



使用者指南

# AWS License Manager



# AWS License Manager: 使用者指南

Copyright © 2024 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，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，或由 Amazon 贊助。

# Table of Contents

什麼是 AWS License Manager ? .....	1
受管理的權利 .....	1
License Manager 使用案例 .....	2
相關服務 .....	2
License Manager 的運作方式 .....	4
開始使用 .....	7
設定 .....	7
註冊一個 AWS 帳戶 .....	7
建立具有管理權限的使用者 .....	8
開始使用 License Manager .....	9
使用 License Manager .....	10
自我管理授權 .....	11
參數和規則 .....	12
根據廠商授權建立規則 .....	13
建立自我管理授權 .....	15
共用自我管理授權 .....	16
編輯自我管理授權 .....	20
停用自我管理授權 .....	21
刪除自我管理授權 .....	21
授權規則 .....	22
建立自我管理授權與 AMI 的關聯 .....	22
取消自我管理授權與 AMI 的關聯 .....	23
用量報告 .....	24
建立用量報告 .....	24
編輯用量報告 .....	25
刪除用量報告 .....	26
授權類型轉換 .....	26
合格的授權類型 .....	27
必要條件 .....	35
轉換授權類型 .....	37
租賃轉換 .....	45
故障診斷 .....	47
主機資源群組 .....	48
建立主機資源群組 .....	49

共用主機資源群組 .....	50
將專用主機新增至主機資源群組 .....	50
在主機資源群組中啟動執行個體 .....	51
修改主機資源群組 .....	51
從主機資源群組移除專用主機 .....	51
刪除主機資源群組 .....	52
庫存搜索 .....	52
使用庫存搜尋 .....	53
自動探索庫存 .....	58
授予的授權 .....	60
檢視您授予的授權 .....	60
管理您授予的授權 .....	61
分發權利 .....	63
授予接受和激活 .....	65
授權狀態 .....	67
買家帳戶的指標 .....	68
賣家發出的授權 .....	69
權利 .....	70
授權使用 .....	70
請求 .....	70
建立賣家核發的授權 .....	72
授予客戶授權 .....	73
取得客戶的臨時登入資料，而無需AWS帳戶 .....	74
使用授權 .....	75
刪除賣家核發的授權 .....	76
基於用戶的訂閱 .....	76
必要條件 .....	77
考量事項 .....	80
支援的軟體 .....	81
開始使用 .....	83
修改目錄設定 .....	92
修改 VPC 設定 .....	92
取消使用者關聯 .....	93
取消訂閱使用者 .....	93
終止執行個體 .....	94
移除目錄 .....	94

故障診斷 .....	95
訂閱 .....	97
管理探索 .....	98
檢視執行個 .....	102
帳單資訊 .....	103
使用量度和警示 .....	105
設定 .....	108
受管理授權 .....	108
訂閱 .....	110
基於用戶的訂閱 .....	110
委派的管理員 .....	111
Dashboard (儀表板) .....	115
監視 License Manager .....	117
使用監控 CloudWatch .....	117
建立 CloudWatch 鬧鐘 .....	119
使用 CloudTrail 記錄 API 呼叫 .....	119
License Manager 資訊 CloudTrail .....	119
瞭解 License Manager 記錄檔項目 .....	120
安全性 .....	122
資料保護 .....	122
靜態加密 .....	123
身分與存取管理 .....	123
建立使用者、群組和角色 .....	124
IAM 政策 .....	124
建立 License Manager 的 IAM 政策 .....	125
向使用者、群組和角色授予許可 .....	126
服務連結角色 .....	127
核心角色 .....	127
管理帳戶角色 .....	130
會員帳號角色 .....	132
使用者型訂閱角色 .....	133
訂閱角色 .....	135
AWS 管理的政策 .....	136
AWSLicenseManagerServiceRolePolicy .....	137
AWSLicenseManagerMasterAccountRolePolicy .....	139
AWSLicenseManagerMemberAccountRolePolicy .....	143

AWSLicenseManagerConsumptionPolicy .....	144
AWSLicenseManagerUserSubscriptionsServiceRolePolicy .....	144
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy .....	145
政策更新 .....	146
授權簽署 .....	148
法規遵循驗證 .....	149
恢復能力 .....	150
基礎設施安全性 .....	151
VPC 端點 (AWS PrivateLink) .....	151
為 License Manager 建立界面 VPC 端點 .....	151
為 License Manager 建立 VPC 端點政策 .....	152
疑難排解 .....	153
跨帳戶探索錯誤 .....	153
管理帳戶無法取消資源與自我管理授權的關聯 .....	153
Systems Manager 庫存已過期 .....	153
取消註冊 AMI 的明顯持久性 .....	153
新的子帳號實例在資源清查中顯示緩慢 .....	154
啟用跨帳戶模式後，子帳戶實例出現緩慢 .....	154
無法停用跨帳戶探索 .....	154
子帳戶使用者無法將共用的自我管理授權與執行個體建立 .....	154
連結 AWS Organizations 帳號失敗 .....	154
文件歷史紀錄 .....	155
.....	clix

# 什麼是 AWS License Manager ？

AWS License Manager 是一項服務，可讓您更輕鬆地在內部部署環境中集中管理軟體廠商提供的軟體授權 (例如 Microsoft、SAP、Oracle AWS 和 IBM)。這提供了對授權使用情況的控制和可見性，使您能夠限制授權超額，並降低不合規和錯誤報告的風險。

在建置雲端基礎架構時 AWS，您可以使用自攜授權模式 (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，以便與雲端資源搭配使用。

License Manager 可透過直接繫結至 AWS 服務的庫存追蹤，降低授權超額和罰款的風險。透過對授權使用的規則式控制，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 可協助停止不符合規範的伺服器使用，然後再發生。

License Manager 的內建儀表板提供授權使用情況的持續可見性，並協助廠商稽核。

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

您可以透過維持所有已簽出的權利計數，集中追蹤授權並在多個區域強制執行限制。AWS License Manager 還會追蹤與每次簽出相關聯的一般使用者身分識別和基礎資源識別碼 (如果有的話)，以及簽出時間。此時間序列資料可透過 CloudWatch 量度和事件追蹤至 ISV。ISV 可將此資料用於分析、稽核及其他類似用途。

AWS License Manager 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 [AWS CloudFormation](#)、AWS 資源標記和 [AWS X-Ray](#)。

## 受管理的權利

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

獨立軟體廠商 (ISV) 可以使用受管理的權利 AWS License Manager 來管理軟體授權和資料，並將其分發給終端使用者。身為發行者，您可以使用 License Manager 儀表板集中追蹤賣家核發授權的使用情況。ISV 透過自動授權建立和發佈作為交易工作流程的一部分，從中 AWS Marketplace 受益銷售。ISV 也可以使用 License Manager 為沒有 AWS 帳戶的客戶建立授權金鑰和啟用授權。

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

您可以在中建立授權，AWS License Manager 並使用 IAM 身分或透過由 AWS License Manager 產生的數位簽章權杖將授權散發給最終使用者。使用的終端使用者 AWS 可以進一步將授權權利重新分配給其各自組織中的 AWS 身分。擁有分散式權利的終端使用者可以透過與您的軟體整合，從該授權中簽出並簽入所需的權利。AWS License Manager 每個授權簽出都會指定權利、關聯的數量和出庫時間期間，例如將 10 簽 `admin-users` 出 1 小時。您可以根據分散式授權的基礎 IAM 身分，或根據 AWS License Manager 透過 AWS License Manager 服務產生的長期使用權杖來執行此檢查。

## License Manager 使用案例

以下是 License Manager 針對各種使用案例提供的功能範例：

- [License Manager 中的自我管理授權](#)— 用於根據企業合約的條款來定義授權規則，這些條款決定了如何 AWS 處理使用這些授權的命令。
- [賣家在 License Manager 中核發授權](#)— 用於管理和分發軟件許可證給最終用戶。
- [授與 License Manager 中的授權](#)— 用於管理從、或直接向賣方取得之授權的使用 AWS Marketplace AWS Data Exchange，該賣方將其軟體與受管理權利整合。
- [License Manager 中的授權類型轉換](#)— 用於在 AWS 提供的授權與自攜授權模式 (BYOL) 之間變更授權類型，而無需重新部署工作負載。
- [在 License Manager 中搜尋庫存](#)— 用於使用 AWS Systems Manager 庫存和授權規則探索和追蹤內部部署應用程式。
- [License Manager 中的使用者型訂閱](#)— 用於為支援的軟體購買完全合規的 Amazon 提供的授權，且需支付每位使用者訂閱費用。
- [授權管理員中的 Linux 訂閱](#)— 用於查看和管理您擁有和運行的商業 Linux 訂閱 AWS。

## 相關服務

License Manager 與 Amazon EC2，亞馬遜 RDS 和 AWS Organizations。AWS Marketplace AWS Systems Manager

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中強制執行授權規則：

- [Amazon EC2 執行個體](#)
- [專用執行個體](#)
- [專用主機](#)
- [Spot 執行個體和 Spot 叢集](#)

- [受管節點](#)

當您搭配使用 License Manager 時 AWS Systems Manager，您可以管理託管於以外的實體或虛擬伺服器上的授權 AWS。您可以搭配使用 License Manager AWS Organizations 來集中管理所有組織帳戶。

此外，您還可以管理向或直接從 AWS Marketplace 與其軟體整合的賣家購買授權的使用 AWS License Manager。AWS Data Exchange 您可以用 AWS License Manager 來將使用權 (稱為權利) 分發給特定 AWS 帳戶。

License Manager 程式與適用 Amazon RDS for Oracle 文和 Amazon RDS 的 Db2 vCPU 為基礎的 BYOL 授權整合。透過此整合，您可以查看適用於 Oracle 的 RDS 和適用於 Db2 資料庫執行個體的 vCPU 使用率。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使用的授權數量。如需詳細資訊，請參閱 Amazon RDS 使用者指南中的下列相關連結。

- [適用於 Oracle 授權的 RDS 選項](#)
- [適用於 Db2 的 RDS 授權選項](#)

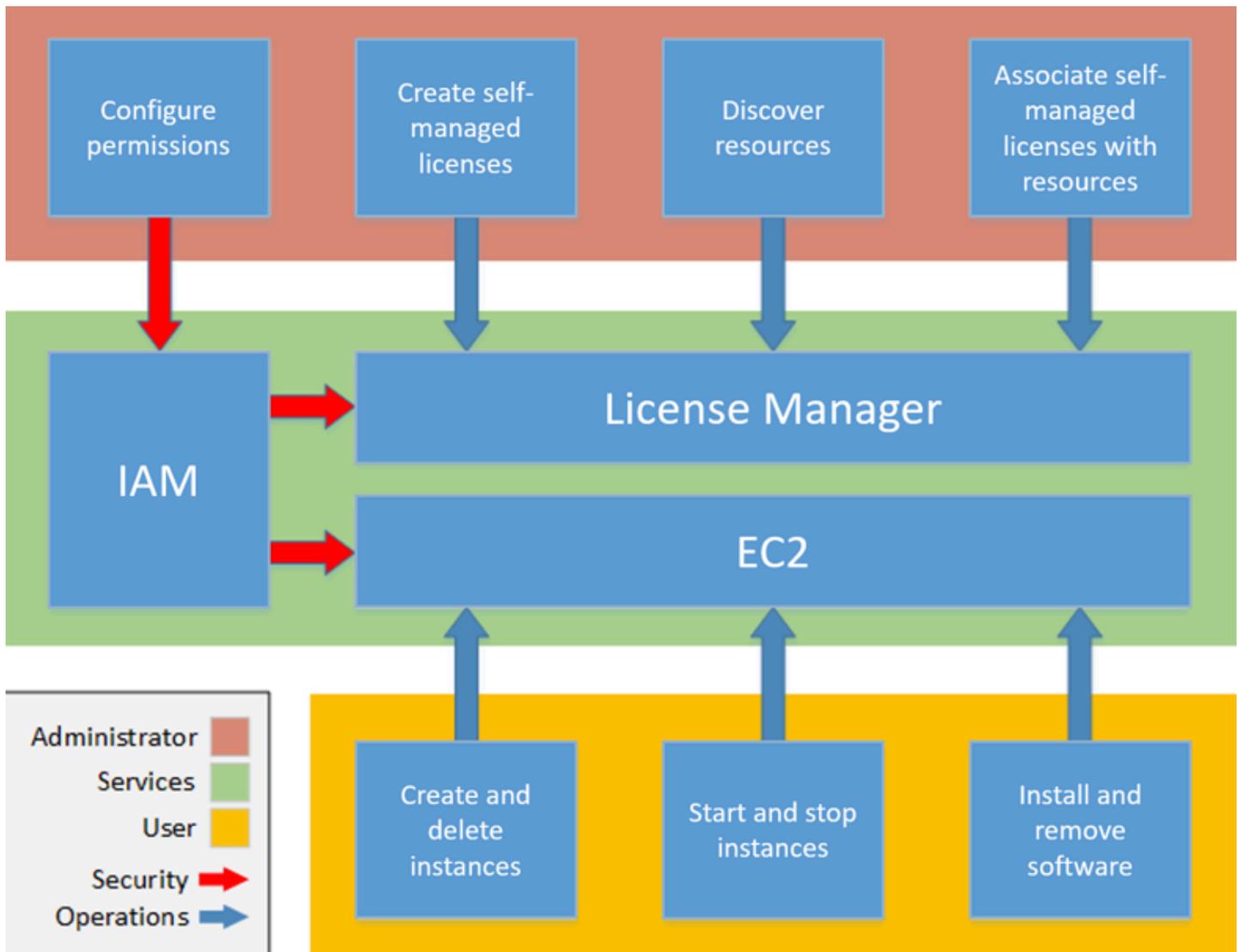
# License Manager 的運作方式

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，它成為有效溝通的問題，尤其是許可證專家和系統管理員之間。License Manager 提供了一種從各個領域匯集知識的方法。至關重要的是，它還與AWS服務原生整合，例如，與建立和刪除執行個體的 Amazon EC2 控制平面整合。這意味著 License Manager 規則和限制捕獲的業務和操作知識，並轉化為實例創建和應用程序部署的自動化控制。

下圖說明 License Manager 管理許可和設定授權管理員以及透過 Amazon EC2 主控台建立、管理和刪除資源的使用者的明確但協調的職責。



如果您負責管理組織中的授權，則可以使用 License Manager 來設定授權規則、將它們附加到您的啟動中，以及追蹤使用情況。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。

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，此工作會透過 License Manager 主控台進行整合。如圖所示，這包括設定服務權限、建立自我管理授權、清查內部部署和雲端中的運算資源，以及將自我管理授權與探索到的資源建立關聯。實際上，這可能意味著將自我管理授權與經核准的 Amazon 機器映像 (AMI) 產生關聯，該映像檔 (AMI) 將其用作所有 Amazon EC2 執行個體部署的範本。

License Manager 可節省因違反授權而損失的成本。雖然內部稽核僅在事實發生後才會揭露違規行為，但為時已晚而無法避免不遵循法規遵循的處罰時，License Manager 可防止昂貴的事件發生。License Manager 使用內建儀表板顯示授權消耗和追蹤資源，簡化報告作業

# 開始使用 AWS License Manager

以下各節將引導您設定 AWS 帳戶 和使用者，以及如何開始使用 License Manager。如需管理使用者、群組和角色以利用 License Manager 的權限，同時遵循 AWS 最佳作法的更多資訊，請參閱[適用於 AWS License Manager 的 Identity and Access Management](#)。如需設定與 License Manager 整合的 Amazon EC2 資源的詳細資訊，請參閱 [Amazon 彈性運算雲端使用者指南中的設定以使用 Amazon EC2](#)。

## 主題

- [設定](#)
- [在板載上使用 License Manager AWS Management Console](#)

## 設定

以下部分詳細介紹了您的 AWS 帳戶 和用戶的設置。

### 註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

1. 開啟 <https://portal.aws.amazon.com/billing/signup>。
2. 請遵循線上指示進行。

部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 [root 使用者來執行需要 root 使用者存取權](#)的工作。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時登錄 <https://aws.amazon.com/> 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

## 建立具有管理權限的使用者

註冊後，請保護您的 AWS 帳戶 AWS 帳戶根使用者 AWS IAM Identity Center、啟用和建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

### 保護您的 AWS 帳戶根使用者

1. 選擇 Root 使用者並輸入您的 AWS 帳戶 電子郵件地址，以帳戶擁有者身分登入。[AWS Management Console](#)在下一頁中，輸入您的密碼。

如需使用根使用者登入的說明，請參閱 AWS 登入 使用者指南中的[以根使用者身分登入](#)。

2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

如需指示，請參閱《IAM 使用者指南》中的[為 AWS 帳戶 根使用者啟用虛擬 MFA 裝置 \(主控台\)](#)。

### 建立具有管理權限的使用者

1. 啟用 IAM Identity Center。

如需指示，請參閱 AWS IAM Identity Center 使用者指南中的[啟用 AWS IAM Identity Center](#)。

2. 在 IAM 身分中心中，將管理存取權授予使用者。

[若要取得有關使用 IAM Identity Center 目錄 做為身分識別來源的自學課程，請參閱《使用指南》IAM Identity Center 目錄中的「以預設值設定使用AWS IAM Identity Center 者存取」。](#)

### 以具有管理權限的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

如需使用 IAM 身分中心使用者[登入的說明，請參閱使用AWS 登入 者指南中的登入 AWS 存取入口網站](#)。

### 指派存取權給其他使用者

1. 在 IAM 身分中心中，建立遵循套用最低權限許可的最佳做法的權限集。

如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「[建立權限集](#)」。

2. 將使用者指派給群組，然後將單一登入存取權指派給群組。

如需指示，請參閱《AWS IAM Identity Center 使用指南》中的「[新增群組](#)」。

## 在板載上使用 License Manager AWS Management Console

若要開始使用 License Manager，需要執行下列程序。完成初始需求後，您可以繼續使用 License Manager 來處理所需的使用案例。

開始使用 License Manager 的步驟

1. 開啟 License Manager 主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
2. 系統會提示您設定 License Manager 及其支援服務的權限。依照指示設定所需的權限。
3. 初始設置完成後，您可以繼續使用許可證管理員根據需要進行操作[License Manager 使用案例](#)。

# 使用 AWS License Manager

License Manager 可以套用至具有AWS資源和內部部署資源混合基礎結構的企業的標準案例。您可以建立自我管理授權、清查耗用授權的資源、將自我管理授權與資源建立關聯，以及追蹤庫存與合規性。

## AWS Marketplace 產品授權

使用 License Manager，您現在可以透過 Amazon EC2 啟動範本、範本或 Service Catalog 產品將授權規則與AWS Marketplace BYOL AMI 產品建立關聯。AWS CloudFormation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 AMI 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 [Systems Manager 詳細目錄](#) 以外執行AWS的應用程式，然後將授權規則附加到這些應用程式。附加授權規則後，您可以在 License Manager 主控台中追蹤內部部署伺服器及AWS資源。

## 區分包含的授權與 BYOL

使用 License Manager，您可以識別哪些資源具有產品隨附的授權，以及哪些資源使用您擁有的授權。這可讓您準確地報告您使用 BYOL 授權的方式。此篩選需要 SSM 2.3.722.0 版或更新版本。

## 跨AWS帳戶的 License Manager

License Manager 可讓您管理所有AWS帳戶的授權。您可以在AWS Organizations管理帳戶中建立一次授權組態，然後使用AWS Resource Access Manager或使用 License Manager 設定連結帳戶，在AWS Organizations帳戶之間共用這些設定。這也可讓您執行跨帳戶探索，以便跨AWS帳戶搜尋庫存。

## 內容

- [License Manager 中的自我管理授權](#)
- [License Manager 中的授權規則](#)

- [License Manager 中的使用報告](#)
- [License Manager 中的授權類型轉換](#)
- [主機資源群組AWS License Manager](#)
- [在 License Manager 中搜尋庫存](#)
- [授與 License Manager 中的授權](#)
- [賣家在 License Manager 中核發授權](#)
- [License Manager 中的使用者型訂閱](#)
- [授權管理員中的 Linux 訂閱](#)
- [中的設定AWS License Manager](#)
- [儀表板 AWS License Manager](#)

## License Manager 中的自我管理授權

自我管理授權是 License Manager 的核心。自我管理授權先前稱為「授權組態」。自我管理授權包含以企業合約條款為基礎的授權規則。您建立的規則會決定如何 AWS 處理使用授權的指令。建立自我管理授權時，請與組織的合規團隊密切合作，以檢閱您的企業合約。

### 限制

- 每個資源的自我管理授權數目：10
- 自我管理授權總數：25
- 系統管理員受控執行個體必須與 vCPU 和執行個體類型自我管理授權相關聯。

### 目錄

- [自我管理的授權參數和規則](#)
- [根據廠商授權建立 License Manager 規則](#)
- [建立自我管理授權](#)
- [共用自我管理授權](#)
- [編輯自我管理授權](#)
- [停用自我管理授權](#)
- [刪除自我管理授權](#)

## 自我管理的授權參數和規則

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。您也可以自我管理授權中新增標籤。建立自我管理的授權後，管理員可以修改授權數目和使用限制，以反映不斷變化的資源需求。

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。
- (選擇性) 說明 — 自我管理授權的說明。
- 授權類型 — 用來計算授權數的度量。支援的值包括 vCPUs、核心、通訊端和執行個體。
- (選擇性) 數目 <option>— 資源使用的授權數目。
- 狀態 — 指示模型組態是否處於使用中狀態。
- 產品資訊 — 用於[自動探索](#)的產品名稱和版本。支援的產品是視窗服務器，SQL 服務器，Amazon RDS for Oracle 和 Amazon RDS 為 Db2。
- (選擇性) 規則 — 包括下列項目。可用的規則因計數類型而異。
  - 授權與主機相似性 (以天為單位) — 將授權使用限制在指定天數內的主機。範圍是 1 到 180 之間。計數類型必須是「核心」或「通訊端」。相似性期間過後，授權將可在 24 小時內重複使用。
  - 最大核心數 — 資源的核心數目上限。
  - 最大通訊端數 — 資源的最大計數通訊端數。
  - 最大 vCPUs 數量 — 資源的 vCPUs 數目上限。
  - 最小核心數 — 資源的核心數下限。
  - 最小通訊端 — 資源的最小通訊端計數。
  - 最低 vCPUs 數量 — 資源的 vCPUs 數目下限。
  - 租用 — 將授權使用限制為指定的 EC2 租用。如果計數類型為「核心」或「通訊端」，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。控制台 (和 API) 名稱如下：
    - 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 優化](#) 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。

下表說明每種計數類型可用的授權規則。

主控台名稱	API 名稱	核心	執行個體	通訊埠	vCPU
授權與主機的關聯性 (以天為單位)	licenseAf finityToHost	✓		✓	
最大核心	maximumCores	✓	✓		
最大插槽	maximumSockets		✓	✓	
最大 vCPUs 數量	maximumVcpus		✓		✓
最小核心	minimumCores	✓	✓		
最小插槽	minimumSockets		✓	✓	
最低 vCPUs 數量	minimumVcpus		✓		✓
租用	allowedTenancy	✓	✓	✓	✓
vCPU 最佳化	honorVcpu Optimization				✓

## 根據廠商授權建立 License Manager 規則

您可以根據軟體廠商授權的語言建立「License Manager」規則集。下列範例不適用於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。供應商授權規定也會與 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 不參與軟體供應商的審計過程。客戶必須負責遵循法規，並負責根據其授權合約，仔細瞭解 License Manager 並將規則擷取到授權管理員中。

## 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。

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供應商授權需求相關聯。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	核心數目設定為 <b>96</b> 。
vCPUs 或核心數目下限/最大值	「最小核心」設定為 <b>8</b> 。 最大核心數設定為 <b>16</b> 。
授權計數硬性限制	已選擇 Enforce license limit (強制授權限制)。
允許的租賃	租賃已設定為 <b>Dedicated Host</b> 。

## 建立自我管理授權

自我管理授權代表與軟體廠商簽訂的合約中的授權條款。您的自我管理授權指定應如何計算授權 (例如，依 vCPUs 或執行個體數目)。它還指定了您的使用限制，以便您可以防止使用超過已配置的許可證數量。此外，它也可以指定授權的其他限制，例如租用類型。

適用於甲骨文和 Amazon RDS 的 Db2 資料庫的亞馬遜 RDS 的注意事項

當您新增產品資訊以設定 Amazon RDS for Oracle 或 Amazon RDS for Db2 資料庫的自動化探索時，適用下列要求：

- 支援的授權計數類型為 vCPU。
- 不支援規則。
- 不支援硬式授權限制。
- 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. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格中，選擇自我管理授權。
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。
  - 說明 — 自我管理授權的選擇性描述。
  - 授權類型 — 此授權的計數模式 (vCPUs、核心、通訊端或執行個體)。
  - 數目 <option> — 顯示的選項取決於授權類型。當超過授權限制時，License Manager 會通知您 (軟限制) 或防止資源部署 (硬性限制)。
  - 強制授權限制 — 如果選取此選項，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. (選擇性) 在「自動探索規則」面板中，執行下列動作：
  - a. 選擇產品名稱、產品類型和資源類型，以便使用 [自動化](#) 探索來探索和追蹤每項產品。

- b. 選取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任何授權相似性期間已經過後，使授權可供重複使用。
  - c. (選擇性) 如果您的帳戶是 Organizations 的 License Manager 管理帳戶，您必須選擇定義要從自動探索中排除的資源。若要執行此動作，請選取 [新增排除規則]，選擇要篩選依據的內容、支援 AWS 帳號 ID 和資源標籤，然後輸入資訊以識別該屬性。
6. (選擇性) 展開「標記」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。

### 使用指令列建立自我管理授權的步驟

- [create-license-configuration](#) (AWS CLI)
- [新 LCM \(\) LicenseConfiguration](#) AWS Tools for PowerShell

## 共用自我管理授權

您可以使用 AWS Resource Access Manager 與任何 AWS 帳戶或透過 AWS Organizations 共用您的自我管理授權。如需詳細資訊，請參閱 AWS RAM 使用指南中的「共用 AWS [資源](#)」。

### 支援的帳號配額

如果您在 2023 年 10 月 14 日 AWS License Manager 之前啟用授權共用，則組織內 License Manager 支援的最大帳號數量配額將小於新的預設上限。您可以使用下一節所提供的 AWS RAM API 作業來增加此配額。如需有關 License Manager 中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](#)。

### 必要條件

若要完成下列程序，您必須以具有下列權限的組織管理帳戶中的主參與者身分登入：

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

## 增加支援的帳戶配額

下列程序會將目前的配額增加Number of accounts per organization for License Manager到目前的預設上限。

### 增加 License Manager 支援的帳戶配額

1. 使用指[describe-organization](#) AWS CLI 令來判斷您組織的 ARN，方法是使用下列作業：

```
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. 使用指[get-resource-shares](#) AWS CLI 令來判斷您組織的 ARN，方法是使用下列作業：

```
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 指令啟用資源共用 AWS RAM :

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

{
  "returnValue": true
}
```

您可以使用此指[list-aws-service-access-for-organization](#) AWS CLI 令來驗證 Organizations 清單的服務主體是否已啟用 License Manager，以及 AWS RAM：

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

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

**⚠ Important**

您的組織最多可能需 AWS RAM 要六個小時才能完成此作業。必須先完成此程序，才能繼續進行。

4. 使用指[associate-resource-share](#) AWS CLI 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 命令來驗證資源共用關聯的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
  }
]
}
```

## 編輯自我管理授權

您可以在自我管理的授權中編輯下列欄位的值：

- 自我管理授權名稱
- 描述
- 數量 <option>
- 執行授權類型限制

### 編輯自我管理授權

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

### 使用指令列編輯自我管理授權

- [update-license-configuration](#) (AWS CLI)
- [更新 LCM \( \) LicenseConfiguration](#) AWS Tools for PowerShell

## 停用自我管理授權

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，使用授權的 AMI 仍然可以啟動。不過，將不再追蹤授權使用數。

停用自我管理授權時，不得將其附加至任何執行中的執行個體。停用後，無法使用自我管理授權執行啟動。

### 停用自我管理授權

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格中，選擇自我管理授權。
3. 選取自我管理授權。
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)
- [更新 LCM \( \) LicenseConfiguration](#) AWS Tools for PowerShell

## 刪除自我管理授權

您必須先取消任何資源的關聯，才能刪除自我管理授權。如果您需要重新開始使用新的授權規則，可以刪除自我管理授權。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授權

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，以開啟授權詳細資料頁面。
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授權

- [delete-license-configuration](#) (AWS CLI)

- [移除程式 \(\) LicenseConfiguration](#) AWS Tools for PowerShell

## License Manager 中的授權規則

建立自我管理授權規則之後，可以將它們附加至相關的啟動機制，在此機制可以直接防止部署不符合規範的新資源。組織中的使用者可以從指定的 AMI 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 不參與軟件供應商的審計過程。客戶必須負責遵循法規，並負責根據其授權合約，仔細瞭解 License Manager 並將規則擷取到授權管理員中。

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。您可以定義使用限制和授權規則，License Manager 會追蹤部署，同時也會警示您違反規則。如果您已設定硬性限制，License Manager 可以防止資源啟動。

當追蹤的伺服器停止或終止時，其授權將釋出並返回可用授權集區。

由於組織在操作和合規方面有不同的方法，因此 License Manager 支援多種啟動機制：

- 手動將自我管理授權與 AMI 建立關聯 — 若要追蹤作業系統或其他軟體的授權，您可以在發佈 AMI 之前將授權規則附加至 AMI，以便在組織中更廣泛使用。然後，使用 License Manager 會自動追蹤來自這些 AMI 的任何部署，而不需要使用者執行任何其他動作。您也可以將授權規則附加到目前的 AMI 建置機制，例如 [Systems Manager 自動化](#)、[VM 匯入/匯出](#) 和 [封裝](#) 程式。
- Amazon EC2 啟動範本和 AWS CloudFormation — 如果將授權規則附加到 AMI 不是偏好選項，您可以在 [EC2 啟動範本或 AWS CloudFormation 範本](#) 中將它們指定為選用參數。使用這些範本的部署會使用 License Manager 追蹤。您可以在自我管理授權欄位中指定一或多個自我管理授權 ID，在 EC2 啟動 AWS CloudFormation 範本或範本上強制執行規則。

AWS 將授權追蹤資料視為只能透過擁有該資料的帳戶存取的敏感客 AWS 戶資料。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。

## 建立自我管理授權與 AMI 的關聯

以下程序示範如何使用 License Manager 主控台將自我管理授權與 AMI 建立關聯。此程序假設您至少擁有一個現有的自我管理授權。您可以將自我管理授權與您有權存取的任何 AMI 建立關聯，無論是擁

有的或共用的。如果已與您共用 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，還是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 AMI 的執行個體啟動情況。達到硬性限制時，License Manager 會封鎖其他執行個體啟動。達到軟限制時，License Manager 會通知您其他執行個體啟動。

如果您在相同區域內複製 AMI，且該 AMI 具有關聯的授權組態，則這些授權組態會自動與新的 AMI 產生關聯。當您從新 AMI 啟動執行個體時，License Manager 會追蹤它。同樣地，如果您從具有相關授權組態的執行中執行個體建立新的 AMI，則這些授權組態會自動與新 AMI 產生關聯，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。如果您將具有相關授權組態的 AMI 複製到不同的區域，License Manager 會封鎖從新 AMI 啟動的所有執行個體。

### 建立自我管理授權與 AMI 的關聯

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，以開啟授權詳細資料頁面。若要檢視目前關聯的 AMI，請選擇關聯的 AMI。
4. 選擇「關聯 AMI」。
5. 在可用的 AMI 中，選取一或多個 AMI，然後選擇「關聯」。
  - 如果您的帳戶擁有至少一個 AMI，系統會提示您為您擁有的 AMI 選擇 AMI 關聯範圍。與其他帳戶共享的任何 AMI 僅與您的帳戶相關聯。選擇確認。
  - 如果 AMI 是從其他帳戶與您共享的，則這些 AMI 僅與您的帳戶相關聯。

新關聯的 AMI 現在會顯示在授權詳細資料頁面的 [關聯的 AMI] 索引標籤上。

### 取消自我管理授權與 AMI 的關聯

以下程序示範如何使用 License Manager 主控台取消自我管理授權與 AMI 的關聯。您無法取消註冊 AMI 的關聯。License Manager 每 8 小時檢查一次已取消註冊的 AMI，並自動取消關聯。

## 取消自我管理授權與 AMI 的關聯

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，以開啟授權詳細資料頁面。
4. 選擇 Associated AMIs (關聯的 AMI)。
5. 選擇 AMI，然後選擇「取消關聯 AMI」。

## License Manager 中的使用報告

使用時，AWS License Manager 您可以透過排程授權使用量的定期快照來追蹤自我管理授權的歷史記錄。透過設定使用情況報告，License Manager 會根據您的規格，自動將自我管理授權的報告上傳到 S3 儲存貯體。使用情況報告先前稱為報告產生器。您可以設定多個使用情況報告，以有效地追蹤環境中不同授權類型的組態。

### Note

AWS License Manager 不會儲存您的報告。License Manager 報告會直接發佈到您的 S3 儲存貯體。刪除使用情況報告後，報告就不會再發佈到 S3 儲存貯體。

## 建立用量報告

當您建立使用情況報告時，您可以指定要追蹤 License Manager 的自我管理授權類型、定義產生報告頻率的頻率間隔，以及報告類型。所有報告會以 CSV 格式產生，並將報告發佈到 S3 儲存貯體。使用情況報告可以產生下列一或多種報告類型。

### 自行管理授權摘要報告

此報告類型包含已使用授權數目的資訊，以及有關自我管理授權的詳細資料。追蹤的自我管理授權類型會列出詳細資料，例如授權計數、授權規則，以及在不同資源類型之間的授權分佈。

### 資源使用報告

此報告類型為您提供有關追蹤資源及其授權使用的詳細資訊。使用指定的自我管理授權類型的每個追蹤資源都會列出詳細資料，例如授權 ID、資源狀態以及擁有該資源的 AWS 帳號 ID。

## 若要建立使用情況報告

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 從導覽面板中選擇「使用情況報告」。
3. 選擇「建立使用情況報告」，然後從「建立使用情況報表」窗格中定義報表的參數：
  - a. 輸入使用情況報告的「名稱」與選擇性「說明」。
  - b. 從下拉式清單中選取自我管理的授權類型。這是使用情況報告將用於產生資料的授權類型。
  - c. 選擇要產生的報告類型。
  - d. 選擇「License Manager」發佈報告的頻率，您可以選擇「每 24 小時一次」、「每 7 天一次」或「每 30 天一次」。
  - e. (選用) 新增標籤以追蹤使用情況報告資源。
4. 選取建立使用情況報告。

新的使用情況報告將在 60 分鐘內開始發行報告。

如果您還沒有與帳戶相關聯的 S3 儲存貯體，當您建立用量報告時，License Manager 會在您的帳戶中建立新的 Amazon S3 儲存貯體。如果您先前已啟用跨帳戶庫存搜尋報告，則在啟用跨帳戶庫存搜尋時，將傳送至 License Manager 建立的 S3 儲存貯體。

報告會以下列 Amazon S3 URI 模式存放在儲存貯體中：

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

## 編輯用量報告

您可以隨時從 License Manager 主控台檢視和變更使用情況報告。使用情況報告表格列出為您的帳戶建立的所有使用情況報告，您可以從表格中取得不同報告的概觀、轉向至與使用量報告相關聯的 Amazon S3 儲存貯體，以及檢視報告產生的狀態。

### 若要編輯使用情況報告

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 從導覽面板中選擇「使用情況報告」。
3. 從表格中選擇您要編輯的使用情況報告，然後選取檢視詳細資訊。

4. 選取「編輯」以變更使用情況報告。
5. 對使用情況報告進行所需的變更，然後選擇 [儲存變更]。

更新後的使用情況報告會在一小時內產生新的報告。

#### Note

變更使用報告的名稱會將 future 的報告傳送至 License Manager S3 儲存貯體中的新資料夾，反映新名稱。

## 刪除用量報告

刪除使用量報告會停止產生新報告，但是 Amazon S3 儲存貯體和所有先前的報告都不會受到影響。

#### Note

如果您的帳戶有相關聯的使用情況報告，您將無法刪除自我管理授權。您必須先刪除該用量報告。

若要編輯使用情況報告

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 從導覽面板中選擇「使用情況報告」。
3. 從表格中選擇您要編輯的使用情況報告，然後選取檢視詳細資訊。
4. 選取 Delete (刪除)。此動作會永久刪除使用情況報告。

## License Manager 中的授權類型轉換

使用 License Manager，您可以在 AWS 提供的授權與自攜授權模式 (BYOL) 或自攜訂閱模式 (BYOS) 之間變更您的授權類型，隨著業務需求的變更。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：

## 將現場部署工作負載遷移到 Amazon EC2

在移轉期間，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。移轉完成後，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 或 BYOS，以便使用在移轉期間發行的授權。

### 使用即將到期的授權合約繼續執行工作

您可以使用 License Manager 授權類型轉換，從 BYOL 或 BYOS 切換至提供的授權。AWS 此切換器可讓您使用靈活的 pay-as-you Go 授權模式提供的完全合規軟體授權，繼續執行工作負載。AWS 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，且您不打算續約，您可以選擇這樣做。

### 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 或 BYOS 時，這些選項可能需要較長期的承諾。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) 映像啟動的，您可以切換回 BYOL 或 BYOS。當工作負載更穩定或可預測時，您可以選擇這樣做。

### 延長維護

如果您的 Ubuntu 作業系統已達到標準支援的結束，您可以新增 Ubuntu Pro 的付費訂閱。將訂閱新增至 Ubuntu pro 可延長一段時間內提供安全性更新。如需詳細資訊，請參閱標準文件中的 [Ubuntu 專業版](#)。

### 主題

- [授權類型轉換的合格授權類型](#)
- [轉換先決條](#)
- [轉換授權類型](#)
- [租賃轉換](#)
- [排解授權類型轉換](#)

## 授權類型轉換的合格授權類型

您可以將 License Manager 授權類型轉換與支援的 Windows 伺服器和 Microsoft SQL Server 授權的版本和組合搭配使用。您也可以透過 Ubuntu 訂閱使用授權類型轉換。

## 內容

- [適用於視窗和 SQL 伺服器的合格授權類型](#)
  - [SQL Server 版本](#)
  - [SQL 伺服器版本](#)
  - [使用量操作值](#)
  - [媒體相容性](#)
  - [轉換路徑](#)
- [適用於 Linux 的合格訂閱類型](#)

## 適用於視窗和 SQL 伺服器的合格授權類型

### Important

最初從 Amazon 啟動的執行個體提供 Amazon 機器映像 (AMI) 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 伺服器版本](#)
- [使用量操作值](#)
- [媒體相容性](#)
- [轉換路徑](#)

## SQL Server 版本

License Manager 支援下列 SQL Server 版本：

- SQL 伺服器標準版
- SQL Server Enterprise Edition
- SQL 伺服器網頁版

## SQL 伺服器版本

License Manager 支援下列 SQL Server 版本：

- SQL 伺服器
- SQL 伺服器
- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019
- SQL 伺服器

## 使用量操作值

授權類型轉換會變更與執行個體相關聯的使用操作值。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](#)。

操作系統詳情	使用操作
視窗伺服器作為自攜裝置	RunInstances:0800
視窗伺服器作為自攜裝置	RunInstances:0800
SQL 伺服器 (任何版本) 做為自攜裝置	
Windows 服務器作為許可證包括	RunInstances:0002
Windows 服務器作為許可證包括	RunInstances:0002
SQL 伺服器 (任何版本) 做為自攜裝置	
Windows 服務器作為許可證包括	RunInstances:0202
SQL 伺服器網頁作為授權包含	
Windows 服務器作為許可證包括	RunInstances:0006
包含 SQL 伺服器標準作為授權	

操作系統詳情	使用操作
Windows 服務器作為許可證包括	RunInstances:0102
SQL 伺服器企業作為授權包含	

## 媒體相容性

下表確認哪些媒體可用於執行個體授權模式。

來源	目標	
	BYOL	包括許可證
AWS 提供視窗伺服器映像	否	是
AWS 提供的 SQL 伺服器映像	否	是
您的視窗伺服器媒體 <sup>1</sup>	是	是
您的 SQL 伺服器媒體 <sup>2</sup>	是	是

<sup>1</sup> 表示執行個體最初是從您自己匯入的虛擬機器 (VM) 啟動的。您可以使用虛擬機器匯入/[匯出或等服務來匯入虛擬機器AWS Application Migration Service](#)。

<sup>2</sup> 表示您已採購自己的 SQL 伺服器安裝媒體 (.iso、.exe)。

## 轉換路徑

下表確認在 BYOL 和包含的授權之間是否可以將來源授權模式轉換為另一種授權模式。如需詳細資訊，請參閱 [轉換授權類型](#)。

### Important

- 視窗伺服器做為包含 SQL 伺服器作為授權的 BYOL 是不受支援的組態。
- 指定為「不需要」的轉換不會變更使用量作業值。

來源	目標					
	視窗伺服器 作為自攜裝置	Windows 伺服器作為 許可證包括	視窗伺服器 作為自攜裝置	Windows 伺服器作為 許可證包括	視窗伺服器 作為自攜裝置	Windows 伺服器作為 許可證包括
			SQL 伺服器 做為自攜 裝置	SQL 伺服器 做為自攜 裝置	SQL 伺服器 做為授權 包含	SQL 伺服器 做為授權 包含
視窗伺服器 做為自攜裝置 (您的媒體)	不需要	是	不需要	是 <sup>1</sup>	不支援	是 <sup>1</sup>
Windows 伺服器作為 許可證包 含 ( 您的媒 體 )	是 <sup>2</sup>	不需要	是	不需要 <sup>3</sup>	不支援	是 <sup>1</sup>
Windows 伺服器作為 許可證包括 ( AWS 提 供的圖像 )	沒有 x	不需要	沒有 x	不需要 <sup>3</sup>	不支援	是 <sup>1</sup>
視窗伺服器 做為自攜裝置 (您的媒 體)	不需要 <sup>4</sup>	是	不需要	是	不支援	是
SQL 伺服器 做為自攜 裝置 (您的 媒體)						
Windows 伺服器作為	是 <sup>2</sup>	不需要 <sup>4</sup>	是 <sup>2</sup>	不需要	不支援	是

來源	目標					
許可證包 含 ( 您的媒 體 )						
SQL 伺服 器做為自攜 裝置 (您的 媒體)						
Windows 服務器作為 許可證包括 ( AWS 提 供的圖像 )	沒有 <i>x</i>	不需要 <sup>4</sup>	沒有 <i>x</i>	不需要	不支援	是
SQL 伺服 器做為自攜 裝置 (您的 媒體)						
視窗伺服器 做為自攜裝 置 (您的媒 體)	不支援	不支援	不支援	不支援	不支援	不支援
SQL 伺服 器作為授權 包含						

來源	目標						
Windows 服務器作為許可證包括 ( AWS 提供的圖像或您的媒體 )	沒有 x	沒有 x	沒有 x	沒有 x	不支援	不需要	
SQL 伺服器作為授權包含 (AWS 提供的影像)							
Windows 服務器作為許可證包含 ( 您的媒體 )	是	是 <sup>5</sup>	是 <sup>2</sup>	是	不支援	不需要	
SQL 伺服器作為授權包含 (您的媒體)							
Windows 服務器作為許可證包括 ( AWS 提供的圖像 )	沒有 x	是 <sup>5</sup>	沒有 x	是	不支援	不需要	
SQL 伺服器作為授權包含 (您的媒體)							

x 您必須部署具有替代組態的新執行個體，因為不支援轉換為目標授權類型。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 伺服器，然後才能轉換為 SQL 伺服器的 BYOL。
- <sup>2</sup> 您必須先修改 Windows 組態，才能使用自己的 KMS 伺服器進行授權啟用。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 的目標時 (無論 SQL Server 授權類型為何)，您都必須先安裝 SQL Server。
- <sup>4</sup> 當您從具有 SQL Server 的來源轉換為不含 SQL 伺服器的目標時 (無論 SQL Server 授權類型為何)，您必須先解除安裝 SQL Server。
- <sup>5</sup> 您必須先解除安裝 SQL 伺服器，才能轉換為包含授權的 SQL 伺服器。
- <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 Windows 伺服器作為包含的授權，然後再次將授權類型轉換為 Windows 伺服器做為 BYOL。

## 適用於 Linux 的合格訂閱類型

許可證類型轉換可用於支持的 Ubuntu 版本。支持的版本包括更新，如 Ubuntu 18.04.1 LTS。當您將訂閱轉換為 Ubuntu Pro 時，會額外提供五年的安全性更新。如需詳細資訊，請參閱標準文件中的 [Ubuntu 專業版](#)。

您可以在以下 Ubuntu 版本中使用許可證類型轉換：

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

操作系統詳情	使用操作
Linux/UNIX	RunInstances
Ubuntu Pro	RunInstances : 0 克

## 轉換路徑

您可以將任何受支持的版本轉換為 Ubuntu 專業版。如果您需要從 Ubuntu 專業版轉換為 Ubuntu LTS，您將需要提出一個請求 AWS Support。如需詳細資訊，請參閱[建立支援案例](#)。

## 轉換先決條

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

在執行授權類型轉換之前，您必須符合下列一般先決條件：

- 您 AWS 帳戶 必須加入 License Manager。請參閱[開始使用 AWS License Manager](#)。
- 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和啟動執行個體](#)。
- 如果在目標執行個體上啟用了停止保護，轉換程序將會失敗。如需詳細資訊，請參閱[排解授權類型轉換](#)。
- 目標執行個體必須設定為「AWS Systems Manager 庫存」。如需詳細資訊，請參閱[AWS Systems Manager 使用者指南中的 EC2 執行個體和 AWS Systems Manager 庫存設定 Systems Manager](#)。
- 您的使用者或角色必須具有下列權限：
  - `ssm:GetInventory`
  - `ssm:StartAutomationExecution`
  - `ssm:GetAutomationExecution`
  - `ssm:SendCommand`
  - `ssm:GetCommandInvocation`
  - `ssm:DescribeInstanceInformation`
  - `ec2:DescribeImages`
  - `ec2:DescribeInstances`

- `ec2:StartInstances`
- `ec2:StopInstances`
- `license-manager:CreateLicenseConversionTaskForResource`
- `license-manager:GetLicenseConversionTask`
- `license-manager:ListLicenseConversionTasks`
- `license-manager:GetLicenseConfiguration`
- `license-manager:ListUsageForLicenseConfiguration`
- `license-manager:ListLicenseSpecificationsForResource`
- `license-manager:ListAssociationsForLicenseConfiguration`
- `license-manager:ListLicenseConfigurations`

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 啟動的執行個體提供 Amazon 機器映像 (AMI) 不符合將授權類型轉換為 BYOL 的資格。原始 Amazon EC2 執行個體必須從您自己的虛擬機器 (VM) 映像啟動。如需將虛擬機器轉換為 Amazon EC2 的詳細資訊，請參閱[虛擬機器匯入/匯出](#)。
- 若要將您的 SQL 伺服器授權變更為 BYOL，必須使用您自己的媒體來安裝 SQL Server。

## Linux

Linux 執行個體必須符合下列先決條件：

- 執行個體必須執行 Ubuntu LTS。
- Ubuntu 專業版用戶端必須安裝在您的 Ubuntu 作業系統中。
  - 執行下列命令以確認是否已安裝 Ubuntu 專業版用戶端：

```
pro --version
```

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

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

- 執行個體必須能夠連線到多個端點，才能啟用其 Ubuntu Pro 訂閱並接收更新。您必須允許執行個體透過 TCP 連接埠 443 傳出的輸出流量才能連接下列端點：
  - 合同. 卡尼卡爾-用於 Ubuntu 專業版激活。
  - 互聯網-用於大多數服務的 APT 存儲庫訪問。
  - 卡扣 — 用於安裝和運行卡扣。
  - 儀表板-用於安裝和運行快照。
  - 登入 — 用於安裝和執行快照。
  - 雲前鋒網站 — 用於從內容開發網絡下載 (CDN).
  - 生活修補程式 — 用於下載修補程式從服務器。

如需詳細資訊，請參閱 [Ubuntu 專業版用戶端](#) 文件中的 [Ubuntu 專業用戶端網路需求](#) 和規範快照文件中的網路需求。

## 轉換授權類型

您可以使用 License Manager 主控台或轉換視窗授權、Microsoft SQL 伺服器授權和 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計費產品。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 指令來檢查授權類型轉換的狀態。

License Manager 可能會在授權類型轉換過程中更新與您自我管理授權相關聯的資源。具體來說，對於任何具有自動探索規則類型為類型的自我管理授權 `License Included`，如果 `license included` 自動化探索規則明確排除資源，License Manager 會將授權類型轉換中的資源與授權取消關聯。

例如，如果您的自我管理授權包含兩個自動探索規則，且每個規則不包含授權的 Windows Server，則從 BYOL 轉換為授權的授權類型會導致解除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` 則，則該執行個體不會取消關聯。

您不應在授權類型轉換過程中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 `IN_PROGRESS` 為 `SUCCEEDED`。如果 License Manager 在工作流程中遇到問題，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

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，如果您有從 AMI 搜尋帳單資訊的現有工作流程，請更新要使用 `DescribeInstances` 的工作流程。

## 內容

- [轉換視窗和 SQL 伺服器的授權類型](#)
  - [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](#)
- [轉換 Linux 的授權類型](#)
  - [授權類型轉換考量](#)
  - [使用 License Manager 主控台轉換授權類型](#)
  - [使用轉換授權類型 AWS CLI](#)
  - [移除訂閱](#)

## 轉換視窗和 SQL 伺服器的授權類型

您可以使用 License Manager 主控台或 AWS CLI 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 軟件的使用受 Microsoft 的許可條款約束。貴用戶必須負責遵守 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 軟體的授權權限有任何疑問，請洽詢您的法律團隊、Microsoft 或您的 Microsoft 經銷商。

License Manager 會限制您可以根據 Microsoft 服務提供者授權合約 (SPLA) 建立的授權轉換類型。授權類型轉換所受限制的一些限制如下所示。這不是一份完整的清單，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 伺服器執行個體必須至少有 4 個 vCPUs。

### 使用 License Manager 主控台轉換授權類型

您可以使用 License Manager 主控台轉換授權類型。

#### Note

只會顯示處於停止狀態且已與「AWS Systems Manager 詳細目錄」相關聯的執行處理。

### 在主控台中開始授權類型轉換

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格中，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：
  1. Ubuntu LTS
  2. 視窗自攜
  3. 包含視窗授權
4. (選擇性) 指定「執行個體 ID」或「使用量」作業值的值，以篩選可用的執行個體。
5. 選取您要轉換授權的執行個體，然後選擇 [下一步]。
6. 輸入授權類型的 [使用] 作業值，選取要轉換的授權，然後選擇 [下一步]。
7. 確認您對授權類型轉換組態滿意，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 伺服器從包含的授權轉換為 BYOL，您必須根據您的 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. 請確認您已安裝並設定 AWS CLI。如需詳細資訊，請參閱[安裝、更新 AWS CLI 和解除安裝 AWS CLI](#)。

**⚠ Important**

您可能需要更新才能執行 AWS CLI 行某些命令，並在下列步驟中接收所有必要的輸出。

2. 請確認您具有執行 `create-license-conversion-task-for-resource` AWS CLI 命令的權限。如需此說明，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 取代為您要決定其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}"
```

4. 以下是對 `describe-instances` 指令的範例回應。請注意，該 `UsageOperation` 值是與授權相關聯的帳單資訊代碼。 `UsageOperationUpdateTime` 這是計費代碼更新的時間。如需詳細資訊，請參閱[DescribeInstances](#) 亞 Amazon EC2 API 參考資料中的。

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

**Note**

搭配 SQL 伺服器企業 BYOL 的 Windows 伺服器使用量作業與視窗 BYOL 的使用量作業相同，因為它們的計費方式相同。

## 將 Windows 伺服器從包含的授權轉換為 BYOL

當您將 Windows 伺服器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。如需將虛擬機器轉換為 Amazon EC2 的詳細資訊，請參閱[虛擬機器匯入/匯出](#)。最初從 Amazon 機器映像 (AMI) 啟動的執行個體不符合將授權轉換為 BYOL 的資格。

檢查您的 Microsoft 許可協議，以確定您可以使用哪些方法來激活 Microsoft Windows 服務器。例如，如果您使用 KMS 伺服器，則必須從執行個體的原始 BYOL 組態取得 KMS 伺服器的位址。

1. 若要轉換執行個體的授權類型，請執行下列命令，將 ARN 取代為您要轉換的執行個體的 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. 若要在轉換授權之後啟用 Windows，您必須將作業系統的 Windows 伺服器 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>
```

## 將視窗伺服器從 BYOL 轉換為包含的授權

當您將 Windows 伺服器從 BYOL 轉換為包含的授權時，License Manager 會自動將執行個體的 KMS 伺服器切換至 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，並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
```

將視窗伺服器和 SQL 伺服器從 BYOL 轉換為包含的授權

您可以同時切換多個產品。例如，您可以在一次授權類型轉換中轉換 Windows 伺服器和 SQL 伺服器。

若要將 Windows 伺服器執行個體的授權類型從 BYOL 轉換為包含的授權，並將 SQL Server 標準從 BYOL 轉換為包含的授權，請執行下列命令，並以您要轉換的執行個體的 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
```

## 轉換 Linux 的授權類型

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

### 主題

- [授權類型轉換考量](#)
- [使用 License Manager 主控台轉換授權類型](#)
- [使用轉換授權類型 AWS CLI](#)
- [移除訂閱](#)

### 授權類型轉換考量

授權類型轉換的一些注意事項如下所示。這不是一份完整的清單，可能會有所變更。

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

- 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，我們建議您使用 Ubuntu Pro 搭配 Savings Plans。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[什麼是 Savings Plans ?](#) 於「S avings Plans 用戶指南」內。

## 使用 License Manager 主控台轉換授權類型

您可以使用 License Manager 主控台轉換授權類型。

### Note

只會顯示處於停止狀態且已與「AWS Systems Manager 詳細目錄」相關聯的執行處理。

## 在主控台中開始授權類型轉換

1. 開啟 License Manager 主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
2. 在左側導覽窗格中，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：
  1. Ubuntu LTS
  2. 視窗自攜
  3. 包含視窗授權
4. (選擇性) 指定「執行個體 ID」或「使用量」作業值的值，以篩選可用的執行個體。
5. 選取您要轉換授權的執行個體，然後選擇 [下一步]。
6. 輸入授權類型的 [使用] 作業值，選取要轉換的授權，然後選擇 [下一步]。
7. 確認您對授權類型轉換組態滿意，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，以變更為所需的訂閱。如需有關合格訂閱類型的詳細資訊，請參閱[適用於 Linux 的合格訂閱類型](#)。

## 判斷執行個體的授權類型

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

### ⚠ Important

您可能需要更新才能執行 AWS CLI 行某些命令，並在下列步驟中接收所有必要的輸出。請確認您具有執行 `create-license-conversion-task-for-resource` AWS CLI 命令的權限。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 取代為您要決定其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}"
```

以下是對 `describe-instances` 指令的範例回應。UsageOperation 值是與授權相關聯的帳單資訊代碼。的使用操作值 `RunInstances` 表示執行個體正在使用 AWS 提供的授權。UsageOperationUpdateTime 這是計費代碼更新的時間。如需詳細資訊，請參閱亞 Amazon EC2 API 參考 [DescribeInstances](#) 中的。

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

## 轉換為

當您將執行個體從 Ubuntu LTS 轉換為 Ubuntu Pro 時，您必須擁有來自執行個體的輸出網際網路存取權，才能從標準伺服器擷取授權權杖，並安裝 Ubuntu Pro 用戶端。如需詳細資訊，請參閱 [轉換先決條件](#)。

要將 LTS 轉換為 Ubuntu 專業版：

1. 在指定執行個體的 ARN AWS CLI 時，從執行下列命令：

```
aws license-manager create-license-conversion-task-for-resource \  
--resource-arn <instance_arn> \  

```

```
--source-license-context UsageOperation=RunInstances \
--destination-license-context UsageOperation=RunInstances:0g00
```

2. 在執行個體內執行下列命令，以擷取有關 Ubuntu Pro 訂閱狀態的詳細資料：

```
pro status
```

3. 確認輸出結果表示執行個體擁有有效的 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
```

## 移除訂閱

許可證類型轉換只能用於從 Ubuntu LTS 轉換為 Ubuntu 專業版。如果您需要從 Ubuntu 專業版轉換為 Ubuntu LTS，您將需要提出一個請求 AWS Support。如需詳細資訊，請參閱[建立支援案例](#)。

## 租賃轉換

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[修改執行個體放置](#) AWS CLI 指令在下列租用期間切換：

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

您的帳戶必須擁有具有可用容量的專用主機才能啟動執行個體，才能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 彈性運算雲端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，執行個體必須擁有與主機資源群組相關聯的同一組授權。如需詳細資訊，請參閱 [主機資源群組AWS License Manager](#)。

## 租賃轉換限制

以下限制適用於租賃轉換：

- 所有租賃類型都允許使用 Linux 帳單代碼。
- 共用租用不允許使用 Windows BYOL 帳單代碼。
- 所有租用類型都允許使用 Windows 伺服器授權包含的計費代碼。
- 共用租用和專用執行個體允許所有支援的 SQL Server 版本、紅帽 (RHEL) 和 SUSE (SLES) 授權包含帳單代碼。但是，專用主機和主機資源群組不允許使用這些帳單代碼。
- 在專用主機和主機資源群組上，不允許包含 Windows Server 以外的授權計費代碼。

## 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
```

若要將執行個體從任何租用變更為具有自動放置功能的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host租用變更為租用，請執行下列命令：

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

## 排解授權類型轉換

### 故障診斷主題

- [視窗啟動](#)
- [執行個體 \[執行個體\] 是從 Amazon 擁有的 AMI 啟動的。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 啟動的。確定 SSM 代理程式在您的執行個體上執行。](#)
- [呼叫CreateLicenseConversionTaskForResource作業時發生錯誤 \(InvalidParameterValueException\)：ResourceId -\[執行個體\] 變更授權類型的狀態無效。](#)
- [EC2 實例 \[實例\] 無法停止。確保您擁有 EC2 的許可 StopInstances。](#)

### 視窗啟動

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 轉換為包含的授權時，會成功更新執行個體上的計費產品。不過，KMS 伺服器可能不會切換到 AWS KMS 伺服器。

若要修正此問題，請依照[為什麼 EC2 Windows 執行個體上的 Windows 啟用失敗？](#) 使用 Systems Manager [AWSSupport-ActivateWindowsWithAmazonLicense](#) 自動化執行手冊啟用 Windows，或登入執行個體並手動切換至 AWS KMS 伺服器。

[執行個體 \[執行個體\]](#) 是從 Amazon 擁有的 AMI 啟動的。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帶授權模式 (BYOL)。最初從亞馬遜擁有的 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 [轉換先決條](#)。

無法驗證該執行個體 [執行個體] 是從 BYOL AMI 啟動的。確定 SSM 代理程式在您的執行個體上執行。

若要順利轉換授權類型，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) 會從您的執行個體收集清查，其中包含作業系統的詳細資料。如需詳細資訊，請參閱AWS Systems Manager 使用[指南中的檢查 SSM 代理程式狀態和啟動代理程式](#)和 [SSM 代理程式疑難排解](#)。

呼叫**CreateLicenseConversionTaskForResource**作業時發生錯誤 (InvalidParameterValueException)：ResourceId -[執行個體] 變更授權類型的狀態無效。

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 彈性運算雲端使用者指南中的[停止執行個體轉換先決條件和疑難排解](#)。

**EC2 實例 [實例] 無法停止。確保您擁有 EC2 的許可 StopInstances。**

您必須擁有在目標執行StopInstances個體上執行 EC2 API 動作的許可。此外，如果在目標執行個體上啟用了停止保護，轉換程序將會失敗。如需詳細資訊，請參閱 Amazon 彈性運算雲端使用者指南中的[停用執行中或已停止執行個體的停止保護](#)。

## 主機資源群組AWS License Manager

Amazon EC2 專用執行個體是具有專供您使用之 EC2 執行個體容量的實體伺服器。主機資源群組是一組專用主機集合，您可將它視為單一實體管理的專用主機集合。當您啟動執行個體時，License Manager 會根據您設定的設定來配置主機並在其上啟動執行個體。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的優勢。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按用途分隔主機，例如，開發測試主機與生產、組織單位或授權限制。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：

- 自動分配主機 — 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主機。

- 自動釋放主機 — 指出 Amazon EC2 是否可以代表您釋放未使用的主機。未使用的主機沒有執行個體。
- 自動復原主機 — 指出 Amazon EC2 是否可以將執行個體從意外故障的主機移至新主機。
- 關聯的自我管理授權 — 可用於在此主機資源群組中啟動執行個體的自我管理授權。
- (選擇性) 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-based](#) 執行個體，則可以在相同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，您必須只啟動相同主機資源群組中具有相同執行個體類型的執行個體。

## 內容

- [建立主機資源群組](#)
- [共用主機資源群組](#)
- [將專用主機新增至主機資源群組](#)
- [在主機資源群組中啟動執行個體](#)
- [修改主機資源群組](#)
- [從主機資源群組移除專用主機](#)
- [刪除主機資源群組](#)

## 建立主機資源群組

設定主機資源群組，以啟用 License Manager 來管理您的專用主機。為了充分利用最昂貴的授權，您可以將一或多個以核心或插槽為基礎的自我管理授權與主機資源群組建立關聯。為了最佳化主機使用率，您可以允許主機資源群組中的所有核心或插槽型自我管理授權。

### 建立主機資源群組

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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. 對於主機資源群組詳細資訊，請指定主機資源群組的名稱和說明。
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：
  - 自動分配主機
  - 自動釋放主機

- 自動復原主機
6. (選擇性) 對於其他設定，請選取可在主機資源群組中啟動的執行個體系列。
  7. 對於自我管理授權，請選取一或多個以核心或套接字為基礎的自我管理授權。
  8. (選用) 對於標籤，新增一或多個標籤。
  9. 選擇 **建立**。

## 共用主機資源群組

您可以透過以AWS Resource Access Manager下方式使用共用主機資源群組AWS Organizations。共用主機資源群組和自我管理授權後，成員帳戶可以在共用主機資源群組中啟動執行個體。新主機會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](#)。

## 將專用主機新增至主機資源群組

您可以從AWS Management Console、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的AWS帳戶擁有者。如果您的主機資源群組列出了允許的自我管理授權和執行個體類型，則您新增的主機必須符合這些需求。

### Note

假設您停止執行個體並想要重新啟動它們。您必須執行下列兩項工作：

- [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。

如需有關 Resource Groups 的詳細資訊，請參閱[AWS Resource Groups使用者指南](#)。

請遵循下列步驟，將一或多台專用主機新增至資源群組：

1. 登入 License Manager 主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
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 Add (新增)。

6. 選擇一或多個要新增至主機資源群組的專用主機。
7. 選擇 Add (新增)。

新增主機可能需要 1-2 分鐘的時間，然後它就會出現在專用主機清單中。

## 在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[執行個體](#)命令。您必須將以核心或通訊端為基礎的自行管理授權與 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[將執行個體啟動至主機資源群組](#)。

## 修改主機資源群組

您可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目。如果主機資源群組中有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. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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)。

## 從主機資源群組移除專用主機

從主機資源群組移除主機時，主機上執行的執行個體仍保留在主機上。連結至主機資源群組的執行個體會與群組保持關聯，而透過相似性直接連結至主機的執行個體則維持相同的屬性。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，且取用者會收到驅逐通知，在 15 天內將其執行個體從主機移出。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](#)。

請遵循下列步驟將專用主機移除至主機資源群組：

1. 登入 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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搜尋專用主機。
6. 選擇 Remove (移除)。
7. 再次選擇「移除」以確認。

## 刪除主機資源群組

如果主機資源群組沒有主機，您可以刪除該群組。

### 刪除主機資源群組

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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)。

## 在 License Manager 中搜尋庫存

License Manager 可讓您使用 [Systems Manager 詳細目錄](#) 探索內部部署應用程式，然後將授權規則附加至這些應用程式。將授權規則附加至這些伺服器後，您可以在 [License Manager] 儀表中追蹤這些規則以及您的 AWS 伺服器。

但是，License Manager 無法在啟動或終止時驗證這些伺服器的授權規則。若要保留非AWS 伺服器的相關資訊 up-to-date，您必須使用 License Manager 主控台的 [詳細目錄] 搜尋區段定期重新整理庫存資訊。

Systems Manager 會將資料儲存在其「庫存」資料中 30 天。在此期間，License Manager 會將代管執行個體計為作用中執行個體，即使該執行個體不可執行 Ping 從系統管理員清除庫存資料之後，License Manager 會將執行個體標示為非作用中，並更新本機庫存資料。為了保持代管執行個體計數的正確

性，建議您在 Systems Manager 中手動取消註冊執行個體，以便 License Manager 可以執行清除作業。

查詢 Systems Manager 庫存需要使用資源資料同步將庫存存放在 Amazon S3 儲存貯體中，Amazon Athena 才能彙總組織帳戶的庫存資料，並 AWS Glue 提供快速的查詢體驗。如需詳細資訊，請參閱 [使用 AWS License Manager 的服務連結角色](#)。

如果您的組織不限制使用 AWS 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，則資源庫存追蹤也很有用。License Manager 提供一種機制，可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

- [使用庫存搜尋](#)
- [自動探索庫存](#)

## 使用庫存搜尋

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

## 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授權](#)
- [將自我管理授權與庫存搜尋產生關聯](#)
- [取消自我管理授權與資源的關聯](#)

## 設定庫存搜尋

使用資源庫存搜尋之前，請先完成下列需求：

- 將 License Manager 與您的帳戶整合，以啟用跨 AWS Organizations 帳戶庫存探索。如需詳細資訊，請參閱 [中的設定AWS License Manager](#)。
- 為要管理的伺服器和應用程式建立自我管理的授權。例如，建立一個自我管理的授權，以反映您與 Microsoft 適用於 SQL Server 企業的授權合約條款。

## 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，不適用於「SQL Server Web」的授權) 來搜尋應用程式。

### 搜尋您的資源庫存

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在功能窗格中，選擇 [庫存搜尋]。
3. (選擇性) 您可以指定篩選選項以簡化搜尋結果，如下所示。

### Amazon EC2 資源

篩選器名稱	描述	邏輯運算子	支援的值
資源 ID	資源的 ID。	Equals, Not equals	
帳戶 ID	擁有資源之 AWS 帳號的識別碼。	Equals, Not equals	
平台名稱	資源的作業系統平台。	Equals, Not equals, Begins with, Contains	
應用程式名稱	應用程式名稱。	Equals, Begins with	
包含授權名稱	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> </ul>

篩選器名稱	描述	邏輯運算子	支援的值
			<ul style="list-style-type: none"> <li>Windows Server Datacenter</li> </ul>
Tag	<p>指派給資源的中繼資料標籤鍵和選用值。</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	描述	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	描述	邏輯運算子	支援的值
授權套件 (僅限 Oracle 管理系統)	與亞馬遜 RDS 適用甲骨文授權相關聯的管理組件。	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>

如需有關 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 授權選項或適用於 Db2 的 RDS 授權選項](#)。

## 將自動探索規則新增至自我管理授權

將產品資訊新增至自我管理的授權後，License Manager 可以追蹤已安裝這些產品之執行個體的授權使用情況。如需詳細資訊，請參閱 [自動探索庫存](#)。

### 將自動探索規則新增至自我管理授權

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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. 對於自我管理授權，請選取自我管理授權。

5. 指定要探索和追蹤的產品。
6. (選擇性) 選取解除安裝軟體時停止追蹤執行個體，以便在 License Manager 偵測到已解除安裝軟體且已經過任何授權相似性期間後，使授權可供重複使用。
7. (選擇性) 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 ( 例如適用於甲骨文的 RDS 和適用於 Db2 的 RDS ) 。

- a. 選擇要篩選的屬性，目前支援帳號 ID 和標籤。
  - b. 輸入資訊以識別該屬性。對於帳戶 ID，請指定 12 位數的「AWS 帳戶 ID」作為值。對於「標籤」，請輸入鍵/值配對。
  - c. 重複步驟 7 以新增其他規則。
8. 選擇新增。

## 將自我管理授權與庫存搜尋產生關聯

確定需要管理的未受管理資源後，您可以手動將它們與自我管理的授權建立關聯，而不是使用自動探索。

### 將自我管理授權與資源建立關聯

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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. 對於自我管理的授權名稱，請選取自我管理授權。
5. (選擇性) 選取 [與我的所有成員帳戶共用自我管理授權]。
6. 選擇關聯。

## 取消自我管理授權與資源的關聯

如果軟體廠商的授權條款有所變更，您可以取消手動關聯資源的關聯，然後刪除自我管理授權。

## 取消自我管理授權與資源關聯的步驟

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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. 選取要取消與自我管理授權關聯的每個資源，然後選擇「取消關聯資源」。

## 自動探索庫存

License Manager 使用 [Systems Manager 庫存](#) 來探索 Amazon EC2 執行個體和現場部署執行個體的軟體使用。您可以將產品資訊新增至您的自我管理授權，License Manager 會追蹤已安裝這些產品的執行個體。此外，您可以根據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 帳號 ID 或與資源標籤相關聯的執行個體，不被視為自動探索。

自動探索可新增至新的授權集、現有的自我管理授權或詳細目錄中的資源。您可以使用 [UpdateLicenseConfiguration](#) API 命令隨時透過 CLI 編輯自動探索的規則。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授權。

若要使用自動探索，您必須將產品資訊新增至您的自我管理授權。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所追蹤執行個體的關聯性。根據預設，在解除安裝軟體後，自動探索不會取消追蹤執行個體的關聯。您可以設定自動化探索，以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] 儀表板追蹤授權使用情況。

### 必要條件

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

#### 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。

若要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 [建立自我管理授權](#)。

### 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，您也可以透過選取資源 ID 並選取 [新增自動探索規則]，從 [詳細目錄] 搜尋窗格執行此操作。

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，以開啟授權詳細資料頁面。
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。
6. (選擇性) 選取解除安裝軟體時停止追蹤執行個體，以便在 License Manager 偵測到已解除安裝軟體且已經過任何授權相似性期間後，使授權可供重複使用。
7. (選擇性) 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 和適用於 Db2 的亞馬遜 RDS)。
- 排除規則只有在 [Cross-account resource discovery \(跨帳戶資源探索\)](#) 已啟用的情況下才可用。

- a. 選擇要篩選的屬性，目前支援帳號 ID 和標籤。
  - b. 輸入資訊以識別該屬性。對於帳戶 ID，請指定 12 位數的 AWS 帳戶 ID 作為值。對於「標籤」，請輸入鍵/值配對。
  - c. 重複步驟 7 以新增其他規則。
8. 完成後，選擇 [新增] 以套用自動探索規則。

## 授與 License Manager 中的授權

授權是您的組織的授權 [AWS Marketplace](#)，或直接向將其軟體與受管 [AWSData Exchange](#) 權整合的賣方，或直接向將其軟體與受管理權整合的賣方。授權管理員可以用AWS License Manager來管理這些授權的使用，以及將使用權 (稱為權利) 散發給特定AWS帳戶。

分發至 Data Exchange 產品的AWS資料授權可透過「AWSData Exchange」提供給AWS帳戶。您必須先啟用訂閱共用AWS Marketplace，才能發佈授權。如需詳細資訊，請參閱[在組織中共用訂閱](#)。

授權管理員將權利從AWS Marketplace授權分配至AWS帳戶，且收件者接受並啟用授與的授權後，該訂閱即可透過AWS Marketplace以下方式使用該AWS帳戶。帳戶也可以存取產品的存取權。例如，如果授權管理員從您的帳戶購買 Amazon 機器映像 (AMI)，AWS Marketplace並將權利分配到您的AWS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](#)
- [管理您授予的授權](#)
- [分發權利](#)
- [授予接受和激活](#)
- [授權狀態](#)
- [買家帳戶的指標](#)

## 檢視您授予的授權

License Manager 會顯示索引標籤，以根據您驗證的權限來檢視和管理授與的授權。授與的授權頁面可以顯示下列索引標籤：

### 我的授權

此標籤適用於任何有權在 License Manager 中檢視授與授權之授權的使用者。此索引標籤包含 [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]。您可以從此頁面檢視有關每個授權的其他資訊。

### 授權摘要 (針對組織管理員)

此標籤僅供組織管理員使用。此索引標籤包含「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總數。它也會顯示「產品」區段，其中包含詳細說明每個產品屬性的表格，例如「產品名稱」和「授與的授權數目」。

## 彙總授權 (適用於組織管理員)

此標籤僅供組織管理員使用。此索引標籤有一個章節，詳細說明為我的組織授予的授權，其中包括有關每個授權的資訊，例如授權 ID 和產品名稱。您可以從此頁面檢視有關每個授權的其他資訊。

## 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。收件者必須先接受並啟用授與的授權，才能使用產品。您接受和啟用授權的方式取決於授權是否來源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了所有功能。

授與的授權需要跨區域複寫授權中繼資料。License Manager 會自動將每個授與的授權及其相關資訊複製到其他AWS 區域授權。這可讓您在授予授權給您的所有區域中集中檢視。

### 授權AWS Marketplace與 AWS Data Exchange

- 系統會自動接受並啟用您所購買訂閱的授權。
- 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配給成員帳戶，則會自動在成員帳戶中接受授權。管理帳戶或成員帳戶之後都可以啟用授權。
- 如果僅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配給成員帳戶，則每個成員帳戶都必須接受並啟用授權。

### 賣家的授權

- 您必須接受並啟用使用 License Manager 來散佈授權的產品的授權。
- 如果已啟用所有功能的組織的管理帳戶購買了產品並將授權分配給成員帳戶，則會自動在成員帳戶中接受授權。管理帳戶或成員帳戶之後都可以啟用授權。
- 如果僅啟用合併帳單功能的組織的管理帳戶購買了產品並將授權分配給成員帳戶，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授與的授權AWS 帳戶。

#### 管理您帳戶中授予的授權

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。

2. 在導覽窗格中，選擇授權授權。
3. 選擇 [我的授權] 索引標籤，如果它不是目前的選項。
4. (選用) 使用以下所顯示授權的清單範圍，來限定所顯示授權的清單範圍。
  - 產品 SKU — 此授權的產品識別碼，由授權簽發者在建立授權時所定義。相同的產品 SKU 可能存在於多個 ISV 中。
  - 「收件者」 — 授權接受者的 ARN。
  - Sending — 授權的狀態。例如，可用。
5. 若要檢視有關授權的其他資訊，請選擇授權 ID 以開啟 [授權概觀] 頁面。
6. 如果授權簽發者是其他實體AWS Marketplace，則初始授權狀態為「等待接受」。執行下列任意一項：
  - 選擇接受並激活許可證。產生的授權狀態為「作用中」。
  - 選擇 [接受授權]。產生的授權狀態為 [已停用]。當您準備好使用授權時，請選擇 [啟用授權]。
  - 選擇 [拒絕授權]。產生的授權狀態為「已拒絕」。拒絕授權後，您將無法啟用它。

如果您不想繼續使用已啟動的授權，可以返回 [授權概觀] 頁面並選擇 [停用授權]。如果您要繼續使用已停用的授權，請返回 [授權概觀] 頁面並選擇 [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授權。

### Important

若要針對授與的授權使用組織的全視圖，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[中的設定AWS License Manager](#)。

若要管理所有帳戶中授予的授權 AWS Organizations

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在導覽窗格中，選擇授權授權。
3. 選擇 [彙總授權] 索引標籤 (如果它不是目前的選取項目)。
4. (選用) 使用以下所顯示授權的清單範圍，來限定所顯示授權的清單範圍。

- 產品 SKU — 此授權的產品識別碼，由授權簽發者在建立授權時所定義。相同的產品 SKU 可能存在於多個 ISV 中。
  - 受益人 — 您組織中授予授權的帳戶。
5. 若要檢視有關授權的其他資訊，請選擇授權 ID 以開啟授權詳細資料頁面。
  6. 如果授權發行者不是以外的實體AWS Marketplace，請執行下列任一項：
    - 選擇 [啟用授權]。產生的授權狀態為「作用中」。
    - 選擇 [停用授權]。產生的授權狀態為 [停用]。

如果您不想繼續使用已啟動的授權，可以返回 [授權概觀] 頁面並選擇 [停用授權]。如果您要繼續使用已停用的授權，請返回 [授權概觀] 頁面並選擇 [啟用授權]。

## AWS CLI

您可以使用授與AWS CLI的授權搭配使用。

要使用以下命令管理您授予的許可證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](#)

## 分發權利

如果您是在組織的管理帳戶中操作且已啟用[所有功能](#)的授權管理員，您可以透過建立授權，將權利從授與的授權分配給您的組織。如需詳細資訊AWS Organizations，請參閱[AWS Organizations術語和概念](#)。

您可以指定授權的接收方為下列其中一個：

- 一個AWS 帳戶，只包含指定的帳戶。

- 組織根目錄，包含組織中的所有帳戶。
- 組織單位 (OU)，包含指定 OU 下的所有帳戶。

#### Note

每個授權最多可以建立 2,000 個授權。

您可以使用AWS License Manager控制台或分AWS CLI發您的權利。您可以在主控台中建立授權時指定組織 ID 或組織 ARN，但 ARN 格式必須與 AWS CLI 例如，ARN 將類似下列：

#### 組織識別碼 ARN

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

#### 組織 OU ARN

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

## Console

### 若要建立授權 (主控台)

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在導覽窗格中，選擇授權授權。
3. 選擇授權 ID 以開啟 [授權概觀] 頁面。
4. 從 [授權] 區段中，選擇 [建立授權]。
5. 在授權詳細資料面板中，執行下列操作：
  - a. 輸入授權的名稱，以協助您識別授權的目的或接受者。
  - b. 輸入授與收AWS 帳戶件者的識別碼、AWS Organizations OU AWS Organizations 識別碼或 ARN 或識別碼或 ARN。
  - c. 選擇 [建立授權]。
6. 在「授權概觀」頁面上，您會在「授權」面板中看到授權條目。授權的初始狀態為 Pending 接受。當收件者接受授權時，狀態會變更為 [使用中]，或 [當收件者拒絕授權時已拒絕]。

## AWS CLI

您可以使用AWS CLI來散佈軟體權利文件。使用 AWS License Manager API 時，您必須使用 ARN 格式指定組織識別碼或 OU。

要使用以下命令創建和列出您的贈款AWS CLI：

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

授與詳細資料頁面會顯示您已授與權利存取權的帳戶清單。將授權分配給組織後，您可以在每個帳戶上個別停用或啟用授權。

## 授予接受和激活

當針對授與的授權建立授權時，會將其分配給收件者。授與的授權必須先接受並啟用，才能由授與的收件者使用。授予啟用程序可以包括其他選項，適用於來自AWS Marketplace。

依預設，授與授權的 [授與概觀] 頁面的狀態為Pending Acceptance。您可以選擇Accept Accept and Activate、或Reject授予。已接受但尚未啟動的授權狀態為Disabled。已接受和已啟動的授權的狀態為Active。

授與的授權必須先接受並啟用，才能由授與的收件者使用。根據預設，授與授權的授與詳細資料頁面的狀態為 [等待接受]。您可以選擇「接受」、「接受」和「啟用」或「拒絕授權」。已接受但尚未啟動的授權狀態為 [已停用]。已接受和已啟動的授權的狀態為 [作用中]。

### Tip

您可以自動接受來自組織的管理帳戶。若要啟用授與自動接受，請從管理帳戶連結AWS License Manager主控台的[設定](#)頁面上的組織帳戶。

您無法同時啟用同一產品AWS Marketplace的兩個授權。如果您有兩個訂閱 (例如，產品和非公開優惠的公開選件，或是產品的訂閱授權以及相同產品的授權)，您可以採取下列其中一項動作：

1. 停用相同產品的現有授權，然後啟用新授權。
2. 啟動新的授權，並指定您要停用，並以新的授權取代現有的作用中授權。您可以使用 License Manager 主控台或AWS CLI：
  - a. 使用 License Manager 主控台，在選取要取代作用中授與的是時啟用新授權。

- b. 使用 `CreateGrantVersion` API，透過指定 `ActivationOverrideBehavior` 與 `a Status` 的來啟用 `ALL_GRANTS_PERMITTED_BY_ISSUER` 用新授權 `Active`。

## Console

您可以使用 License Manager 主控台來啟用授權。當您啟動源自的授權時 AWS Marketplace，您可能看到是否要取代作用中授權的選項：

- 身為授權管理員，您必須指定是否要在啟用授權時取代作用中授權。
- 身為授與者，您可以選擇性地指定當您啟動組織中其他帳戶的授權時，是否要取代作用中的授權。
- 身為受權者，如果建立分散式授權的授與者未指定是否要取代作用中授權，您必須在啟動授權時進行選取。

### 啟動授權 (控制台)

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在導覽窗格中，選擇授權授權。
3. 選擇授權 ID 以開啟 [授權概觀] 頁面。
4. 選擇授權名稱以開啟 [授權概觀] 頁面。
5. 如果顯示，請選取您是否要取代作用中授權的啟用選項：
  - a. 否 — 此選項會啟動授權，而不會取代收件者 (受權者) 的任何現有作用中授權。
  - b. 是 — 此選項會停用相同產品的授權，並為已定義的收件者 (受權者) 啟動新授權：
    - i. 一個指定的 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. (選擇性) 提供啟動授權的原因。
7. 在輸入方塊 `activate` 中輸入，然後選擇「啟用」。

## AWS CLI

您可以使用授與 AWS CLI 的授權搭配使用。

若要使用分散式授權，請使用AWS CLI：

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

## 授權狀態

授權有兩種狀態：「授權」狀態 (顯示授權的整體可用性和可共用性) 以及授予狀態 (顯示使用授權的能力)。

下表顯示授與授權的各種狀態：

狀態	描述
AVAILABLE (可用)	該許可證可用於使用和共享。
已擱置 _ 可用	授權無法使用，因為它仍在處理中。
解除	由於授權簽發者已停用授權，因此無法使用授權。
SUSPENDED	由於授權已暫停，因此無法使用。
過期	授權無法使用，因為已到期結束。
擱置 _ 刪除	授權無法使用，因為正在被刪除。
DELETED (已刪除)	授權無法使用，因為授權合約已取消。

下表顯示授權的各種狀態：

狀態	描述
擱置工作流程	授權正在分發的過程中。

狀態	描述
待定 _ 接受	已建立授權，且授與收件者尚未接受。
REJECTED	授權接受者已拒絕授權。
作用中	授權已接受並啟用，以供授權收件者使用。可以使用授權的資源。
失敗 (_ 工作流程)	授權未能分發。
DELETED (已刪除)	授予者已刪除授權。
擱置 _ 刪除	正在被分配的授權正在被刪除。
DISABLED	授權接受者已接受授權，但尚未啟動以供使用。
工作流程 (_ 完成)	已分配或召回給組織的授權。撥款詳細信息顯示了組織中每個帳戶的子授予的狀態。

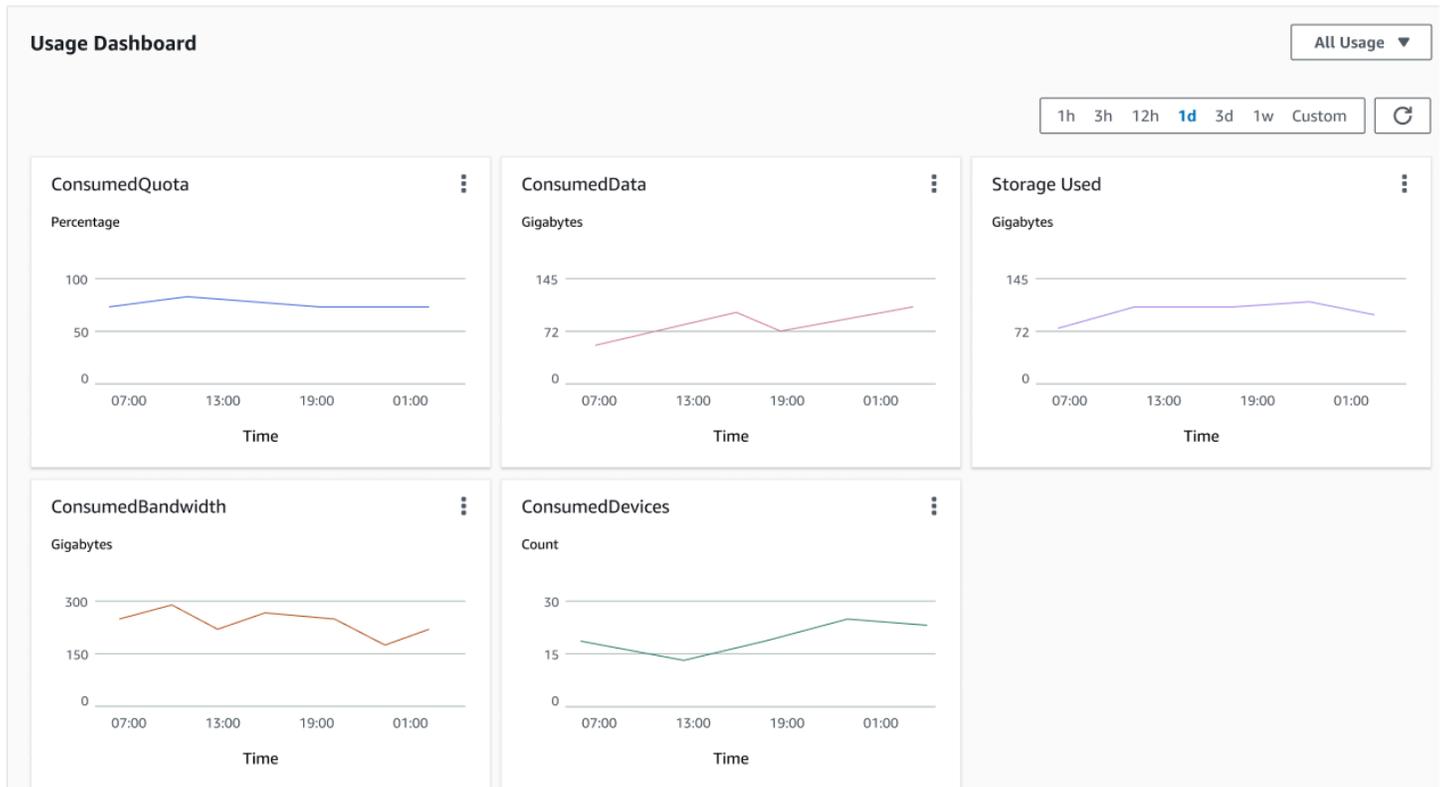
## 買家帳戶的指標

當賣家核發授權的授權設定為允許提交選取的使用記錄時，License Manager 會向賣方帳戶、超級買家帳戶，以及記錄使用情況的帳戶發出CloudWatch指標。買方帳戶是指AWS 帳戶已購買或獲得賣家核發授權的人。如需詳細資訊，請參閱[授權授權給客戶](#)。

## 使用儀表板

當賣方或獨立軟體廠商 (ISV) 應用程式記錄購買者帳戶授權的使用情況時，記錄使用狀況的帳戶和 root 購買者帳戶會在 License Manager 主控台的「使用情況」儀表板頁面上看到包含使用記錄的 CloudWatch Widget。購買者也可以查看他們擁有分配授權的帳戶指標AWS Organizations。「使用情況控制面板」頁面上的圖形適用於已傳送使用記錄的每個授權。

以下影像是使用情況儀表板的範例：



## 賣家在 License Manager 中核發授權

獨立軟體廠商 (ISV) 可以使用 AWS License Manager 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，集中追蹤賣家核發授權的使用情況。

License Manager 使用開放、安全的業界標準來代表授權，並允許客戶以密碼方式驗證其真實性。License Manager 將每個授權與非對稱金鑰建立關聯。作為 ISV，您擁有不對稱的 AWS KMS 密鑰並將其存儲在您的帳戶中。

賣方核發的授權需要跨區域複製授權中繼資料。License Manager 會自動將每位賣家核發的授權及其相關資訊複製到其他區域。

License Manager 支援各種不同的授權模式，包括：

- 永久— 沒有到期日的終身許可證，授權用戶無限期使用該軟件。
- 浮動— 具有多個應用程序實例的可共享許可證。您可以預付授權，並新增一組固定的權利。
- 訂閱— 具有到期日期的許可證，除非特別停用，否則可以自動續訂。
- 使用用量— 根據使用情況（例如 API 請求數量，交易或存儲功能）具有特定條款的許可證。

您可以在 License Manager 中建立授權，並使用 AWS IAM 身份或通過 License Manager 生成的承載令牌。客戶 AWS 帳戶可以將授權權利重新分配給 AWS 各自組織中的身份。擁有分散式權利的客戶可以透過與 License Manager 的軟體整合，從該授權中簽出並簽入所需的權利。

## 權利

License Manager 將授權功能擷取為權利在許可證中。權利的特徵可以有限或無限數量。有限權利的範例為「40 GB 的資料傳輸」。無限數量禮遇的一個例子是「白金級」。

授權會擷取所有授與的權利、啟動和到期日，以及發行者詳細資料。許可證是版本化的實體，每個版本都是不可變的。每當授權變更時，授權版本都會更新。

若要簽出或簽入有限的權利，ISV 應用程式必須指定每個有限容量的數量。針對無限制的權利，ISV 應用程式只需指定要再次簽出或簽入的相關權利。最後，有限的功能還支援「超額」旗標，指出使用者是否可以超過其初始權利的使用量。License Manager 會追蹤 ISV 並向 ISV 報告使用情況，以及任何超額情況。

## 授權使用

License Manager 可讓您集中追蹤多個區域的授權，方法是維持所有已簽出的權利計數。License Manager 也會追蹤使用者的身分識別，以及與每次出庫相關聯的基礎資源識別碼 (如果有的話)，以及簽出的時間。您可以通過跟踪此時間序列數據 CloudWatch 事件。

使用下列狀態之一來刪除下列狀態：

- 已建立— 即會建立授權。
- 已更新— 授權已更新。
- 停用— 授權已停用。
- 已刪除— 即會刪除授權。

## 請求

要搭配使用此功能，您必須具備對下列 License Manager API 動作呼叫。

```
{
  "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 集成，以便客戶沒有 AWS 帳戶可以使用以外銷售的授權 AWS Marketplace，您必須建立可讓您的軟體應用程式呼叫 License Manager API 的角色。例如使用 AWSCLI。首先，使用 [創建角色](#) 使用命令來刪除名為的角色 `AWSLicenseManagerConsumptionRole`。

```

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

```

下列是 `trust-policy-document.json`。

```

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

```

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

接下來，使用[attach-role-policy](#)指令以新增AWSLicenseManagerConsumptionPolicy AWS管政策。AWSLicenseManagerConsumptionRole角色。

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

## 建立賣家核發的授權

使用下列程序建立許可，使用AWS Management Console。或者使用下列程序來刪除授權[CreateLicenseAPI](#) 動作。

使用控制台來刪除授權

1. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
2. 選擇賣家發出的授權從左側菜單。
3. 選擇建立授權。
4. 對於授權元數據，提供下列資訊：
  - 授權名稱— 要向買家顯示的名稱，最多 150 個字元。
  - 授權說明— 可選描述，最多 400 個字元，可區分此授權與其他授權。
  - 產品貨號— 產品的 SKU。
  - 收件人— 收件人的姓名（公司或個人）。
  - 家居地區— 該AWS授權的區域。雖然授權可以全球使用，但您只能在本地區域變更授權。使用授權來刪除授權的主地區。
  - 授權開始日期— 啟用日期。

- 授權結束日期— 使用授權的終止日期。
5. 對於消費配置，提供下列資訊：
    - 更新頻率— 是否每週，每月或根本不續訂。
    - 消費配置— 選擇暫時使用組態選項如果許可證將用於連續連接或借如果授權要離線使用。輸入最長存活時間 (分鐘)以設定授權的可用性長度。
  6. 對於發行人，提供下列資訊：
    - 輸入一個AWS KMS鍵— 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[授權的密碼編譯簽署](#)。
    - 發行人名稱— 賣家的商家名稱。
    - 記錄賣方— 選擇性的企業名稱。
    - 協議網址— 授權合約的網址。
  7. 對於權利，提供有關授權授與收件者之權能的下列資訊：
    - 姓名— 收件者的姓名。
    - 單位類型— 選擇單位類型，然後提供最大計數。
    - 檢查允許入庫如果收件人必須在續訂前簽入許可證。
    - 檢查允許超額如果收件人可以使用超過最大計數的資源。此選項可能會向收件者產生額外費用。
  8. 選擇建立授權。

## 授予客戶授權

新增授權後，您可以將授權授予客戶AWS帳戶使用AWS Management Console。收件者必須先接受授權，才能使用授權。如需詳細資訊，請參閱[授與 License Manager 中的授權](#)。

或者，如果客戶沒有AWS使用授權管理程序來使用 License Manager API 來使用授權管理程序來[使用授權](#)。

使用主控台將授權授予客戶

1. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
2. 選擇賣家發出的授權從左側菜單。
3. 選擇授權的 ID 來刪除其詳細資料頁。
4. 對於補助金，選擇創建授予。

5. 對於授予細節，提供下列資訊：
  - 授予名稱— 授予名稱。這是用來啟用搜尋功能。
  - AWS帳戶識別碼— 該AWS授權接受者的帳號。
  - 授權權利
    - 選擇消費如果收件者可以使用授與的權利。
    - 選擇分佈如果收件者可以將授與的權利分發給其他人AWS帳戶。
    - 選擇允許內部部署令牌生成無需使用即可驗證共用授權AWS身分或認證。
    - 選擇允許提交使用記錄允許授權接收者發出使用類型的使用記錄。
  - 家居地區— 該AWS 區域使用許可證。
6. 選擇創建授予。

## 取得客戶的臨時登入資料，而無需AWS帳戶

對於沒有AWS帳戶，您可以使用相同的方式為您的客戶使用權利AWS帳戶。使用下列程序來刪除臨時AWS為您的客戶提供認證，而無需AWS帳戶。API 呼叫必須在本地區域中進行。

取得要在呼叫 License Manager API 時使用的臨時登入資料

1. 呼叫[CreateToken](#)用於獲取編碼為 JWT 令牌的刷新令牌的 API 操作。
2. 呼叫[GetAccessToken](#)API 動作，指定您從中接收的重新整理權杖CreateToken在上一步中，接收臨時訪問令牌。
3. 呼叫[AssumeRoleWithWebIdentity](#)API 動作，指定您從中接收的存取權杖GetAccessToken在上一個步驟中，AWSLicenseManagerConsumptionRole您創建的角色，以獲得臨時AWS認證。

若要從AWS License Manager安慰

1. 來刪除[使用 License Manager](#)，導覽至您想要在不使用的情況下使用的特定授權權利的 [授權詳細資料] 頁面AWS帳戶。
2. 選擇創建令牌生成一個臨時訪問令牌。

### Note

第一次產生臨時存取權杖時，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。會建立下列服務角色：AWSLicenseManagerConsumptionRole。

3. 下載網域。token.csv文件，或者在生成時複製令牌字符串。

### Important

這是您唯一查看或下載此權杖。建議您下載令牌，並將檔案儲存在安全的位置。您可以隨時創建新令牌，最多[服務限制](#)。

## 使用授權

License Manager 可讓多位使用者同時使用單一授權的權限，但功能有限。呼叫 [CheckoutLicense](#) API 動作。下列參數的說明。

- 鑰匙指紋— 受信任的授權發行者。

範例：問題:問題:發行者-指紋

- 產品貨號— 此授權的產品識別元，由授權發行者建立授權時所定義。相同的產品 SKU 可能存在於多個 ISV 中。因此，受信任的金鑰指紋扮演著重要的角色。

範例：1A2B3C4D2F5E69F440 電子郵件資料庫

- 權益— 要簽出的功能。如果您指定無限制的權能，則數量為零。範例：

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

- 受益人— 軟體即服務 (SaaS) ISV 可以透過包含客戶識別碼，代表客戶簽出授權。License Manager 會將呼叫限制在 SaaS ISV 帳戶中建立的授權存放庫。

範例：user@domain.com

- 節點識別碼— 用於將授權鎖定至單一應用程式執行個體的節點的識別碼。

範例：10 月 21 日

## 刪除賣家核發的授權

刪除授權後，您可以重新建立授權。授權及其資料會保留，授權發行者和授權受權者以唯讀模式提供六個月。

使用下列程序來刪除使用下列程序來刪除使用下列程序來刪除使用AWS Management Console。或者使用刪除授權使用[DeleteLicenseAPI](#) 動作。

### 使用控制台刪除授權

1. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
2. 選擇賣家發出的授權從左側菜單。
3. 選擇授權旁邊的選項按鈕來刪除使用授權來刪除授權。
4. 選擇 刪除。當系統提示進行確認時，輸入 `delete` 並選擇刪除。

## License Manager 中的使用者型訂閱

使用者型訂閱時 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 機器映像 (AMI) 搭配受支援的軟體，以及包含授權的 Windows 伺服器授權。這些授權無需長期授權承諾即可使用。

若要使用以使用者為基礎的訂閱，您可以將 [AWS Directory Service for Microsoft Active Directory](#)(AWS Managed Microsoft AD) 或自我管理 (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。若要讓授權軟體可用，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 AMI 啟動的執行個體產生關聯。 [AWS Systems Manager](#)將設定並強化您啟動的包含授權執行個體。使用者必須連線至遠端桌面軟體，才能存取提供軟體的執行個體。

包含授權執行個體的每個關聯使用者和 [vCPU](#) 都會產生費用。Amazon EC2 預留執行個體和 Savings Plan 定價模式可協助您優化 Amazon EC2 成本。如需詳細資訊，請參閱 Amazon 彈性運算雲端使用者指南中的[預留執行個體](#)。以使用者為基礎的訂閱會從上半年開始計費至月底。

### 內容

- [必要條件](#)
- [考量事項](#)

- [適用於使用者訂閱的軟體](#)
  - [支援使用者訂閱的軟體](#)
    - [Microsoft Visual Studio](#)
    - [Microsoft 辦公室](#)
    - [從支援的 AMI 啟動](#)
  - [附加軟體](#)
- [開始使用基於使用者的訂閱](#)
  - [步驟 1：設定您 AWS Directory Service for Microsoft Active Directory 的虛擬私有雲 \(VPC\)](#)
  - [步驟 2：訂閱產品](#)
  - [步驟 3：啟動執行個體以提供使用者型訂閱](#)
  - [步驟 4：將使用者與使用者型訂閱執行個體建立關聯](#)
  - [步驟 5：Connect 至以使用者為基礎的訂閱執行個體](#)
- [修改使用者型訂閱的目錄設定](#)
- [修改以使用者為基礎的訂閱的 VPC 設定](#)
- [取消使用者與使用者型訂閱的關聯](#)
- [從基於使用者的訂閱中取消訂閱使用者](#)
- [終止提供使用者訂閱的 EC2 執行個體](#)
- [移除以使用者為基礎的訂閱的目錄](#)
- [疑難排解使用者訂閱](#)
  - [執行個體合規性](#)
  - [授權合規性疑難](#)
  - [疑難排解執行個](#)
  - [加入網域失敗的疑難排解](#)
  - [疑難排解 Systems Manager](#)
  - [故障診斷 Systems Manager 執行命令](#)

## 必要條件

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。

- 您必須允許 License Manager 建立服務連結角色，才能加入以使用者 AWS 帳戶 為基礎的訂閱。在 License Manager 主控台的「以使用者為基礎的訂閱」區段中會出現一次提示，您可以在其中同意授

與 License Manager 建立所需服務連結角色的權限。授予 License Manager 權限後，您可以選擇 [建立]，以建立服務連結角色。如需詳細資訊，請參閱 [使用 AWS License Manager 的服務連結角色](#)。

- 您必須建立一個 AWS Managed Microsoft AD 目錄。AWS Managed Microsoft AD 不支援已共用的目錄。如需有關建立 AWS Managed Microsoft AD 目錄的詳細資訊，請參閱 AWS Directory Service 使用指南中的 [AWS Managed Microsoft AD 先決條件和建立 AWS Managed Microsoft AD 目錄](#)。
- 您必須將使用者與目錄或自我管理的 Active AWS Managed Microsoft AD Directory 建立關聯，才能使用以使用者為基礎的訂閱。
  - 若要將使用者與之建立關聯 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](#)》[AWS Managed Microsoft AD 中的〈管理使用者和群組〉](#)。AWS Directory Service
  - 若要建立自我管理目錄中的使用者關聯，您必須在自我管理的目錄與目錄之間建立雙向樹系信任。AWS Managed Microsoft AD 如需詳細資訊，請參閱《[管理指南](#)》中的 [教學課程：在您 AWS Managed Microsoft AD 與您自我管理的 Active Directory 網域之間建立信任關係](#)。AWS Directory Service
  - 為您的目錄設定的子網路必須全部來自相同的 VPC。AWS 帳戶
- 必須設定來自提供使用者訂閱的執行個體或 [VPC 端點](#) 的輸出網際網路存取，讓您的執行個體與之通訊。AWS Systems Manager 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](#)。
- License Manager 會建立兩個網路介面，這兩個介面使用佈建您 AWS Managed Microsoft AD 的 VPC 的預設安全性群組。這些介面可用於目錄中所需的服務功能。請確定您的預設安全性群組允許輸出流量到每個網域控制站的網路介面 IPv4 位址，或網域控制站使用的安全性群組。如需詳細資訊，請參閱《[AWS Directory Service 管理指南](#)》中的 [〈建立的內容〉 步驟 1：設定您 AWS Directory Service for Microsoft Active Directory 的虛擬私有雲 \(VPC\)](#) 和 [〈建立](#)

佈建程序完成後，您可以將不同的安全性群組與 License Manager 建立的介面相關聯。您選取的安全性群組也必須允許必要的流量傳送至每個網域控制站的網路介面 IPv4 位址或安全性群組。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](#)。

- 您必須為任何其他 VPC 設定 DNS 轉送至您註冊以使用者為基礎的訂閱的 VPC。AWS Managed Microsoft AD 您可以使用 Amazon 路線 53 或其他 DNS 服務進行 DNS 轉發。如需詳細資訊，請參閱 [整合目錄服務的 DNS 解析與 Amazon Route 53 解析器的](#) 部落格文章。
- 如果您使用以使用者為基礎的訂閱來訂閱 Microsoft Office，您必須：
  - 為您的 VPC 擬私人雲端啟用 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](#)。
  - 確定為向 Microsoft Office 提供以使用者為基礎的訂閱而啟動的執行個體具有通往佈建 VPC 端點之子網路的路由。

- 為允許輸入 TCP 連接埠 1688 連線的 VPC 端點識別或建立安全群組。當您設定虛擬私有雲設定時，會指定此安全性群組。如需詳細資訊，請參閱[使用安全性群組](#)。License Manager 會在設定 VPC 時，將此安全性群組與其代表您建立的 VPC 端點相關聯。如需 VPC 端點的詳細資訊，請參閱[指AWS PrivateLink 南中的使用介面 VPC 端點存取 AWS 服務](#)。
- 為啟動的執行個體識別或建立安全群組，以提供以使用為基礎的訂閱，該訂閱允許來自核准的連線來源輸入 TCP 連接埠 3389 連線。安全性群組也應允許輸出 TCP 連接埠 1688 連線到 VPC 端點。如需詳細資訊，請參閱[使用安全性群組](#)。

如果您準備好第一次使用以使用者為基礎的訂閱，請[開始使用基於使用者的訂閱](#)完成列出的必要條件，然後參閱。如果您已設定以使用者為基礎的訂閱，而且想要將這些產品新增至您的，AWS Managed Microsoft AD 並為 Microsoft Office 產品設定您的 VPC，請完成列出的先決條件，然後參閱。[修改使用者型訂閱的目錄設定](#)

- 您必須將執行個體設定檔角色附加至提供使用者型訂閱產品的執行個體，以便管理資 AWS Systems Manager 源。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](#)。

#### Warning

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，才能擁有健全狀態。此外，您的執行個體必須能夠啟用其以使用者為基礎的訂閱授權，並在授權啟用後保持合規性。License Manager 會嘗試復原狀況不良的執行個體，但無法恢復正常狀態的執行個體將會終止。如需維持由 Systems Manager 管理的執行個體以及執行個體合規性的疑難排解資訊，請參閱本指南的[疑難排解使用者訂閱](#)章節。

- 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權限：
  - ec2:CreateNetworkInterface
  - ec2>DeleteNetworkInterface
  - ec2:DescribeNetworkInterfaces
  - ec2:CreateNetworkInterfacePermission
  - ec2:DescribeSubnets
  - ds:DescribeDirectories
  - ds:AuthorizeApplication
  - ds:UnauthorizeApplication
  - ds:GetAuthorizedApplicationDetails
  - ds:DescribeDomainControllers

- 若要為 Microsoft Office 產品建立以使用者為基礎的訂閱，您的使用者或角色也必須具有下列其他權限：
  - `ec2:CreateVpcEndpoint`
  - `ec2>DeleteVpcEndpoints`
  - `ec2:DescribeVpcEndpoints`
  - `ec2:ModifyVpcEndpoint`
  - `ec2:DescribeSecurityGroups`

## 考量事項

搭配使用 License Manager 使用以使用者為基礎的訂閱時，需要考量

- Win 遠端桌面服務 SAL 授權不能與支援的使用者型訂閱產品分開使用。
- 提供使用者訂閱的執行個體一次最多支援兩個作用中使用者工作階段。
- 當您在提供使用者訂閱的執行個體上建立具有管理員權限的本機使用者時，執行個體的健全狀況狀態可能會變更為狀況不良。License Manager 可以終止因不合規而健康狀態不佳的執行個體。如需詳細資訊，請參閱[疑難排解執行個體符](#)
- 若要停止向使用者訂閱產生費用，您必須取消使用者與其相關聯之所有執行個體的關聯。如需詳細資訊，請參閱[取消使用者與使用者型訂閱的關聯](#)。
- 當您使用 Microsoft Office 產品設定目錄時，您的 VPC 必須在至少一個子網路中佈建 [VPC 端點](#)。如果要移除 License Manager 建立的所有 VPC 端點資源，則必須執行下列動作：
  - 取消所有使用者與其基於使用者訂閱的關聯。如需詳細資訊，請參閱[取消使用者與使用者型訂閱的關聯](#)。
  - 移除從 License Manager 設定中設定的任何目錄。如需詳細資訊，請參閱[移除以使用者為基礎的訂閱的目錄](#)。
  - 終止所有提供使用者訂閱產品的執行個體。如需詳細資訊，請參閱[終止提供使用者訂閱的 EC2 執行個體](#)。
- 不得變更或刪除由 License Manager UserSubscriptions 指定給實例的值的標籤金鑰。AWSLicenseManager
- 不得變更或刪除為 License Manager 建立的兩個彈性網路介面 (ENI)，服務才能正常運作。
- 不得變更或刪除 License Manager 在 AWS Managed Microsoft AD 目錄的 AWS 保留組織單位 (OU) 中建立的物件。

- 針對使用者型訂閱部署的執行個體必須是具有相同網域 AWS Systems Manager 並加入相同網域的受管節點。如需讓執行個體由系統管理員管理的相關資訊，請參閱本指南[疑難排解使用者訂閱](#)章節。

## 適用於使用者訂閱的軟體

AWS License Manager 支持 Microsoft 視覺工作室和 Microsoft 辦公室基於用戶的訂閱。每個使用者都需要單一訂閱 Windows Server 遠端桌面服務使用者存取授權 (RDS SAL)，才能存取包含授權的執行個體，該執行個體提供以使用者為基礎的訂閱產品。受支援的軟體將由 License Manager 追蹤其使用率。如需詳細資訊，請參閱 [開始使用基於使用者的訂閱](#)。

### 支援的視窗作業系統平台

您可以找到包含適用於下列視窗作業系統平台之 RDS SAL 授權所涵蓋之產品的視窗 AMI：

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

### 支援使用者訂閱的軟體

License Manager 通過以下軟件支持基於用戶的許可。

#### Microsoft Visual Studio

Microsoft Visual Studio 是一個集成的開發環境 ( IDE )，使開發人員能夠創建，編輯，調試和發布應用程序。所提供的 Microsoft 視覺工 [AWS 具包 AMI 包括. AWS Toolkit for Visual Studio](#)

#### 支援的版本

- 視覺工作室專業
- 視覺工作室企業

下表詳細說明用於 License Manager 使用者訂閱 API 作業的軟體訂閱名稱及其相關產品值。

軟體訂閱名稱	產品價值
視覺工作室企業	VISUAL_STUDIO_ENTERPRISE

軟體訂閱名稱	產品價值
視覺工作室專業	VISUAL_STUDIO_PROFESSIONAL

## Microsoft 辦公室

Microsoft Office 是由 Microsoft 為各種生產力使用案例開發的軟件集合，包括使用文檔，電子表格和幻燈片演示文稿。

### 支援的版本

- 辦公室 LSC 專業加強版 2021

下表詳細說明用於 License Manager 使用者訂閱 API 作業的軟體訂閱名稱及其相關產品值。

軟體訂閱名稱	產品價值
辦公室 LSC 專業加強版 2021	OFFICE_PROFESSIONAL_PLUS

## 從支援的 AMI 啟動

當您從支援的 AMI Office LTSC Professional Plus 或 Microsoft Visual Studio 啟動執行個體時，啟動預設為 AMI 的最新視窗作業系統平台版本 (例如視窗伺服器 2022)。若要以較早的作業系統平台版本啟動，請依照下列步驟執行。

1. [請在以下位置開啟 AWS Marketplace 主控台。](https://console.aws.amazon.com/marketplace) <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 2021 或 Visual Studio Enterprise。
4. 從訂閱面板中選取 [啟動新執行個體]。這會開啟啟動設定頁面。
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」版本下方的完整 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取。
6. 此清單會顯示支援 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。

## 附加軟體

您可以在執行個體上安裝其他軟體，而這些軟體無法作為使用者訂閱提供。License Manager 不會追蹤其他軟體安裝。這些安裝必須使用預設在您 AWS Managed Microsoft AD 目錄中建立的 Admin 帳戶來執行。如需詳細資訊，請參閱 [《管理指南》中的 AWS Directory Service 管理員帳戶](#)。

若要使用 Admin 帳戶安裝其他軟體，您必須：

- 將 Admin 帳戶訂閱至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 Connect 至執行個體以執行安裝。

如需詳細資訊，請參閱 [開始使用基於使用者的訂閱](#)。

## 開始使用基於使用者的訂閱

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必要條件。如需更多資訊，請參閱 [必要條件](#)。

如果您已經針對以使用者為基礎的訂閱設定 AWS Managed Microsoft AD 目錄，而且想要使用 Microsoft Office，請參閱 [修改以使用者為基礎的訂閱的 VPC 設定](#)。

### 步驟

- [步驟 1：設定您 AWS Directory Service for Microsoft Active Directory 的虛擬私有雲 \(VPC\)](#)
- [步驟 2：訂閱產品](#)
- [步驟 3：啟動執行個體以提供使用者型訂閱](#)
- [步驟 4：將使用者與使用者型訂閱執行個體建立關聯](#)
- [步驟 5：Connect 至以使用者為基礎的訂閱執行個體](#)

### 步驟 1：設定您 AWS Directory Service for Microsoft Active Directory 的虛擬私有雲 (VPC)

License Manager 需要 AWS Managed Microsoft AD 將使用者與以使用者為基礎的訂閱建立關聯。在設定目錄時，您必須選取所需的所有產品，以使用者為基礎的訂閱，因為使用者只能訂閱已設定的產品。當您註冊 AWS Managed Microsoft AD 目錄時，License Manager 會建立兩個彈性網路介面 (ENI)，以便服務與您的目錄進行通訊，其描述與建立的網路介面類似。LicenseManager

**⚠ Important**

您必須先允許 License Manager 建立必要的[服務連結角色](#)，才能繼續。如需更多資訊，請參閱[必要條件](#)。

若要將 Microsoft Office 與以使用者為基礎的訂閱搭配使用，您必須授與 License Manager 權限，才能更新您的 VPC 設定。設定 VPC 時，License Manager 會代表您建立 [VPC 端點](#)。您的資源需要這些端點才能連線到啟用伺服器並保持合規。

您必須為任何其他 VPC 設定 DNS 轉送至 AWS Managed Microsoft AD 您註冊以使用者為基礎的訂閱。如果您有多個以使用者為基礎的訂閱 AWS 區域，則每個區域都必須具有自己 AWS Managed Microsoft AD 的 DNS 轉送設定，如下所示。

您可以使用下列其中一種方法，針對以使用者為基礎的訂閱設定環境。

#### Console (Active Directory)

若要設定以使 AWS Managed Microsoft AD 用者為基礎的訂閱 (主控台)

1. 開啟 License Manager 主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
2. 選擇左側導覽窗格中的 [設定]，或選擇橫幅中的 [開啟設定]，以導覽至 [設定] 頁面。
3. 在 [設定] 頁面的 AWS Managed Microsoft AD 區段下，選擇 [設定]。
4. 針對 AWS 受管理的目錄名稱和 ID，選擇包含您要為其建立以使用者為基礎之訂閱之使用者的目錄。
5. 針對「產品名稱和 ID」，選取任何必要的產品，然後選擇「設定」。

選擇設定之後，[設定] 頁面上的 AWS Managed Microsoft AD 區段會顯示 [目錄 ID] 及 [狀態] 為 [設定]。組態程序完成後，「狀態」會顯示「已設定」，您可以繼續執行其餘步驟。

#### Console (Active Directory and VPC)

若要設定以使 AWS Managed Microsoft AD 用者為基礎的訂閱 (主控台)

1. 開啟 License Manager 主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
2. 選擇左側導覽窗格中的 [設定]，或選擇橫幅中的 [開啟設定]，以導覽至 [設定] 頁面。
3. 在 [設定] 頁面的 AWS Managed Microsoft AD 區段下，選擇 [設定]。

4. 針對AWS 受管理的目錄名稱和 ID，選擇包含您要為其建立以使用者為基礎之訂閱之使用者的目錄。
5. 針對「產品名稱」和「ID」，選取任何必要的產品。
6. 對於虛擬私有雲，請選擇 VPC 以進行其他配置。
7. 對於 vpc-*x* 的子網路，請至少選擇一個要佈建 VPC 端點的子網路。
8. 對於 vpc-*x* 的安全性群組，請選擇您建立要與 VPC 端點關聯的安全性群組，然後選擇設定。

選擇 [設定] 後，[設定] 頁面上的AWS Managed Microsoft AD和 [虛擬私有雲] 區段將會顯示您的目錄 ID 和 VPC ID，其狀態為 [設定]。組態程序完成後，每個「狀態」都會顯示為「已設定」，您可以繼續執行其餘步驟。

## AWS CLI

若要設定以使 AWS Managed Microsoft AD 用者為基礎的訂閱 ()AWS CLI

您可以在[RegisterIdentityProvider](#)作業中註冊 AWS Managed Microsoft AD 為以使用者為基礎的訂閱的身分識別提供者。

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

若要針對以使用者為基礎的訂閱設定 AWS Managed Microsoft AD 和您的 VPC ()AWS CLI

您可以將您的身分識別提供者註冊 AWS Managed Microsoft AD 為身分識別提供者，並將 VPC 設定為以使用者為基礎的[RegisterIdentityProvider](#)訂閱。

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

如需有關可用軟體產品的更多資訊，請參閱[適用於使用者訂閱的軟體](#)。

## 步驟 2：訂閱產品

若要訂閱中的已設定產品 AWS Marketplace

使用所需產品設定目錄後，您可能還需要訂閱所需的產品。Marketplace 訂閱狀態為「非作用中」的產品需要您先訂閱，才能將使用者與執行個體建立關聯並使用它們。

您的帳戶必須有 Windows 伺服器遠端桌面服務使用者存取授權 (RDS SAL) 的訂閱。Microsoft 遠程桌面服務 (RDS)，被稱為終端服務器在 Windows 服務器 2008 年及更早版本，是 Microsoft 視窗，允許用戶採取遠程計算機或虛擬機的控制通過網絡連接的組成部分之一。RDS 允許使用者遠端存取圖形桌面和 Windows 應用程式。

除了想要使用的任何其他產品之外，與提供以使用者為基礎的訂閱產品的執行個體相關聯的所有使用者必須擁有此授權的單一有效訂閱。當您的使用者訂閱以使用者為基礎的訂閱產品時，將代表他們訂閱 RDS SAL。

#### Note

RDS SAL 授權無法與支援的使用者型訂閱產品分開使用。如需詳細資訊，請參閱 [考量事項](#)。

您可以 AWS Marketplace 使用以下鏈接直接訂閱您的產品：

- [視覺工作室專業](#)
- [視覺工作室企業](#)
- [辦公室 LSC 專業加強版 2021](#)
- [贏取遠端桌面服務 SAL](#)

從 License Manager 主控台探索並訂閱產品

您也可以從 License Manager 主控台探索要訂閱的必要產品。

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的 [以使用者為基礎的訂閱] 下，選擇 [產品]。
3. 選擇產品名稱以顯示訂閱詳細資料。
4. 選擇 [檢視於] AWS Marketplace。
5. 檢閱訂閱詳細資料，然後選擇「繼續訂閱」。
6. 如果您要繼續，請檢閱條款，然後選擇「接受條款」。

如果您接受條款，則需要處理產品訂閱。訂閱將會有一則進行中訊息，直到完成為止。您可以針對您需要的任何其他已設定產品重複這些步驟。一旦所有必要的產品都具有有效的訂閱，您就可以繼續向使用者訂閱產品。

#### Note

如果帳單週期尚未結束 (標示為「待處理帳單狀態」)，系統將需要 48 小時才會顯示使用者人數和相關費用的估計費用 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 3：啟動執行個體以提供使用者型訂閱

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 連線到。啟動執行個體之後，AWS Systems Manager 會嘗試將執行個體加入網域，並對資源執行其他設定和強化。讓執行個體準備好可供使用的設定大約需要 20 分鐘才能完成。您可以從 License Manager 主控台的 [使用者關聯] 頁面，檢查執行個體的 [Health 全狀況] 狀態為 [作用中]，確認資源已準備就緒。

#### 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。無法完成初始設定的資源將會終止。如需詳細資訊，請參閱《[必要條件](#)》和《[疑難排解使用者訂閱](#)》。

以使用者為基礎的訂閱啟動執行個體

1. 訪問 Amazon EC2 控制台 <https://console.aws.amazon.com/ec2/>。
2. 在 [影像] 下，選擇 AMI 目錄。
3. 選擇 AWS Marketplace AMI。
4. 在搜索框中輸入產品名稱，然後按 Enter 鍵。例如，您可以搜尋 **Visual Studio**。
5. 在「發行者」下，選取「Amazon Web Services」。
6. 針對您要啟動執行個體以提供使用者訂閱的產品，選擇 [選取]。
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. 選擇非以重力子為基礎的 Nitro 實體類型。
  - b. 選擇 VPC 和子網路，您的執行個體可從中連線到您的 AWS Managed Microsoft AD 目錄。
  - c. 選擇允許從執行個體連線到 AWS Managed Microsoft AD 目錄的安全性群組。
  - d. 展開 [進階詳細資料]，然後選擇允許執行個體的 Systems Manager 功能的 IAM 角色。
10. 選擇啟動執行個體。

從 AWS Marketplace AMI 執行執行個體之後，您必須向使用者訂閱產品，並將其與執行個體建立關聯，這些執行個體會提供產品，讓他們能夠利用產品。

#### 步驟 4：將使用者與使用者型訂閱執行個體建立關聯

一旦您訂閱了所需產品的 AWS Marketplace AMI，您就可以為使用者訂閱產品，並將他們與提供產品的執行個體建立關聯。您可以透過單一步驟或分別為使用者訂閱產品，並將其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份存在。系統會為您訂閱產品的每位使用者建立一個訂閱。

#### Note

每個使用者都必須擁有 Windows 伺服器遠端桌面服務使用者存取使用授權 (RDS SAL) 及其將使用的產品的訂閱。如果您的帳戶已訂閱 RDS SAL (如中所述)[步驟 2：訂閱產品](#)，當您的使用者訂閱以使用者為基礎的訂閱產品時，就會代表他們訂閱 RDS SAL。

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。在產品的詳細資料頁面中，License Manager 會顯示使用中使用者訂閱，其狀態為「已訂閱」。

#### Important

如果您的目錄未使用產品配置，控制台頂部將出現一個通知欄，建議您調整目錄的設置。在通知列上，選擇 [開啟設定] 以存取 [License Manager] 中的 [設定] 頁面並編輯您的目錄。每個使用者都必須擁有 RDS SAL 及其將使用之產品的訂閱。如果使用者訂閱 Marketplace 訂閱狀態為「非作用中」的產品，則會失敗。

為使用者訂閱產品，並將其與執行個體建立關聯

您可以透過下列程序將使用者訂閱產品，並將他們與執行個體建立關聯。

## 若要訂閱使用者並將其關聯至執行個體

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的以使用者為基礎的訂閱下，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 [訂閱並關聯使用者]。
4. 指定目錄中最多五個使用者名稱，包括網域名稱 (如果存在於信任的網域中)，然後選擇「訂閱與關聯」。

在 [使用者關聯] 頁面上，您選取的使用者應該會顯示在 [關聯狀態為關聯的使用者] 下方。此外，在「產品」頁面上，您可以選擇產品名稱來查看產品的詳細資訊頁面。已訂閱的使用者會顯示在 [狀態為已訂閱的使用者] 下方。

## 為使用者訂閱產品

您可以使用下列其中一種方法來訂閱使用者訂閱產品。

### Console

#### 若要訂閱使用者使用產品 (主控台)

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的 [以使用者為基礎的訂閱] 下，選擇 [產品]。
3. 選取要訂閱 Marketplace 訂閱狀態為作用中的使用者的產品，然後選擇 [訂閱使用者]。
4. 指定目錄中最多五個使用者名稱，包括網域名稱 (如果存在於信任的網域中)，然後選擇 [訂閱]。

擁有訂閱的使用者會顯示在 [狀態為已訂閱的使用者] 下方。

### AWS CLI

#### 若要訂閱使用者的產品 (AWS CLI)

您可以使用此操作向您的身分提供者註冊的產品訂閱使 [StartProductSubscription](#) 用者。

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

使用自我管理的作用中目錄訂閱使用者的產品 ( )AWS CLI

您可以將使用者從自我管理的 Active Directory 訂閱到使用此[StartProductSubscription](#)作業在 AWS Managed Microsoft AD 目錄中註冊的產品。

```
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>
```

如需有關可用軟體產品的更多資訊，請參閱[適用於使用者訂閱的軟體](#)。

擁有訂閱的使用者會顯示在 [狀態為已訂閱的使用者] 下方。

將使用者關聯至執行個體

您可以使用下列其中一種方法將使用者與執行個體建立關聯。

#### Important

在將產品與執行個體建立關聯之前，您必須先訂閱使用者訂閱產品。

## Console

將使用者與執行個體建立關聯 (主控台)

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的以使用者為基礎的訂閱下，選擇 [使用者關聯]。
3. 選取您要與使用者建立關聯的執行環境，然後選擇關聯使用者。
4. 指定目錄中最多五個使用者名稱，包括網域名稱 (如果存在於信任的網域中)，然後選擇「關聯」。

在 [使用者關聯] 頁面上，您選取的使用者應該會顯示在 [關聯狀態為關聯的使用者] 下方。

## AWS CLI

將使用者與實例建立關聯 (AWS CLI)

您可以將使用者與啟動的執行個體建立關聯，以提供以使用者為基礎的訂閱與 [AssociateUser](#) 作業。

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

將自我管理的作用中目錄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，以提供以使用者為基礎的訂閱與作業。 [AssociateUser](#)

```
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>
```

如需有關可用軟體產品的更多資訊，請參閱 [適用於使用者訂閱的軟體](#)。

在 [使用者關聯] 頁面上，您選取的使用者應該會顯示在 [關聯狀態為關聯的使用者] 下方。

## 步驟 5：Connect 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 Health 全狀態為「作用中」，他們就可以連線至執行個體。使用者必須使用其網域的使用者認證連線，才能將產品與其相關聯的身分使用。

### Important

建立 EC2 執行個體並為使用者做好準備的程序可能需要大約 20 分鐘的時間。執行個體的關聯狀態必須為「作用中」，才能存取並使用產品。

連線到以使用者為基礎的訂閱的執行個體

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的以使用者為基礎的訂閱下，選擇 [使用者關聯]。
3. 在 [使用者關聯] 頁面上，確認執行個體的 Health 全狀態為 [作用中]。
4. 記下實例 ID，因為您需要它來收集連接詳細信息。
5. 請遵循 [使用 RDP Connect 到 Windows 執行個體](#) 中所列的步驟，同時確保指定關聯使用者的完整使用者名稱。

## 修改使用者型訂閱的目錄設定

您可以在 [License Manager] 設定頁面中，從設定的目錄中新增或移除以使用者為基礎的訂閱的產品。如果您使用 Microsoft Office 產品，這些步驟會有所不同，因為 License Manager 必須為這些訂閱帳戶建立 [VPC 端點](#)。

在沒有 Microsoft Office 產品的情況下修改目錄組態

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面的AWS Managed Microsoft AD區段下，選擇 [編輯]。
4. 對於「產品名稱和 ID」，請選取其他產品並視需要清除先前的選取項目，然後選擇「儲存變更」。

若要使用 Microsoft Office 產品修改目錄組態

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 選擇左側導覽窗格中的 [設定]，或選擇橫幅中的 [開啟設定]，以導覽至 [設定] 頁面。
3. 在 [設定] 頁面的AWS Managed Microsoft AD區段下，選擇 [編輯]。
4. 針對產品名稱和識別碼，選取任何必要的產品，包括 Microsoft Office。
5. 對於虛擬私有雲，請選擇 VPC 以進行其他配置。
6. 對於 vpc-x 的子網路，請至少選擇一個要佈建 VPC 端點的子網路。
7. 對於 vpc-x 的安全性群組，請選擇您建立要與 VPC 端點關聯的安全性群組，然後選擇 [儲存變更]。

選擇 [儲存變更] 後，[設定] 頁面上的AWS Managed Microsoft AD和 [虛擬私有雲] 區段會顯示您的目錄 ID 和 VPC ID，其狀態為 [設定]。在 Microsoft Office 中使用以使用者為基礎的訂閱之前，您必須等到目錄狀態為 [已設定] 且 VPC 的 [狀態] 為 [作用中] 為止。

## 修改以使用者為基礎的訂閱的 VPC 設定

如果您新增了 Microsoft Office 產品，您可以修改虛擬私人雲端的設定。License Manager 將在您指定的子網路中代表您建立 [VPC 端點](#)，以便連接啟用伺服器並保持合規性。您必須至少指定一個子網路。如需詳細資訊，請參閱 [必要條件](#)。

**Note**

只有在您的目錄已設定 Microsoft Office 產品時，才能修改 VPC 設定。如需詳細資訊，請參閱 [開始使用基於使用者的訂閱](#)。

如果要移除所有 VPC 端點，請參閱 [考量事項](#)。

### 修改目錄組態

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面的 [已設定的虛擬私人雲端] 區段下，選擇 [編輯]。
4. 視需要變更已設定 VPC 的子網路和安全性群組，然後選擇 [儲存變更]。

## 取消使用者與使用者型訂閱的關聯

您可以取消使用者與執行個體的關聯，以移除對資源的存取權。

**Note**

從目錄中刪除使用者並不會改變使用者關聯或訂閱。您必須取消 License Manager 中使用者與產品詳細資料頁面的關聯，才能移除與執行個體的關聯。

### 取消以使用者為基礎的訂閱使用者

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的以使用者為基礎的訂閱下，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「取消使用者關聯」。

## 從基於使用者的訂閱中取消訂閱使用者

您可以從產品中取消訂閱使用者，以移除存取權，並停止為這些使用者產品產生費用。

**⚠ Important**

您必須先取消使用者與目前關聯的執行個體之間的關聯，才能取消訂閱。

### 若要取消訂閱使用者型訂閱

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的 [以使用者為基礎的訂閱] 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。

### 終止提供使用者訂閱的 EC2 執行個體

如果不再需要，您可以刪除提供以使用者為基礎的訂閱的執行個體。這稱為終止執行個體。您應該先取消所有使用者與執行個體的關聯，然後從 Amazon EC2 主控台終止執行個體。

**ℹ Note**

使用者必須取消與執行個體的關聯，才能停止產生訂閱費用。如需詳細資訊，請參閱 [取消使用者與使用者型訂閱的關聯](#)。

### 識別和終止提供使用者型訂閱的執行個體

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的以使用者為基礎的訂閱下，選擇 [使用者關聯]。
3. 在 [使用者關聯] 頁面上，選擇要存取執行個體詳細資訊頁面的執行個體 ID。
4. 請記下執行個體 ID，因為您需要它才能終止執行個體。
5. 取消所有使用者與執行個體的關聯。
6. 遵循「[終止執行個體](#)」中列出的步驟。

### 移除以使用者為基礎的訂閱的目錄

如果您不想再將目錄用於以使用者為基礎的訂閱，可以移除該目錄。從 License Manager 中移除目錄的組態並不會刪除目錄本身。移除目錄時，您無法將目錄中的使用者建立關聯以使用者為基礎的訂閱。

### ⚠ Important

您必須先取消使用者的關聯，並終止提供以使用者為基礎之訂閱的執行個體，才能從 License Manager 移除目錄。

#### 若要移除目錄

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側的導覽窗格中，選擇設定。
3. 在 [設定] 頁面的 AWS Managed Microsoft AD 區段下，選擇 [移除]。
4. 輸入必要的文字以確認您要移除目錄，然後選擇 [移除]。

選擇 [移除] 之後，[設定] 頁面上的 AWS Managed Microsoft AD 區段會顯示 [目錄 ID] 及 [狀態] 為 [設定]。設定程序完成後，應該從 AWS Managed Microsoft AD 區段中移除目錄。

## 疑難排解使用者訂閱

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

### 內容

- [執行個體合規性](#)
- [授權合規性疑難](#)
- [疑難排解執行個](#)
- [加入網域失敗的疑難排解](#)
- [疑難排解 Systems Manager](#)
- [故障診斷 Systems Manager 執行命令](#)

## 執行個體合規性

提供以使用者為基礎的訂閱的執行個體必須維持健全狀態，才能符合規範。標示為狀態不良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狀態，但無法恢復正常狀態的執行個體則會終止。

為提供以使用者為基礎的訂閱而啟動而無法完成初始設定的執行個體將會終止。在此案例中，您必須更正設定問題並啟動新執行個體，以提供以使用者為基礎的訂閱。如需更多資訊，請參閱[必要條件](#)。

## 授權合規性疑難

如果您將目錄設定為向 Microsoft Office 提供以使用者為基礎的訂閱，則必須確保您的資源可以連線到 License Manager 建立的 VPC 端點。端點需要來自提供使用者訂閱的執行個體的 TCP 連接埠 1688 上的輸入流量。

您可以使用可 [Reachability Analyzer](#) 來協助確認提供使用者訂閱和 VPC 端點的執行個體的網路組態設定是否正確。您可以指定在子網路中啟動的執行個體識別碼，提供以使用者為基礎的訂閱做為來源，並指定為 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 做為要分析之路徑的目的地通訊埠。如需詳細資訊，請參閱[如何疑難排解闡道和介面 VPC 端點上的連線問題？](#)。

## 疑難排解執行個

使用者必須能夠使用 RDP 連線至提供使用者訂閱的執行個體，才能使用其中的產品。如需執行個體連線[疑難排解的詳細資訊](#)，請參閱 [Amazon EC2 使用者指南中的疑難排解連線到 Windows 執行個體](#)。

## 加入網域失敗的疑難排解

使用者必須能夠從 License Manager 設定中設定的目錄連線至提供以使用者為基礎之訂閱產品的執行個體。無法加入網域的執行個體將會終止。

若要進行疑難排解，您可能需要啟動執行個體並[手動加入網域](#)，以便資源不會終止，才能進行調查。執行個體必須成功接收並執行 Systems Manager 執行命令，而且執行個體也必須能夠在作業系統內完成網域加入。如需詳細資訊，請參閱《AWS Systems Manager 使用手冊》中的[了解命令狀態](#)和[如何疑難排解將 Windows 電腦加入 Microsoft 網站上的網域時所發生的錯誤](#)。

## 疑難排解 Systems Manager

提供以使用者為基礎的訂閱的執行個體必須由執行個體管理，AWS Systems Manager 否則將終止。如需詳細資訊，請參閱使用指南中的 [SSM 代理程式疑難排解](#)和[疑難排解受管節點可AWS Systems Manager 用性](#)。

## 故障診斷 Systems Manager 執行命令

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，以及針對包含的產品執行存取稽核。若要取得更多資訊，請參閱《使用指南》中的AWS Systems Manager [〈認識指令狀態](#)

## 授權管理員中的 Linux 訂閱

AWS License Manager 提供檢視及管理您擁有並執行之商業 Linux 訂閱的功能 AWS。您可以跨帳戶追蹤授權使用率，AWS 區域並在中追蹤 AWS Organizations。一旦發現並彙總資料，您就可以深入瞭解使用商業 Linux 訂閱的所有執行個體。此外，您探索到的訂閱資料將以 Amazon CloudWatch 儀表板的形式顯示在授權管理員主控台中。如果您的帳戶位於「組織」中，則可以將成員帳戶註冊為管理工作的委派管理員。如需詳細資訊，請參閱 [委派的管理員](#)。

您可以追蹤多個訂閱的使用率，例如：

- RHEL 企業版 (RHEL) 已包含訂閱
- RHEL 使用 Red Hat 雲端存取計畫的自攜訂閱模式 (BYOS)
- SUSE Linux Enterprise Server
- Ubuntu Pro

Linux 訂閱使用最終的一致性模型。一致性模型決定資料載入和呈現在 Linux 訂閱檢視中的方式和時間。使用此模式，授權管理員可確保您的 Linux 訂閱資料會定期從您的資源更新。如果在這些間隔期間沒有擷取某些資料，則會以下一個度量排放傳送資訊。此行為可能會延遲資源 (例如新啟動的 EC2 商業 Linux 執行個體)，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 小時才會被發現並報告。探索到您的資源後，系統會每小時針對 Linux 訂閱資料發出 Amazon CloudWatch 指標。

### 內容

- [管理 Linux 訂閱的探索](#)
  - [啟用 Linux 訂閱的探索](#)
  - [資源探索狀態原因](#)
  - [停用 Linux 訂閱的探索](#)
- [檢視發現的執行個體](#)
  - [檢視所有執行處理的資料](#)
  - [檢視每個訂閱的執行個體資料](#)

- [Linux 訂閱的帳單資訊](#)
- [Linux 訂閱的使用量指標和亞馬遜CloudWatch警示](#)
  - [Linux 訂閱的使用量測量結果](#)
  - [為 Linux 訂閱建立警示](#)
  - [修改 Linux 訂閱的警示](#)
  - [刪除 Linux 訂閱的警示](#)

## 管理 Linux 訂閱的探索

您可以使用授權管理員主控台管理 Linux 訂閱的探索。當您針對指定的啟用 Linux 訂閱的探索時，您可以選擇性地將此探查延伸至中的帳戶AWS Organizations。AWS 區域如果您不想再追蹤訂閱使用率，也可以停用探索。

### Note

AWS 區域依預設，每個帳號最多可以探索並顯示 5,000 個資源。若要要求提高這些限制，請使用[提高限制表單](#)。

### 主題

- [啟用 Linux 訂閱的探索](#)
- [資源探索狀態原因](#)
- [停用 Linux 訂閱的探索](#)

## 啟用 Linux 訂閱的探索

若要啟用 Linux 訂閱的探索，您需要在授權管理員中設定必要的設定。在設定頁面中，您可以建立服務連結角色、指定AWS 區域要在中啟用探索的角色，以及是否要探查中帳戶中AWS Organizations的資源。

若要啟用 Linux 訂閱的探索

1. 開啟授權管理員主控台，[網址為 https://console.aws.amazon.com/license-manager/](https://console.aws.amazon.com/license-manager/)。
2. 在左側的導覽窗格中，選擇 Settings (設定)。
3. 在「設定」頁面上，選擇 Linux 訂閱索引標籤，然後選擇「設定」。

4. 針對來源 AWS 區域，選擇您要探查其 Linux 訂閱的區域。
5. 如果您想要在中彙總所有帳戶的訂閱資料AWS Organizations，請選取 [連結] AWS Organizations。
6. 檢閱並認AWS License Manager可授與為 Linux 訂閱建立服務連結角色之權限的選項。
7. 選擇 Save configuration (儲存組態)。

## 資源探索狀態原因

AWS License Manager會針對AWS 區域您選擇啟用 Linux 訂閱的探索，顯示狀態和對應的狀態原因。如果您將 Linux 訂閱與以下項目連結，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。下表提供了更多詳細信息：

狀態原因動作	描述
船上帳戶	加入單一帳戶。
帳戶離線	註銷單一帳戶。
船上組織	加入整個組織。
板外組織	卸載整個組織。

您可以呼叫 UpdateServiceSettings API，然後呼叫 GetServiceSettings API 來監視啟用 Linux 訂閱的進度。每個狀態和狀態原因都可以同時套用至多個區域。下表提供狀態與狀態原因的詳細資訊：

狀態	狀態原因	描述
進行中	"Region": "Account-Onboard: Pending"	正在為單一帳戶啟用 Linux 訂閱。

狀態	狀態原因	描述
成功	"Region": "Org-Onboard: Pending"	正在為組織啟用 Linux 訂閱。
	"Region": "Account-Offboard: Pending"	停用單一帳戶的 Linux 訂閱正在進行中。
	"Region": "Org-Offboard: Pending"	正在停用組織的 Linux 訂閱。
	"Region": "Account-Onboard: Successful"	已成功啟用單一帳戶的 Linux 訂閱。
	"Region": "Org-Onboard: Successful"	已成功啟用組織的 Linux 訂閱。
	"Region": "Account-Offboard: Successful"	停用單一帳戶的 Linux 訂閱成功。
	"Region": "Org-Offboard: Successful"	已成功停用組織的 Linux 訂閱。
	失敗	"Region": "Account-Onboard: Failed - Service-linked role not present"
"Region": "Account-Onboard: Failed - An internal error occurred"		為單一帳戶啟用 Linux 訂閱失敗，因為發生內部錯誤。
"Region": "Org-Onboard: Failed - Account isn't the management account"		啟用組織的 Linux 訂閱失敗，因為執行作業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	描述
	"Region": "Org-Onboard: Failed - Account isn't part of an organization"	啟用組織的 Linux 訂閱失敗，因為執行作業的帳戶不在組織中。嘗試從組織中的帳戶進行操作，或將此帳戶添加到組織中，然後再試一次。
	"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"	啟用組織的 Linux 訂閱失敗，因為授權管理員沒有存取組織的權限。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。

### Warning

如果您停用探索，您先前針對 Linux 訂閱探索到的所有資料都會從中移除AWS License Manager。

### 若要停用 Linux 訂閱的探索

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側的導覽窗格中，選擇 Settings (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. (選擇性) 移除 Linux 訂閱所使用的服務連結角色。如需詳細資訊，請參閱[刪除授權管理員的服務連結角色](#)。
6. (選擇性) 停用授權管理員與組織之間的受信任存取。如需詳細資訊，請參閱 [AWS License Manager 及 AWS Organizations](#)。

## 檢視發現的執行個體

初始資源探索完成後，您將能夠檢視在AWS 區域您選取的中探索到的 Linux 訂閱。如果您選擇連結 AWS Organizations，來自整個組織帳戶的資料也會進行彙總。您可以瀏覽至主AWS License Manager 控制台的「執行個體」區段，以檢視資料表格。您可以瀏覽至主AWS License Manager控制台的「執行個體」區段，以檢視資料表格。

每個執行個體的資料包括下列項目：

- 執行個體 ID — 執行個體的 ID。
- 執行個體類型 — 執行個體的類型。
- 帳號 ID — 擁有執行個體的帳號 ID。
- 狀態 — 執行個體的状态。
- 區域 — 執行處理所AWS 區域在的位置。
- 使用操作 — 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[使用量操作值](#)。
- 產品代碼 — 與用於啟動實例的 AMI 相關聯的產品代碼。如需詳細資訊，請參閱[AMI 產品代碼](#)。
- AMI ID — 用來啟動執行個體的 AMI 識別碼。

### 主題

- [檢視所有執行處理的資料](#)
- [檢視每個訂閱的執行個體資料](#)

## 檢視所有執行處理的資料

您可以檢視所選區域內組織中所有帳戶的所有執行個體彙總資料。

若要檢視所有執行個體的探索資料

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在左側導覽窗格的 Linux 訂閱下，選擇 [執行個體]。
3. 視需要在主控台中檢閱資料。您可以通過以下方式過濾數據：
  - 執行個體 ID
  - 帳戶
  - 區域

- AMI ID
  - 使用操作
  - 產品代碼
4. (選擇性) 選擇「將檢視表匯出為 CSV」，將所有執行個體的資料匯出為逗號分隔值檔案 (CSV)。

## 檢視每個訂閱的執行個體資料

您可以檢視所選區域內組織中所有帳戶的所有執行個體已彙總的資料。

若要檢視具有特定訂閱的執行個體探索資料

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，然後視需要在主控台中檢閱資料。您可以通過以下方式過濾數據：
  - 執行個體 ID
  - 帳戶
  - 區域
  - AMI ID
  - 使用操作
  - 產品代碼
5. (選擇性) 選擇「將檢視表匯出為 CSV」，將具有此訂閱的執行個體資料匯出為逗號分隔值檔案 (CSV)。

## Linux 訂閱的帳單資訊

在亞馬遜 EC2 上執行的每個商業 Linux 訂閱都會有與亞馬遜機器映像 (AMI) 相關聯的帳單資訊。商用 Linux 訂閱將具有亞馬遜 EC2 使用操作、AWS Marketplace 產品代碼或兩者的組合。如需詳細資訊，請參閱《AWS Marketplace 賣家指南》中的 [Amazon 彈性運算雲端使用者指南和 AMI 產品代碼中的 AMI 帳單資訊](#) 欄位。

訂閱名稱	亞馬遜 EC2 使用操作	AWS Marketplace 產品代碼	訂閱類型
紅帽企業 Linux 伺服器自攜裝置	RunInstances:	X	攜帶您自己的訂閱模式 (BYOS)
紅帽企業伺服器	RunInstances:0010	X	已包含 EC2 訂閱
具有高可用性附加元件的紅帽企業 Linux	RunInstances : 1010	X	已包含 EC2 訂閱
具備 SQL 伺服器標準與高可用性的 RHEL	RunInstances : 1014	X	已包含 EC2 訂閱
紅帽企業 Linux 與 SQL 伺服器企業版和高可用性	RunInstances:1110	X	已包含 EC2 訂閱
帶 SQL Server Standard 的 Red Hat Enterprise Linux	RunInstances:0014	X	已包含 EC2 訂閱
帶 SQL Server Web 的 Red Hat Enterprise Linux	RunInstances:0210	X	已包含 EC2 訂閱
帶 SQL Server Enterprise 的 Red Hat Enterprise Linux	RunInstances : 0110	X	已包含 EC2 訂閱
SUSE Linux Enterprise Server	RunInstances : 千克	X	已包含 EC2 訂閱
適用於 SAP 的 RHEL，具有高可用性和更新服務	RunInstances:0010	✓	AWS Marketplace 訂閱 <sup>1</sup>
配備 SAP 的 SUSE 企業伺服器	X	✓	AWS Marketplace 訂閱

訂閱名稱	亞馬遜 EC2 使用操作	AWS Marketplace 產品代碼	訂閱類型
Ubuntu Pro	RunInstances : 0 克	✓	AWS Marketplace 訂閱
紅帽企業 Linux 工作站	x	✓	AWS Marketplace 訂閱

<sup>1</sup> 此訂閱同時具有 Amazon EC2 用量作業和AWS Marketplace產品代碼。

## Linux 訂閱的使用量指標和亞馬遜CloudWatch警示

AWS License Manager主控台的「訂閱」區段會列出您在購買AWS或使用「自攜訂閱」模式 (BYOS) 引入的探索到的商業 Linux 訂閱。所有商業 Linux 訂閱均以每個執行個體為基礎進行授權。

針對發現的 Linux 訂閱提供下列詳細資訊：

- 訂閱名稱
- 訂閱類型
- 每個訂閱的執行中執行個體數
- 配置亞馬遜CloudWatch警報

當您從摘要頁面選擇 Linux 訂閱時，使用狀況測量結果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 儀表板會在授權管理員主控台中顯示所選訂閱的訂閱。您可以調整儀表板以涵蓋特定時間範圍或評估範圍，以小時、天或一週為單位 (從選定日期開始)。

在使用量度和警示索引標籤中，每個訂閱都有「警示」區段，其中詳細說明下列內容：

- 警示名稱 — 警示的名稱。
- 狀態 — 警示的狀態。
- 尺寸 — 警報的尺寸。尺寸將包括已定義的AWS 區域和例證類型。
- 條件 — 警報的狀況。條件將包括比較運算子和已定義的警示臨界值。

您可以使用您定義的維度和條件來建立CloudWatch警示，以根據您目前的訂閱使用率追蹤和警示。Linux 訂閱主控台會顯示使用中的訂閱名稱、訂閱類型、每個執行個體的執行中執行個體數量，以及警示狀態的摘要。

以下是可能的CloudWatch警報狀態：

- 確定 — 測量結果或表示式在定義的臨界值內。
- ALARM — 測量結果或表示式超出定義的臨界值。
- UNAD@@ ICIENT\_DATA — 警示剛剛啟動、無法使用量度，或沒有足夠的資料可供指標判斷警示狀態。

## 主題

- [Linux 訂閱的使用量測量結果](#)
- [為 Linux 訂閱建立警示](#)
- [修改 Linux 訂閱的警示](#)
- [刪除 Linux 訂閱的警示](#)

## Linux 訂閱的使用量測量結果

下列量度和維度可供 Linux 訂閱使用：

指標	描述
RunningInstancesCount	<p>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：計數</p> <p>維度：</p> <p>SubscriptionName：訂閱的名稱。</p> <p>Region：發現使用商業 Linux 訂閱之資源的區域。</p>

## 為 Linux 訂閱建立警示

您可以為在執行中 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尺寸和條件的警示。

若要使用主控台建立 Linux 訂閱的CloudWatch警示

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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，選擇要建立鬧鐘的訂閱，然後選擇「建立鬧鐘」。
4. 為警示指定下列項目：
  - 警示名稱 — 指定類似AWS-LM-LS-*AlarmName*的名稱。
  - 執行個體類型 — 選擇要使用所選訂閱的執行個體類型。
  - 使用區域 — 選擇要建立警報的區域。
  - 比較運算子 — 警示臨界值的比較運算子。
  - 警示臨界值 — 警示臨界值的值。
5. 選擇 [建立] 以建立鬧鐘。

## 修改 Linux 訂閱的警示

您可以從 License Manager 主控台修改現有警示，以適應不斷變化的需求。

若要使用主控台修改 Linux 訂閱的CloudWatch警示

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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. 選擇編輯以修改鬧鐘。

## 刪除 Linux 訂閱的警示

您可以從 License Manager 主控台刪除現有警示，以適應不斷變化的需求。

若要使用主控台刪除 Linux 訂閱的CloudWatch警示

1. 開啟授權管理員主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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」。

## 中的設定AWS License Manager

該設定的部分AWS License Manager控制台顯示當前帳戶的設置。您必須配置設定以啟用某些功能，例如將受管理的權利和自我管理授權分配給組織，以及執行跨帳戶資源探索。

若要編輯 License Manager 設定

1. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
2. 在左側的導覽窗格中，選擇 Settings (設定)。
3. 選擇包含您要設定或修改之設定的索引標籤。例如，選擇受管理授權進行配置帳戶資料。
4. 針對您要設定或修改的設定選擇相關動作。例如，您可以選擇編輯或者開啟。

設定主題

- [受管理授權](#)
  - [帳戶詳細資訊](#)
  - [Cross-account resource discovery \(跨帳戶資源探索\)](#)
  - [Simple Notification Service \(SNS\)](#)
- [訂閱](#)
- [基於用戶的訂閱](#)
  - [AWS Managed Microsoft AD](#)
  - [虛擬私有雲](#)
- [委派的管理員](#)
  - [委派管理員支援的區域](#)
  - [註冊委派管理員](#)
  - [取消註冊委派的管理員](#)

## 受管理授權

管理的授權可以使用以下設定。

## 帳戶詳細資訊

您可以檢視您的帳戶詳細資料，以查看帳戶類型、帳戶是否在AWS Organizations已連結，帳戶的License Manager S3 儲存貯體 ARN，以及AWS Resource Access Manager分享 ARN。本節還使您可以鏈接AWS Organizations帳戶。

若要在組織內散佈受管理的權利或自我管理授權，請選擇鏈接AWS Organizations帳戶。您的所有成員帳戶都會自動接受受管理權利的分散式授權。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，您必須登入您的管理員帳戶，且所有功能都必須在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](#)。此選取也會建立AWS Resource Access Manager管理帳戶中的資源共用，可讓您順暢地共用自我管理授權。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)

您可以開啟跨帳號資源探索，以便管理所有帳號的授權使用情況AWS Organizations。

若要在組織中啟用跨帳號資源探索，請選擇開啟用於探索跨帳號的資源追蹤。當您開啟跨帳號資源探索時，AWS Organizations系統會自動連結，以便在您的所有帳號中執行資源探索。

License Manager 使用[Systems Manager 存放區](#)發現軟件的使用情況。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：

- [資源資料同步](#)存放庫存放在 Amazon S3 存放區。
- [Amazon Athena](#)以匯總您帳戶的庫存資料AWS Organizations。
- [AWS Glue](#)提供快速的查詢體驗。

### Note

以下AWS 區域不需要Amazon Athena或者AWS Glue查詢或彙總 Systems Manager 庫存的庫存資料，以探索軟體使用情況：

- 亞太區域 (雅加達)
- 以色列 (特拉維夫)

## Simple Notification Service (SNS)

您可以設定 Amazon SNS 以接收來自 License Manager 的通知和警示。

若要設定 Amazon SNS 主題

1. 選擇編輯旁邊的 Simple Notification Service (SNS)。
2. 以下列格式指定 SNS 主題：

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

3. 選擇 Save Changes (儲存變更)。

## 訂閱

您可以設定 Linux 訂閱的設定，以控制如何執行訂閱的探索和彙總。您可以選擇要探索其 Linux 訂閱的區域，以及是否要彙總帳戶中的訂閱資料 AWS Organizations。如需詳細資訊，請參閱[授權管理員中的 Linux 訂閱](#)。

## 基於用戶的訂閱

根據您需要使用者訂閱的產品，可以使用下列設定。

### AWS Managed Microsoft AD

License Manager 需要 AWS Managed Microsoft AD 在您可以使用以使用者為基礎的訂閱之前進行配置。如需詳細資訊，請參閱[License Manager 中的使用者型訂閱](#)。

### 虛擬私有雲

許可證管理器除了您的 VPC 之外，還要求配置您的 VPC AWS Managed Microsoft AD，當您使用以使用者為基礎的訂閱搭配 Microsoft Office 時。如需詳細資訊，請參閱[License Manager 中的使用者型訂閱](#)。

## 委派的管理員

您可以註冊委派的管理員，以管理員，以管理員，以管理員的管理員，以管 License Manager 員工作。為了簡化管理，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。使用此方法，您的組織中將擁有一個 License Manager 的單一委派管理員。

使用AWS CLI或 SDK，您可以將組織中的不同成員帳戶註冊為 License Manager 每個受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針對受管理的授權和 Linux 訂閱執行管理工作。

### Important

若要在 License Manager 主控台中使用委派的系統管理功能，您必須擁有與 License Manager 每個功能之委派系統管理員相同的成員帳戶。如果您將多個會員帳戶註冊為委派的管理員，則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。

在註冊委派管理員之前，您必須先啟用 Organizations 的信任存取權。如需詳細資訊，請參閱[邀請AWS 帳戶以加入您組織的帳戶](#)和[啟用的可信任存取AWS Organizations](#)。

下列是您可以註冊委派管理員的功能：

### 受管理授權

您可以執行管理工作，例如與其他成員帳戶共用自我管理授權、執行跨帳號資源探索，以及將受管理的權利分配給其他成員帳戶。

### 訂閱

您可以執行管理工作，例如檢視和管理您擁有和執行的商業 Linux 訂閱AWS 區域和您的帳戶AWS Organizations。您還可以創建和管理員工 CloudWatch 為您的 Linux 訂閱提供警示。必須先探查並彙總資料，然後才能在 License Manager 主控台中看到該資料，如果已設定警示，任何警示都可以運作。

### Important

註冊後，委派的管理員即可查看組織中帳戶所擁有的 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。

## 委派管理員支援的區域

下列區域支援 License Manager 委派的管理員：

- 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)
- 亞太區域 (雪梨)
- 亞太區域 (東京)
- 亞太區域 (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)

## 註冊委派管理員

您可以註冊委派的管理員，AWS CLI或者AWS Management Console。

### Console

註冊委派的管理員，AWS License Manager控制台，執行以下步驟：

1. 登入AWS作為管理帳戶的管理員。

2. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
3. 選擇設定從左側的導航窗格。
4. 選擇合適的委派的管理標籤。
5. 選擇 Register delegated administrator (註冊委派管理員)。
6. 輸入要註冊為委派管理員的成員帳戶 ID，確認您要授與 License Manager 必要的權限，然後選擇註冊。
7. 會出現一則訊息，指出指定的帳戶是否已成功註冊為委派的系統管理員 License Manager。

## AWS CLI

若要註冊管理員，以管理員的管理員，以AWS CLI，執行下列步驟：

1. 從命令列執行以下命令AWS CLI命令：

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

2. 執行下列命令，以驗證指定的管理員，以委派的管理員，以委派的管理員身分成功：

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

使用註冊委派的管理員，以註冊委派的管理員，AWS CLI，執行下列步驟：

1. 從命令列執行以下命令AWS CLI命令：

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

2. 執行下列命令，以驗證指定的管理員，以委派的管理員，以委派的管理員身分成功：

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

## 取消註冊委派的管理員

您可以註冊委派的管理員，AWS CLI或者AWS Management Console。

## Console

若要取消註冊委派的管理員，AWS License Manager控制台，執行以下步驟：

1. 登入AWS作為管理帳戶的管理員。
2. 開啟 License Manager 主控台，位於<https://console.aws.amazon.com/license-manager/>。
3. 選擇設定從左側的導航窗格。
4. 選擇合適的委派的管理標籤。
5. 選擇 Remove (移除)。
6. 輸入文字**remove**以確認您要移除 License Manager 的委派系統管理員，然後選擇移除。
7. 會出現一則訊息，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AWS CLI，執行下列步驟：

1. 從命令列執行以下命令AWS CLI命令：

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

2. 執行下列命令，以驗證指定的管理員，以委派的管理員，以委派的管理員身分成功：

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

若要使用AWS CLI，執行下列步驟：

1. 從命令列執行以下命令AWS CLI命令：

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

2. 執行下列命令，以驗證指定的管理員，以委派的管理員，以委派的管理員身分成功：

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

您可以隨時註冊一個註冊的帳戶。

## 儀表板 AWS License Manager

License Manager 主控台的 [儀表板] 區段提供使用詳細資料，以追蹤與每個自我管理授權相關聯的授權使用量、授與的授權權利、使用者型訂閱的訂閱使用者以及執行中的執行個體。該儀表板也會顯示因違反授權規則產生的提醒。

### 概要

概觀區段提供下列有關授權的詳細資訊。

#### 授予的授權

此區域中此帳戶授予的授權總數。

#### 自我管理的授權

此區域中此帳戶中自我管理授權的總數量。

#### 賣家核發的授權

此帳戶在此區域中，賣家核發的授權總數。

### 產品

「產品」區段提供以使用者為基礎的訂閱的下列詳細資訊

#### 產品名稱

以使用者為基礎的訂閱的名稱產品。

#### 訂閱使用者

產品的訂閱使用者數量。

## 授與的授權利

授與的授權區段提供下列詳細資訊。

### 產品名稱

授與授權的產品名稱。

### Entitlement

權利的名稱。

### 用量

權利的使用。

## 自我管理的授權

自我管理授權提供下列詳細資料。

### 執照名稱

自我管理的授權名稱。

### Entitlement

權利的名稱。

### 用量

權利的使用。

## 執行個體用量

執行處理使用段落提供下列詳細資訊。

### 執行執行個體數

此區域中此帳戶中執行中的執行個體總數。

### 彙總執行執行個體數

您在此區域中所有帳戶彙總的執行AWS Organizations中執行個體總量。此圖表只能從管理帳戶和委派的系統管理員帳戶中看到。

# 監控 AWS License Manager

您可以監控AWS License Manager使用 Amazon 追蹤的授權和訂閱的使用情況 CloudWatch。CloudWatch 收集原始資料並將該資料處理成可讀且近乎即時的指標。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。如需詳細資訊，請參閱[使用 Amazon Amazon Simple 使用 Amazon CloudWatch](#)。

您可以擷取來自或代表您使用的 API 呼叫和相關事AWS 帳戶件AWS CloudTrail。事件會以日誌檔案的形式傳遞到您指定的 Amazon S3 儲存貯體。您可以找出哪些使用者和帳戶呼叫 AWS、發出呼叫的來源 IP 地址，以及呼叫的發生時間。如需詳細資訊，請參閱[使用 AWS CloudTrail 記錄 AWS License Manager API 呼叫](#)。

## 內容

- [使用 Amazon Amazon Simple 使用 Amazon CloudWatch](#)
  - [建立立立立立立警示來 License Manager 立立](#)
- [使用 AWS CloudTrail 記錄 AWS License Manager API 呼叫](#)
  - [License Manager 資訊 CloudTrail](#)
  - [瞭解 License Manager 記錄檔項目](#)

## 使用 Amazon Amazon Simple 使用 Amazon CloudWatch

您可以使用 Amazon 監控 License Manager 的指標統計資料 CloudWatch。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，您可以觀察使用LicenseConfigurationUsagePercentage指標的授權百分比，並在超出限制之前採取行動。如需詳細資訊，請參閱[Amazon Amazon Amazon Amazon Amazon CloudWatch 使用者指南](#)。

License Manager 會在AWSLicenseManager/licenseUsage命名空間中每小時發出下列量度：

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：計數 維度：

指標	描述
	SubscriptionName : 訂閱的名稱。
AggregateRunningInstancesCount	<p>目前在AWS Organizations您所有帳戶上執行的執行個體彙總總數AWS 區域。</p> <p>單位：計數</p> <p>維度：</p> <p>SubscriptionName : 訂閱的名稱。</p>
TotalLicenseConfigurationUsageCount	<p>可以使用的授權組態總數。</p> <p>單位：計數</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：計數</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>此授權組態的已使用授權，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>

## 建立立立立立立立警示來 License Manager 立立

您可以建立 CloudWatch 警示，並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呼叫動作。CloudWatch 警示不會只叫用動作，因為它們處於特定狀態；狀態必須已變更，並且已維護指定數目的時段。如需詳細資訊，請參閱 [CloudWatch 閱](#)。

## 使用 AWS CloudTrail 記錄 AWS License Manager API 呼叫

AWS License Manager 整合了 AWS CloudTrail，這種服務提供由使用者、角色或使用 License Manager 中 AWS 服務所採取之行動的記錄。CloudTrail 將 License Manager 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 License Manager 主控台進行的呼叫，以及對 License Manager API 操作的程式碼呼叫。如果您建立追蹤，就可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 License Manager 的事件。即使未設定追蹤，您依然可以在 CloudTrail 主控台中檢視最新事件。您可以使用 CloudTrail 收集的資訊來判斷向 License Manager 發出的請求，以及發出請求的 IP 地址、人員、時間和其他詳細資訊。

若要進一步了解 CloudTrail，請參閱 [AWS CloudTrail 使用者指南](#)。

## License Manager 資訊 CloudTrail

CloudTrail 當您建立 AWS 帳戶時，系統會在帳戶中啟用。此外，License Manager 發生活動時，系統便會將該活動記錄至 CloudTrail 事件，並將其他 AWS 服務事件記錄至事件歷史記錄中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。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 AWS 帳戶中的事件，包括 License Manager 的事件，請建立追蹤。線索能 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 Amazon S3 儲存貯體。此外，您還能設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料，並採取相應動作。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](#)
- [設定的 Amazon SNS 通知通知通知 CloudTrail](#)
- [從多個區域接收 CloudTrail 日誌檔案，以及從多個帳戶接收 CloudTrail 日誌檔案項目](#)

所有 License Manager 動作都會記錄在 [License Manager API 參考](#) 中。CloudTrail 例如，呼叫 `ListResourceInventory` 和 `DeleteLicenseConfiguration` 動作會 `CreateLicenseConfiguration` 在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 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。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 [CloudTrail 使用者身分元素](#)。

## 瞭解 License Manager 記錄檔項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付至您指定的 Amazon S3 儲存貯體。CloudTrail 記錄檔項目。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 日誌檔案並非依公有 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"  
}
```

# AWS License Manager 中的安全性

雲端安全是 AWS 最重視的一環。身為 AWS 客戶的您，將能從資料中心和網路架構的建置中獲益，以滿足組織最為敏感的安全要求。

安全是 AWS 與您共同肩負的責任。[共同責任模型](#)將其描述為雲端的安全性和雲端中的安全性：

- 雲端本身的安全 – AWS 負責保護在 AWS Cloud 中執行 AWS 服務的基礎設施。AWS 也提供您可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全性的有效性，作為 [AWS 合規計劃](#) 的一部分。若要了解適用於 License Manager 的合規計劃，請參閱合規計劃的 [AWS 服務範圍合規計劃](#) 的服務範圍。
- 雲端內部的安全 – 您的責任取決於所使用的 AWS 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

本文件有助於您了解如何在使用 License Manager 時套用共同責任模型。說明如何設定以符 License Manager 您的安全性和合規目標。您也將了解如何使用其他 AWS 服務來協助監控並保護 License Manager 資源。

## 內容

- [AWS License Manager 中的資料保護](#)
- [適用於 AWS License Manager 的 Identity and Access Management](#)
- [使用 AWS License Manager 的服務連結角色](#)
- [AWS License Manager 的 AWS 受管政策](#)
- [授權的密碼編譯簽署](#)
- [符合性驗證 AWS License Manager](#)
- [AWS License Manager 中的恢復能力](#)
- [AWS License Manager 中的基礎設施安全](#)
- [AWS License Manager 和介面 VPC 端點 \(AWS PrivateLink\)](#)

# AWS License Manager 中的資料保護

AWS [共同的責任模型](#)適用於 AWS License Manager 中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端的全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務的安全組態和管理任務。如需有關資料隱私權的更多相關資訊，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 共同的責任模型](#) 和 [GDPR](#) 部落格文章。

基於資料保護目的，建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶憑證，並設定個人使用者。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 AWS CloudTrail 設定 API 和使用者活動日誌記錄。
- 使用 AWS 加密解決方案，以及 AWS 服務內的所有預設安全控制項。
- 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。
- 如果您在透過命令列介面或 API 存取 AWS 時，需要 FIPS 140-2 驗證的加密模組，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 \(FIPS\) 140-2 概觀](#)。

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 Name (名稱) 欄位。這包括當您使用 License Manager 或其他 AWS 服務使用主控台 AWS CLI、API 或 AWS SDK 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 將資料存放在管理帳戶的 Amazon S3 儲存貯體中。儲存貯體是使用 Amazon S3 受管加密金鑰 (SSE-S3) 進行設定。

## 適用於 AWS License Manager 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務，讓管理員能夠安全地控制對 AWS 資源的存取權限。IAM 管理員可以控制「已驗證」(已登入) 和「已授權」(具有許可) 來使用 AWS 資源。有了 IAM，您可以在 AWS 帳戶下建立使用者與群組。您可以控制使用者使用 AWS 資源執行任務所具有的許可。您可以免費使用 IAM。

根據預設，使用者不具備 License Manager 資源和操作的許可。若要允許使用者管理 License Manager 資源，您必須建立一個 IAM 策以明確授予許可。

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 AWS 帳戶 建立使用者和群組，然後為其指派所需的許可。作為最佳實務，使用者應透過擔任 IAM 角色來取得許可。如需有關如何為設定使用者與群組的詳細資訊AWS 帳戶，請參閱[開始使用 AWS License Manager](#)。

[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，因為同樣是 AWS 身分，也有許可政策可決定該身分在 AWS 中可執行和不可執行的操作。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

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"
      }
    }
  ]
}
```

陳述式由各種元素組成：

- **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。明確允許覆寫預設值。明確拒絕覆寫任何允許。
- **動作**：動作是您授與或拒絕權限的特定 API 作業。

- 資源：資源受動作影響。有些 License Manager API 操作可讓您在政策中包含可由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 [AWS License Manager 定義的動作](#)。
- 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 [條件金鑰AWS License Manager](#)。

## 建立 License Manager 的 IAM 政策

在 IAM 政策陳述式中，您可以從任何支援 IAM 的服務指定任何 API 操作。License Manager 會在 API 作名稱使用下列字首：

- 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

如需有關可用 License Manager API 的詳細資訊，請參閱下列 API 參考資料：

- [AWS License Manager API 參考](#)
- [AWS License Manager 使用者訂閱 API 參考](#)
- [AWS License Manager 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，您可以指定名稱開頭有 List 文字的所有 License Manager API 操作，如下所示：

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

若要指定所有的 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 範例原則

透過 License Manager 散發授權的 ISV 需要下列權限：

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

## 向使用者、群組和角色授予許可

建立所需的 IAM 政策後，您必須將這些權限授與使用者、群組和角色。

若要提供存取權，請新增許可到您的使用者、群組或角色：

- AWS IAM Identity Center 中的使用者和群組：

建立許可集合。請遵循《AWS IAM Identity Center 使用者指南》的[建立許可集合](#)中的指示。

- 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。請遵循《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。請遵循《IAM 使用者指南》的[為 IAM 使用者建立角色](#)中的指示。
- (不建議) 將政策直接連接至使用者，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 AWS License Manager 的服務連結角色

AWS License Manager 使用 AWS Identity and Access Management (IAM) [服務連結的角色](#)。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，並包含服務代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓您輕鬆設定 License Manager，因為您不必手動新增必要的權限。License Manager 會定義其服務連結角色的權限，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。這樣可以保護您的 License Manager 資源，因為您無法意外移除存取資源的權限。

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 — 使用者型訂閱角色](#)
- [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。

## 核心角色的權限

名為的服務連結角色 `AWSServiceRoleForAWSLicenseManagerRole` 可讓 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。

若要檢閱的權限 `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](#)。

## 為 License Manager 建立服務連結角色

您不需要手動建立一個服務連結角色。當您第一次造訪 License Manager 主控台時完成 License Manager 首次執行體驗表單時，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，License Manager 會在您的帳戶中建立 `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 主控台建立服務連結角色。

### 建立 服務連結角色

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 選擇開始使用 License Manager。
3. 在 IAM 許可 (one-time-setup) 表單中，選取 [我授與必要 AWS License Manager 的權限]，然後選擇 [繼續]。

您也可以使用 IAM 主控台，透過 License Manager 使用案例建立服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用 IAM 建立具有 `license-manager.amazonaws.com` 服務名稱的服務連結角色。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。如需更多資訊，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，您就只有受到主動監視或維護的實體。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授權與相關執行個體和 AMI 的關聯，然後刪除自我管理授權。

#### Note

當您嘗試刪除資源時，如果 License Manager 正在使用此角色，則刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試該動作。

### 刪除核心角色使用的 License Manager 資源

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
2. 在瀏覽窗格中，選擇 [自我管理授權]。
3. 選擇您身為擁有者的自我管理授權，並取消關聯 AMI 和資源索引標籤中所有項目的關聯。針對每個授權組態重複此程序。
4. 仍在自我管理的授權頁面上時，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。如果您同時使用 [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。

### 管理帳戶角色的權限

名為的服務連結角色 `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` 可讓 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。

若要檢閱的權限 `AWSLicenseManagerMasterAccountRolePolicy`，請參閱 [AWS 受管政策：AWSLicenseManagerMasterAccountRolePolicy](#)。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。當您在中配置跨帳戶授權管理時 AWS Management Console，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，當它開始支援服務連結

角色時，則AWSServiceRoleForAWSLicenseManagerMasterAccountRole在您的帳戶中建立 License Manager。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. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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 管理帳戶使用案例建立服務連結角色。或者，在AWS CLI或 AWS API 中，使用 IAM 建立具有license-manager.master-account.amazonaws.com服務名稱的服務連結角色。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。如需更多資訊，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，您就只有受到主動監視或維護的實體。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 主控台或 AWS CLI 或 AWS API 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，以允許管理帳戶管理授權。

### 成員帳戶角色的權限

名為的服務連結角色 `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` 可讓 License Manager 代表您從已設定的管理帳戶存取授權管理動作的 AWS 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。

若要檢閱的權限 `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 AWS Organizations 從 [設定] 頁面上的 [License Manager] 主控台管理帳戶啟用與整合。您也可以使用 AWS CLI ( 運行 `update-service-settings` ) 或 AWS API ( 調 `UpdateServiceSettings` 用 ) 來執行此操作。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 主控台或 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的角色時，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. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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[AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#)在所有子帳號中建立角色[AWSServiceRoleForAWSLicenseManagerRole](#)。

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license-manager.member-account.amazonaws.com服務名稱建立服務連結角色。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](#)。

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。如需更多資訊，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，您就只有受到主動監視或維護的實體。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AWS CLI台或 AWS API 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 — 使用者型訂閱角色

License Manager 需要服務連結角色，才能管理將提供以使用者為基礎的訂閱的AWS資源。

## 以使用者為基礎的訂閱角色的權限

名為的服務連結角色 `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` 可讓 License Manager 利用 AWS Systems Manager 和管理提供以使用者為基礎的訂閱的 Amazon EC2 資源，以及描述 AWS Directory Service 資源。

若要檢閱的權限 `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 主控台以使用者為基礎的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 主控台建立服務連結角色。

### 建立 服務連結角色

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。
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 `license-manager-user-subscriptions.amazonaws.com` 服務名稱建立服務連結角色。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](#)。

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。如需更多資訊，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，您就只有受到主動監視或維護的實體。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 主控台或 AWS CLI 或 AWS API 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，才能管理將提供 Linux 訂閱的 AWS 資源。

### Linux 訂閱角色的權限

名為的服務連結角

色 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 可讓 License Manager 探索 Amazon EC2 和 AWS Organizations 資源，以彙總 Linux 訂閱的使用量。

若要檢閱的權限 `AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`，請參閱[AWS 受管政策：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。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，因為系統會在 License Manager 主控台 Linux 訂閱頁面上提示您建立角色。

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 主控台或 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 主控台建立服務連結角色。

### 建立 服務連結角色

1. 開啟 License Manager 主控台，網址為 <https://console.aws.amazon.com/license-manager/>。

2. 在左側導覽窗格中，選擇 [訂閱] 或 [執行個體]。
3. 同意 License Manager 的條款，以建立 Linux 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 - Linux subscriptions 使用案例的服務連結角色。或者，在 AWS CLI 或 AWS API 中，使用 `license-manager-linux-subscriptions.amazonaws.com` 服務名稱建立服務連結角色。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](#)。

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。如需更多資訊，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，您就只有受到主動監視或維護的實體。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 AWS CLI 台或 AWS API 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 AWS 受管政策

若要新增許可給使用者、群組和角色，使用 AWS 受管政策比自己撰寫政策更容易。[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 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中可用。如需 AWS 受管政策的更多相關資訊，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。您無法更改 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 支援跨越多項服務之任務職能的受管政策。例如，ReadOnlyAccess AWS 受管政策提供針對所有 AWS 服務和資源的唯讀存取權限。當服務啟動新功能時，AWS 會為新的操作和資源新增唯讀許可。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

此原則會附加至名為的服務連結角色，AWSServiceRoleForAWSLicenseManagerRole以允許 License Manager 呼叫 API 動作以代表您管理授權。如需服務連結角色的詳細資訊，請參閱[核心角色的權限](#)。

角色權限原則可讓 License Manager 對指定的資源完成下列動作。

動作	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>

動作	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	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

若要在中檢視此原則的權限AWS Management Console，請參閱[AWSLicenseManagerServiceRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerMasterAccountRolePolicy

此原則會附加至名為的服務連結角

色，AWSServiceRoleForAWSLicenseManagerMasterAccountRole以允許 License Manager 呼叫 API 動作，以代表您對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](#)。

角色權限原則可讓 License Manager 對指定的資源完成下列動作。

動作	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-*
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-*

動作	資源 ARN
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3>DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	請參閱註腳 <sup>1</sup>
glue:UpdateTable	請參閱註腳 <sup>1</sup>
glue>DeleteTable	請參閱註腳 <sup>1</sup>
glue:UpdateJob	請參閱註腳 <sup>1</sup>
glue:UpdateCrawler	請參閱註腳 <sup>1</sup>
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*

動作	資源 ARN
<code>organizations:ListParents</code>	*
<code>organizations:ListAccountsForParent</code>	*
<code>organizations:ListRoots</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*
<code>ram:GetResourceShares</code>	*
<code>ram:GetResourceShareAssociations</code>	*
<code>ram:TagResource</code>	*
<code>ram:CreateResourceShare</code>	*
<code>ram:AssociateResourceShare</code>	*
<code>ram:DisassociateResourceShare</code>	*
<code>ram:UpdateResourceShare</code>	*
<code>ram&gt;DeleteResourceShare</code>	*
<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>

動作	資源 ARN
<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>

<sup>1</sup> 以下是針對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`

若要在中檢視此原則的權限AWS Management Console，請參閱[AWSLicenseManagerMasterAccountRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerMemberAccountRolePolicy

此原則會附加至名為的服務連結角

色，AWSServiceRoleForAWSLicenseManagerMemberAccountRole以允許 License Manager 代表您從已設定的管理帳戶呼叫 API 動作以進行授權管理。如需詳細資訊，請參閱 [License Manager — 成員帳戶角色](#)。

角色權限原則可讓 License Manager 對指定的資源完成下列動作。

動作	資源 ARN
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:GetLicenseConfiguration	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:CreateResourceDataSync	*
ssm>DeleteResourceDataSync	*
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

若要在中檢視此原則的權限AWS Management Console，請參閱[AWSLicenseManagerMemberAccountRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerConsumptionPolicy

您可將 AWSLicenseManagerConsumptionPolicy 政策連接到 IAM 身分。此原則授與允許存取使用授權所需的 License Manager API 動作的權限。如需詳細資訊，請參閱 [授權使用](#)。

若要檢視此政策的許可，請參閱 AWS Management Console 中的 [AWSLicenseManagerConsumptionPolicy](#)。

## AWS 受管政策：AWSLicenseManagerUserSubscriptionsServiceRolePolicy

此原則會附加至名為

原AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService則的服務連結角色，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 — 使用者型訂閱角色](#)。

角色權限原則可讓 License Manager 對指定的資源完成下列動作。

動作	資源 ARN
ds:DescribeDirectories	*
ds:GetAuthorizedApplicationDetails	*
ec2:CreateTags	ARN : awy : ec2 : * : * : 實例 /* <sup>1</sup>
ec2:DescribeInstances	*
ec2:DescribeVpcPeeringConnections	*
ec2:TerminateInstances	ARN : awy : ec2 : * : * : 實例 /* <sup>1</sup>
ssm:DescribeInstanceInformation	*
ssm:GetCommandInvocation	*
ssm:GetInventory	*
ssm:ListCommandInvocations	*
ssm:SendCommand	ARN : AWS : SSM : * : : 文檔/ AWS- <sup>2</sup> RunPowerShellScript

動作	資源 ARN
	arn : awy : ec2 : * : * : 實例 /* <sup>2</sup>

<sup>1</sup> License Manager 只能在具有產品代碼 `bz0vcy31` 的執行個體上建立標籤和終止執行個體，或 `d44g89hc0gp9jdzm99rzw`。

<sup>2</sup> License Manager 只能在標籤名稱 `AWSLicenseManager` 且值為的執行個體上執行 `AWS-RunPowerShellScript` 文件的 SSM Run 指令。UserSubscriptions

若要在中檢視此原則的權限AWS Management Console，請參閱 [AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。

## AWS 受管政策：AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

此原則會附加至名為

原 `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` 則的服務連結角色，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](#)。

角色權限原則可讓 License Manager 對指定的資源完成下列動作。

動作	資源 ARN
<code>ec2:DescribeInstances</code>	*
<code>ec2:DescribeRegions</code>	*
<code>organizations:DescribeOrganization</code>	*
<code>organizations:ListAccounts</code>	*
<code>organizations:DescribeAccount</code>	*
<code>organizations:ListChildren</code>	*
<code>organizations:ListParents</code>	*
<code>organizations:ListAccountsForParent</code>	*

動作	資源 ARN
<code>organizations:ListRoots</code>	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	*
<code>organizations:ListDelegatedAdministrators</code>	*

若要在中檢視此原則的權限AWS Management Console，請參閱[AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

## AWS受管理策略的 License Manager 更新

檢視由於此服務開始追蹤這些變更以來，License Manager 的AWS受管理原則更新的詳細資料。

變更	描述	日期
<a href="#">AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy</a> – 新政策	License Manager 新增了建立名為AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService 的服務連結角色的權限。此角色提供 License Manager 列出AWS Organizations和 Amazon EC2 資源的權限。	2022 年 12 月 21 日
<a href="#">AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> – 更新現有政策	License Manager 已新增ec2:DescribeVpcPeeringConnections 權限。	2022 年 11 月 28 日
<a href="#">AWSLicenseManagerUserSubscriptionsServiceRolePolicy</a> – 新政策	License Manager 新增了建立名為AWSLicenseManagerUserSubscriptionsServiceRolePolicy 的服務連結角色的權限。此角色提供	2022 年 7 月 18 日

變更	描述	日期
	License Manager 權限，以列出AWS Directory Service資源、使用 Systems Manager 功能，以及管理針對使用者訂閱建立的 Amazon EC2 資源。	
<a href="#">AWSLicenseManagerMasterAccountRolePolicy</a> – 更新現有政策	License Manager 新增了由管理之資源群組的resource-groups:PutGroupPolicy 權限AWS Resource Access Manager。	2022 年 6 月 27 日
<a href="#">AWSLicenseManagerMasterAccountRolePolicy</a> – 更新現有政策	License Manager 將的AWS受管理原則AWSLicenseManagerMasterAccountRolePolicy <a href="#">條件金鑰AWS Resource Access Manager</a> 從使用變更ram:ResourceTag 為aws:ResourceTag 。	2021 年 11 月 16 日
<a href="#">AWSLicenseManagerConsumptionPolicy</a> – 新政策	License Manager 新增了授與使用授權之權限的新原則。	2021 年 8 月 11 日
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 新增了列出委派管理員的權限，以及建立名為AWSServiceRoleForAWSLicenseManagerMemberAccountRole 之服務連結角色的權限。	2021 年 6 月 16 日
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 添加了列出所有 License Manager 資源的權限，例如許可證配置，許可證和授予。	2021 年 6 月 15 日

變更	描述	日期
<a href="#">AWSLicenseManagerServiceRolePolicy</a> – 更新現有政策	License Manager 新增了建立名為AWSServiceRoleForMarketplaceLicenseManagement 的服務連結角色的權限。此角色提供在 License Manager 中建立和管理授權的權限。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 開始追蹤變更	License Manager 開始追蹤其 AWS 受管理策略的變更。	2021 年 3 月 9 日

## 授權的密碼編譯簽署

License Manager 可以透過密碼編譯方式簽署由 ISV 或代表 ISV 核 AWS Marketplace 發的授權。簽署允許廠商在應用程式本身內驗證授權的完整性和來源，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 且在 AWS Key Management Service (AWS KMS) 中受保護的非對稱。這個客戶管理的 CMK 由數學相關的公鑰和私 key pair 組成。當使用者請求授權時，License Manager 會產生列出授權權利的 JSON 物件，並使用私密金鑰簽署此物件。簽名和純文字 JSON 物件會傳回給使用者。與這些物件一起呈現的任何一方都可以使用公開金鑰來驗證授權文字尚未變更，以及授權是否由私密金鑰的擁有者簽署。key pair 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 < [使用對稱與非對稱金鑰](#) >。

### Note

License Manager 會在簽署 AWS KMS [Sign](#)和驗證授權時呼叫和 [Verify](#)API 作業。CMK 必須具有 [SIGN\\_VERIFY](#) 的索引鍵使用值，這些作業才能使用它。這種 CMK 不能用於加密和解密。

下列工作流程描述發行密碼編譯簽署的授權：

1. 在 AWS KMS 主控台、API 或 SDK 中，授權管理員會建立非對稱的客戶管理 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 CMK](#) 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 的耗用配置。組態可以指定「借入」和「暫時」選項之一，也可以同時指定。如需詳細資訊，請參閱[建立賣家發出的授權區塊](#)。
3. 終端使用者使用[CheckoutLicense](#)或 [CheckoutBorrowLicense](#)API 作業取得授權。僅在已設定「借用」的授權上執CheckoutBorrowLicense行此作業。它返回一個數字簽名作為響應的一部分以及 JSON 對象列表權利。純文字 JSON 類似下列內容：

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

## 符合性驗證 AWS License Manager

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱[AWS 服務 遵循規範計劃](#)方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱[AWS 規範計劃](#)。

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[下載中的報告中的 AWS Artifact](#)。

您在使用時的合規責任取決 AWS 服務 於您資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- [安全性與合規性快速入門指南](#) — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- [在 Amazon Web Services 上架構 HIPAA 安全性與合規性](#) — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

#### Note

並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 [HIPAA 資格服務參照](#)。

- [AWS 合規資源AWS](#) — 此工作簿和指南集合可能適用於您的產業和所在地。
- [AWS 客戶合規指南](#) — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- [使用AWS Config 開發人員指南中的規則評估資源](#) — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- [AWS Security Hub](#) — 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 [Security Hub controls reference](#)。
- [Amazon GuardDuty](#) — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，例如 PCI DSS 等各種合規性需求。
- [AWS Audit Manager](#) — 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

## AWS License Manager 中的恢復能力

AWS 全球基礎設施是以 AWS 區域與可用區域為中心建置的。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、容錯能力和擴充能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域與可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

## AWS License Manager 中的基礎設施安全

作為託管服務，AWS License Manager 受到 AWS 全球網絡安全的保護。如需有關 AWS 安全服務以及 AWS 如何保護基礎設施的詳細資訊，請參閱 [AWS 雲端安全](#)。若要使用基礎設施安全性的最佳實務來設計您的 AWS 環境，請參閱安全性支柱 AWS 架構良好的框架中的 [基礎設施保護](#)。

您可以使用 AWS 已發佈的 API 呼叫透過網路存取授權管理員。用戶端必須支援下列項目：

- 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。

此外，請求必須使用存取索引鍵 ID 和與 IAM 主體相關聯的私密存取索引鍵來簽署。或者，您可以使用 [AWS Security Token Service](#) (AWS STS) 來產生暫時安全憑證來簽署請求。

## AWS License Manager 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 Virtual Private Cloud (VPC) 和 AWS License Manager 建立介面 VPC 端點之間打造私有連線。介面端點由提供技術支援 [AWS PrivateLink](#)，這項技術可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連接的情況下私密地存取 License Manager API。VPC 中的執行個體不需要公有 IP 地址，即能與 License Manager 通訊。您的 VPC 與 License Manager 之間的網路流量都會在 Amazon 網路的範圍內。

每個介面端點都是由您子網路中的一或多個 [彈性網絡介面](#) 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 \(AWS PrivateLink\)](#)。

## 為 License Manager 建立介面 VPC 端點

使用以下服務名稱之一為 License Manager 建立介面端點：

- COM. 亞馬遜。### 許可證經理
- COM. 亞馬遜。### license-manager-fips

如果您為端點啟用私有 DNS，則可以使用該區域的預設 DNS 名稱向 License Manager 發出 API 要求。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](#)。

## 為 License Manager 建立 VPC 端點政策

您可以將政策連接到 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
- 可供執行動作的資源

以下是端點政策的 License Manager。附加至端點後，此政策會針對所有資源上的所有委託人，授與指定的 License Manager 動作的存取。

```
{
  "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](#)。

# 疑難排 AWS License Manager

下列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 設置符合中所述的需求 [中的設定AWS License Manager](#)。

## 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-執行查詢的權限不足。請移轉您的目錄以啟用此資料庫的存取權。

如果您的 Athena 服務使用由 Athena 管理的資料型錄，而非使用 AWS Glue Data Catalog 如需升級指示，請參閱 [逐步升級至 AWS Glue 資料目錄](#)。

## 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刪除了其帳戶中的 `AWSManagedServiceRoleForAWSLicenseManagerMemberAccountRole` 服務連結角色 (SLR)，並且存在與自我管理授權相關聯的成員擁有的資源，則管理帳戶將無法中斷授權與這些成員帳戶資源的關聯。這表示成員帳戶資源將繼續使用管理帳戶集區中的授權。若要允許管理帳戶取消資源的關聯，請還原 SLR。

這種行為考量了客戶不希望允許管理帳戶執行某些影響成員帳戶資源的動作的情況。

## Systems Manager 庫存已過期

Systems Manager 會將資料儲存在其「庫存」資料中 30 天。在此期間，License Manager 會將代管執行個體計為作用中執行個體，即使它不可執行 Ping 操作。從系統管理員清除庫存資料之後，License Manager 會將執行個體標示為非作用中，並更新本機庫存資料。為了保持代管執行個體計數的正確性，建議您在 Systems Manager 中手動取消註冊執行個體，以便 License Manager 可以執行清除作業。

## 取消註冊 AMI 的明顯持久性

License Manager 會每隔幾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，則 AMI 可能會在清除之前短暫地繼續出現在 License Manager 資源庫存中。

## 新的子帳號實例在資源清查中顯示緩慢

啟用跨帳戶支援時，依預設，License Manager 會在每天下午 1 點更新客戶帳戶。當天晚些時候新增的執行個體會在次日顯示在管理帳號資源庫存中。您可以以 `LicenseManagerResourceSynDataProcessJobTrigger` 在管理帳戶的 AWS Glue 主控台中編輯，以變更更新指令碼的執行頻率。

## 啟用跨帳戶模式後，子帳戶實例出現緩慢

當您在 License Manager 中啟用跨帳戶模式時，子帳號中的執行個體可能需要幾分鐘到幾小時的時間，才會顯示在資源清查中。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，就無法還原為單一帳戶探索。

## 子帳戶使用者無法將共用的自我管理授權與執行個體建立

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。
- 子帳號已從管理帳號中建立的資源共用中移除。
- 自我管理授權已從資源共用中移除。

## 連結 AWS Organizations 帳號失敗

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。
- 客戶已從管理帳戶的組織主控台關閉 License Manager 的存取權。

## 的文件歷史記錄 AWS License Manager

下表說明的發行版本 AWS License Manager。

變更	描述	日期
增加了對 Amazon RDS 的 Db2 vCPU 為基礎的 BYOL 許可證的支持	License Manager 新增了對 Amazon RDS 適用於 Db2 vCPU 的 BYOL 授權的支援。	2024年3月20日
新增視窗伺服器 2019 支援 Microsoft 辦公室使用者型訂閱	AWS 增加了對 Windows 服務器 2019 在 Amazon 機器映像 (AMI) 與 Amazon 提供的許可證 Microsoft 辦公室 LTSC 專業加 2021 Amazon EC2 上的許可證。	2023 年 12 月 4 日
自我管理 (內部部署) 網域使用者可利用以使用者為基礎	License Manager 新增了對自我管理 Active Directory 網域中的使用者的支援，以便在您的目 AWS Managed Microsoft AD 錄建立信任時使用以使用者為基礎的訂閱。	2023 年 9 月 6 日
LTS 訂閱的授權類型轉換	License Manager 添加了對 Ubuntu LTS 實例的支持，以使用許可證類型轉換添加 Ubuntu Pro 訂閱。	2023 年 4 月 20 日
取代作用中授權	License Manager 已新增功能，可在授權啟用期間選擇性地取代授與授權的使用中授權	2023 年 3 月 31 日
Linux 訂閱的委派管理	License Manager 新增了對 Linux 訂閱委派管理員的支援。	2023 年 3 月 3 日

變更	描述	日期
訂閱	License Manager 添加了對商業 Linux 訂閱的跟踪。	2022 年 12 月 21 日
Amazon CloudWatch 指標	License Manager 現在會針對授權組態使用情況和訂閱發出 CloudWatch 指標。	2022 年 12 月 21 日
Microsoft 辦公室為基礎的用戶訂閱	License Manager 添加 Microsoft Office 作為基於用戶的訂閱支持的軟件。	2022 年 11 月 28 日
將權利分配給組織單位	將權利分發至組織中特定的 OU。	2022 年 11 月 17 日
組織全視角 (控制台)	AWS Organizations 使用 License Manager 主控台管理所有帳戶中授予的授權。	2022 年 11 月 11 日
基於用戶的訂閱	在 Amazon EC2 上使用支援的使用者訂閱產品。	2022 年 8 月 2 日
記錄並提交授權使用資料 (主控台)	使用 License Manager 主控台記錄並提交授權使用資料。	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式 (BYOL) 之間變更授權類型，而無需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 CLI 不重新部署現有工作負載的情況下，在 AWS 提供的授權和自攜授權模式 (BYOL) 之間變更授權類型。	2021 年 9 月 22 日
分享權利	只要一次要求，就能與整個組織共用受管理的授權權利。	2021 年 7 月 16 日

變更	描述	日期
用量報告	使用 License Manager 使用報告追蹤授權類型組態的歷程記錄。使用情況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 ID 和標籤從 License Manager 自動探索中排除執行個體。	2021 年 3 月 5 日
受管理的權利	針對向購買的產品以及使用 License Manager 散發授權的賣家，追蹤 AWS Marketplace 和散發授權的授權權利。	2020 年 12 月 3 日
已卸載軟件的自動核算	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
基於標籤的過濾	使用標籤搜尋資源庫存。	2020 年 12 月 3 日
AMI 關聯範圍	將您的自我管理授權和與帳戶共用的 AMI 建立關聯 AWS。	2020 年 11 月 23 日
授權與主機的親和性	在特定天數內強制將授權指派給專用硬體。	2020 年 8 月 12 日
追蹤 Amazon RDS 上的甲骨文部署	在 Amazon RDS 上追蹤 Oracle 資料庫引擎版本和授權套件的授權使用情況。	2020 年 3 月 23 日
主機資源群組	設定主機資源群組，以啟用 License Manager 來管理您的專用主機。	2019 年 12 月 1 日
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附加至執行個體。	2019 年 12 月 1 日

變更	描述	日期
區分包含的授權與自攜授權	根據您使用的是 Amazon 提供的授權還是您自己的授權來篩選搜尋結果。	2019 年 11 月 8 日
附加授權至內部部署資源	將授權附加至內部部署執行個體後，License Manager 會定期收集軟體清查、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。