面服務

Microsoft 遠端桌面服務授權伺服器需要相關 Active Directory 中定義的管理使用者。該使用者必須能夠執行下列任務：

- 在 Active Directory 網域下建立 OU
- 建立之 OU 內的網域聯結執行個體（建立電腦）
- 將電腦物件新增至 Active Directory 網域中的終端機伺服器群組

- 對 Active Directory 網域中的使用者物件進行委派控制，以讀取和寫入終端機伺服器授權伺服器，以產生授權伺服器報告。

若要進一步了解委派，請參閱 [Active Directory Domain Services 中的控制委派](#)。

### 管理登入資料秘密

License Manager 使用 AWS Secrets Manager 來管理 Microsoft Remote Desktop Services 授權伺服器上使用者管理任務所需的登入資料。您必須先在 Secrets Manager 中建立秘密，其中包含在授權伺服器上執行使用者管理任務之使用者的登入資料，才能設定授權伺服器。當您設定授權伺服器設定時，必須提供您建立的秘密 ID。

#### Note

這必須與您為產生 RDS 授權伺服器報告所定義的使用者相同。

若要建立秘密，請遵循 Secrets Manager 使用者指南中 [建立 AWS Secrets Manager 秘密](#) 頁面上的詳細說明，以及 License Manager 特有的下列設定。

#### Important

若要使用秘密，License Manager 取決於確切的金鑰名稱、使用者名稱值，以及下列清單中指定的加密金鑰。秘密名稱必須以下列字首開頭：`license-manager-user-`。

在選擇秘密類型頁面：

- 秘密類型 – 選擇其他類型的秘密。
- 金鑰/值對 – 指定要存放在秘密中的下列金鑰對。

#### 使用者名稱

- 索引鍵：`username`
- 值：`Administrator`

#### 密碼

- 索引鍵：`password`
- 值：`##`

- 加密金鑰 – 若要指定金鑰以外的 KMS `aws/secretsmanager` 金鑰，您必須將政策連接至您用來存取 License Manager 操作的角色。如需詳細資訊，請參閱 [IAM 角色和許可](#)。

在設定秘密頁面上：

- 秘密名稱 – 為您的秘密指定名稱，其開頭為 License Manager 用來識別授權伺服器登入資料秘密的字首。例如：

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

這些指示假設您使用 AWS 管理主控台 來建立秘密。Secrets Manager 使用者指南也包含其他方法的詳細說明。如需 Secrets Manager 的詳細資訊，請參閱 [什麼是 Secrets Manager](#)。如需與成本特別相關的資訊，請參閱《Secrets Manager 使用者指南》中的 [定價 AWS Secrets Manager](#)。

## License Manager 中使用者型訂閱支援的軟體產品

AWS License Manager 支援 Microsoft Visual Studio 和 Microsoft Office 的使用者型訂閱。License Manager 會追蹤支援的軟體使用率。每個使用者都需要 Windows Server 遠端桌面服務訂閱者存取授權 (RDS SAL) 的單一訂閱，才能存取提供使用者型訂閱產品的包含授權的執行個體。如需詳細資訊，請參閱 [License Manager 中的使用者型訂閱入門](#)。

支援的 Windows 作業系統 (OS) 平台

您可以找到包含下列 Windows 作業系統平台之 RDS SAL 授權涵蓋之產品的 Windows AMIs：

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019

## 支援以使用者為基礎的訂閱軟體

License Manager 支援使用下列軟體的使用者型授權。

- [Microsoft Visual Studio](#)
- [Microsoft Office](#)

## Microsoft Visual Studio

Microsoft Visual Studio 是一種整合式開發環境 (IDE)，可讓開發人員建立、編輯、偵錯和發佈應用程式。提供的 Microsoft Visual Studio AMIs 包含 [AWS Toolkit for .NET Refactoring](#) 和 [AWS Toolkit for Visual Studio](#)。

### 支援的版本

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

下表詳細說明用於 License Manager 使用者型訂閱 API 操作的軟體訂閱名稱及其相關產品值。

軟體訂閱名稱	產品值
Visual Studio Enterprise 2022	VISUAL_STUDIO_ENTERPRISE
Visual Studio Professional 2022	VISUAL_STUDIO_PROFESSIONAL

## Microsoft Office

Microsoft Office 是 Microsoft 針對各種生產力使用案例開發的一組軟體，包括使用文件、試算表和投影片簡報。

### 支援的版本

- Office LTSC Professional Plus 2021
- Office LTSC Professional Plus 2024
- Office LTSC Professional Plus 2021 32 位元 (x86)
- Office LTSC Professional Plus 2024 32 位元 (x86)

下表詳細說明用於 License Manager 使用者型訂閱 API 操作的軟體訂閱名稱及其相關產品值。

軟體訂閱名稱	產品值
--------	-----

軟體訂閱名稱	產品值
Office LTSC Professional Plus 2021	OFFICE_PROFESSIONAL_PLUS
Office LTSC Professional Plus 2024	OFFICE_PROFESSIONAL_PLUS

## Active Directory

License Manager 支援 Microsoft Visual Studio、Microsoft Office 和遠端桌面服務訂閱者存取授權 (RDS SAL) 的使用者型訂閱。產品可能支援 AWS Managed Microsoft AD 或自我管理的 Active Directory，該目錄部署在您的 AWS 環境內，或與您 AWS 環境中的 VPC 具有網路連線能力。

此資料表指出當與以使用者為基礎的訂閱搭配使用時，每個軟體產品支援哪些類型的 Active Directory：

軟體產品	AWS Managed Microsoft AD	自我管理 AD
Microsoft Visual Studio	支援	不支援
Microsoft Office	支援	不支援
RDS SAL 產品	支援	支援

## 其他軟體

您可以在執行個體上安裝無法以使用者為基礎的訂閱的其他軟體。License Manager 不會追蹤其他軟體安裝。這些安裝必須使用 Active Directory 的管理帳戶來執行。如果您使用 AWS Managed Microsoft AD，系統預設會在您的目錄中建立管理帳戶 (Admin)。如需詳細資訊，請參閱《[管理指南](#)》中的[管理員帳戶](#)。Directory Service

若要使用 Active Directory 管理帳戶安裝其他軟體，您必須：

- 將管理帳戶訂閱執行個體提供的產品。
- 將管理帳戶與執行個體建立關聯。
- 使用管理帳戶連線至執行個體以執行安裝。

如需詳細資訊，請參閱[License Manager 中的使用者型訂閱入門](#)。

## License Manager 中的使用者型訂閱入門

下列步驟詳細說明如何開始使用以使用者為基礎的訂閱。這些步驟假設您已實作必要的先決條件。如需更多資訊，請參閱[在 License Manager 中建立使用者型訂閱的先決條件](#)。

### 步驟

- [步驟 1：訂閱產品](#)
- [步驟 2：在 License Manager 中註冊 Active Directory](#)
- [步驟 3：設定 RDS 授權伺服器](#)
- [步驟 4：啟動執行個體以提供以使用者為基礎的訂閱](#)
- [步驟 5：將使用者與以使用者為基礎的訂閱執行個體建立關聯](#)

### 步驟 1：訂閱產品

Office 或 Visual Studio 等 Microsoft 產品需要作用中的訂閱，才能將 Active Directory 使用者與包含這些產品的執行個體建立關聯。Marketplace 訂閱狀態欄中在 AWS Marketplace 中顯示訂閱按鈕的訂閱產品尚未訂閱。

當您從訂閱 Microsoft 使用者型訂閱產品時 AWS Marketplace，如果您還沒有訂閱，License Manager 會自動將訂閱新增至帳戶的 Microsoft 遠端桌面服務 (RDS)。若要從包含授權的 AMIs 啟動的 EC2 執行個體上遠端存取圖形桌面和以訂閱為基礎的 Windows 應用程式，需要 RDS。

您可以使用 AWS Marketplace 以下連結直接在上訂閱您的產品：

- [Visual Studio Professional](#)
- [Visual Studio Enterprise](#)
- [Office LTSC Professional Plus](#)
- [Win 遠端桌面服務 SAL](#)

從 License Manager 主控台探索和訂閱產品

您也可以從 License Manager 主控台探索訂閱所需的產品。

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇產品。
3. 選擇產品的名稱，或選擇在 AWS Marketplace 中訂閱按鈕以顯示訂閱詳細資訊。

4. 針對每個列出的 Marketplace 產品，選取檢視訂閱選項。檢閱詞彙，然後選擇訂閱以繼續。

如果您接受條款，則需要處理產品訂閱。訂閱會有一個進行中的訊息，直到完成為止。您可以針對您需要的任何其他設定產品重複這些步驟。一旦所有必要的產品都具有作用中的訂閱，您就可以繼續向產品註冊 Active Directory。

#### Note

對於尚未關閉（標記為待定帳單狀態）的計費期間，您的使用者數量和相關費用預估帳單需要 48 小時才會顯示 AWS Billing。詳情請參閱 AWS Billing 使用者指南中的[檢視您的每月費用](#)。

## 步驟 2：在 License Manager 中註冊 Active Directory

License Manager 要求在 Active Directory 中定義訂閱使用者，以便將使用者與以使用者為基礎的訂閱建立關聯。這可以是 AWS Managed Microsoft AD 或自我管理 Active Directory，視您的訂閱而定。

- 如果您只訂閱獨立的 Microsoft Office 或 Visual Studio 產品，則必須設定 AWS Managed Microsoft AD。
- 如果您訂閱 [Win Remote Desktop Services SAL](#)，則可以使用 AWS Managed Microsoft AD 或自我管理的 Active Directory。

若要搭配以使用者為基礎的訂閱使用 Microsoft Office，您必須授予 License Manager 更新 VPC 組態的許可。當您設定 VPC 時，License Manager 會代表您建立 [VPC 端點](#)。這些端點是資源連線到啟用伺服器並保持合規的必要端點。

您必須為註冊以使用者為基礎的訂閱的任何其他 VPCs 設定 DNS 轉送。如果您在多個中有使用者型訂閱 AWS 區域，則每個區域都必須設定自己的 Active Directory 並設定 DNS 轉送。

#### Important

您必須允許 License Manager 建立所需的[服務連結角色](#)，才能繼續。如需更多資訊，請參閱在[License Manager 中建立使用者型訂閱的先決條件](#)。

主控台內的註冊步驟會有所不同，取決於您訂閱的產品。如果您已訂閱 Win Remote Desktop Services SAL，請選取 Microsoft RDS SAL 標籤。如果您訂閱 Microsoft Office 或 Visual Studio，但未訂閱 RDS SAL，請選取獨立 MSO 訂閱索引標籤。

## Microsoft RDS SAL

### 註冊 AWS Managed Microsoft AD

若要註冊 AWS Managed Microsoft AD 為以使用者為基礎的訂閱的 Active Directory，請依照下列步驟進行：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的設定下導覽至以使用者為基礎的訂閱。
3. 在以使用者為基礎的訂閱頁面上的遠端桌面服務 (RDS) 索引標籤中，選擇註冊 Active Directory。
4. 選取 AWS Managed Active Directory 選項以輸入詳細資訊。
5. 從 AWS Active Directory 清單中選取您的受管目錄，或建立新的受管目錄，然後返回並選取它。
6. 選擇註冊以註冊您的 AWS Managed Active Directory。

### 註冊自我管理 Active Directory

若要註冊以使用者為基礎的訂閱的自我管理 Active Directory，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的設定下導覽至以使用者為基礎的訂閱。
3. 在以使用者為基礎的訂閱頁面上的遠端桌面服務 (RDS) 索引標籤中，選擇註冊 Active Directory。
4. 選取自我管理 Active Directory 選項以輸入詳細資訊。
5. 輸入 Active Directory 網域。
6. 選取 Active Directory IP 地址的版本，然後輸入目錄的主要和次要 IP 地址。
7. 在聯網區段中，選取 Active Directory 所在的 VPC 和兩個子網路。
8. 選取您在 Microsoft RDS 訂閱先決條件中建立的管理登入資料秘密。

## Stand-alone MSO subscriptions

### 註冊 AWS Managed Microsoft AD

若要註冊 AWS Managed Microsoft AD 為以使用者為基礎的 Microsoft Office 和 Visual Studio 訂閱的 Active Directory，請依照下列步驟進行：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的設定下導覽至以使用者為基礎的訂閱。
3. 在以使用者為基礎的訂閱頁面上，選取要註冊的 Microsoft Office 或 Visual Studio 訂閱產品的索引標籤，然後選擇註冊 Active Directory。
4. 從 AWS Active Directory 清單中選取您的受管目錄，或建立新的受管目錄，然後返回並選取它。
5. 選擇註冊以註冊您的 AWS 受管 Active Directory。

當您註冊 Active Directory 時，License Manager 會建立兩個網路介面，以便服務可以與您的目錄通訊。網路界面會有類似 AWS LicenseManager `<directory_id>` 建立的網路界面的說明。

### 從註冊 Active Directory AWS CLI

您可以使用 [RegisterIdentityProvider](#) 操作，將 Active Directory 註冊為使用者型訂閱的身分提供者。

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

### 為以使用者為基礎的訂閱設定 Active Directory 和您的 VPC (AWS CLI)

您可以將 Active Directory 註冊為身分提供者，並使用 [RegisterIdentityProvider](#) 操作為以使用者為基礎的訂閱設定 VPC。

```
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"
```

如需可用軟體產品的詳細資訊，請參閱 [License Manager 中使用者型訂閱支援的軟體產品](#)。

## 步驟 3：設定 RDS 授權伺服器

Microsoft 遠端桌面服務 (RDS) 授權伺服器會在 Active Directory 使用者存取提供使用者型訂閱 Microsoft 產品的 EC2 執行個體時，向他們發出訂閱者存取授權 (SALs)。完成步驟 1 和 2 之後，您可以設定授權伺服器，如下所示。

開始之前，請確定您已完成 RDS [以使用者為基礎的訂閱先決條件](#)的。此程序假設您已設定 Active Directory。

為以使用者為基礎的訂閱設定 RDS 授權伺服器（主控台）

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 導覽至左側導覽窗格中設定下的以使用者為基礎的訂閱頁面。
3. 在遠端桌面服務 (RDS) 索引標籤上，您應該會在清單中看到一或多個作用中目錄。可能會顯示提示，讓您知道需要為 Active Directory 設定 RDS。
4. 從提示或動作功能表中，選擇設定 RDS 授權伺服器。
5. 在設定 RDS License Server 對話方塊中，您可以設定下列設定：

### Active Directory

本節包含連線至您設定之 RDS 授權伺服器的目錄的金鑰詳細資訊。

### Secret

您必須為授權伺服器上用於使用者管理任務的登入資料選擇現有的秘密或建立新的秘密。秘密名稱的第一部分必須遵循 [管理登入資料秘密一節](#)中所述的模式 [以使用者為基礎的訂閱先決條件](#)。

### Tags (標籤)

您可以選擇性地輸入授權伺服器資源的標籤。

6. 選擇設定以儲存您的設定。

## 步驟 4：啟動執行個體以提供以使用者為基礎的訂閱

訂閱產品之後，您必須啟動執行個體，讓使用者從包含產品的 AWS Marketplace AMI 連線至。啟動執行個體之後，AWS Systems Manager 會嘗試將執行個體加入 Active Directory 網域，並對資源執行額外的組態和強化。讓執行個體可供使用的組態大約需要 20 分鐘才能完成。您可以從 License Manager 主控台的使用者關聯頁面確認資源已準備好使用，方法是檢查執行個體的運作狀態是否為作用中。

若要使用以使用者為基礎的訂閱啟動執行個體，請參閱 [從包含的授權 AMI 啟動執行個體](#)。

## 步驟 5：將使用者與以使用者為基礎的訂閱執行個體建立關聯

訂閱所需產品的 AWS Marketplace AMI 後，您就可以訂閱使用者產品，並將他們與提供產品的執行個體建立關聯。您可以訂閱使用者使用產品，並在單一步驟中或個別地將他們與執行個體建立關聯。當您訂閱使用者時，會檢查目錄，以確保使用者身分存在。系統會為您訂閱產品的每個使用者建立一個訂閱。

每個使用者都必須同時訂閱 Windows Server 遠端桌面服務訂閱者存取授權 (RDS SAL) 和他們將使用的產品。

當您的帳戶已如中所述訂閱 RDS SAL 時 [步驟 1：訂閱產品](#)，License Manager 會在訂閱以使用者為基礎的訂閱產品時，自動將 Active Directory 中的使用者訂閱至 RDS SAL。

### Note

如果使用者從未訂閱與 RDS SAL 相關聯的執行個體的日誌，則 License Manager 會自動訂閱它們並開始 Microsoft RDS 計費。帳單會持續進行，直到取消訂閱且 RDS SAL 授權伺服器發出的授權字符過期為止。

同樣地，如果先前訂閱的使用者取消訂閱，但在 RDS SAL 授權字符過期後仍繼續登入，則會自動重新訂閱使用者，計費會持續，直到再次取消訂閱且其字符過期為止。

如需訂閱費用和帳單的詳細資訊，請參閱 [License Manager 中的訂閱費用](#)。

License Manager 中的產品頁面會將其 Marketplace 訂閱狀態列為作用中，以顯示作用中的訂閱。在產品詳細資訊頁面中，License Manager 會顯示狀態為已訂閱的作用中使用者訂閱。

### Important

如果您的 Active Directory 未使用產品設定，通知列會出現在主控台頂端，建議您調整目錄設定。在通知列上，選擇開啟設定以存取 License Manager 中的設定頁面，然後編輯您的目錄。每個使用者都必須同時訂閱 RDS SAL 和他們將使用的產品。將使用者訂閱至 Marketplace 訂閱狀態為非作用中的產品將會失敗。

## 將使用者訂閱至產品，並將其與執行個體建立關聯

當您選取要與使用者建立關聯的執行個體時，您可以選擇性地將他們訂閱到執行個體提供的產品，如果他們尚未訂閱。使用下列其中一種方法來訂閱和關聯使用者。

### Console

若要將使用者與執行個體建立關聯，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇使用者關聯。
3. 選取您要與使用者建立關聯的執行個體，然後選擇下列其中一個選項：

#### 關聯使用者

指定您目錄中最多 5 個使用者名稱，包含信任網域中存在的網域名稱，然後選擇關聯。如果您使用此方法，使用者必須已訂閱執行個體提供的產品。

#### 訂閱並關聯使用者

指定您目錄中最多 5 個使用者名稱，包含信任網域中存在的網域名稱，然後選擇訂閱和關聯。

#### (選用) 檢閱使用者關聯

在使用者關聯頁面上，您選取的使用者會顯示在關聯狀態為 的使用者下方。

#### (選用) 檢閱訂閱的使用者

在產品頁面上，選擇產品名稱。已訂閱的使用者會顯示在狀態為已訂閱的使用者下。

### AWS CLI

您可以將使用者與啟動的執行個體建立關聯，以提供使用者型訂閱與 [AssociateUser](#) 操作。

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

將自我管理 Active Directory 使用者與執行個體建立關聯 (AWS CLI)

您可以將自我管理 Active Directory 中的使用者與啟動的執行個體建立關聯，以提供 [AssociateUser](#) 操作的使用者型訂閱。

```
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>
```

如需可用軟體產品的詳細資訊，請參閱 [License Manager 中使用者型訂閱支援的軟體產品](#)。

將使用者訂閱至產品

您可以使用下列其中一種方法來訂閱產品。

### Console

將使用者訂閱至產品（主控台）

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇產品。
3. 選取要訂閱使用者的產品，其中 Marketplace 訂閱狀態為作用中。
4. 如果產品是 Microsoft RDS，請選取包含要訂閱之使用者的已註冊 Active Directory。
5. 選擇訂閱使用者以繼續。
6. 指定您目錄中最多 20 個使用者名稱，包含信任網域中存在的網域名稱，然後選擇訂閱。

具有訂閱的使用者會顯示在狀態為已訂閱的使用者下。

### AWS CLI

將使用者訂閱至產品 (AWS CLI)

您可以使用 [StartProductSubscription](#) 操作，將使用者訂閱到向您的身分提供者註冊的產品。

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

使用自我管理 Active Directory (AWS CLI) 訂閱產品的使用者

您可以使用 [StartProductSubscription](#) 操作，將使用者從自我管理 Active Directory 訂閱至已向 AWS Managed Microsoft AD 目錄註冊的產品。

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

如需可用軟體產品的詳細資訊，請參閱 [License Manager 中使用者型訂閱支援的軟體產品](#)。

具有訂閱的使用者會顯示在狀態為訂閱的使用者下。

## 為更活躍的遠端使用者工作階段設定 Active Directory GPO

根據預設，Microsoft RDS 最多允許在提供以使用者為基礎的訂閱產品的 EC2 Windows 執行個體上同時有兩個使用者工作階段。設定 RDS License Server 端點之後，您可以設定 Microsoft RDS 以允許兩個以上的使用者工作階段同時使用 Active Directory 群組政策物件 (GPO)，如下所示。

### 先決條件

您必須在環境中建立授權伺服器。若要建立授權伺服器，請參閱 [步驟 3：設定 RDS 授權伺服器](#)。

1. 您用來設定 GPO 的工具取決於您從何處執行，如下所示：

#### 網域控制器的中央組態

以管理員身分登入 Active Directory 網域控制站，然後開啟 Windows 群組政策管理主控台。

#### 在工作階段主機上設定群組政策

以管理員身分登入您的授權伺服器，並開啟本機群組政策編輯器。

2. 從管理主控台或政策編輯器，編輯群組政策以指定透過 Microsoft RDS 連線的工作階段主機。您可以在 License Manager 產品詳細資訊頁面或中的 [list-license-server-endpoints](#) 命令中找到 RDS License Server 的端點 AWS CLI。
3. 將遠端桌面工作階段主機的授權模式設定為 Per User，然後儲存。

如需設定 RDS License Server for License Manager 的詳細資訊，請參閱 入門主題 [the section called “步驟 3：設定 RDS”](#) 中的。如需 Microsoft RDS 工作階段主機組態的詳細資訊，請參閱 [授權遠端桌面工作階段主機](#)。

# AWS License Manager 使用共用的跨帳戶入門 AWS Managed Microsoft AD

AWS License Manager 支援使用共用的跨帳戶功能 AWS Managed Microsoft AD，可讓組織從目錄擁有者帳戶集中管理使用者訂閱，同時跨多個帳戶部署執行個體。

## 術語

- 目錄擁有者帳戶 - 受管 AD 存在且也負責管理訂閱的授權管理員帳戶。
- 目錄消費者帳戶 - 您使用共用 AD 來啟動使用者訂閱執行個體 AWS 的帳戶。

## 先決條件

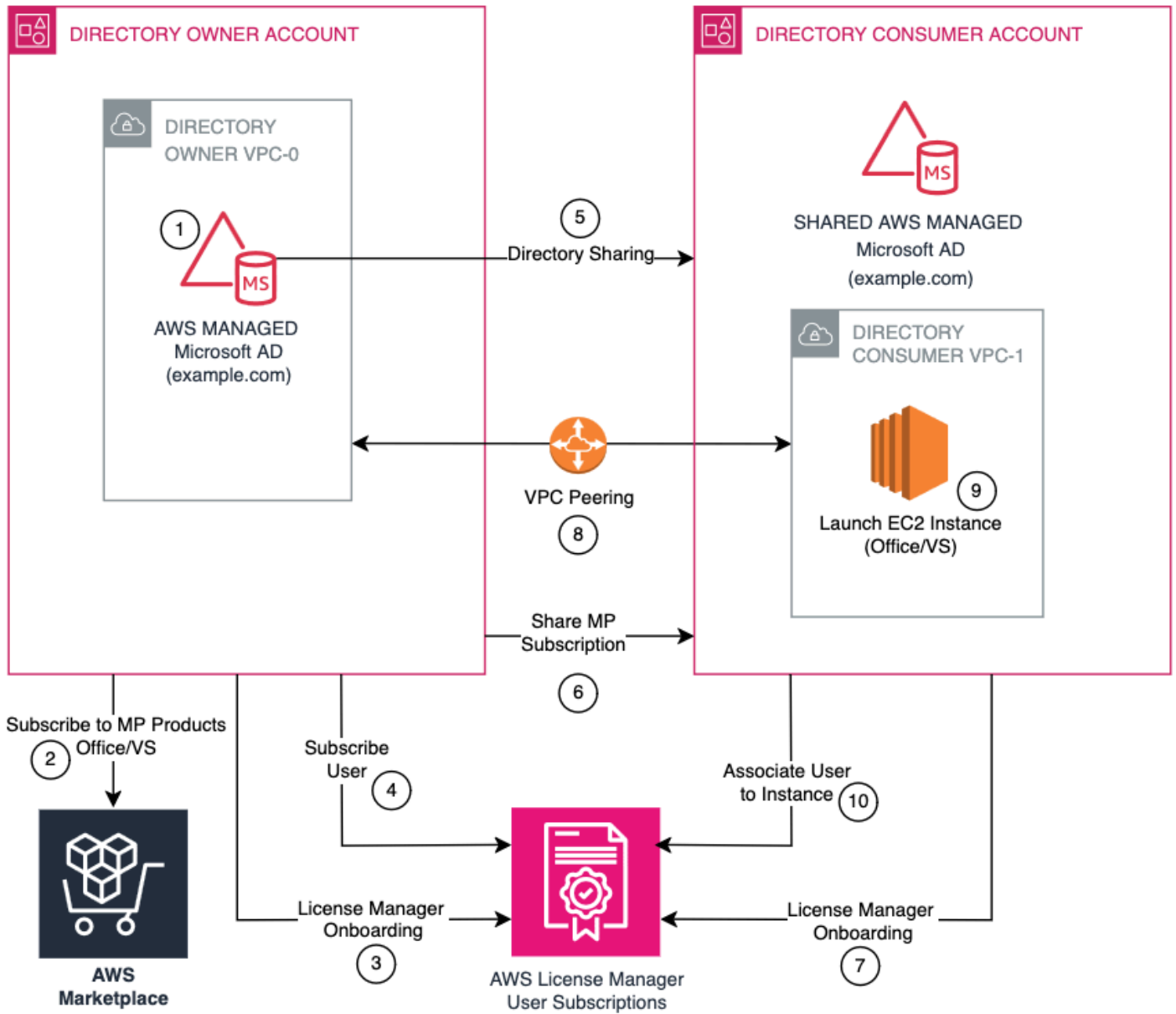
開始前，請確保您具備以下條件：

- 目錄擁有者帳戶中 AWS Managed Microsoft AD 的 - 在您要控制訂閱的目錄擁有者帳戶/授權管理員帳戶中設定。
- 目錄擁有者帳戶與所有目錄取用者帳戶之間的網路連線。
- 必要的 IAM 許可 - 請參閱以[使用者為基礎的訂閱 IAM 角色](#)。
- 在目錄擁有者帳戶中，訂閱 AWS Marketplace 中所需的 License Manager 產品：
  - [Visual Studio Professional 2022](#)
  - [Visual Studio Enterprise 2022](#)
  - [Office LTSC Professional Plus](#)

## 限制

- 使用者訂閱管理僅限於目錄擁有者帳戶。
- 不支援跨區域共用。
- 透過目錄擁有者帳戶合併計費 - 所有訂閱成本都會向目錄擁有者帳戶計費，不過訂閱可以存在於多個帳戶中。
- 帳戶之間需要網路連線。

## 網路架構



## 如何設定跨帳戶 License Manager 功能

若要設定跨帳戶 License Manager 功能：

1. 設定目錄擁有者帳戶/授權管理員帳戶。
2. 設定目錄取用者帳戶。
3. 建立網路連線。
4. 部署執行個體和管理使用者關聯。

## 步驟 1：設定目錄擁有者/授權管理員帳戶

### 建立和共用 AWS Managed Microsoft AD

1. 如果 VPC 中不存在，請在 VPC AWS Managed Microsoft AD 中建立。
2. 與目錄消費者帳戶共用目錄，如[共用目錄](#)中所述。
3. 確定目錄已正確設定必要的使用者和群組。

### 訂閱 產品

1. 導覽至 AWS Marketplace。
2. 尋找並訂閱您需要的產品、Visual Studio 或 Office 和 RDS SAL。
3. 使用 License Manager Create Grants 與目錄消費者帳戶共用 Visual Studio 或 Office 訂閱。或者，您可以訂閱這些帳戶中 AWS Marketplace 的產品，因為這不會影響帳單。請參閱[授予的授權](#)。
4. 確認訂閱狀態為作用中。

### 向 License Manager 註冊

1. 開啟 License Manager 主控台。
2. 導覽至以使用者為基礎的訂閱設定。
3. 選取註冊身分提供者。
4. 選擇您的 AWS Managed Microsoft AD。
5. 完成註冊程序。

## 步驟 2：設定目錄消費者帳戶 - 具有共用 AD 的帳戶

### 接受共用目錄

1. 開啟 AWS Directory Service 主控台。
2. 導覽至共用目錄。
3. 尋找並接受共用目錄邀請。
4. 請注意您帳戶中指派的新目錄 ID。

## 接受 MP 訂閱

在 License Manager Grants 中，接受 AWS Marketplace 產品的授權。或者，AWS Marketplace 訂閱產品。在 [CreateGrant API](#) 中進一步了解 )。

## 向 License Manager 註冊

1. 開啟 License Manager 主控台。
2. 導覽至以使用者為基礎的訂閱，然後選擇產品。
3. 使用共用目錄 ID 和產品註冊。
4. 驗證註冊狀態。

## 步驟 3：在 VPCs 之間建立網路連線

若要將 Amazon Amazon EC2 執行個體加入目錄，您需要在 VPCs 之間建立網路連線。有幾個選項可在兩個 VPCs 之間建立網路連線。本節說明如何使用 Amazon VPC 對等互連。

## 設定 VPC 對等互連

1. [在目錄擁有者 VPC-0 和目錄消費者 VPC-1 之間建立一個 VPC 互連連線](#)，然後在目錄擁有者 VPC-0 和目錄消費者 VPC-2 之間建立另一個連線。VPC-0 VPC-1
2. 將路由新增至指向 [VPCs 對等連線的 VPC 路由表](#)，以將流量路由至對等連線中的其他 VPC，以啟用對等 VPC 之間的流量路由。
3. 透過新增與目錄擁有者 VPC-0 的對等連線，設定每個目錄消費者 VPC 路由表。如果需要，您也可以建立網際網路閘道並將其連接至目錄消費者 VPCs。這可讓目錄消費者 VPCs 中的執行個體與執行網域聯結的 Amazon EC2 Systems Manager 代理程式通訊。

## 設定安全群組

將 [AWS Managed Microsoft AD 通訊協定和連接埠](#) 新增至傳出規則表，以設定目錄消費者 VPCs 的 [安全群組](#) 來啟用傳出流量。此外，請將目錄網域控制站 VPCs 的安全群組設定為透過將 AWS Managed Microsoft AD 通訊協定和連接埠新增至傳入規則表來啟用傳入流量，以允許來自目錄消費者帳戶的流量。

## 安全群組要求

消費者帳戶 VPCs：

- 啟用對目錄擁有者 VPC 的傳出流量

- 允許在必要的 AD 連接埠上進行通訊

目錄擁有者 VPC :

- 設定來自消費者 VPCs 傳入流量
- 新增必要的 AWS Managed Microsoft AD 通訊協定和連接埠，包括：
  - TCP 53 (DNS)
  - UDP 53 (DNS)
  - TCP 88 (Kerberos)
  - UDP 88 (Kerberos)
  - TCP 135 (RPC)
  - TCP 389 (LDAP)
  - UDP 389 (LDAP)
  - TCP 445 (SMB)
  - TCP 464 (Kerberos 密碼)
  - UDP 464 (Kerberos 密碼)
  - TCP 636 (LDAPS)
  - TCP 9389 (Active Directory Web Services)
  - TCP 3268-3269 (全域目錄)
  - TCP 1024-65535 (動態 RPC)

Active Directory Web Services (ADWS) 需要連接埠 9389，Active Directory PowerShell 模組和其他管理工具會使用此連接埠與網域控制站通訊。

步驟 4：部署執行個體和管理使用者關聯

訂閱使用者（僅限目錄擁有者帳戶）

1. 開啟 License Manager 主控台。
2. 導覽至以使用者為基礎的訂閱。
3. 選取訂閱使用者
4. 輸入 AWS Managed Microsoft AD 使用者識別符
5. 選擇產品並確認訂閱。

## 啟動執行個體

在任何帳戶中執行此步驟。

1. 導覽至 Amazon EC2 主控台。
2. 選擇啟動執行個體。
3. 選取適當的 License Manager AMI。
4. 設定聯網設定。
5. 檢閱並啟動。

## 將使用者與執行個體建立關聯

在執行個體存在的任何帳戶中執行此步驟。

1. 開啟 License Manager 主控台。
2. 導覽至 使用者關聯。
3. 選取目標執行個體。
4. 選擇關聯使用者。
5. 輸入 AWS Managed Microsoft AD 使用者名稱。
6. 確認關聯。

## 疑難排解

常見問題和解決方案：

### 網域連結失敗

1. 驗證帳戶之間的網路連線。
2. 檢查安全群組組態。
3. 確認 DNS 解析正常運作。
4. 驗證路由表項目。

### 使用者訂閱問題

1. 確認使用者存在於其中 AWS Managed Microsoft AD。

2. 驗證目錄擁有者帳戶中的訂閱狀態。
3. 檢查網路連線。
4. 檢閱錯誤日誌。

### 網路連線問題

1. 測試 VPC 對等互連狀態。
2. 驗證路由表組態。
3. 檢查安全群組規則。
4. 確認 DNS 解析。

### DNS 解析問題

1. 驗證 DHCP 選項集。
2. 檢查 DNS 伺服器組態。
3. 從取用者執行個體測試名稱解析。

### 其他資源

- [AWS License Manager 使用者指南](#)
- [AWS Directory Service 文件](#)
- [共用您的目錄](#)
- [如何將 Amazon EC2 執行個體加入網域以跨多個帳戶和 VPCs 進行 AWS Managed Microsoft AD 目錄](#)
- [授予的授權](#)

## 從包含的授權 AMI 啟動執行個體

訂閱產品後，您必須啟動執行個體，讓使用者從包含產品的 AWS Marketplace AMI 連線至。啟動執行個體之後，AWS Systems Manager 會嘗試將執行個體加入 Active Directory 網域，並對資源執行額外的組態和強化。讓執行個體可供使用的組態大約需要 20 分鐘才能完成。您可以從 License Manager 主控台的使用者關聯頁面確認資源已準備好使用，方法是檢查執行個體的運作狀態是否為作用中。

**⚠ Important**

您啟動的執行個體必須符合必要的先決條件，才能符合規範。無法完成初始組態的資源會終止。如需詳細資訊，請參閱《[在 License Manager 中建立使用者型訂閱的先決條件](#)》和《[對 License Manager 中的使用者型訂閱進行故障診斷](#)》。

使用以使用者為基礎的訂閱啟動執行個體

1. 前往 <https://console.aws.amazon.com/ec2/> 存取 Amazon EC2 主控台。
2. 在影像下，選擇 AMI Catalog。
3. 選擇 AWS Marketplace AMIs。
4. 在搜尋方塊中輸入產品名稱，然後按 Enter 鍵。例如，您可以搜尋 **Visual Studio**。
5. 在發佈者下，選取 Amazon Web Services。
6. 針對您要啟動執行個體的產品選擇選取，以提供以使用者為基礎的訂閱。
7. 選擇繼續以繼續。
8. 選擇使用 AMI 啟動執行個體。
9. 完成精靈，同時確保您：
  - a. 選擇非以 Graviton 為基礎的 Nitro 型執行個體類型。
  - b. 選擇執行個體可從中連線到 AWS Managed Microsoft AD 目錄的 VPC 和子網路。
  - c. 選擇允許從執行個體連線至 Active Directory 的安全群組。
  - d. 展開進階詳細資訊，然後選擇允許執行個體使用 Systems Manager 功能的 IAM 角色。
10. 選擇啟動執行個體。

當您從 AWS Marketplace AMI 執行執行個體時，您必須訂閱使用者產品，並將他們與執行個體建立關聯，以提供產品以便他們可以使用。

### 從特定作業系統版本 AMI 啟動執行個體

當您從支援 Office LTSC Professional Plus 或 Microsoft Visual Studio 的 AMI 啟動執行個體時，啟動預設為 AMI 的最新 Windows 作業系統版本（例如 Windows Server 2025）。若要使用特定作業系統版本 AMI 啟動，請遵循下列步驟。

1. 在 <https://console.aws.amazon.com/marketplace> 開啟 AWS Marketplace 主控台。

2. 從導覽窗格中選擇管理訂閱。
3. 若要簡化訂閱結果，您可以搜尋全部或部分訂閱名稱。例如 Office LTSC Professional Plus 或 Visual Studio Enterprise。
4. 從訂閱面板選取啟動新執行個體。這會開啟啟動組態頁面。
5. 若要從以舊版 Windows 作業系統平台為基礎的 AMI 啟動執行個體，請選取位於軟體版本下的完整 AWS Marketplace 網站連結。這會帶您前往組態頁面，您可以在其中從版本清單中選擇。
6. 此清單顯示支援 Windows 作業系統平台的最新 AMI 版本。選取您要從中啟動的 Windows 作業系統版本。

## 使用 RDP 連線至以使用者為基礎的訂閱執行個體

將使用者與提供產品的執行個體建立關聯後，如果執行個體的運作狀態為作用中，他們可以連線到執行個體。使用者需要與其網域的使用者登入資料連線，才能使用具有其關聯身分的產品。

### Important

建立 EC2 執行個體並為使用者做好準備的程序大約需要 20 分鐘。執行個體的關聯狀態必須為作用中，才能存取它並使用產品。

使用以使用者為基礎的訂閱連線到執行個體

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇使用者關聯。
3. 在使用者關聯頁面上，確認執行個體的運作狀態為作用中。
4. 請記下執行個體 ID，因為您將需要它來收集連線詳細資訊。
5. 遵循[使用 RDP 連線至 Windows 執行個體](#)中列出的步驟，同時確保指定相關聯使用者的完整使用者名稱。

## 修改 Microsoft Office 訂閱的防火牆設定

防火牆可保護您的網路資源免於未經授權的傳入或傳出流量。您為安全群組定義的規則充當 VPC 資源的防火牆，這些資源共同提供以使用者為基礎的訂閱 Microsoft Office on EC2 Windows 執行個體。

您可以使用下列步驟來編輯子網路和安全群組。License Manager 使用您的設定來佈建 Microsoft Office 的端點 AWS PrivateLink。如需 VPC 端點的詳細資訊，請參閱 Amazon Virtual Private Cloud 文件中的[什麼是 AWS PrivateLink？](#)。

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 導覽至左側導覽窗格中設定下的以使用者為基礎的訂閱頁面。
3. 若要編輯防火牆設定，請選取 Microsoft Office 訂閱產品索引標籤，然後從防火牆區段頂端選擇編輯。這會開啟編輯防火牆對話方塊。
4. 變更設定後，請選擇儲存以更新，或取消以保留目前的設定。

License Manager 可能需要幾分鐘的時間才能完成這些設定的變更。

## 管理 License Manager 使用者型訂閱的訂閱使用者

為了確保 License Manager 中 Microsoft Office 和 Visual Studio 產品訂閱的計費和報告準確性，以及防止未經授權存取訂閱資源，您可以管理使用者存取權，如下所示。

### [取消使用者與執行個體的關聯](#)

將使用者與託管 License Manager 使用者型 Microsoft Office 或 Visual Studio 產品訂閱的執行個體取消關聯，以移除對資源的存取。

### [取消訂閱使用者](#)

在 中取消訂閱以使用者為基礎的 Microsoft Office 或 Visual Studio 產品訂閱 AWS License Manager，以停止對這些個人產生訂閱費用。

#### Note

從 Active Directory 刪除使用者不會改變 Microsoft Office 和 Visual Studio 產品的使用者關聯或訂閱。您必須取消 License Manager 中的使用者與訂閱產品詳細資訊頁面的關聯，才能移除其與執行個體的關聯。然後，您必須取消訂閱使用者。  
本主題不包含 Active Directory 管理。

## 目錄

- [取消使用者與提供 License Manager 使用者型訂閱之執行個體的關聯](#)

- [在 License Manager 中取消訂閱使用者型產品訂閱](#)

## 取消使用者與提供 License Manager 使用者型訂閱之執行個體的關聯

若要移除提供 License Manager 使用者型訂閱之執行個體的使用者存取權，您可以將訂閱的使用者與該執行個體取消關聯。此變更不會影響使用者的訂閱狀態。若要取消訂閱使用者並停止該個人的訂閱費用，請參閱 [在 License Manager 中取消訂閱使用者型產品訂閱](#)。

### 取消訂閱使用者與執行個體的關聯

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇使用者關聯。
3. 選取您要取消使用者關聯的執行個體。
4. 選取要取消關聯的使用者名稱，然後選擇取消關聯的使用者。

## 在 License Manager 中取消訂閱使用者型產品訂閱

您必須從 Microsoft Office 或 Visual Studio 使用者型訂閱產品取消訂閱使用者，才能停止產生費用。Microsoft RDS 會根據使用者訂閱和使用者連線到提供訂閱產品的執行個體時，從授權伺服器發出的用戶端存取授權 (CAL) 字符的組合，按每位使用者每月計費。如需詳細資訊，請參閱 [License Manager 中的 Microsoft RDS 帳單](#)。

### Important

對於 Microsoft Office 或 Visual Studio 使用者型訂閱產品，您必須先取消 Active Directory 使用者與其目前關聯之所有執行個體的關聯，才能取消訂閱。

### 將使用者取消訂閱以使用者為基礎的產品訂閱

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的使用者型訂閱下，選擇產品。
3. 選取您要取消訂閱使用者的產品。
4. 選取要取消訂閱的使用者名稱，然後選擇取消訂閱使用者。

## 從 License Manager 設定取消註冊 Active Directory

如果您不想再將其用於以使用者為基礎的訂閱，您可以從 License Manager 設定取消註冊 Active Directory。從 License Manager 設定取消註冊目錄組態並不會刪除目錄。當您從設定取消註冊目錄時，您無法再將該目錄的使用者與 License Manager 中以使用者為基礎的訂閱建立關聯。

### 先決條件

從 License Manager 設定取消註冊目錄之前，您必須執行下列任務：

1. [取消使用者與執行個體的關聯](#) 從每個參考您要取消註冊之目錄的執行個體。
2. 取消所有訂閱使用者與執行個體的關聯後，請終止執行個體。重複此動作，直到所有參考 Active Directory 的執行個體都終止為止。
3. 您也需要屬於您要取消註冊的 Active Directory [取消訂閱使用者](#)的，才能停止變更。

### 取消註冊

#### Important

如果您的 Active Directory 用於 Microsoft RDS SAL 使用者，您必須先刪除相關聯的授權伺服器端點，才能取消註冊並刪除 AD。

### 從 License Manager 設定取消註冊 Active Directory

完成所有先決條件任務後，請開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。

1. 在左側的導覽窗格中，選擇設定。
2. 在設定頁面的 AWS Managed Microsoft AD 區段下，選擇移除。
3. 輸入所需的文字以確認您想要移除目錄，然後選擇移除。

選擇移除後，設定頁面上的 AWS Managed Microsoft AD 區段會顯示具有設定狀態的目錄 ID。組態程序完成後，目錄會從 AWS Managed Microsoft AD 區段中移除。

## 對 License Manager 中的使用者型訂閱進行故障診斷

以下是疑難排解秘訣，可協助解決 中以使用者為基礎的訂閱可能發生的問題 AWS License Manager。

## 內容

- [對執行個體合規進行故障診斷](#)
- [使用者訂閱產品組態失敗的故障診斷](#)
- [使用者訂閱執行個體啟動失敗的故障診斷](#)
- [對授權合規進行故障診斷](#)
- [執行個體連線故障診斷](#)
- [對加入網域的失敗進行故障診斷](#)
- [Systems Manager 連線故障診斷](#)
- [Systems Manager Run Command 故障診斷](#)
- [故障診斷 Microsoft RDS 授權失敗](#)
- [故障診斷 Microsoft Office 啟用失敗](#)
- [故障診斷無法刪除 Active Directory](#)
- [故障診斷無法刪除 AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service Linked Role \(SLR\)](#)
- [RDS SAL 產品的訂閱故障診斷不存在錯誤](#)
- [故障診斷授權計數未正確顯示](#)
- [故障診斷 RDS License Diagnoser 問題](#)
- [對信任進行故障診斷](#)
- [使用者訂閱的帳單問題疑難排解](#)
- [故障診斷非作用中的市集訂閱狀態](#)
- [對每個執行個體的使用者限制進行故障診斷](#)
- [對遷移至 RDS SAL 後未提供的 CAL 字符進行故障診斷](#)
- [無縫網域聯結不適用於具有使用者訂閱產品的 EC2 執行個體](#)
- [已在我的帳戶中建立 VPC 端點](#)
- [移除 License Manager 建立的所有 VPC 端點資源](#)
- [在 Managed Active Directory 上變更使用者名稱](#)
- [取消使用者與已終止執行個體的關聯](#)
- [在使用者訂閱執行個體上安裝其他軟體](#)
- [使用者訂閱執行個體上的日文語言套件](#)
- [使用者訂閱執行個體上的本機管理員使用者](#)

- [可 RDP 至使用者訂閱執行個體的使用者數量](#)
- [我的自我管理 AD for Office 和 Visual Studio 產品中的使用者](#)
- [支援的 Windows 作業系統](#)
- [支援的 Office 和 Visual Studio 版本](#)
- [搭配較舊的 Windows Server 版本使用使用者訂閱](#)
- [跨帳戶或區域使用 License Manager 使用者訂閱](#)
- [聯絡 AWS Support 的提示](#)

## 對執行個體合規進行故障診斷

提供以使用者為基礎的訂閱的執行個體必須保持運作狀態，才能符合規範。標示為運作狀態不佳的執行個體不再符合必要的先決條件。License Manager 會嘗試將執行個體恢復為正常運作狀態，但無法恢復正常運作狀態的執行個體會終止。

啟動以提供以使用者為基礎的訂閱，且無法完成初始組態的執行個體將會終止。您必須修正組態問題並啟動新的執行個體，才能在此案例中提供以使用者為基礎的訂閱。如需更多資訊，請參閱在 [License Manager 中建立使用者型訂閱的先決條件](#)。

## 使用者訂閱產品組態失敗的故障診斷

您的產品組態可能因為傳出網路存取問題而失敗。若要解決此問題，請確定預設安全群組允許傳出流量傳送到每個網域控制器網路介面和 SSM 的 IP 地址。

- 確認預設安全群組設定有助於傳出流量到網域控制器網路介面的 IP 地址。
  - License Manager 會建立兩個網路介面，使用 AWS Managed Microsoft AD 佈建您之 VPC 的預設安全群組。這些介面用於目錄所需的服務功能。請確定您的預設安全群組允許傳出流量傳送到每個網域控制器的網路介面 IP 地址，或網域控制器使用的安全群組。如需詳細資訊，請參閱 [管理指南](#) 中 Directory Service [建立使用者型訂閱的先決條件](#) 和 [建立的內容](#)。
- 從提供使用者型訂閱或 VPC 端點的執行個體設定傳出網際網路存取。
  - 必須設定來自提供使用者型訂閱或 VPC 端點之執行個體的傳出網際網路存取，您的執行個體才能與 SSM 通訊。如需詳細資訊，請參閱 AWS Systems Manager 《[使用者指南](#)》中的 [為 EC2 執行個體設定 Systems Manager](#)。

佈建程序完成後，您可以將不同的安全群組與 License Manager 建立的介面建立關聯。您選取的安全群組也必須允許每個網域控制器的網路介面 IPv4 地址或安全群組所需的流量。如需詳細資訊，請參閱《[Amazon Virtual Private Cloud 使用者指南](#)》中的 [使用安全群組](#)。

## 使用者訂閱執行個體啟動失敗的故障診斷

由於多個原因，您的執行個體啟動可能會失敗。以下是執行個體啟動可能失敗的一些常見問題：

- 確保您的執行個體可由 SSM 探索，請參閱 [the section called “執行個體連線故障診斷”](#)。
- 確保您的執行個體能夠加入您的網域，請參閱 [the section called “對加入網域的失敗進行故障診斷”](#)。
- 確定已設定 Route53 傳出解析程式端點規則。如需詳細資訊，請參閱部落格文章 [將 Directory Service 的 DNS 解析與 Amazon Route 53 解析程式整合](#)。
- 如果從使用者訂閱 AMIs 上建立的自訂 AMIs 啟動執行個體，請務必執行 Sysprep，並在從自訂 AMIs 建立和啟動執行個體時確保唯一的電腦名稱。

## 對授權合規進行故障診斷

如果您將 Active Directory 設定為透過 Microsoft Office 提供以使用者為基礎的訂閱，您必須確保您的資源可以連線到 License Manager 建立的 VPC 端點。端點需要 TCP 連接埠 1688 上來自提供使用者型訂閱之執行個體的傳入流量。

您可以使用 [Reachability Analyzer](#) 來協助確認來自提供使用者型訂閱之執行個體的聯網組態，以及 VPC 端點已正確設定。您可以指定在子網路中啟動的執行個體 ID，提供以使用者為基礎的訂閱做為來源，以及為 Microsoft Office 產品佈建的 VPC 端點做為目的地。指定 TCP 做為通訊協定，並指定 1688 做為要分析路徑的目的地連接埠。如需詳細資訊，請參閱 [如何對閘道和界面 VPC 端點的連線問題進行疑難排解？](#)。

## 執行個體連線故障診斷

使用者必須能夠使用 RDP 連線到提供使用者型訂閱的執行個體，才能使用其中的產品。如需執行個體連線故障診斷的詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [連線至 Windows 執行個體的故障診斷](#)。

## 對加入網域的失敗進行故障診斷

使用者必須能夠連線至執行個體，從 License Manager 設定中設定的 Active Directory 提供使用者型訂閱產品及其使用者身分。無法加入網域的執行個體將會終止。

若要疑難排解，您可能需要啟動執行個體並 [手動加入網域](#)，才不會終止資源，才能進行調查。執行個體必須成功接收並執行 Systems Manager Run Command，而且執行個體也必須能夠在作業系統內完成網域聯結。如需詳細資訊，請參閱 AWS Systems Manager 《使用者指南》中的 [了解命令狀態](#)，以及 [如何針對將 Windows 型電腦加入 Microsoft 網站上的網域時發生的錯誤進行故障診斷](#)。

如果您從使用使用者型訂閱產品 AMI 作為其基礎映像的自訂 AMI 啟動執行個體，您必須在自訂 AMI 上執行 Sysprep 步驟，以確保啟動時的唯一電腦名稱。使用 /generalize 執行 Sysprep 之前，請確定機器已從網域中移除。

## Systems Manager 連線故障診斷

提供使用者型訂閱的執行個體必須由管理 AWS Systems Manager，否則將會終止。如需詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的[對 SSM 代理程式進行故障診斷](#)和[對受管節點可用性進行故障診斷](#)。

## Systems Manager Run Command 故障診斷

Run Command 是 Systems Manager 的一項功能，可與提供以使用者為基礎的訂閱的執行個體搭配使用，以加入網域、強化作業系統，以及對包含的產品執行存取稽核。如需詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的[了解命令狀態](#)。

## 故障診斷 Microsoft RDS 授權失敗

如果您遇到 CAL（用戶端存取授權）發行的問題，請檢查您的伺服器陣列或終端機伺服器群組中是否存在其他 Microsoft RDS 授權伺服器。我們不建議在這些位置擁有額外的授權伺服器，因為這可能會干擾 CAL 發行並導致授權複雜性。

若要解決此問題，請確保只有預期的 Microsoft RDS 伺服器保留在您的伺服器陣列和終端機伺服器群組中。

疑難排解授權問題時，請注意使用 /admin 旗標略過標準授權檢查的連線，因為此旗標旨在用於管理目的，且不會使用 CAL。這可能會掩蓋基礎授權問題。若要診斷授權問題，請驗證標準使用者連線（不含 /admin 旗標）是否正常運作以進行授權管理。

## 故障診斷 Microsoft Office 啟用失敗

如果 Microsoft Office 啟用失敗，請確認您的執行個體可存取 License Manager 定義的 VPC。下列其中一個選項符合此要求：

- 您的執行個體正在已加入 License Manager 的 VPC 中執行（透過 VPC 端點）
- 您的執行個體正在與已加入 VPC 的 License Manager 對等的 VPC 中執行。

若要解決此問題，請確定您的執行個體已移至正確的 VPC，或與已加入 License Manager 的 VPC 建立 VPC 對等互連。

## 故障診斷無法刪除 Active Directory

License Manager 會在組態期間向 Directory Service 註冊為授權應用程式，藉此在設定後保護作用中目錄免於刪除。在標準程序中，客戶需要先移除所有執行個體、執行個體關聯和使用者訂閱。之後，他們可以繼續從 License Manager 中移除作用中目錄，然後刪除目錄本身。

## 故障診斷無法刪除 AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service Linked Role (SLR)

License Manager 需要「AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService」服務連結角色來管理將提供使用者型訂閱 AWS 的資源。服務連結角色可讓您更輕鬆地設定 License Manager，因為您不必手動新增必要的許可。License Manager 會定義其服務連結角色的許可，除非另有定義，否則只有 License Manager 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

如需詳細資訊，請參閱 [the section called “以使用者為基礎的訂閱先決條件”](#)和 [License Manager – 以使用者為基礎的訂閱角色和服務連結角色](#)。

## RDS SAL 產品的訂閱故障診斷不存在錯誤

您的帳戶必須擁有 Windows Server 遠端桌面服務訂閱者存取授權 (RDS SAL) 的訂閱。與提供使用者型訂閱產品的執行個體相關聯的所有使用者，除了想要使用的任何其他產品之外，還必須擁有此授權的單一作用中訂閱。您的使用者訂閱以使用者為基礎的訂閱產品時，將會代表他們訂閱 RDS SAL。

但是，如果由於其他合規原因而取消訂閱或移除，您可能需要重新訂閱。如果您已訂閱，您可以嘗試取消訂閱並重新訂閱，這不會影響您的 License Manager 使用者訂閱。

## 故障診斷授權計數未正確顯示

初始設定或組態變更後，授權伺服器最多可能需要 24 小時才能在 License Diagnoser 中顯示所有授權類型的正確授權計數。

處理方式：

- 在設定後等待最多 24 小時，再預期準確的授權計數報告

此延遲是正常的，可讓授權伺服器有足夠的時間正確同步和更新不同授權類型的所有授權資訊。如果您遇到錯誤，請參閱 [the section called “故障診斷 RDS License Diagnoser 問題”](#)。

## 故障診斷 RDS License Diagnoser 問題

這些錯誤通常是由登入資料或許可問題造成。若要解決問題：

1. 驗證使用者登入資料：確保您使用的使用者帳戶與加入期間提供給 License Manager 的使用者帳戶相同
2. 检查工作階段登入資料：如果您在摘要區段中看到伺服器的「憑證不可用」：
  - a. 在顯示「憑證不可用」的摘要區段中，按一下授權伺服器
  - b. 在開啟的右側選單中，新增已加入 License Manager 的使用者憑證
  - c. 按一下「重新整理」

如果問題仍然存在，請遵循 Microsoft 文件中所述的其他疑難排解步驟：[無法連線至 RDS - 無授權伺服器](#)

這應該會解決 License Diagnoser 的大多數登入資料和許可相關問題。

## 對信任進行故障診斷

根據我們與許多客戶合作的經驗，絕大多數的信任組態問題是 DNS 解析或網路連線錯誤。以下是一些疑難排解步驟，可協助您解決常見問題：

- 檢查您是否允許上的傳出聯網流量 AWS Managed Microsoft AD。
- 如果現場部署網域的 DNS 伺服器或網路使用公有（非 RFC 1918）IP 地址空間，請遵循下列步驟：
  - 在 Directory Service 主控台中，前往目錄的 IP 路由區段，選擇動作，然後選擇新增路由。
  - 使用 CIDR 格式輸入 DNS 伺服器或內部部署網路的 IP 地址區塊，例如 203.0.113.0/24。
  - 如果您的 DNS 伺服器和內部部署網路都使用 RFC 1918 私有 IP 地址空間，則不需要此步驟。
- 驗證安全群組並檢查是否需要任何適用的路由後，請啟動 Windows Server 執行個體並將其加入 AWS Managed Microsoft AD 目錄。執行個體啟動後：
  - 執行此 PowerShell 命令來測試 DNS 連線：

```
Resolve-DnsName -Name 'example.local' -DnsOnly
```

你也應該查看文件信任[建立狀態原因指南](#)中的 Directory Service 訊息說明。

## 使用者訂閱的帳單問題疑難排解

AWS 會根據包含授權的 Microsoft Office 或 Visual Studio 執行個體相關聯的使用者數量，透過每月訂閱向您收費。這些每個使用者的費用會按每個日曆月計費，而帳單會從您訂閱產品時開始計算。如果您在現有的月份移除對使用者的存取權，則會在該月的剩餘時間內向使用者收費。您將在下個月停止對使用者產生費用。

此外：

- 計費是以使用者訂閱內的每個使用者為基礎。只有訂閱產品的使用者才會產生費用，而不是作用中目錄中的所有使用者。
- 帳單會以每月週期運作，從每個日曆月的第一天開始。無論訂閱啟用的特定日期為何，都會收取整個月的費用。
- 每個需要存取 Office/VS 執行個體的使用者都需要 RDS SAL。
- 若要停止產生以使用者為基礎的訂閱費用，您必須取消使用者與其關聯之所有執行個體的關聯。從 Active Directory 刪除使用者不會取消使用者與執行個體的關聯。如需詳細資訊，請參閱[the section called “取消使用者與執行個體的關聯”](#)。
- 使用者只會計算一次。無論使用者連線的 EC2 執行個體數量為何，都會向您收取每位 Microsoft Office 和 Visual Studio 的費用。無論使用者是否使用多個執行個體，都會收取一次訂閱費用。

## 故障診斷非作用中的市集訂閱狀態

使用必要產品設定目錄之後，您需要訂閱必要產品。處於非作用中 Marketplace 訂閱狀態的產品會要求您先訂閱，才能將使用者與執行個體建立關聯並加以利用。

## 對每個執行個體的使用者限制進行故障診斷

每位使用者限制 25 個執行個體。如果您需要調整，請聯絡 AWS Support。無論使用者是否使用多個執行個體，都會收取一次訂閱費用。

## 對遷移至 RDS SAL 後未提供的 CAL 字符進行故障診斷

如果您使用自己的 Microsoft RDS 授權伺服器，任何已發行的用戶端存取授權 (CAL) 權杖都會保持有效，直到過期為止。在此期間，具有有效 CAL 權杖的使用者不會自動訂閱 RDS SAL 產品。即使已設定 License Manager，新使用者工作階段也不會自動訂閱 RDS SAL。License Manager 不會覆寫您自己的授權伺服器發行的現有 CAL 權杖。服務受管授權伺服器只會在現有的 CAL 權杖過期後，才會開始發出權杖並處理新請求。一旦目前發行的 CAL 權杖達到過期日期，新的權杖請求將由服務受管授權伺服器處理，使用者會視需要自動訂閱 RDS SAL 產品。

## 無縫網域聯結不適用於具有使用者訂閱產品的 EC2 執行個體

License Manager 需要使用 SSM 在這些執行個體上執行網域聯結，僅允許訂閱產品的使用者獲得授權存取。因此，無縫網域聯結功能會停用。

### 已在我的帳戶中建立 VPC 端點

License Manager 會建立 資源所需的 VPC 端點，以連線至啟用伺服器，並在設定 VPC 時保持合規。

### 移除 License Manager 建立的所有 VPC 端點資源

若要刪除 VPC 端點資源，您必須執行下列動作：

- 取消所有使用者與其以使用者為基礎的訂閱的關聯。如需詳細資訊，請參閱[the section called “取消使用者與執行個體的關聯”](#)。
- 從 License Manager 設定中移除任何已設定的目錄。如需詳細資訊，請參閱[the section called “取消註冊 Active Directory”](#)。
- 終止提供以使用者為基礎的訂閱產品的所有執行個體。如需詳細資訊，請參閱[the section called “從包含的授權 AMI 啟動執行個體”](#)。

### 在 Managed Active Directory 上變更使用者名稱

變更使用者名稱不會影響其將 RDP 轉換為相關聯執行個體的能力。相關聯的使用者應該能夠將 RDP 的更新登入詳細資訊用於使用者訂閱執行個體。

### 取消使用者與已終止執行個體的關聯

每當終止使用者訂閱執行個體時，與執行個體相關聯的所有使用者都會取消關聯。您不需要手動取消使用者關聯。

#### Note

如果執行個體停止，使用者不會取消關聯。

### 在使用者訂閱執行個體上安裝其他軟體

您可以在執行個體上安裝無法以使用者為基礎的訂閱的其他軟體。License Manager 不會追蹤其他軟體安裝。這些安裝必須使用 AWS Managed Microsoft AD 目錄中預設建立的管理員帳戶來執行。如需詳細資訊，請參閱《[管理指南](#)》中的[管理員帳戶](#)。Directory Service

若要使用 Admin 帳戶安裝其他軟體，您必須：

- 將 Admin 帳戶訂閱執行個體提供的產品。
- 將管理員帳戶與執行個體建立關聯。
- 使用 Admin 帳戶連線至執行個體以執行安裝。

如需詳細資訊，請參閱[the section called “開始使用”](#)。

## 使用者訂閱執行個體上的日文語言套件

使用者訂閱執行個體支援日文套件安裝。

## 使用者訂閱執行個體上的本機管理員使用者

我們僅允許使用者受管 Active Directory 網域下的使用者與使用者訂閱執行個體建立關聯，以防止未經授權存取這些 Microsoft 產品。當您在提供使用者型訂閱的執行個體上建立具有管理員權限的本機使用者時，執行個體的運作狀態會變更為運作狀態不佳。

## 可 RDP 至使用者訂閱執行個體的使用者數量

提供使用者型訂閱的執行個體一次最多支援兩個作用中的使用者工作階段，如[針對支援的軟體產品使用 License Manager 使用者型訂閱](#)中所述。根據預設，Windows 在所有版本的 Windows 伺服器中最多允許 2 個遠端桌面連線，包括任何指定時間的 Admin 連線。若要使用超過 2 個並行使用者，客戶需要設定 RDS 授權伺服器。

## 我的自我管理 AD for Office 和 Visual Studio 產品中的使用者

若要關聯自我管理目錄中的使用者，您必須在自我管理目錄和 AWS Managed Microsoft AD 目錄之間建立雙向樹系信任。如需詳細資訊，請參閱《管理指南》中的 Directory Service [教學課程：在 AWS Managed Microsoft AD 與自我管理的 Active Directory 網域之間建立信任關係](#)。

## 支援的 Windows 作業系統

如需有關支援的 Windows 作業系統平台的資訊，請參閱 [the section called “支援的軟體訂閱”](#)。

## 支援的 Office 和 Visual Studio 版本

如需使用者型訂閱支援軟體的詳細資訊，請參閱 [the section called “支援的軟體”](#)。

## 搭配較舊的 Windows Server 版本使用使用者訂閱

當您從支援 Office LTSC Professional Plus 或 Microsoft Visual Studio 的 AMI 啟動執行個體時，啟動預設為 AMI 的最新 Windows 作業系統平台版本（例如 Windows Server 2022）。若要使用舊版作業系統平台啟動，請遵循下列步驟：

1. 在開啟 AWS Marketplace 主控台 <https://console.aws.amazon.com/marketplace>。
2. 從導覽窗格中選擇管理訂閱。
3. 若要簡化訂閱結果，您可以搜尋全部或部分訂閱名稱。例如，Office LTSC Professional Plus 或 Visual Studio Enterprise。
4. 從訂閱面板選取啟動新執行個體。這會開啟啟動組態頁面。
5. 若要從以舊版 Windows 作業系統平台為基礎的 AMI 啟動執行個體，請選取位於軟體版本下的完整 AWS Marketplace 網站連結。這會帶您前往組態頁面，您可以在其中從版本清單中選擇。
6. 此清單顯示支援 Windows 作業系統平台的最新 AMI 版本。選取您要從中啟動的 Windows 作業系統版本。

## 跨帳戶或區域使用 License Manager 使用者訂閱

支援以下案例：

- 跨帳戶使用 License Manager 使用者訂閱
- 搭配共用 Active Directory 使用 License Manager 使用者訂閱

不支援這些案例：

- 跨區域使用 License Manager 使用者訂閱

## 聯絡 AWS Support 的提示

- 聯絡 AWS 支援時，請使用與已終止執行個體相同的設定建立執行個體，並啟用執行個體終止保護以快速回應。
- 對於任何 RDP 相關問題，我們需要 RDP 相關日誌來協助偵錯這些問題。請針對具有網際網路存取的環境使用 'AWSSupport-RunEC2RescueForWindowsTool'。如需詳細資訊，請參閱 [EC2Rescue for Windows Server](#)。

- 透過使用 Office 執行個體做為工作執行個體，並掛載從原始執行個體磁碟區的快照還原的磁碟區，即使在沒有網際網路存取的環境中，也可以收集資料。
- 從備份 AMIs 啟動執行個體的故障診斷：如果您從備份 AMI 啟動執行個體，則必須終止原始執行個體。

## 在 License Manager 中管理 Linux 訂閱

透過 AWS License Manager，您可以檢視和管理 Amazon EC2 執行個體使用的商業 Linux 訂閱。您可以追蹤您在設定中定義之 AWS 區域和帳戶的 Linux AWS Organizations 訂閱使用率。License Manager 可讓您全面檢視使用 Linux 訂閱的執行中執行個體。它也會指出執行個體何時定義了多個訂閱。

License Manager 探索的資料會彙總並顯示在 License Manager 主控台和 Amazon CloudWatch 儀表板中。您也可以透過 AWS CLI 和 License Manager Linux 訂閱 API 或相關聯的 SDKs 存取您的訂閱資料。

Linux 授權訂閱可以來自下列來源：

### 包含訂閱 AMIs

- Red Hat Enterprise Linux (RHEL)
- RHEL 使用 Red Hat Cloud Access Program 自攜訂閱模型 (BYOS)
- SUSE Linux Enterprise Server
- Ubuntu Pro 包含訂閱的 AMI

### 第三方訂閱供應商

- Red Hat Subscription Manager (RHSM) 的 RHEL 訂閱

Linux 訂閱探索使用最終一致性模型。一致性模型會決定載入資料並在 Linux 訂閱檢視中呈現的方式和時間。透過此模型，License Manager 可確保您的 Linux 訂閱資料從您的資源定期更新。如果在這些間隔期間未擷取某些資料，則會在下一個指標發射時傳送資訊。這種行為可能會延遲資源，例如新啟動的 EC2 商業 Linux 執行個體，使其無法顯示在 Linux 訂閱儀表板中。

**Note**

初始資源探索最多可能需要 36 小時才能完成，新啟動的執行個體最多可能需要 12 小時才能被探索和報告。一旦發現您的資源，就會每小時針對 Linux 訂閱資料發出 Amazon CloudWatch 指標。

如果您的帳戶位於 中 AWS Organizations，您可以將成員帳戶註冊為委派管理員。如需詳細資訊，請參閱[License Manager 中的委派管理員設定](#)。

### 偵測到重複的訂閱

當 License Manager 在同一個 EC2 執行個體上偵測到兩個 Linux 訂閱時，它會設定重複的訂閱提醒。您可以從 License Manager 主控台的執行個體頁面檢視和篩選 Linux 訂閱資料。

Red Hat Enterprise Linux 7 延長生命週期支援 (RHEL 7 ELS) 執行個體：當您從包含 RHEL 7 ELS 訂閱的 AMI 啟動執行個體時，您仍應該向 Red Hat 註冊執行個體並取用權利。在此情況下，License Manager 會報告重複的訂閱，但這是預期的行為。

其他 Red Hat Linux 執行個體：我們建議您在 [Red Hat 混合雲端主控台](#) 中搜尋訂閱庫存，以了解執行個體使用的訂閱。

### 其他主題

- [在 License Manager 中設定 Linux 訂閱探索](#)
- [在 License Manager 中檢視探索到的執行個體資料](#)
- [License Manager 中 Linux 訂閱的帳單資訊](#)
- [在 License Manager 中管理 Linux 訂閱的 Amazon CloudWatch 警示](#)

## 在 License Manager 中設定 Linux 訂閱探索

您可以透過 License Manager 主控台、AWS CLI、License Manager Linux 訂閱 API 或相關聯的 SDKs 來設定 Linux 訂閱的探索。當您為 AWS 區域 指定的 啟用 Linux 訂閱探索時，您可以選擇將探索擴展到您的帳戶 AWS Organizations。如果您不想再追蹤訂閱使用率，您也可以停用探索。

**Note**

根據 AWS 區域 預設，每個帳戶最多可以探索和顯示 5,000 個資源。若要請求提高這些限制，請使用[提高限制表單](#)。

## 主題

- [設定 Linux 訂閱探索](#)
- [啟用 Red Hat Subscription Manager 訂閱探索](#)
- [資源探索狀態原因](#)
- [停用 Linux 訂閱的探索](#)

## 設定 Linux 訂閱探索

若要從 License Manager 主控台的設定頁面設定 Linux 訂閱探索，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇設定。這會開啟設定頁面。
3. 開啟 Linux 訂閱索引標籤，然後選擇設定。這會開啟設定 Linux 訂閱設定面板。
4. 選取 Linux 訂閱探索應執行的來源 AWS 區域。
5. 若要彙總您帳戶中的訂閱資料 AWS Organizations，請選取連結 AWS Organizations。只有在已為您的帳戶設定時 AWS Organizations，才會顯示此選項。
6. 檢閱並確認授予為 Linux 訂閱建立服務連結角色之 AWS License Manager 許可的選項。
7. 選擇 Save configuration (儲存組態)。

## 啟用 Red Hat Subscription Manager 訂閱探索

若要代表您從 Red Hat Subscription Manager (RHSM) 擷取訂閱資訊，授權管理員必須提供您的 Red Hat 客戶帳戶 API 登入資料。

### 先決條件

啟用訂閱探索之前，請確定您已符合下列先決條件。

- 您必須先為 啟用 Linux 訂閱的預設探索，AWS 帳戶 才能設定 microSDHCM 訂閱探索。如果未啟用預設探索，請參閱 [設定 Linux 訂閱探索](#)。
- 如果您使用組織管理員提供的公司 Red Hat 登入，請確定您的登入 ID 已指派下列角色和許可：
  - 角色：管理您的訂閱
  - 許可：View All或 View/Edit All

如果您的登入 ID 沒有必要的角色和許可，請聯絡您的 Red Hat 入口網站組織管理員，並請求將其新增至您的登入。如需 Red Hat 角色和許可的詳細資訊，請參閱 [Red Hat 客戶入口網站的角色和](#)

**許可。** 如需如何聯絡 Red Hat 入口網站組織管理員的詳細資訊，請參閱 Red Hat 客戶入口網站知識庫中的 [如何知道我的組織管理員是誰？](#)。

- 若要啟用 microSDHCM 訂閱探索，您必須提供 Red Hat 客戶帳戶 API 離線權杖，或包含離線權杖的 AWS Secrets Manager 秘密。若要取得離線權杖，請遵循 Red Hat 文件網站上 [產生新的離線權杖](#) 中所述的步驟。

#### Important

您的安全對我們很重要。您的 Red Hat 離線存取權杖會安全地存放在 Secrets Manager 中。License Manager 每次向 Red Hat 請求訂閱詳細資訊時，都會使用您的秘密來產生臨時存取字符。

## 啟用

若要從 License Manager 主控台的設定頁面啟用 microSDHCM 探索，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇設定。
3. 在設定頁面上，開啟 Linux 訂閱索引標籤。
4. 選擇編輯以更新您的 Linux 訂閱設定。這會開啟設定 Linux 訂閱探索頁面。
5. 若要開始啟用程序，請選取啟用 Red Hat Subscription Manager (RHSM) 探索核取方塊。這會顯示 Link RHSM 帳戶面板。
6. 選取適用於您秘密的秘密（權杖）選項，然後遵循取決於您選擇的選項的剩餘步驟。
7. 選項：建立新的秘密 – 建議

提供 Red Hat 離線存取字符，並讓 License Manager 代表您在 Secrets Manager 中建立存取秘密。

- a. 在秘密名稱中輸入秘密的名稱。
- b. 將您的 Red Hat 離線存取權杖貼到離線權杖方塊中。請確定字符值之前或之後沒有額外的空格或換行符號。您可以在 Red Hat [Subscription Manager API Tokens 頁面上產生 Red Hat 離線存取字符](#)。

選項：選取秘密

在 Secrets Manager 中選取包含 Red Hat 離線存取權杖的現有秘密。

8. (選用) 新增秘密的標籤。
9. 選取頁面底部的核取方塊，確認透過啟用 Red Hat Subscription Manager 探索，您授予 AWS License Manager 服務的存取權，以收集與 Amazon EC2 執行個體上使用的 Red Hat 訂閱相關的資料。
10. 選擇 Activate (啟用)。

## 資源探索狀態原因

AWS License Manager 會顯示您選擇為 Linux 訂閱啟用探索的每個 AWS 區域 狀態和對應的狀態原因。如果您已將 Linux 訂閱與下列項目連結，則狀態原因會有所不同 AWS Organizations：

- In progress (正在進行)
- 成功
- 失敗

針對您選擇的每個區域顯示的狀態原因一次最多會顯示兩個狀態原因。下表提供更多詳細資訊：

狀態原因動作	Description
帳戶加入	加入單一帳戶。
帳戶離線	將單一帳戶卸任。
組織加入	加入整個組織。
Org-offboard	讓整個組織離職。

您可以呼叫 UpdateServiceSettings API，然後呼叫 GetServiceSettings API 來監控啟用 Linux 訂閱的進度。每個狀態和狀態原因可以一次套用到多個區域。下表提供有關狀態和狀態原因的詳細資訊：

狀態	狀態原因	Description
進行中	"Region": "Account-Onboard: Pending"	正在為單一帳戶啟用 Linux 訂閱。
	"Region": "Org-Onboard: Pending"	正在為組織啟用 Linux 訂閱。
	"Region": "Account-Offboard: Pending"	正在停用單一帳戶的 Linux 訂閱。
	"Region": "Org-Offboard: Pending"	正在停用組織的 Linux 訂閱。
成功	"Region": "Account-Onboard: Successful"	為單一帳戶啟用 Linux 訂閱成功。
	"Region": "Org-Onboard: Successful"	成功啟用組織的 Linux 訂閱。
	"Region": "Account-Offboard: Successful"	成功停用單一帳戶的 Linux 訂閱。
	"Region": "Org-Offboard: Successful"	成功停用組織的 Linux 訂閱。
失敗	"Region": "Account-Onboard: Failed - Service-linked role not present"	由於未建立所需的服務連結角色，因此單一帳戶啟用 Linux 訂閱失敗。建立所需的角色，然後再試一次。
	"Region": "Account-Onboard: Failed - An internal error occurred"	由於內部錯誤，為單一帳戶啟用 Linux 訂閱失敗。
	"Region": "Org-Onboard: Failed - Account isn't the management account"	為組織啟用 Linux 訂閱失敗，因為執行操作的帳戶不是組織的管理帳戶。登入管理帳戶，然後再試一次。

狀態	狀態原因	Description
	"Region": "Org-Onboard: Failed - Account isn't part of an organization"	為組織啟用 Linux 訂閱失敗，因為執行操作的帳戶不在組織中。嘗試從組織中的帳戶執行操作，或將此帳戶新增至組織，然後再試一次。
	"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"	為組織啟用 Linux 訂閱失敗，因為 License Manager 沒有存取組織的許可。建立 Linux 訂閱的服務連結角色，然後再試一次。

## 停用 Linux 訂閱的探索

您可以從 AWS License Manager 設定頁面停用 Linux 訂閱的探索。不過，如果您已啟用的探索

### Warning

如果您停用探索，先前針對 Linux 訂閱探索的所有資料都會從中移除 AWS License Manager。

## 停用 Linux 訂閱的探索

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 在設定頁面上，選擇 Linux 訂閱索引標籤，然後選擇停用 Linux 訂閱探索。
4. 輸入 **Disable**，然後選擇停用以確認停用。
5. （選用）移除用於 Linux 訂閱的服務連結角色。如需詳細資訊，請參閱 [刪除 License Manager 的服務連結角色](#)。
6. （選用）停用 License Manager 與您的組織之間的受信任存取。如需詳細資訊，請參閱 [AWS License Manager 和 AWS Organizations](#)。

## 在 License Manager 中檢視探索到的執行個體資料

License Manager 在所選中完成初始資源探索程序後 AWS 區域，您可以在主控台中檢視結果。如果您選擇連結 AWS Organizations，License Manager 會從整個組織的帳戶彙總資料。若要檢視訂閱符

合您篩選條件的執行個體清單，請導覽至 AWS License Manager 主控台的執行個體區段。清單會顯示下列金鑰欄位。

- 執行個體 ID – 執行個體的 ID。
- 狀態 – 執行個體的状态。
- 執行個體類型 – 執行個體的類型。
- 訂閱 – 執行個體使用的授權訂閱名稱。
- 重複提醒 – 表示您的執行個體上相同軟體有兩個不同的授權訂閱。
- 帳戶 ID – 擁有執行個體的帳戶 ID。
- 區域 – AWS 區域 執行個體所在的。
- AMI ID – 用來啟動執行個體的 AMI ID。
- 用量操作 – 執行個體的操作，以及與 AMI 相關聯的帳單代碼。如需詳細資訊，請參閱[用量操作值](#)。
- 產品代碼 – 與用來啟動執行個體的 AMI 相關聯的產品代碼。如需詳細資訊，請參閱[AMI 產品代碼](#)。
- LastUpdatedTime – 上次探索更新執行個體詳細資訊的時間。

## 主題

- [檢視所有執行個體的資料](#)
- [依訂閱檢視執行個體的資料](#)

## 檢視所有執行個體的資料

您可以檢視和篩選 License Manager 為您帳戶中的執行個體探索的 Linux 訂閱資料 AWS Organizations，如下所示。

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的 Linux 訂閱下，選擇執行個體。這會顯示具有 Linux 訂閱資料的執行個體清單。
3. (選用) 您可以使用下列篩選條件來簡化結果：
  - 帳戶
  - AMI ID
  - 重複訂閱
  - 執行個體 ID
  - 區域

- 產品代碼
  - 使用操作
4. (選用) 選擇匯出檢視至 CSV，將所有執行個體的資料匯出為逗號分隔值檔案 (CSV)。

## 依訂閱檢視執行個體的資料

您可以檢視所有執行個體的資料已彙總至您組織中所選區域內的帳戶。

檢視具有特定訂閱之執行個體的探索資料

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的 Linux 訂閱下，選擇訂閱。
3. 在訂閱名稱欄下，選擇您要檢視資料的訂閱。
4. 選擇執行個體索引標籤，並視需要在主控台中檢閱資料。您可以依下列條件篩選資料：
  - 執行個體 ID
  - 帳戶
  - 區域
  - AMI ID
  - 使用操作
  - 產品代碼
5. (選用) 選擇匯出檢視至 CSV，以將此訂閱的執行個體資料匯出為逗號分隔值檔案 (CSV)。

## License Manager 中 Linux 訂閱的帳單資訊

在 Amazon EC2 上執行的每個商業 Linux 訂閱都有與 Amazon Machine Image (AMI) 相關聯的帳單資訊。商業 Linux 訂閱具有 Amazon EC2 用量操作、AWS Marketplace 產品程式碼或兩者的組合。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud Linux 執行個體使用者指南》中的 [AMI 帳單資訊欄位](#)，以及《AWS Marketplace 賣方指南》中的 [AMI 產品代碼](#)。

訂閱名稱	Amazon EC2 用量操作	AWS Marketplace 產品代碼	訂閱類型
Red Hat Enterprise Linux 伺服器 BYOS	RunInstances:00g0	X	使用您自己的訂閱模型 (BYOS)
Red Hat Enterprise Linux 伺服器	RunInstances:0010	X	包含 EC2 訂閱
具有高可用性附加元件的 Red Hat Enterprise Linux	RunInstances:1010	X	包含 EC2 訂閱
具有 SQL Server Standard 和高可用性的 Red Hat Enterprise Linux	RunInstances:1014	X	包含 EC2 訂閱
Red Hat Enterprise Linux 搭配 SQL Server Enterprise 和高可用性	RunInstances:1110	X	包含 EC2 訂閱
帶 SQL Server Standard 的 Red Hat Enterprise Linux	RunInstances:0014	X	包含 EC2 訂閱
帶 SQL Server Web 的 Red Hat Enterprise Linux	RunInstances:0210	X	包含 EC2 訂閱
帶 SQL Server Enterprise 的 Red Hat Enterprise Linux	RunInstances:0110	X	包含 EC2 訂閱
SUSE Linux Enterprise Server	RunInstances:000g	X	包含 EC2 訂閱

訂閱名稱	Amazon EC2 用量操作	AWS Marketplace 產品代碼	訂閱類型
Red Hat Enterprise Linux for SAP 搭配高可用性和更新服務	RunInstances:0010	✓	AWS Marketplace 訂閱 1
SUSE Linux Enterprise Server 搭配 SAP	x	✓	AWS Marketplace 訂閱
Ubuntu Pro	RunInstances:0g00	✓	AWS Marketplace 訂閱
Red Hat Enterprise Linux 工作站	x	✓	AWS Marketplace 訂閱

1 此訂閱同時具有 Amazon EC2 用量操作和 AWS Marketplace 產品代碼。

## Linux 訂閱的使用量指標

下列指標和維度適用於 Linux 訂閱：

指標	Description
RunningInstancesCount	<p>在目前帳戶中執行的執行個體總數，依訂閱名稱或訂閱名稱和區域分組。</p> <p>單位：Count</p> <p>維度：</p> <p>SubscriptionName：訂閱的名稱。</p> <p>Region：探索使用商業 Linux 訂閱之資源的區域。</p>

## 在 License Manager 中管理 Linux 訂閱的 Amazon CloudWatch 警示

License Manager 主控台內的 Linux 訂閱清單頁面會顯示下列金鑰詳細資訊，包括您為 License Manager 在執行個體中找到的每個 Linux 訂閱設定的 Amazon CloudWatch 警示。

- 訂閱名稱
- 訂閱類型
- 每個訂閱的執行中執行個體數量
- 設定的 Amazon CloudWatch 警示

當您從清單頁面選擇 Linux 訂閱時，用量指標和警示索引標籤會顯示該訂閱的資料。在此索引標籤中，Amazon CloudWatch 儀表板會在 License Manager 主控台中顯示所選訂閱的。您可以調整儀表板，以包含特定時間範圍或評估範圍，從所選日期起算，以小時、天數或一週為單位。

在用量指標和警示索引標籤中，每個訂閱都有一個警示區段，其中包含下列詳細資訊：

- 警示名稱 – 警示的名稱。
- 狀態 – 警示的狀態。
- 維度 – 警示的維度。維度將包含定義的 AWS 區域 和 執行個體類型。
- 條件 – 警示的條件。條件將包含定義的比較運算子和警示閾值。

您可以使用您定義的維度和條件來建立 CloudWatch 警示，以根據目前的訂閱使用率來追蹤和提醒。Linux 訂閱主控台會顯示使用中的訂閱名稱摘要、訂閱類型、每個訂閱的執行中執行個體數量，以及警示狀態。

以下是可能的 CloudWatch 警示狀態：

- OK – 指標或表達式在定義的閾值內。
- ALARM – 指標或表達式超出定義的閾值。
- INSUFFICIENT\_DATA – 警示剛啟動、指標無法使用，或沒有足夠的資料可供指標判斷警示狀態。

## 主題

- [為 Linux 訂閱建立 CloudWatch 警示](#)
- [修改 Linux 訂閱的 CloudWatch 警示](#)
- [刪除 Linux 訂閱的 CloudWatch 警示](#)

## 為 Linux 訂閱建立 CloudWatch 警示

您可以為執行中 EC2 執行個體上探索到的每個商業 Linux 訂閱建立警示。如有必要，您可以為每個訂閱建立多個具有不同維度和條件的警示。

## 從主控台建立 Linux 訂閱的 CloudWatch 警示

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的 Linux 訂閱下，選擇訂閱。
3. 在訂閱名稱欄下，選擇要為其建立警示的訂閱，然後選擇建立警示。
4. 為警示指定下列項目：
  - 警示名稱 – 指定類似的名稱 `AWS-LM-LS-AlarmName`。
  - 執行個體類型 – 選擇將使用所選訂閱的執行個體類型。
  - 用量區域 – 選擇要為其建立警示的區域。
  - 比較運算子 – 警示閾值的比較運算子。
  - 警示閾值 – 警示閾值的值。
5. 選擇建立以建立警示。

## 修改 Linux 訂閱的 CloudWatch 警示

您可以從 License Manager 主控台修改現有的 CloudWatch 警示，以適應不斷變化的需求。

### 從主控台修改 Linux 訂閱的 CloudWatch 警示

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的 Linux 訂閱下，選擇訂閱。
3. 在訂閱名稱欄下，選擇要修改的訂閱，然後選擇編輯。
4. 視需要修改定義的值。
5. 選擇編輯以修改警示。

## 刪除 Linux 訂閱的 CloudWatch 警示

您可以從 License Manager 主控台刪除現有的 CloudWatch 警示，以適應不斷變化的需求。

### 從主控台刪除 Linux 訂閱的 CloudWatch 警示

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格的 Linux 訂閱下，選擇訂閱。
3. 在訂閱名稱欄下，選擇要修改的訂閱，然後選擇刪除。

## 賣方在 License Manager 中發行的授權

獨立軟體廠商 (ISVs) 可以使用 AWS License Manager 來管理和分發軟體授權給最終使用者。身為發行者，您可以使用 License Manager 儀表板，集中追蹤您發行的授權使用情況。

License Manager 使用開放、安全、業界標準來代表授權，並允許客戶以密碼編譯方式驗證其真實性。License Manager 會將每個授權與非對稱金鑰建立關聯。作為 ISV，您擁有非對稱 AWS KMS 金鑰並將其存放在您的帳戶中。

賣方發行的授權需要跨區域複寫授權中繼資料。License Manager 會自動將每個賣方發行的授權及其相關資訊複寫到其他區域。

License Manager 支援各種不同的授權模式，包括下列項目：

- 永久 – 沒有過期日期的生命週期授權，可授權使用者無限期使用軟體。
- 浮動 – 具有多個應用程式執行個體的可共用授權。授權可以預付，並新增一組固定的權限。
- 訂閱 – 除非特別停用，否則具有可自動續約過期日期的授權。
- 以用量為基礎 – 根據用量具有特定條款的授權，例如 API 請求、交易或儲存功能的數目。

您可以在 License Manager 中建立授權，並使用 IAM AWS 身分或透過 License Manager 產生的承載字符將授權分發給您的客戶。擁有 AWS 帳戶的 ISV AWS 客戶可以將授權權利重新分配給其各自組織中的身分。具有分散式權利的客戶可以透過與 License Manager 的軟體整合，從該授權簽出和簽入所需權利。

## 賣方在 License Manager 中授予的授權權利

License Manager 會將賣方發行的授權功能擷取為授權中的權利。權利的特性可以是有限或無限制的數量。有限權利的範例為「40 GB 的資料傳輸」。無限數量權利的範例為「Platinum Tier」。

授權會擷取所有授予的權限、啟用和過期日期，以及發行者詳細資訊。授權是版本控制的實體，每個版本都是不可變的。授權版本會在變更授權時更新。

若要簽出或簽入有限權利，ISV 應用程式必須指定每個有限容量的數量。對於無限制權利，ISV 應用程式可以直接指定相關權利以簽出或再次簽入。最後，有限功能也支援「超額」旗標，這表示最終使用者是否可以超過初始權利的使用量。License Manager 會追蹤並向 ISV 報告用量以及任何超額。

## 賣方在 License Manager 中發行的授權使用量

License Manager 可讓您透過維護所有簽出權利的計數，集中追蹤多個區域的授權。License Manager 也會追蹤使用者身分和基礎資源識別符，如果可用的話，與每個簽出相關聯，以及簽出的時間。您可以透過 CloudWatch Events 追蹤此時間序列資料。

授權可能處於下列其中一種狀態：

- 已建立 – 已建立授權。
- 已更新 – 授權已更新。
- 已停用 – 授權已停用。
- 已刪除 – 授權已刪除。

## 在 License Manager 中追蹤賣方發行的授權用量所需的許可

若要開始使用此功能，您需要呼叫下列 License Manager API 動作的許可。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "license-manager:CreateLicense",
        "license-manager:CreateLicenseVersion",
        "license-manager:ListLicenses",
        "license-manager:ListLicenseVersions",
        "license-manager:GetLicense",
        "license-manager>DeleteLicense",
        "license-manager:CheckoutLicense",
        "license-manager:CheckInLicense",
        "license-manager:ExtendLicenseConsumption",
        "license-manager:GetLicenseUsage",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager>DeleteGrant",
        "license-manager:GetGrant",

```

```

        "license-manager:ListDistributedGrants"
      ],
      "Resource": "*"
    }
  ]
}

```

如果您將與 License Manager 整合，讓沒有 AWS 帳戶的客戶可以使用 外部販售的授權 AWS Marketplace，您必須建立 IAM 角色，讓您的軟體應用程式能夠呼叫 License Manager API。

如果您使用 AWS 管理主控台 為沒有的客戶分發臨時登入資料 AWS 帳戶，License Manager 將AWSLicenseManagerConsumptionRole代表您自動建立。如需詳細資訊，請參閱[為沒有 AWS 帳戶的 ISV 客戶取得臨時登入資料](#)。若要從 建立此角色 AWS CLI，請使用 AWS IAM [create-role](#) 命令，如下列範例所示。

```

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檔案看起來應該類似下列範例，並將您自己的 AWS 帳戶 ID 取代為字符發行者帳戶。

## JSON

```

{
  "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-123456789012:123456789012"
        }
      }
    }
  ]
}

```

```
    }  
  }  
]  
}
```

接著，使用 [attach-role-policy](#) 命令，將 AWSLicenseManagerConsumptionPolicy AWS 受管政策新增至 AWSLicenseManagerConsumptionRole 角色。

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

## 在 License Manager 中建立賣方發行的授權

使用下列程序建立授權區塊，以使用 授予客戶 AWS 管理主控台。或者，您可以使用 [CreateLicense](#) API 動作來建立授權。

使用主控台建立授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從左側選單中選擇賣方發行的授權。
3. 選擇建立授權。
4. 針對授權中繼資料，請提供下列資訊：
  - 授權名稱 – 要向買方顯示的名稱，最多 150 個字元。
  - 授權描述 – 選用的描述，最多 400 個字元，可區分此授權與其他授權。
  - 產品 SKU – 產品 SKU。
  - 收件人 – 收件人的名稱（公司或個人）。
  - 主區域 – 授權 AWS 的區域。雖然授權可以全域使用，但您只能變更主區域中的授權。您無法在建立授權之後變更授權的主區域。
  - 授權開始日期 – 啟用日期。
  - 授權結束日期 – 授權的結束日期，如適用。
5. 針對使用組態，請提供下列資訊：
  - 續約頻率 – 是否每週續約、每月續約，還是完全不續約。

- 耗用組態 – 如果授權用於持續連線，請選擇佈建耗用組態選項；如果授權用於離線，請選擇借用。輸入存留時間上限（分鐘），以設定授權的可用性長度。
6. 對於發行者，請提供下列資訊：
    - 輸入 AWS KMS 金鑰 – License Manager 使用此金鑰來簽署和驗證發行者。如需詳細資訊，請參閱[License Manager 中授權的密碼編譯簽署](#)。
    - 發行者名稱 – 賣方的商業名稱。
    - 記錄賣方 – 選用的商業名稱。
    - 協議 URL – 授權合約的 URL。
  7. 針對權利，提供授權授予收件人之功能的下列資訊：
    - 名稱 – 收件人的名稱。
    - 單位類型 – 選取單位類型，然後提供最大計數。
    - 勾選允許簽入 收件人是否必須在續約之前簽入授權。
    - 如果收件人可以使用超過最大計數的資源，請檢查允許的超額。此選項可能會對收件人產生額外費用。
  8. 選擇建立授權。

## 將 License Manager 賣方核發的授權授予 ISV 客戶

新增授權之後，您可以使用 將授權授予擁有 AWS 帳戶的客戶 AWS 管理主控台。收件人必須先接受授予，才能使用授權。如需詳細資訊，請參閱[License Manager 中授予的授權](#)。

或者，如果客戶沒有 AWS 帳戶，您可以使用 License Manager API 讓客戶[能夠使用授權](#)。

### 使用主控台將授權授予客戶

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從左側選單中選擇賣方發行的授權。
3. 選擇授權的 ID 以開啟其詳細資訊頁面。
4. 針對授予，選擇建立授予。
5. 如需授予詳細資訊，請提供下列資訊：
  - 授予名稱 – 授予名稱。這用於啟用搜尋功能。
  - AWS 帳戶 ID – 授權收件人的 AWS 帳號。

- 授權權利
    - 如果收件人可以使用授予的權限，請選取使用。
    - 如果收件人可以將授予的權限分發給其他 AWS 帳戶，請選取分發。
    - 選取允許現場部署字符產生以驗證共用授權 AWS ，而不使用身分或登入資料。
    - 選取允許提交用量記錄，以允許授權收件人發出用量類型的用量記錄。
  - 主區域 – 授權 AWS 區域 的。
6. 選擇建立授予。

## 為沒有 AWS 帳戶的 ISV 客戶取得臨時登入資料

對於沒有 AWS 帳戶的客戶，您可以使用與使用 AWS 帳戶為客戶相同的方式使用權利。使用下列程序為沒有 AWS 帳戶的客戶取得臨時 AWS 登入資料。API 呼叫必須在主區域中進行。

取得用於呼叫 License Manager API 的臨時登入資料

1. 呼叫 [CreateToken](#) API 動作，以取得編碼為 JWT 權杖的重新整理權杖。
2. 呼叫 [GetAccessToken](#) API 動作，指定您在上一個步驟CreateToken中從 收到的重新整理權杖，以接收臨時存取權杖。
3. 呼叫 [AssumeRoleWithWebIdentity](#) API 動作，指定您在上一個步驟GetAccessToken中從 收到的存取字符，以及您建立的 AWSLicenseManagerConsumptionRole 角色，以取得臨時 AWS 憑證。

從 AWS License Manager 主控台建立字符

1. 從 [License Manager 主控台](#)，導覽至授權詳細資訊頁面，以取得您想要在沒有 AWS 帳戶的情況下使用的特定授權權利。
2. 選擇建立權杖以產生臨時存取權杖。

### Note

第一次產生臨時存取字符時，系統會要求您建立服務角色，以便 License Manager 可以代表您存取服務。已建立下列服務角色：AWSLicenseManagerConsumptionRole。

3. 下載 token.csv 檔案，或在產生時複製字符字串。

**⚠ Important**

這是您唯一可以檢視或下載此字符的時間。我們建議您下載權杖，並將檔案存放在安全的位置。您可以隨時建立新的權杖，最多可達 [服務限制](#)。

## 在 License Manager 中查看賣方發行的授權

License Manager 允許多個使用者同時從單一授權使用功能有限的權利。呼叫 [CheckoutLicense](#) API 動作。以下是參數的描述。

- 金鑰指紋 – 信任的授權發行者。

範例：aws : 123456789012 : issuer : issuer-fingerprint

- 產品 SKU – 此授權的產品識別符，如授權發行者建立授權時所定義。多個 ISVs 之間可能存在相同的產品 SKU。因此，信任的金鑰指紋扮演重要角色。

範例：1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE

- 權利 – 簽出的功能。如果您指定無限功能，數量為零。範例：

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

- 受益人 – 軟體即服務 (SaaS) ISVs 可以透過包含客戶識別符來代表客戶簽出授權。License Manager 會限制對 SaaS ISV 帳戶中建立之授權儲存庫的呼叫。

範例：user@domain.com

- 節點 ID – 用來將授權鎖定到應用程式的單一執行個體的識別符。

範例：10.0.21.57

## 在 License Manager 中刪除賣方發行的授權

刪除授權之後，您可以重新建立授權。授權及其資料會以唯讀模式保留並提供給授權發行者和授權承授者六個月。

使用下列程序來刪除您使用 建立的授權 AWS 管理主控台。或者，您可以使用 [DeleteLicense](#) API 動作來刪除授權。

### 使用主控台刪除授權

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 從左側選單中選擇賣方核發的授權。
3. 選擇授權旁的選項按鈕，以選取要刪除。
4. 選擇 刪除。出現確認提示時，請輸入 **delete**，然後選擇刪除。

## License Manager 中的設定

AWS License Manager 主控台的設定區段會顯示目前帳戶的設定。您必須設定 設定以啟用相關聯的功能。

### Managed licenses

下列設定可針對受管授權進行設定：

- 將受管權利和自我管理授權分發到您的組織
- Cross-account resource discovery (跨帳戶資源探索)
- Amazon SNS 通知
- 授權資產群組的授權資產探索和規則集組態

對於使用授權資產群組的組織，其他設定可用於跨區域探索和跨多個 AWS 區域和帳戶的整個組織授權管理。

如需詳細資訊，請參閱[License Manager 中的受管授權設定](#)。

## Linux subscriptions

Linux 訂閱可設定下列設定：

- [探索和彙總商業 Linux 授權訂閱資料](#)
- [Linux 訂閱的 Red Hat Subscription Manager \(RHSM\) 探索](#)

如需詳細資訊，請參閱[License Manager 中的 Linux 訂閱設定](#)。

## User-based subscriptions

下列設定可供使用者型訂閱設定：

- [AWS Managed Microsoft AD](#)
- [Virtual Private Cloud \(VPC\)](#)

如需詳細資訊，請參閱[License Manager 中的使用者型訂閱設定](#)。

## Delegated administration

如果您的帳戶具有組織的管理存取權，則會顯示此標籤。身為管理員，您可以從 AWS CLI 或註冊委派管理員 AWS 管理主控台。如需詳細資訊，請參閱[License Manager 中的委派管理員設定](#)。

## 設定主題

- [編輯 License Manager 設定](#)
- [License Manager 中的受管授權設定](#)
  - [授權資產探索和規則集設定](#)
  - [帳戶詳細資訊](#)
  - [Cross-account resource discovery \(跨帳戶資源探索\)](#)
  - [簡易通知服務 \(SNS\)](#)
- [License Manager 中的 Linux 訂閱設定](#)
  - [Linux 訂閱設定](#)
  - [Red Hat Subscription Manager 探索](#)
- [License Manager 中的使用者型訂閱設定](#)
  - [AWS Managed Microsoft AD](#)
  - [虛擬私有雲端](#)

- [License Manager 中的委派管理員設定](#)
  - [委派的 License Manager 管理員支援的區域](#)
  - [註冊委派的 License Manager 管理員](#)
  - [取消註冊委派的 License Manager 管理員](#)

## 編輯 License Manager 設定

若要編輯您的 License Manager 設定，請遵循下列步驟：

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側的導覽窗格中，選擇設定。
3. 選擇包含要設定之設定的索引標籤。例如，選擇受管授權以設定帳戶詳細資訊。
4. 設定好設定後，請選擇儲存，或選擇取消以退出。

## License Manager 中的受管授權設定

受管授權可使用下列設定。

### 授權資產探索和規則集設定

對於使用授權資產群組的組織，您可以設定授權資產探索和規則集設定，以跨組織內的多個 AWS 區域和帳戶啟用跨區域探索和全 AWS 組織授權管理。

授權資產探索設定包括：

- 區域探索組態，以選取軟體探索的來源 AWS 區域
- 組織擁有者的全組織探索設定

### 帳戶詳細資訊

您可以檢閱帳戶詳細資訊，以查看帳戶類型、中的帳戶是否已 AWS Organizations 連結、帳戶的 License Manager S3 儲存貯體 ARN 以及 AWS Resource Access Manager 共用 ARN 等資訊。本節也可讓您連結 AWS Organizations 帳戶。

若要在組織內分發受管權利或自我管理授權，請選擇連結 AWS Organizations 帳戶。所有成員帳戶都會自動接受受管權利的分散式授予。當您選取此選項時，我們會將服務連結角色新增至[管理和成員](#)帳戶。

**Note**

若要啟用此選項，請登入您的管理帳戶並啟用 中的所有功能 AWS Organizations。如需詳細資訊，請參閱 AWS Organizations 使用者指南中的[啟用組織中的所有功能](#)。

此選擇也會在您的管理帳戶中建立 AWS Resource Access Manager 資源共用，可讓您無縫共用自我管理的授權。如需詳細資訊，請參閱「[AWS Resource Access Manager 使用者指南](#)」。

若要停用此選項，請呼叫 [UpdateServiceSettings](#) API。

## Cross-account resource discovery (跨帳戶資源探索)

您可以開啟跨帳戶資源探索，以管理所有帳戶中的授權用量 AWS Organizations。

若要在您的組織中啟用跨帳戶資源探索，請選擇開啟以進行跨帳戶資源探索。當您開啟跨帳戶資源探索時，AWS Organizations 會自動連結，以跨所有帳戶執行資源探索。

License Manager 使用 [Systems Manager 庫存](#) 來探索軟體用量。確認您已在所有資源上設定 Systems Manager 庫存。查詢 Systems Manager 庫存需要下列項目：

- 將庫存存放在 Amazon S3 儲存貯體的[資源資料同步](#)。
- [Amazon Athena](#) 在中彙總您帳戶中的庫存資料 AWS Organizations。
- [AWS Glue](#) 提供快速的查詢體驗。

**Note**

商業 AWS 分割區區域 (aws) 不需要 Amazon Athena 或 AWS Glue 來查詢或彙總 Systems Manager 庫存的庫存資料，以探索軟體用量。不過，其他分割區 AWS Glue 仍需要 Amazon Athena 和 ，例如 aws-us-gov、aws-cn 和 aws-iso 區域。

## 簡易通知服務 (SNS)

您可以設定 Amazon SNS 接收來自 License Manager 的通知和提醒。

設定 Amazon SNS 主題

1. 選擇 Simple Notification Service (SNS) 旁的編輯。

2. 以下列格式指定 SNS 主題 ARN：

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

3. 選擇儲存變更。

## License Manager 中的 Linux 訂閱設定

在探索過程中，License Manager 會搜尋在 AWS 帳戶 Linux 訂閱下執行的 EC2 執行個體。它會偵測您是否為任何執行個體定義了多個 Linux 訂閱，並彙總資料。

### Linux 訂閱設定

您可以設定 Linux 訂閱的設定，以控制 License Manager 如何處理探索和彙總。預設探索設定適用於所有類型的 Linux 訂閱。

下列動作可用於設定 Linux 訂閱探索。

#### 編輯

變更 Linux 訂閱探索的設定。

#### 停用

停用與 EC2 執行個體相關聯之 Linux 訂閱的探索和彙總。如果您也已針對 Red Hat Subscription Manager 啟用探索，則 License Manager 會先停用已註冊的 microSDHCM 供應商，然後繼續停用 Linux 訂閱探索。

#### Note

停用不會影響您的 Red Hat Subscription Manager (RHSM) 存取秘密。若要避免您不再需要之相關秘密的 AWS 帳單費用，請參閱 AWS Secrets Manager 《使用者指南》中的 [刪除 AWS Secrets Manager 秘密](#)。

下列設定會顯示在適用於 Linux 訂閱探索的 License Manager 主控台中。

## Linux 訂閱探索設定

### Linux 訂閱探索

指出您是否已啟用帳戶的 Linux 訂閱探索。

#### 來源 AWS 區域

AWS 區域 您希望 License Manager 探索訂閱資料的位置。

#### AWS Organizations

選擇性地彙總您帳戶間的訂閱資料 AWS Organizations。

如需詳細資訊，請參閱[在 License Manager 中管理 Linux 訂閱](#)。

## Red Hat Subscription Manager 探索

如果您已啟用 Linux 訂閱探索，您可以設定 License Manager 的存取權，以擷取透過 Red Hat Subscription Manager (RHSM) 管理的 RHEL 訂閱的其他資料。

下列動作可用於設定您的 RHSM 訂閱探索。

### 編輯標籤

變更與您的存取秘密相關聯的標籤。

#### Note

如果您需要對 microSDHCM 訂閱進行其他變更，您必須先停用目前的註冊，然後設定新的註冊。

### 停用

停用已註冊的 microSDHCM 提供者。

#### Note

停用不會影響您的 Red Hat Subscription Manager (RHSM) 存取秘密。若要避免您不再需要之相關秘密的 AWS 帳單費用，請參閱AWS Secrets Manager 《使用者指南》中的[刪除 AWS Secrets Manager 秘密](#)。

下列設定會顯示在 License Manager 主控台中，以供使用。

## Red Hat Subscription Manager 探索設定

### 探索狀態

指出您是否已啟動適用於 RHSM 訂閱的探索。

### 秘密名稱

中包含 Red Hat 離線權杖 AWS Secrets Manager 的 microSDHCM 存取秘密連結。License Manager 使用此秘密產生新的臨時存取權杖，以向 Red Hat Subscription Manager (RHSM) 請求訂閱資料。

您可以透過 Secrets Manager 變更現有的秘密。若要更新秘密的標籤或其他中繼資料，請參閱AWS Secrets Manager 《使用者指南》中的[修改 AWS Secrets Manager 秘密](#)。若要更新秘密值，請參閱[更新 AWS Secrets Manager 秘密的值](#)。

### 上一次在上同步的資料

上次成功更新註冊 Red Hat Subscription Manager (RHSM) 帳戶中訂閱資料的時間戳記。

### Tags (標籤)

您可以在 Secrets Manager 中為 License Manager 指派給您的 RHSM 存取秘密的標籤定義金鑰值對。若要擷取和解密您的 microSDHCM 存取秘密，License Manager 服務連結角色政策需要秘密和任何相關聯的 AWS KMS key，才能指派下列標籤：

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

如果 License Manager 在註冊程序期間建立您的秘密，則會自動指派標籤。如果您為離線權杖建立自己的秘密，請務必將該標籤指派給秘密，並在加密時指派給相關聯的 KMS 金鑰。若要新增標籤，請參閱AWS Secrets Manager 《使用者指南》中的[修改 AWS Secrets Manager 秘密](#)。

## License Manager 中的使用者型訂閱設定

視您所需的使用者型訂閱產品而定，可使用下列設定。

## AWS Managed Microsoft AD

AWS Managed Microsoft AD 您必須先設定 License Manager，才能使用以使用者為基礎的訂閱。如需詳細資訊，請參閱[針對支援的軟體產品使用 License Manager 使用者型訂閱](#)。

### 虛擬私有雲端

當您搭配 Microsoft Office 使用使用者型訂閱時，除了您的之外 AWS Managed Microsoft AD，License Manager 還會要求您設定 VPC。如需詳細資訊，請參閱[針對支援的軟體產品使用 License Manager 使用者型訂閱](#)。

## License Manager 中的委派管理員設定

您可以在 License Manager 中註冊委派管理員，以執行受管授權和 Linux 訂閱的管理任務。為了簡化管理，我們建議您使用 License Manager 主控台，為 License Manager 的每個功能註冊單一委派管理員。當您使用此方法時，組織中會有一個 License Manager 的委派管理員。

您可以使用 AWS CLI 或 SDKs，將組織中的不同成員帳戶註冊為 License Manager 每個支援功能的委派管理員。這會導致組織中的不同成員帳戶能夠執行受管授權和 Linux 訂閱的管理任務。

### Important

若要在 License Manager 主控台中使用委派的管理功能，您必須將相同的成員帳戶註冊為 License Manager 每個功能的委派管理員。如果您將多個成員帳戶註冊為委派管理員，您必須先取消註冊現有的成員帳戶，然後為 License Manager 的每個功能註冊相同的帳戶。

註冊委派管理員之前，您必須啟用 Organizations 的受信任存取。如需詳細資訊，請參閱[邀請 AWS 帳戶加入您的組織並啟用受信任存取 AWS Organizations](#)。

以下是您可以註冊委派管理員的功能：

### 受管授權

您可以執行管理任務，例如與其他成員帳戶共用自我管理的授權、執行跨帳戶資源探索，以及將受管權利分發給其他成員帳戶。

### Linux 訂閱

您可以執行管理任務，例如檢視和管理您擁有並跨 AWS 區域 和您的帳戶執行的商業 Linux 訂閱 AWS Organizations。您也可以為 Linux 訂閱建立和管理 Amazon CloudWatch 警示。必須先探索和彙總資料，才能在 License Manager 主控台中顯示資料，而且如果已設定任何警示，就可以運作。

**⚠ Important**

註冊後，委派管理員即可查看組織中帳戶擁有的 EC2 執行個體。

您可以使用 [AWS License Manager 主控台](#)、[AWS CLI](#) 或 [AWS 開發套件](#) 註冊和取消註冊委派管理員。

## 委派的 License Manager 管理員支援的區域

下列區域支援 License Manager 委派管理員：

- 美國東部 (俄亥俄)
- 美國東部 (維吉尼亞北部)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)
- 亞太區域 (孟買)
- 亞太區域 (首爾)
- 亞太區域 (新加坡)
- 亞太地區 (雪梨)
- 亞太地區 (東京)
- 亞太地區 (香港)
- Middle East (Bahrain)
- 加拿大 (中部)
- 歐洲 (法蘭克福)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)
- 歐洲 (巴黎)
- 歐洲 (斯德哥爾摩)
- 歐洲 (米蘭)
- 非洲 (開普敦)
- 南美洲 (聖保羅)

## 註冊委派的 License Manager 管理員

您可以使用 AWS CLI 或 註冊委派管理員 AWS 管理主控台。

### Console

若要使用 AWS License Manager 主控台註冊委派管理員，請執行下列步驟：

1. 以管理帳戶的管理員 AWS 身分登入。
2. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
3. 從左側導覽窗格中選擇設定。
4. 選擇委派的管理索引標籤。
5. 選擇 Register delegated administrator (註冊委派管理員)。
6. 輸入成員帳戶 ID 以註冊為委派管理員，確認您要授予 License Manager 所需的許可，然後選擇註冊。
7. 訊息指出指定的帳戶是否已成功註冊為委派管理員 License Manager。

### AWS CLI

若要使用 註冊受管授權的委派管理員 AWS CLI，請執行下列步驟：

1. 從命令列執行下列 AWS CLI 命令：

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

2. 執行下列命令，以確認指定的帳戶已成功註冊為委派管理員：

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

若要使用 註冊 Linux 訂閱的委派管理員 AWS CLI，請執行下列步驟：

1. 從命令列執行下列 AWS CLI 命令：

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

2. 執行下列命令，以確認指定的帳戶已成功註冊為委派管理員：

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

## 取消註冊委派的 License Manager 管理員

您可以使用 AWS CLI 或 取消註冊委派管理員 AWS 管理主控台。

### Console

若要使用 AWS License Manager 主控台取消註冊委派管理員，請執行下列步驟：

1. 以管理帳戶的管理員 AWS 身分登入。
2. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
3. 從左側導覽窗格中選擇設定。
4. 選擇委派的管理索引標籤。
5. 選擇移除。
6. 輸入文字 **remove** 以確認您想要移除 License Manager 的委派管理員，然後選擇移除。
7. 訊息指出指定的帳戶是否已成功移除 License Manager 的委派管理員。

### AWS CLI

若要使用 取消註冊受管授權的委派管理員 AWS CLI，請執行下列步驟：

1. 從命令列執行下列 AWS CLI 命令：

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

2. 執行下列命令，以確認指定的帳戶已成功取消註冊為委派管理員：

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

若要用取消註冊 Linux 訂閱的委派管理員 AWS CLI，請執行下列步驟：

1. 從命令列執行下列 AWS CLI 命令：

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

2. 執行下列命令，以確認指定的帳戶已成功取消註冊為委派管理員：

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

您可以隨時重新註冊已取消註冊的帳戶。

# 監控 License Manager

您可以使用 Amazon CloudWatch AWS License Manager 監控 中追蹤的授權和訂閱用量。CloudWatch 可收集原始資料，將這些資料轉換為可讀取且幾近即時的指標。您可以設定監控特定閾值的警示，並在達到這些閾值時傳送通知或採取動作。如需詳細資訊，請參閱[使用 Amazon CloudWatch 監控 License Manager](#)。

您可以擷取 API 呼叫，以及使用 或代表您的 AWS 帳戶 所做的相關事件 AWS CloudTrail。事件會擷取為日誌檔案，並傳送至您指定的 Amazon S3 儲存貯體。您可以識別呼叫哪些使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱[使用 記錄 AWS License Manager API 呼叫 AWS CloudTrail](#)。

## 內容

- [使用 Amazon CloudWatch 監控 License Manager](#)
  - [建立警示以監控 License Manager 指標](#)
- [使用 記錄 AWS License Manager API 呼叫 AWS CloudTrail](#)
  - [CloudTrail 中的 License Manager 資訊](#)
  - [了解 License Manager 日誌檔案項目](#)

## 使用 Amazon CloudWatch 監控 License Manager

您可以使用 Amazon CloudWatch 監控 License Manager 的指標統計資料。這些統計資料會保留 15 個月，以便您存取歷史資訊，並更清楚 Web 應用程式或服務的執行效能。您可以設定留意特定閾值的警示，當滿足這些閾值時傳送通知或採取動作。例如，您可以使用 LicenseConfigurationUsagePercentage 指標觀察授權的百分比，並在超過限制之前採取動作。如需更多資訊，請參閱 [Amazon CloudWatch 使用者指南](#)。

License Manager 每小時會在 AWSLicenseManager/licenseUsage 命名空間中發出下列指標：

指標	描述
RunningInstancesCount	目前帳戶中執行的執行個體總數，依訂閱名稱分組。 單位：Count 維度：

指標	描述
	SubscriptionName : 訂閱的名稱。
AggregateRunningInstancesCount	<p>目前 AWS Organizations 中所有帳戶執行的執行個體彙總總數 AWS 區域。</p> <p>單位 : Count</p> <p>維度 :</p> <p>SubscriptionName : 訂閱的名稱。</p>
TotalLicenseConfigurationUsageCount	<p>可用的授權組態總數。</p> <p>單位 : Count</p> <p>維度 :</p> <ul style="list-style-type: none"> <li>LicenseConfigurationArn : 授權組態 Amazon Resource Name (ARN)。</li> <li>LicenseConfigurationType : 授權組態類型。</li> </ul>
LicenseConfigurationUsageCount	<p>此組態的已使用授權總數。</p> <p>單位 : Count</p> <p>維度 :</p> <ul style="list-style-type: none"> <li>LicenseConfigurationArn : 授權組態 ARN。</li> <li>LicenseConfigurationType : 授權組態類型。</li> </ul>
LicenseConfigurationUsagePercentage	<p>此授權組態的使用授權以百分比表示。</p> <p>單位 : 百分比</p> <p>維度 :</p> <ul style="list-style-type: none"> <li>LicenseConfigurationArn : 授權組態 ARN。</li> <li>LicenseConfigurationType : 授權組態類型。</li> </ul>

指標	描述
InstanceCount	<p>授權資產群組內的執行個體數量。</p> <p>單位：Count</p> <p>維度：</p> <ul style="list-style-type: none"> <li>LicenseAssetGroupArn：授權資產群組 ARN。</li> <li>LicensingModel：授權模型 (LicenseIncluded 或 AWSMarketplace)。僅適用於具有 AWS 受管規則集的授權資產群組。</li> </ul>
InstanceConsumedLicenseCount	<p>授權資產群組內執行個體的已耗用授權數量。</p> <p>單位：Count</p> <p>維度：</p> <ul style="list-style-type: none"> <li>LicenseAssetGroupArn：授權資產群組 ARN。</li> <li>LicenseCountingType：授權計數類型 (執行個體、vCPU、通訊端或核心)。</li> <li>LicensingModel：授權模型 (LicenseIncluded 或 AWSMarketplace)。僅適用於具有 AWS 受管規則集的授權資產群組。</li> </ul>

## 建立警示以監控 License Manager 指標

您可以建立 CloudWatch 警示，在指標值變更並導致警示變更狀態時傳送 Amazon Simple Notification Service (Amazon SNS) 訊息。警示會監看指定時段內的指標，並根據與多個時段內指定閾值相對的指標值來執行動作。警示僅會針對持續狀態變更調用動作。CloudWatch 警示不會只因處於特定狀態就調用動作，狀態必須已變更並已維持一段指定的時間。如需詳細資訊，請參閱[使用 CloudWatch 警示](#)。

## 使用記錄 AWS License Manager API 呼叫 AWS CloudTrail

AWS License Manager 已與服務整合 AWS CloudTrail，此服務會提供使用者、角色或 License Manager 中 AWS 服務所採取動作的記錄。CloudTrail 會將 License Manager 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 License Manager 主控台的呼叫，以及對 License Manager API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 License Manager 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台內的事件歷史記錄檢

視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷向 License Manager 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [「AWS CloudTrail 使用者指南」](#)。

## 主題

- [CloudTrail 中的 License Manager 資訊](#)
- [了解 License Manager 日誌檔案項目](#)

## CloudTrail 中的 License Manager 資訊

當您建立帳戶 AWS 帳戶時，您的上會啟用 CloudTrail。當活動在 License Manager 中發生時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 [中檢視、搜尋和下載最近的事件 AWS 帳戶](#)。如需詳細資訊，請參閱 [「使用 CloudTrail 事件歷史記錄檢視事件」](#)。

若要持續記錄中的事件 AWS 帳戶，包括 License Manager 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案](#)和[接收多個帳戶的 CloudTrail 日誌檔案](#)

CloudTrail 會記錄所有 License Manager 動作，並記錄在 [AWS License Manager API 參考](#)中。例如，呼叫的呼叫 `CreateLicenseConfiguration`，`ListResourceInventory`而 `DeleteLicenseConfiguration`動作會在 CloudTrail 日誌檔案中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

## 了解 License Manager 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 DeleteLicenseConfiguration 動作的 CloudTrail 日誌項目。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIIF2U5EXAMPLEH5AP6",
    "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

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模式](#)將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。作為[AWS 合規計畫](#)的一部分，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 License Manager 的合規計畫，請參閱[AWS 合規計畫的服務範圍](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規

本文件可協助您了解如何在使用 License Manager 時套用共同責任模型。下列主題說明如何設定 License Manager 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 License Manager 資源。

## 主題

- [License Manager 中的資料保護](#)
- [License Manager 的身分和存取管理](#)
- [使用 License Manager 的服務連結角色](#)
- [AWS License Manager 的受管政策](#)
- [License Manager 中授權的密碼編譯簽署](#)
- [License Manager 的合規驗證](#)
- [License Manager 中的復原能力](#)
- [License Manager 中的基礎設施安全性](#)
- [License Manager 和介面 VPC 端點搭配 AWS PrivateLink](#)

## License Manager 中的資料保護

AWS [共同責任模型](#)適用於 中的資料保護 AWS License Manager。如此模型所述，AWS 負責保護執行所有的 全球基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答](#)

**集**。如需有關歐洲資料保護的相關資訊，請參閱AWS 安全性部落格上的[AWS 共同責任模型和 GDPR](#) 部落格文章。

基於資料保護目的，建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 License Manager 或使用主控台、API AWS CLI或其他 AWS 服務 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

## 靜態加密

License Manager 會將資料存放在管理帳戶中的 Amazon S3 儲存貯體中。儲存貯體是使用 Amazon S3 受管加密金鑰 (SSE-S3) 設定。

## License Manager 的身分和存取管理

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證 (登入) 和授權 (具有許可) 來使用 AWS 資源。使用 IAM，您可以在 AWS 您的帳戶下建立使用者和群組。您可以控制使用者使用 AWS 資源執行任務所需的許可。您可以免費使用 IAM。

根據預設，使用者沒有 License Manager 資源和操作的許可。若要允許使用者管理 License Manager 資源，您必須建立明確授予許可的 IAM 政策。

將政策連接到使用者或使用者群組時，政策會允許或拒絕使用者在特定資源上執行特定任務的許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[政策和許可](#)。

## 建立使用者、群組和角色

您可以為 建立使用者和群組，AWS 帳戶 然後將他們所需的許可指派給他們。作為最佳實務，使用者應透過擔任 IAM 角色來取得許可。如需如何為 設定使用者和群組的詳細資訊 AWS 帳戶，請參閱 [License Manager 入門](#)。

[IAM 角色](#)是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。IAM 角色類似於 IAM 使用者，因為它是具有許可政策的 AWS 身分，可決定身分可以和不可以執行的操作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。此外，角色沒有與之關聯的標準長期憑證，例如密碼或存取金鑰。反之，當您擔任角色時，其會為您的角色工作階段提供臨時安全性憑證。

## IAM 政策結構

IAM 政策為包含一或多個陳述式的 JSON 文件。每個陳述式的結構如下所示。

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

各種元素組成一個陳述式：

- **Effect (效果)**：效果 可以是 Allow 或 Deny。根據預設，使用者沒有使用資源和 API 作業的許可，因此所有請求均會遭到拒絕。明確允許會覆寫預設值。明確拒絕會覆寫任何允許。
- **動作**：動作是您授予或拒絕許可的特定 API 操作。
- **資源**：資源會受到 動作的影響。有些 License Manager API 操作可讓您在政策中包含可由 操作建立或修改的特定資源。若要在陳述式中指定資源，您必須使用其 Amazon Resource Name (ARN)。如需詳細資訊，請參閱 [定義的動作 AWS License Manager](#)。
- **Condition (條件)**：條件為選擇性。您可以使用它們來控制何時政策開始生效。如需詳細資訊，請參閱 [的條件金鑰 AWS License Manager](#)。

## 建立 License Manager 的 IAM 政策

在 IAM 政策陳述式中，您可以從支援 IAM 的任何服務指定任何 API 操作。License Manager 使用以下字首搭配 API 操作的名稱：

- `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`

如需可用 License Manager APIs 的詳細資訊，請參閱下列 API 參考：

- [AWS License Manager API 參考](#)
- [AWS License Manager 使用者訂閱 API 參考](#)
- [AWS License Manager Linux 訂閱 API 參考](#)

若要在單一陳述式中指定多個作業，請用逗號分隔，如下所示：

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

您也可以使用萬用字元指定多個作業。例如，您可以指定名稱以清單一詞開頭的所有 License Manager API 操作，如下所示：

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

若要指定所有 License Manager API 操作，請使用 \* 萬用字元，如下所示：

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

## 使用 License Manager 的 ISV 政策範例

透過 License Manager 分發授權ISVs 需要下列許可：

JSON

```
{
  "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": "*"
    }
  ]
}
```

## 向使用者、群組和角色授予許可

建立所需的 IAM 政策後，您必須將這些許可授予使用者、群組和角色。

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 AWS IAM Identity Center：

建立權限合集。請按照《AWS IAM Identity Center 使用者指南》中的[建立權限合集](#)說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。遵循《IAM 使用者指南》的[為第三方身分提供者 \(聯合\) 建立角色](#)中的指示。

- IAM 使用者：
  - 建立您的使用者可擔任的角色。請按照《IAM 使用者指南》的[為 IAM 使用者建立角色](#)中的指示。
  - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的[新增許可到使用者 \(主控台\)](#) 中的指示。

## 使用 License Manager 的服務連結角色

AWS License Manager 使用 AWS Identity and Access Management (IAM) [服務連結角色](#)。服務連結角色是直接連結至 License Manager 的唯一 IAM 角色類型。服務連結角色由 License Manager 預先定義，並包含該服務代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 License Manager，因為您不必手動新增必要的許可。License Manager 會定義其服務連結角色的許可，除非另有定義，否則只有 License Manager 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除相關的資源，才能刪除服務連結角色。這可保護您的 License Manager 資源，因為您不會不小心移除存取資源的許可。

License Manager 動作取決於三個服務連結角色，如以下各節所述。

### 服務連結角色

- [License Manager – 核心角色](#)
- [License Manager – 管理帳戶角色](#)
- [License Manager – 成員帳戶角色](#)
- [License Manager – 以使用者為基礎的訂閱角色](#)
- [License Manager – Linux 訂閱角色](#)

## License Manager – 核心角色

License Manager 需要服務連結角色，才能代表您管理授權。

### 核心角色的許可

名為 `AWSServiceRoleForAWSLicenseManagerRole` 的服務連結角色允許 License Manager 存取 AWS 資源，以代表您管理授權。

`AWSServiceRoleForAWSLicenseManagerRole` 服務連結角色信任 `license-manager.amazonaws.com` 服務來擔任該角色。

若要檢閱的許可 `AWSLicenseManagerServiceRolePolicy`，請參閱 [AWS 受管政策：AWSLicenseManagerServiceRolePolicy](#)。若要進一步了解如何設定服務連結角色的許可，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

## 建立 License Manager 的服務連結角色

您不需要手動建立服務連結角色，當您在第一次造訪 License Manager 主控台時完成 License Manager 初次執行體驗表單時，系統會自動為您建立服務連結角色。

您也可以使用 IAM 主控台 AWS CLI 或 IAM API 手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

### Important

此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。如果您在 2017 年 1 月 1 日之前使用 License Manager，當它開始支援服務連結角色時，則 License Manager 會在您的帳戶中建立該 `AWSServiceRoleForAWSLicenseManagerRole` 角色。如需詳細資訊，請參閱 [我的 IAM 帳戶出現的新角色](#)。

您可以使用 License Manager 主控台來建立服務連結角色。

### 建立 服務連結角色

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 選擇開始使用 License Manager。
3. 在 IAM 許可 one-time-setup) 表單 AWS License Manager 中，選取我授予所需的許可，然後選擇繼續。

您也可以使用 IAM 主控台建立具有 License Manager 使用案例的服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用 IAM 建立具有服務名稱 `license-manager.amazonaws.com` 的服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

如果您刪除這個服務連結角色，則可使用相同的 IAM 程序再次建立該角色。

## 編輯 License Manager 的服務連結角色

License Manager 不允許您編輯 `AWSServiceRoleForAWSLicenseManagerRole` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

## 刪除 License Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您只有主動監控或維護的實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

### 清除服務連結角色

您必須先刪除角色使用的所有資源，才能使用 IAM 刪除服務連結角色。這表示取消任何自我管理的授權與相關聯執行個體和 AMIs 關聯，然後刪除自我管理的授權。

#### Note

如果 License Manager 在您嘗試刪除資源時使用角色，則刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後重試動作。

### 刪除核心角色使用的 License Manager 資源

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在導覽窗格中，選擇自我管理授權。
3. 選擇您為擁有者的自我管理授權，並取消關聯 AMIs 和資源索引標籤中的所有項目的關聯。為每個授權組態重複此程序。
4. 當仍在自我管理授權的頁面上時，選擇動作，然後選擇刪除。
5. 重複上述步驟，直到刪除所有自我管理的授權為止。

### 手動刪除服務連結角色

使用 IAM 主控台、AWS CLI、或 AWS API 來刪

除 `AWSServiceRoleForAWSLicenseManagerRole` 服務連結角色。如果

您也使用 [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) 和

[AWSLicenseManagerMemberAccountRole](#)，請先刪除這些角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## License Manager – 管理帳戶角色

License Manager 需要服務連結角色才能執行授權管理。

### 管理帳戶角色的許可

名為 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 的服務連結角色允許 License Manager 存取 AWS 資源，以代表您管理中央管理帳戶的授權管理動作。

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 服務連結角色信任 `license-manager.master-account.amazonaws.com` 服務來擔任該角色。

若要檢閱 `AWSServiceRoleForAWSLicenseManagerMasterAccountRolePolicy` 的許可，請參閱 [AWS 受管政策：AWSServiceRoleForAWSLicenseManagerMasterAccountRolePolicy](#)。若要進一步了解如何設定服務連結角色的許可，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

### 建立管理帳戶服務連結角色

您不需要手動建立這個服務連結角色。當您在 [IAM 主控台](#) 中設定跨帳戶授權管理時，License Manager 會為您建立服務連結角色。

#### Note

若要在 License Manager 中使用跨帳戶支援，您必須使用 AWS Organizations。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

您也可以使用 IAM 主控台、AWS CLI 或 IAM API 手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

#### Important

此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。如果您在 2017 年 1 月 1 日之前使用 License Manager，則當它開始支援服務連結角色時，授權管理員會在您的帳戶 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 中建立。如需詳細資訊，請參閱 [我的 IAM 帳戶出現的新角色](#)。

您可以使用 License Manager 主控台來建立此服務連結角色。

## 建立 服務連結角色

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 選擇 Settings (設定)，然後選擇 Edit (編輯)。
3. 選擇連結 AWS Organizations 帳戶。
4. 選擇套用。

您也可以使用 IAM 主控台，透過 License Manager–Management 帳戶使用案例來建立服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用 IAM 建立具有服務名稱 `license-manager-master-account.amazonaws.com` 的服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

如果您刪除這個服務連結角色，則可使用相同的 IAM 程序再次建立該角色。

## 編輯 License Manager 的服務連結角色

License Manager 不允許您編

輯 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

## 刪除 License Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您只有主動監控或維護的實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

### 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI 或 AWS API 來刪

除 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## License Manager – 成員帳戶角色

License Manager 需要服務連結角色，允許管理帳戶管理授權。

### 成員帳戶角色的許可

名為 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 的服務連結角色允許 License Manager 代表您從設定的管理帳戶存取授權管理動作 AWS 的資源。

`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服務連結角色信任 `license-manager.member-account.amazonaws.com` 服務來擔任該角色。

若要檢閱的許可 `AWSLicenseManagerMemberAccountRolePolicy`，請參閱 [AWS 受管政策：AWSLicenseManagerMemberAccountRolePolicy](#)。若要進一步了解如何設定服務連結角色的許可，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

## 建立 License Manager 的服務連結角色

您不需要手動建立服務連結角色。您可以在設定頁面的 License Manager 主控台中，AWS Organizations 從管理帳戶啟用與的整合。您也可以使用 AWS CLI（執行 `update-service-settings`）或 AWS API（呼叫）來執行此操作 `UpdateServiceSettings`。當您這麼做時，License Manager 會在 Organizations 成員帳戶中為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

您也可以使用 IAM 主控台、AWS CLI 或 AWS API 手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

### Important

此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。如果您在 2017 年 1 月 1 日之前使用 License Manager 服務，當它開始支援服務連結角色時，則 License Manager 會在您的帳戶中建立該 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 角色。如需詳細資訊，請參閱 [我的 IAM 帳戶出現的新角色](#)。

您可以使用 License Manager 主控台來建立服務連結角色。

### 建立服務連結角色

1. 登入您的 AWS Organizations 管理帳戶。
2. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
3. 在左側導覽窗格中，選擇設定，然後選擇編輯。
4. 選擇連結 AWS Organizations 帳戶。
5. 選擇套用。這會在 [AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) 所有子帳戶中建立角色 [AWSServiceRoleForAWSLicenseManagerRole](#) 和。

您也可以使用 IAM 主控台建立具有 License Manager - Member account 使用案例的服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用服務名稱建立 `license-manager.member-account.amazonaws.com` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

如果您刪除這個服務連結角色，則可使用相同的 IAM 程序再次建立該角色。

## 編輯 License Manager 的服務連結角色

License Manager 不允許您編

輯 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

## 刪除 License Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您只有主動監控或維護的實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

手動刪除服務連結角色

使用 IAM 主控台 AWS CLI 或 AWS API 來刪

除 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## License Manager – 以使用者為基礎的訂閱角色

License Manager 需要服務連結角色來管理將提供使用者型訂閱 AWS 的資源。

### 使用者型訂閱角色的許可

名為 的服務連結角

色 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` 允許 License Manager 利用 AWS Systems Manager 和管理提供使用者型訂閱的 Amazon EC2 資源，以及描述 Directory Service 資源。

若要檢閱 的許可 `AWSLicenseManagerUserSubscriptionsServiceRolePolicy`，請參閱 [AWS 受管政策：AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。若要進一步了解如何設定服務連結角色的許可，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

## 建立 License Manager 的服務連結角色

您不需要手動建立服務連結角色，因為在 License Manager 主控台使用者型訂閱頁面上會提示您建立角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

您也可以使用 IAM 主控台 AWS CLI 或 IAM API 手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的[建立服務連結角色](#)。

您可以使用 License Manager 主控台來建立服務連結角色。

### 建立 服務連結角色

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。
2. 在左側導覽窗格中，選擇使用者關聯或產品。
3. 同意 License Manager 的條款，以建立以使用者為基礎的訂閱角色。
4. 選擇建立。這會建立 角色。

您也可以使用 IAM 主控台建立具有 License Manager - User-based subscriptions 使用案例的服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用服務名稱建立 `license-manager-user-subscriptions.amazonaws.com` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的[建立服務連結角色](#)。

如果您刪除這個服務連結角色，則可使用相同的 IAM 程序再次建立該角色。

## 編輯 License Manager 的服務連結角色

License Manager 不允許您編

輯 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

## 刪除 License Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您只有主動監控或維護的實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

## 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI 或 AWS API 來刪

除 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## License Manager – Linux 訂閱角色

License Manager 需要服務連結角色來管理提供 Linux 訂閱 AWS 的資源。

### Linux 訂閱角色的許可

名為 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 的服務連結角

色 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 允許 License Manager 針對 Linux 訂閱執行下列動作。

- 探索 Amazon Elastic Compute Cloud AWS Organizations 和資源。
- 從擷取標記為 `LicenseManagerLinuxSubscriptions` 的秘密，"LicenseManagerLinuxSubscriptions": "enabled" AWS Secrets Manager 以存取第三方 Linux 訂閱提供者以取得訂閱資訊。
- 使用標記的 KMS 金鑰 "LicenseManagerLinuxSubscriptions": "enabled" 來解密秘密。

若要檢閱 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsServiceRolePolicy` 的許可，請參閱 [AWS 受管政策：AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。若要進一步了解如何設定服務連結角色的許可，請參閱《IAM 使用者指南》中的 [服務連結角色許可](#)。

### 建立 License Manager 的服務連結角色

您不需要手動建立服務連結角色，因為在 License Manager 主控台 Linux 訂閱頁面上會提示您建立角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。

您也可以使用 IAM 主控台 AWS CLI 或 IAM API 手動建立服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

您可以使用 License Manager 主控台來建立服務連結角色。

### 建立 服務連結角色

1. 在 <https://console.aws.amazon.com/license-manager/> 開啟 License Manager 主控台。

2. 在左側導覽窗格中，選擇訂閱或執行個體。
3. 同意 License Manager 建立 Linux 訂閱角色的條款。
4. 選擇建立。這會建立 角色。

您也可以使用 IAM 主控台建立具有 License Manager - Linux subscriptions 使用案例的服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用服務名稱建立 `license-manager-linux-subscriptions.amazonaws.com` 服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的 [建立服務連結角色](#)。

如果您刪除這個服務連結角色，則可使用相同的 IAM 程序再次建立該角色。

## 編輯 License Manager 的服務連結角色

License Manager 不允許您編

輯 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的 [編輯服務連結角色](#)。

## 刪除 License Manager 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您只有主動監控或維護的實體。然而，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

### 手動刪除服務連結角色

使用 IAM 主控台 AWS CLI 或 AWS API 來刪

除 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

## AWS License Manager 的 受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自行撰寫政策更容易。建立 [IAM 客戶受管政策](#) 需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#)。

AWS 服務會維護和更新 AWS 受管政策。您無法變更 AWS 受管政策中的許可。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群

組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管政策中移除許可，因此政策更新不會破壞您現有的許可。

此外，AWS 支援跨多個服務之任務函數的受管政策。例如，ReadOnlyAccess AWS 受管政策提供所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新操作和資源 AWS 新增唯讀許可。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中 [有關任務職能的 AWS 受管政策](#)。

## AWS 受管政策：AWSLicenseManagerServiceRolePolicy

此政策會連接到名為 `AWSServiceRoleForAWSLicenseManagerRole` 的服務連結角色，以允許 License Manager 呼叫 API 動作來代表您管理授權。如需服務連結角色的詳細資訊，請參閱 [核心角色的許可](#)。

角色許可政策允許 License Manager 對指定的資源完成下列動作。

Action	資源 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/AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code>
<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>

Action	資源 ARN
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	*
ssm:GetCommandInvocation	*
ssm:SendCommand	arn:aws:ec2:*:*:instance/*
ssm:SendCommand	arn:aws:ssm:*:*:managed-instance/*
ssm:SendCommand	arn:aws:ssm:*:*:document/AWSLicenseManager-*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*

Action	資源 ARN
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

若要在 中檢視此政策的許可 AWS 管理主控台，請參閱 [AWSLicenseManagerServiceRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerMasterAccountRolePolicy

此政策會連接到名為 的服務連結角

色AWSServiceRoleForAWSLicenseManagerMasterAccountRole，以允許 License Manager 呼叫 API 動作，以代表您為中央管理帳戶執行授權管理。如需服務連結角色的詳細資訊，請參閱[License Manager – 管理帳戶角色](#)。

角色許可政策允許 License Manager 對指定的資源完成下列動作。

Action	資源 ARN
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*

Action	資源 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	請參閱註腳 1

Action	資源 ARN
glue:UpdateTable	請參閱註腳 1
glue>DeleteTable	請參閱註腳 1
glue:UpdateJob	請參閱註腳 1
glue:UpdateCrawler	請參閱註腳 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	*

Action	資源 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&gt;DeleteStack</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>
<code>cloudformation:DescribeStacks</code>	<code>arn:aws:cloudformation::*:stack/LicenseManagerCrossAccountCloudDiscoveryStack/*</code>

1 以下是為 AWS Glue 動作定義的資源：

- `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`

若要在 中檢視此政策的許可 AWS 管理主控台，請參閱 [AWSLicenseManagerMasterAccountRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerMemberAccountRolePolicy

此政策會連接到名為 的服務連結角

色AWSServiceRoleForAWSLicenseManagerMemberAccountRole，以允許 License Manager 代表您從設定的管理帳戶呼叫授權管理的 API 動作。如需詳細資訊，請參閱 [License Manager – 成員帳戶角色](#)。

角色許可政策允許 License Manager 對指定的資源完成下列動作。

Action	資源 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&gt;DeleteResourceDataSync</code>	*
<code>ssm:ListResourceDataSync</code>	*

Action	資源 ARN
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

若要在 中檢視此政策的許可 AWS 管理主控台，請參閱 [AWSLicenseManagerMemberAccountRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerConsumptionPolicy

您可將 AWSLicenseManagerConsumptionPolicy 政策連接到 IAM 身分。此政策授予許可，允許存取取用授權所需的 License Manager API 動作。如需詳細資訊，請參閱 [賣方在 License Manager 中發行的授權使用量](#)。

若要檢視此政策的許可，請參閱 AWS 管理主控台中的 [AWSLicenseManagerConsumptionPolicy](#)。

## AWS 受管政策：AWSLicenseManagerUserSubscriptionsServiceRolePolicy

此政策會連接到名為

AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService 政策的服務連結角色，以允許 License Manager 呼叫 API 動作來管理以使用者為基礎的訂閱資源。如需詳細資訊，請參閱 [License Manager – 以使用者為基礎的訂閱角色](#)。

角色許可政策允許 License Manager 對指定的資源完成下列動作。

Action	資源 ARN
ds:DescribeDirectories	*
ds : GetAuthorizedApplicationDetails	*
ec2 : CreateTags	arn : aws : ec2 : * : * : instance/* 1
ec2:DescribeInstances	*
ec2:DescribeNetworkInterfaces	*

Action	資源 ARN
ec2:DescribeSecurityGroupRules	*
ec2 : DescribeSubnets	*
ec2:DescribeVpcPeeringConnections	*
ec2:TerminateInstances	arn : aws : ec2 : * : * : instance/* 1
route53:GetHostedZone	*
route53:ListResourceRecordSets	*
secretsmanager:GetSecretValue	arn : aws : secretsmanager : * : * : secret : license-manager-user-*
ssm:DescribeInstanceInformation	*
ssm:GetCommandInvocation	*
ssm:GetInventory	*
ssm:ListCommandInvocations	*
ssm:SendCommand	arn : aws : ssm : * : : document/ AWS-RunPowerShellScript 2  arn : aws : ec2 : * : * : instance/* 2

1 License Manager 只能在產品代碼為 [bz0vcy31ooqlzk5tsash4r1ik](#)、[77yzkpa7kvee1y1ttt7wnsdwoc](#) 或 [d44g89hc0gp9jdzm99rznthpw](#) 的執行個體上建立和終止標籤。

2 License Manager 只能在標籤名稱為 `AWSLicenseManager` 且值為 `AWSSSMRunCommandUserSubscriptions` 的執行個體上執行具有 `AWS-RunPowerShellScript` 文件的 SSM Run CommandUserSubscriptions。

若要在 中檢視此政策的許可 AWS 管理主控台，請參閱 [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。

## AWS 受管政策：

### AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

此政策會連接到名為

AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService政策的服務連結角色，以允許 License Manager 呼叫 API 動作來管理 Linux 訂閱資源。如需詳細資訊，請參閱[License Manager – Linux 訂閱角色](#)。

角色許可政策允許 License Manager 對指定的資源完成下列動作。

Action	條件	資源
ec2:DescribeInstances	N/A	*
ec2:DescribeRegions	N/A	*
organizations:DescribeOrganization	N/A	*
organizations:ListAccounts	N/A	*
organizations:DescribeAccount	N/A	*
organizations:ListChildren	N/A	*
organizations:ListParents	N/A	*
organizations:ListAccountsForParent	N/A	*
organizations:ListRoots	N/A	*
organizations:ListAWSServiceAccessForOrganization	N/A	*

Action	條件	資源
organizations:List DelegatedAdministrators	N/A	*
secretsmanager:GetSecretValue	StringEquals : "aws : ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled"  "aws : ResourceAccount" : "\${aws : PrincipalAccount}"	arn:aws:secretsmanager:*:*:secret:*
kms:解密	StringEquals : "aws : ResourceTag/LicenseManagerLinuxSubscriptions" : "enabled" ,  "aws : ResourceAccount" : "\${aws : PrincipalAccount}"  StringLike :  "kms:ViaService" : 【 "secretsmanager.*.amazonaws.com" 】	arn:aws:kms:*:*:key/*

若要在 中檢視此政策的許可 AWS 管理主控台，請參閱 [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

## AWS 受管政策的 License Manager 更新

檢視自此服務開始追蹤這些變更以來，License Manager AWS 受管政策更新的詳細資訊。

變更	描述	Date
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 新增了許可，可透過執行 AWS 受管 SSM 文件來探索執行個體上的授權資產。	2025 年 11 月 19 日
<a href="#">AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> – 更新現有政策	License Manager 新增了下列許可來管理授權和 Active Directory 資料：從 Route 53 取得路由資訊、從 Amazon EC2 取得聯網資訊和安全群組規則，以及從 Secrets Manager 取得秘密。	2024 年 11 月 7 日
<a href="#">AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy</a> – 更新現有政策	License Manager 新增了儲存和擷取秘密的許可 AWS Secrets Manager，以及使用 AWS KMS 金鑰解密自有授權 (BYOL) 訂閱的存取權杖秘密。	2024 年 5 月 22 日
<a href="#">AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy</a> – 新政策	License Manager 新增了建立名為 <code>AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService</code> 之服務連結角色的許可。此角色提供 License Manager 列出 AWS Organizations 和 Amazon EC2 資源的許可。	2022 年 12 月 21 日
<a href="#">AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> – 更新現有政策	License Manager 新增了 <code>ec2:DescribeVpcPeeringConnections</code> 許可。	2022 年 11 月 28 日
<a href="#">AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> – 新政策	License Manager 新增了建立名為 <code>AWSLicenseManagerUserSubscriptionsServiceRolePolicy</code> 之服務連結角色的許可。	2022 年 7 月 18 日

變更	描述	Date
	<p>serSubscriptionsServiceRolePolicy。此角色提供 License Manager 許可，以列出 AWS Directory Service 資源、利用 Systems Manager 功能，以及管理為使用者型訂閱建立的 Amazon EC2 資源。</p>	
<p><a href="#">AWSLicenseManagerMasterAccountRolePolicy</a> – 更新現有政策</p>	<p>License Manager 新增由管理之資源群組的resource-groups:PutGroupPolicy 許可 AWS Resource Access Manager。</p>	<p>2022 年 6 月 27 日</p>
<p><a href="#">AWSLicenseManagerMasterAccountRolePolicy</a> – 更新現有政策</p>	<p>License Manager 將的 AWS 受管政策AWSLicenseManagerMasterAccountRolePolicy 條件金鑰從使用 ram:ResourceTag 變更為 aws:ResourceTag。 <a href="#">AWS Resource Access Manager</a></p>	<p>2021 年 11 月 16 日</p>
<p><a href="#">AWSLicenseManagerConsumptionPolicy</a> – 新政策</p>	<p>License Manager 新增了新的政策，授予使用授權的許可。</p>	<p>2021 年 8 月 11 日</p>
<p><a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策</p>	<p>License Manager 新增了列出委派管理員的許可，以及建立名為之服務連結角色的許可AWSServiceRoleForAWSLicenseManagerMemberAccountRole。</p>	<p>2021 年 6 月 16 日</p>

變更	描述	Date
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 新增了列出所有 License Manager 資源的許可，例如授權組態、授權和授權。	2021 年 6 月 15 日
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 新增了建立名為 <code>AWSServiceRoleForMarketplaceLicenseManagement</code> 之服務連結角色的許可。此角色提供在 License Manager 中建立和管理授權的 AWS Marketplace 許可。如需詳細資訊，請參閱 AWS Marketplace 買家指南中的 <a href="#">AWS Marketplace 的服務連結角色</a> 。	2021 年 3 月 9 日
License Manager 已開始追蹤變更	License Manager 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 9 日

## License Manager 中授權的密碼編譯簽署

License Manager 可以密碼編譯方式簽署 ISV 發出的授權，或是透過 AWS Marketplace 代表 ISV 發出的授權。簽署可讓廠商驗證應用程式本身內授權的完整性和原始伺服器，即使在離線環境中也是如此。

若要簽署授權，License Manager 會使用 AWS KMS key 屬於 ISV 且受保護 in AWS Key Management Service (AWS KMS) 的非對稱。此客戶受管 CMK 包含數學相關的公有金鑰和私有金鑰對。當使用者請求授權時，License Manager 會產生列出授權權限的 JSON 物件，並使用私有金鑰簽署此物件。簽章和純文字 JSON 物件會傳回給使用者。任何出現這些物件的一方都可以使用公有金鑰來驗證授權的文字尚未變更，以及授權是由私有金鑰的擁有者簽署。金鑰對的私有部分永遠不會離開 AWS KMS。如需 中非對稱密碼編譯的詳細資訊 AWS KMS，請參閱 [使用對稱和非對稱金鑰](#)。

**Note**

License Manager 會在 AWS KMS [Sign](#) 簽署和驗證授權時呼叫 和 [Verify](#) API 操作。CMK 必須具有 [SIGN\\_VERIFY](#) 的金鑰用量值，才能讓這些操作使用。此各種 CMK 無法用於加密和解密。

下列工作流程說明密碼編譯簽署授權的發行：

1. 在 AWS KMS 主控台、API 或 SDK 中，授權管理員會建立非對稱客戶受管 CMK。CMK 必須具有使用簽署和驗證的金鑰，並支援 RSASSA-PSS SHA-256 簽署演算法。如需詳細資訊，請參閱[建立非對稱 CMKs](#)和[如何選擇 CMK 組態](#)。
2. 在 License Manager 中，授權管理員會建立包含 AWS KMS ARN 或 ID 的耗用組態。組態可以指定借用和佈建選項之一或兩者。如需詳細資訊，請參閱[建立賣方發行的授權區塊](#)。
3. 最終使用者使用 [CheckoutLicense](#)或 [CheckoutBorrowLicense](#) API 操作取得授權。只有已設定借用的授權才允許CheckoutBorrowLicense此操作。它會傳回數位簽章做為回應的一部分，以及 JSON 物件列出權限。純文字 JSON 類似以下內容：

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

## License Manager 的合規驗證

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

## License Manager 中的復原能力

AWS 全域基礎設施是以 AWS 區域和可用區域為基礎建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域和可用區域的詳細資訊，請參閱[AWS 全球基礎設施](#)。

## License Manager 中的基礎設施安全性

作為受管服務，AWS License Manager 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 License Manager。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

## License Manager 和介面 VPC 端點搭配 AWS PrivateLink

您可以在虛擬私有雲端 (VPC) 與 之間建立私有連線，AWS License Manager 方法是建立介面 VPC 端點。介面端點採用 [AWS PrivateLink](#)技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 Direct Connect 連線的情況下，私下存取 License Manager API。VPC 中的執行個體不需要公有 IP 地址即可與 License Manager 通訊。VPC 和 License Manager 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的[介面 VPC 端點 \(AWS PrivateLink\)](#)。

## 建立 License Manager 的介面 VPC 端點

使用下列其中一個服務名稱建立 License Manager 的介面端點：

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

如果您為端點啟用私有 DNS，您可以使用區域的預設 DNS 名稱向 License Manager 提出 API 請求。例如 `license-manager.region.amazonaws.com`。

如需詳細資訊，請參閱 Amazon VPC 使用者指南中的[建立介面端點](#)。

## 建立 License Manager 的 VPC 端點政策

您可以將政策連接至 VPC 端點，以控制對 License Manager 的存取。此政策會指定下列資訊：

- 可執行動作的委託人
- 可執行的動作
- 可以對其執行動作的資源

以下是 License Manager 的端點政策範例。連接到端點時，此政策會授予所有資源上所有主體的指定 License Manager 動作的存取權。

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

如需詳細資訊，請參閱 [《Amazon VPC 使用者指南》](#) 中的使用 VPC 端點控制對服務的存取。

## 對 License Manager 進行故障診斷

以下資訊可協助您疑難排解使用時的問題 AWS License Manager。開始之前，請確認您的 License Manager 設定符合 [中所述的要求](#) [the section called “設定”](#)。

### 跨帳戶探索錯誤

設定跨帳戶探索時，您可能會在庫存搜尋頁面上遇到下列錯誤訊息：

Athena 例外狀況：Athena 查詢失敗，因為 - 執行查詢的許可不足。請遷移您的目錄，以啟用對此資料庫的存取。

如果您的 Athena 服務使用 Athena 受管資料目錄，而不是 [，](#) 就會發生這種情況 AWS Glue Data Catalog。如需升級說明，請參閱 [Step-by-Step升級至 AWS Glue Data Catalog](#)。

### 管理帳戶無法取消資源與自我管理授權的關聯

如果組織的成員帳戶在其帳戶中刪

除 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 服務連結角色 (SLR)，而且有成員擁有的資源與自我管理的授權相關聯，則管理帳戶將無法取消這些成員帳戶資源的授權關聯。這表示成員帳戶資源將繼續使用來自管理帳戶集區的授權。若要允許管理帳戶取消資源的關聯，請還原 SLR。

此行為會考慮客戶偏好不允許管理帳戶執行一些影響成員帳戶資源的動作的情況。

### Systems Manager 庫存已過期

Systems Manager 會將資料存放在其庫存資料中 30 天。在此期間，License Manager 會將受管執行個體視為作用中，即使無法 ping。從 Systems Manager 清除庫存資料後，License Manager 會將執行個體標記為非作用中，並更新本機庫存資料。為了保持受管執行個體計數的準確性，我們建議在 Systems Manager 中手動取消註冊執行個體，以便 License Manager 可以執行清除操作。

### 取消註冊 AMI 的明顯持久性

License Manager 每隔幾個小時清除一次資源與自我管理授權之間的過時關聯。如果與自我管理授權相關聯的 AMI 透過 Amazon EC2 取消註冊，AMI 可能會在清除之前短暫地繼續出現在 License Manager 資源庫存中。

## 新的子帳戶執行個體在資源庫存中顯示的速度很慢

啟用跨帳戶支援時，根據預設，License Manager 會在每天下午 1 點更新客戶帳戶。當天稍後新增的執行個體會在第二天顯示在管理帳戶資源庫存中。您可以在 AWS Glue 主控台 `LicenseManagerResourceSynDataProcessJobTrigger` 中編輯 管理帳戶，以變更更新指令碼執行的頻率。

## 啟用跨帳戶模式後，子帳戶執行個體的顯示速度會變慢

當您在 License Manager 中啟用跨帳戶模式時，子帳戶中的執行個體可能需要幾分鐘到幾個小時才會出現在資源庫存中。這段時間取決於子帳戶的數量、以及在個別子帳戶中的執行個體數量。

## 無法停用跨帳戶探索

將帳戶設定為跨帳戶探索之後，就無法還原至單一帳戶探索。

## 子帳戶使用者無法將共用自我管理授權與執行個體建立關聯

當這種情況發生且跨帳戶探索已經啟用時，請檢查下列個別項目：

- 子帳戶已從該組織移除。
- 子帳戶已從管理帳戶中建立的資源共用中移除。
- 自我管理的授權已從資源共用中移除。

## 連結 AWS Organizations 帳戶失敗

如果 Settings (設定) 頁面報告此錯誤，即表示某帳戶因下列原因而非某組織的成員：

- 子帳戶已從該組織中移除。
- 客戶從管理帳戶的組織主控台關閉對 License Manager 的存取。

# License Manager 的文件歷史記錄

下表說明 的版本 AWS License Manager。

變更	描述	日期
新增對授權資產群組的支援	License Manager 新增了透過授權資產群組探索授權資產和軟體使用情況的支援。這包括的更新 <a href="#">AWS 受管政策：AWSLicenseManagerServiceRolePolicy</a> 。	2025 年 11 月 19 日
新增對 Microsoft 遠端桌面服務訂閱者存取授權 (RDS SAL) 使用者型訂閱的支援	License Manager 新增了對 RDS SAL 使用者型訂閱管理和組態的支援，包括一次設定兩個以上遠端桌面連線的能力。	2024 年 11 月 14 日
更新以使用者為基礎的訂閱 SLR 受管政策，以取得路由和聯網資訊	License Manager 新增了下列許可來管理授權和 Active Directory 資料：從 Route 53 取得路由資訊、從 Amazon EC2 取得聯網資訊和安全群組規則，以及從 Secrets Manager 取得秘密。如需更多詳細資訊， <a href="#">AWS 受管政策：AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> 。	2024 年 11 月 7 日
從 Red Hat Subscription Manager (RHSM) 擷取 BYOL 訂閱資訊	License Manager 已新增支援，以從 Red Hat Enterprise Linux 執行個體上的 microSDHCM for BYOL 授權擷取訂閱資訊。這包括的更新 <a href="#">AWSLicenseManagerL</a>	2024 年 7 月 10 日

變更	描述	日期
	<a href="#">inuxSubscriptionsServiceRolePolicy</a> 。	
新增對 Amazon RDS for Db2 vCPU 型 BYOL 授權的支援	License Manager 新增對 Amazon RDS for Db2 vCPU 型 BYOL 授權的支援。	2024 年 3 月 20 日
新增對 Microsoft Office 使用者型訂閱的 Windows Server 2019 支援	AWS 在 Amazon Machine Image (AMIs) 中新增對 Windows Server 2019 的支援，其中包含 Amazon EC2 上 Microsoft Office LTSC Professional Plus 提供的授權。	2023 年 12 月 4 日
自我管理（內部部署）網域使用者可以使用以使用者為基礎的訂閱	License Manager 新增支援自我管理 Active Directory 網域中的使用者，以便在建立與 AWS Managed Microsoft AD 目錄的信任時利用使用者型訂閱。	2023 年 9 月 6 日
Ubuntu LTS 訂閱的授權類型轉換	License Manager 新增對 Ubuntu LTS 執行個體的支援，以使用授權類型轉換來新增 Ubuntu Pro 訂閱。	2023 年 4 月 20 日
取代作用中授予	License Manager 新增了可在授予啟用期間選擇性地取代授予授權的作用中授予的功能。	2023 年 3 月 31 日
Linux 訂閱的委派管理	License Manager 新增對 Linux 訂閱委派管理員的支援。	2023 年 3 月 3 日
Linux 訂閱	License Manager 新增了商業 Linux 訂閱的追蹤。	2022 年 12 月 21 日

變更	描述	日期
Amazon CloudWatch 指標	License Manager 現在會針對授權組態用量和訂閱發出 CloudWatch 指標。	2022 年 12 月 21 日
適用於以使用者為基礎的訂閱的 Microsoft Office	License Manager 新增 Microsoft Office 做為使用者型訂閱的支援軟體。	2022 年 11 月 28 日
將權利分配至組織單位	將權利分配至組織中的特定 OU。	2022 年 11 月 17 日
全組織檢視 ( 主控台 )	AWS Organizations 使用 License Manager 主控台在中跨您的帳戶管理授予的授權。	2022 年 11 月 11 日
以使用者為基礎的訂閱	在 Amazon EC2 上使用支援的使用者型訂閱產品。	2022 年 8 月 2 日
記錄並提交授權用量資料 ( 主控台 )	使用 License Manager 主控台記錄並提交授權用量資料。	2022 年 3 月 28 日
授權類型轉換 ( 主控台 )	使用 License Manager 主控台在 AWS 提供的授權和自攜授權模型 (BYOL) 之間變更授權類型，而不重新部署現有的工作負載。	2021 年 11 月 9 日
授權類型轉換 (CLI)	使用在 AWS 提供的授權和自攜授權模型 (BYOL) 之間變更授權類型，AWS CLI 而不重新部署現有的工作負載。	2021 年 9 月 22 日
共用權利	透過一個請求與整個組織共用受管授權權利。	2021 年 7 月 16 日

變更	描述	日期
用量報告	使用 License Manager 用量報告追蹤授權類型組態的歷史記錄。用量報告先前稱為報告產生器和授權報告。	2021 年 5 月 18 日
自動化探索排除規則	根據 AWS 帳戶 IDs 和標籤，從 License Manager 自動化探索中排除執行個體。	2021 年 3 月 5 日
受管權利	針對從購買的產品，以及使用 License Manager 分發授權的賣方，追蹤 AWS Marketplace 並分配授權權利。	2020 年 12 月 3 日
解除安裝軟體的自動化會計	設定自動探索，以在解除安裝軟體時停止追蹤執行個體。	2020 年 12 月 3 日
標籤型篩選	使用標籤搜尋您的資源庫存。	2020 年 12 月 3 日
AMI 關聯範圍	將您的自我管理授權與與您 AWS 帳戶共用 AMIs 建立關聯。	2020 年 11 月 23 日
主機的授權親和性	在特定天數內強制將授權指派至專用硬體。	2020 年 8 月 12 日
在 Amazon RDS 上追蹤 Oracle 部署	追蹤 Amazon RDS 上 Oracle 資料庫引擎版本和授權套件的授權使用量。	2020 年 3 月 23 日
主機資源群組	設定主機資源群組，讓 License Manager 管理您的專用主機。	2019 年 12 月 1 日

變更	描述	日期
自動化軟體探索	設定 License Manager 以搜尋新安裝的作業系統或應用程式，並將對應的自我管理授權連接至執行個體。	2019 年 12 月 1 日
區分包含的授權和自備授權	根據您是否使用 Amazon 提供的授權或您自己的授權來篩選搜尋結果。	2019 年 11 月 8 日
將授權連接至內部部署資源	將授權連接至現場部署執行個體之後，License Manager 會定期收集軟體庫存、更新授權資訊，並報告使用情況。	2019 年 3 月 8 日
AWS License Manager 初始版本	初始服務啟動	2018 年 11 月 28 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。