



ユーザーガイド

AWS License Manager



AWS License Manager: ユーザーガイド

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

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS License Manager?	1
マネージド・エンタイトルメント	2
License Manager のユースケース	2
関連サービス	3
License Managerの仕組み	5
使用を開始する	8
License Manager の使用	9
セルフマネージドライセンス	10
パラメータとルール	11
ベンダーライセンスからのルールの作成	13
セルフマネージドライセンスを作成する	15
セルフマネージドライセンスを共有する	17
セルフマネージドライセンスを編集する	21
セルフマネージドライセンスを非アクティブ化する	21
セルフマネージドライセンスを削除する	22
ライセンスルール	23
セルフマネージドライセンスと の関連付け AMIs	24
セルフマネージドライセンスと の関連付けを解除する AMIs	25
使用状況レポート	25
使用状況レポートを作成する	26
使用状況レポートを編集する	27
使用状況レポートを削除する	28
ライセンスタイプ変換	28
適格なライセンスタイプ	30
前提条件	39
ライセンスタイプを変換する	42
テナンシー変換	52
トラブルシューティング	54
リソースグループをホストします	56
ホストリソースグループの作成	57
ホストリソースグループの共有	58
Dedicated Hosts をホストリソースグループに追加する	58
ホストリソースグループのインスタンスを起動する	59
ホストリソースグループの変更	59

ホストリソースグループから Dedicated Hosts を削除する	59
ホストリソースグループを削除します。	60
インベントリ検索	60
インベントリ検索の使用	61
インベントリの自動検出	67
ライセンスの付与	69
付与されたライセンスを表示する	70
付与されたライセンスを管理する	71
使用権限を配布する	74
権限の受理とアクティベーション	76
ライセンスステータス。	78
購入者アカウントのメトリクス	80
販売者が発行したライセンス	81
エンタイトルメント	82
ライセンス使用量	82
必要なアクセス許可	83
販売者が発行したライセンスを作成する	85
販売者が発行したライセンスの付与	86
ISV 顧客の一時的な認証情報	87
販売者が発行したライセンスを確認する	88
販売者が発行したライセンスを削除する	89
ユーザーベースのサブスクリプション	89
考慮事項	91
ユーザーベースのサブスクリプションの前提条件	92
サポートされているソフトウェアサブスクリプション	99
その他のソフトウェア	101
使用を開始する	101
より多くのセッションGPO用に を設定する	110
含まれているライセンスからインスタンスを起動する AMI	111
インスタンスへの接続	113
Microsoft Office のファイアウォール設定を変更する	114
サブスクリプションユーザーの管理	114
Active Directory の登録解除	116
トラブルシューティング	117
Linux サブスクリプションの管理	119
検出を設定する	121

インスタンスデータの表示	127
請求情報	129
CloudWatch アラームの管理	132
設定	134
License Manager の設定を編集する	136
マネージドライセンス設定	136
Linux サブスクリプション設定	138
ユーザーベースのサブスクリプション設定	141
委任管理者の設定	141
ダッシュボード	146
License Manager のモニタリング	149
によるモニタリング CloudWatch	149
CloudWatch アラームの作成	151
CloudTrail ログ	151
の License Manager 情報 CloudTrail	152
ライセンスLicense Manegerのログ・ ファイルエントリーについて	153
セキュリティ	154
データ保護	155
保管中の暗号化	156
Identity and Access Management	156
ユーザー、グループ、ロールを作成する	156
IAM ポリシー構造	156
License Manager のIAMポリシーを作成する	157
ユーザー、グループ、およびロールに許可を付与する	159
サービスリンクロール	160
コアロール	160
管理アカウントロール	163
メンバーアカウントのロール	165
ユーザーベースのサブスクリプションロール	168
Linux サブスクリプションロール	169
AWS マネージドポリシー	171
AWSLicenseManagerServiceRolePolicy	172
AWSLicenseManagerMasterAccountRolePolicy	174
AWSLicenseManagerMemberAccountRolePolicy	178
AWSLicenseManagerConsumptionPolicy	179
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	179

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	181
ポリシーの更新	183
ライセンス署名	186
コンプライアンス検証	188
耐障害性	189
インフラストラクチャセキュリティ	189
VPC を使用した エンドポイント AWS PrivateLink	190
License Manager のインターフェイスVPCエンドポイントを作成する	190
License Manager のVPCエンドポイントポリシーを作成する	191
トラブルシューティング	192
クロスアカウント検出エラー	192
管理アカウントがセルフマネージドライセンスからリソースの関連付けを解除できない	192
Systems Managerインベントリが古い	192
登録解除された の見かけ上の永続性 AMI	193
リソースインベントリに新しい子アカウントインスタンスが表示されるのが遅い	193
クロスアカウントモード有効にした後、子アカウントのインスタンスが表示されるのが遅い ..	193
クロスアカウント検出を無効化できない	193
子アカウントのユーザーが、共有セルフマネージドライセンスをインスタンスと関連付けられ ない	193
Linking (リンク中) AWS Organizations アカウントが失敗する	194
ドキュメント履歴	195
.....	ccii

とは AWS License Manager?

AWS License Manager は、ソフトウェアベンダー (Microsoft、SAP/Oracle、など IBM) からのソフトウェアライセンスを全体で一元管理しやすくするサービスです。AWS とオンプレミス環境。これにより、ライセンスの使用状況をコントロールし可視化できるため、ライセンスの超過を制限し、コンプライアンス違反や誤報告のリスクを軽減できます。

でクラウドインフラストラクチャを構築する際 AWS では、Bring Your Own License モデル (BYOL) の機会を使用することでコストを削減できます。つまり、クラウドリソースで使用するために、既存のライセンスインベントリを再利用することができます。

License Manager は、に直接関係するインベントリ追跡により、ライセンスの超過やペナルティのリスクを低減します。AWS サービス。管理者は、ライセンスの消費をルールベースでコントロールすることにより、新規および既存のクラウドのデプロイメントにハードまたはソフトな制限を設けることができます。これらの制限に基づいて、License Manager は、非準拠のサーバーの使用を未然に防ぐことができます。

License Manager の組み込みダッシュボードは、ライセンスの使用状況を継続的に可視化し、ベンダー監査をサポートします。

License Manager は、仮想コア (vCPUs)、物理コア、ソケット、またはマシン数に基づいてライセンスされているソフトウェアの追跡をサポートします。これには、Microsoft、IBM/SAP/Oracle、およびその他のベンダーのさまざまなソフトウェア製品が含まれます。

で AWS License Manager では、チェックアウトされたすべての使用権限の数を維持することで、ライセンスを一元的に追跡し、複数のリージョンに制限を適用できます。License Manager は、チェックアウト時間とともに、各チェックアウトに関連付けられたエンドユーザー ID および基礎となるリソース識別子 (利用可能な場合) も追跡します。この時系列データは、メトリクスとイベント ISV を通じて CloudWatch に追跡できます。ISVs は、このデータを分析、監査、その他の同様の目的に使用できます。

AWS License Manager は と統合されています。 [AWS Marketplace](#) および [AWS Data Exchange](#)、および と以下 AWS サービス: [AWS Identity and Access Management \(IAM\)](#), [AWS Organizations](#)、Service Quotas [AWS CloudFormation](#), AWS リソースのタグ付け、および [AWS X-Ray](#).

マネージドエンタイトルメント

License Manager を使用すると、ライセンス管理者は、アカウント全体および組織全体でソフトウェアライセンスを配布、アクティブ化、および追跡できます。

独立系ソフトウェアベンダー (ISVs) が使用できる AWS License Manager は、マネージドエンタイトルメントを使用してソフトウェアライセンスとデータを管理し、エンドユーザーに配布します。発行者は、License Manager ダッシュボードを使用して、出品者が発行したライセンスの使用状況を一元的に追跡できます。ISVs 販売スルー AWS Marketplace トランザクションワークフローの一部として、ライセンスの自動作成と配布のメリットがあります。ISVs では、License Manager を使用してライセンスキーを作成し、を使用しないお客様のライセンスをアクティブ化することもできます。AWS アカウント。

License Manager は、オープンで安全な業界標準を使用してライセンスを表現し、お客様が信頼性を暗号化して検証できるようにします。License Manager は、永久ライセンス、フローティングライセンス、サブスクリプションライセンス、使用量ベースのライセンスなど、さまざまなライセンスモデルをサポートしています。ノードロックする必要があるライセンスがある場合、License Manager は、その方法でライセンスを消費するメカニズムを提供します。

ライセンスは で作成できます。AWS License Manager ID IAM または によって生成されたデジタル署名付きトークンを使用して、エンドユーザーに配布します。AWS License Manager を使用するエンドユーザー AWS はライセンス権限をさらに に再配布できます。AWS それぞれの組織の ID。分散エンタイトルメントを持つエンドユーザーは、 のソフトウェア統合を通じて、そのライセンスから必要なエンタイトルメントをチェックアウトおよびチェックインできます。AWS License Manager。各ライセンスチェックアウトでは、使用権限、関連する数量、10 `admin-users` の 1 時間チェックアウトなどのチェックアウト期間を指定します。このチェックアウトは、分散ライセンスの基盤となる IAM アイデンティティに基づいて、または によって生成された存続期間の長いトークンに基づいて実行できます。AWS License Manager を通じて AWS License Manager サービス。

License Manager のユースケース

License Manager がさまざまなユースケースに提供する機能の例を以下に示します。

- [License Manager のセルフマネージドライセンス](#) - エンタープライズ契約の条件に基づいてライセンスルールを定義し、その方法を決定するために使用されます。AWS は、これらのライセンスを使用するコマンドを処理します。
- [License Manager で販売者が発行したライセンス](#) - ソフトウェアライセンスを管理し、エンドユーザーに配信するために使用されます。

- [ライセンスマネージャーで付与されたライセンス](#) – から取得したライセンスの使用を管理するために使用されます。AWS Marketplace, AWS Data Exchange、またはソフトウェアをマネージドエンタイトルメントと統合した販売者から直接。
- [License Manager でのライセンスタイプの変換](#) – ライセンスタイプを の間で変更するために使用されます。AWS は、ワークロードを再デプロイすることなく、ライセンスと Bring Your Own License モデル (BYOL) を提供しました。
- [License Manager でのインベントリ検索](#) – を使用してオンプレミスアプリケーションを検出および追跡するために使用されます。AWS Systems Manager インベントリとライセンスルール。
- [サポートされているソフトウェア製品の License Manager ユーザーベースのサブスクリプションを使用する](#) - サポート対象ソフトウェアに完全準拠した Amazon 提供型ライセンスを、ユーザーごとのサブスクリプション料金で購入するために使用されます。
- [License Manager で Linux サブスクリプションを管理する](#) – 所有および実行している商用 Linux サブスクリプションを表示および管理するために使用します。AWS。

関連サービス

License Manager は Amazon EC2、Amazon RDS、および と統合されています。AWS Marketplace, AWS Systems Manager および AWS Organizations。

Amazon EC2の統合により、次のリソースのライセンスを追跡し、リソースのライフサイクルを通じてライセンスルールを適用できます。

- [Amazon EC2インスタンス](#)
- [ハードウェア専用インスタンス](#)
- [Dedicated Hosts](#)
- [スポットインスタンスとスポットフリート](#)
- [マネージドノード](#)

License Manager を とともに使用する場合 AWS Systems Managerでは、 の外部でホストされている物理サーバーまたは仮想サーバーのライセンスを管理できます。AWS。License Manager はで使用できます。AWS Organizations すべての組織アカウントを一元管理できます。

さらに、 から購入したライセンスの使用を管理することもできます。AWS Marketplace, AWS Data Exchange、またはソフトウェアを と統合した販売者から直接 AWS License Manager。を使用できます。AWS License Manager 使用権限と呼ばれる使用権限を特定の に配布する AWS アカウント。

License Manager は、Amazon RDS for Oracle および Amazon RDS for Db2 v CPUベースのBYOL ライセンスと統合されています。この統合により、for Oracle および RDS for Db2 DB インスタンスRDSの vCPU 使用状況を可視化できます。このデータを使用して、データベース管理システムベンダーとのライセンス条件に基づいて消費されるライセンスの数を計算できます。詳細については、「Amazon RDSユーザーガイド」の以下の関連リンクを参照してください。

- [RDS for Oracle ライセンスオプション](#)
- [RDS for Db2 ライセンスオプション](#)

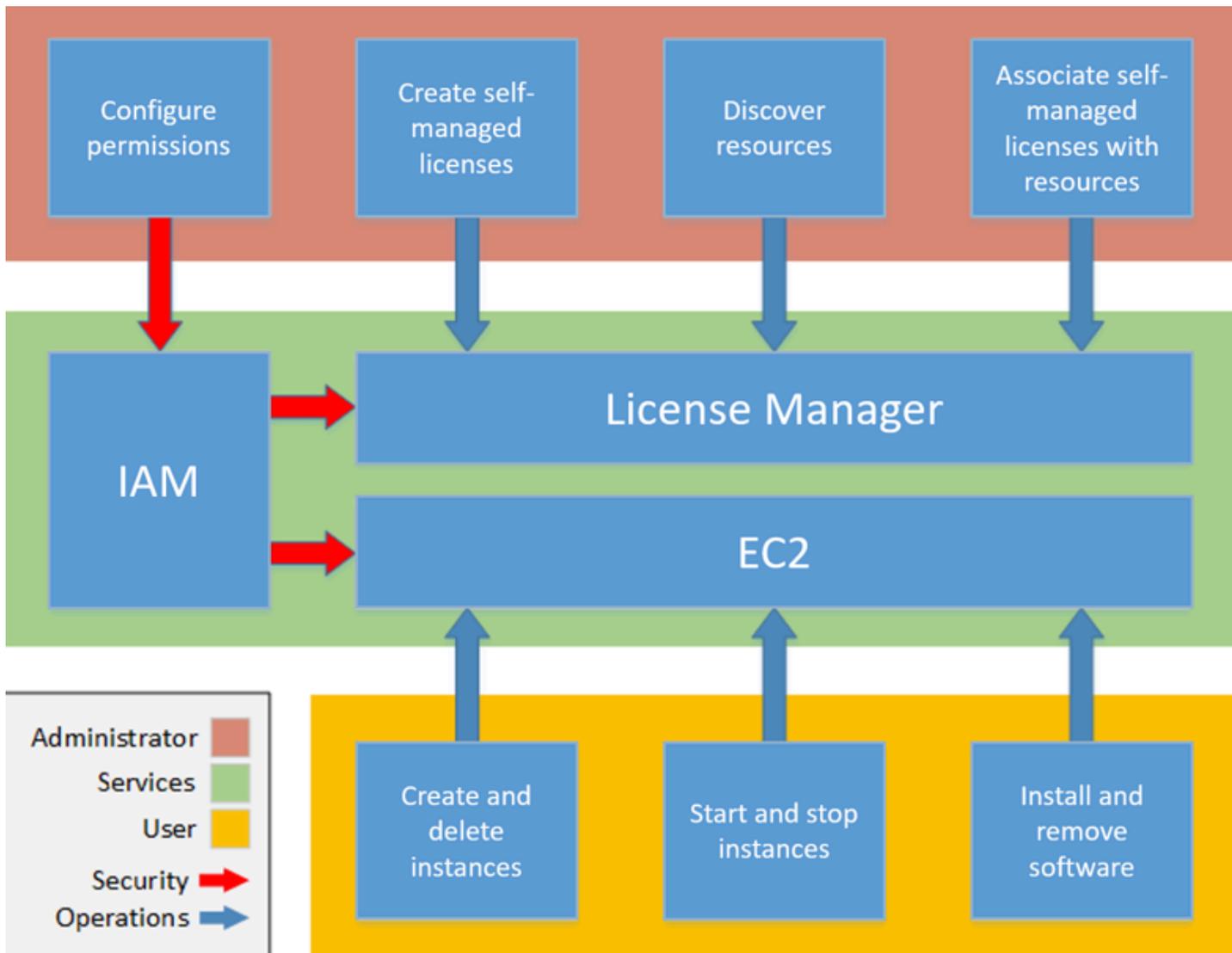
License Managerの仕組み

効果的なソフトウェアライセンス管理は、次の事項に依存します。

- エンタープライズライセンス契約の条件を理解しているエキスパート
- ライセンスを消費する操作に対するアクセスの適切な制限
- ライセンスインベントリの正確な追跡

企業では多くの場合、各分野を担当する専任の担当者またはチームが存在します。そして、特にライセンスのエキスパートとシステム管理者との間の効果的なコミュニケーションについて問題になります。License Managerは、さまざまなドメインからの知識をプールする方法を提供します。重要なのは、とネイティブに統合されることです。AWS サービス - インスタンスが作成および削除される Amazon EC2コントロールプレーンなど。これは、License Managerがビジネス上および運用上の知識の獲得の制御と制限を行い、インスタンスの作成とアプリケーションのデプロイメントの自動制御に変換できることを意味します。

次の図は、アクセス許可を管理して License Manager を設定するライセンス管理者と、Amazon EC2コンソールを使用してリソースを作成、管理、削除するユーザーの、個別に調整された職務を示しています。



組織内のライセンス管理を担当しているライセンス管理者は、License Managerを使用してライセンスルールを設定し、それらを起動にアタッチして、使用状況を追跡できます。組織内のユーザーは、ライセンスを消費するリソースを、追加作業なしで、追加したり削除したりすることができます。

ライセンスのエキスパートが、組織全体のライセンスを管理し、リソースインベントリのニーズを判断し、ライセンスの調達を監督し、ライセンス使用のコンプライアンスを推進します。License Managerを使用している企業では、この作業はLicense Managerコンソールを介して統合されています。図に示すように、これには、サービスのアクセス許可の設定、セルフマネージドライセンスの作成、オンプレミスおよびクラウド上の両方のコンピューティングリソースのインベントリの取得、セルフマネージドライセンスと検出されたリソースの関連付けが含まれます。実際には、これは、ITがすべての Amazon EC2 インスタンスデプロイのテンプレートとして使用する承認済みの Amazon マシンイメージ (AMI) にセルフマネージドライセンスを関連付けることを意味します。

License Managerの活用により、ライセンス違反が発生した場合に失われる可能性のあるコストを節約できます。内部監査では事後にのみ違反が明らかになりますが、それではコンプライアンス違反へのペナルティを回避するには遅すぎます。License Managerにより、コストがかかるインシデントの発生を防ぐことができます。License Managerは、ライセンスの消費とリソースの追跡を示すダッシュボードが組み込まれており、レポート作成を簡素化します。

License Manager の使用を開始する

アプリケーション AWS License Manager、まずオンボーディング手順を完了する必要があります。次の手順では、のオンボーディング手順について説明します。AWS Management Console.

License Manager の使用を開始する

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. License Managerとそのサポートサービスの権限を設定するよう求められます。指示に従って、必要なアクセス許可を設定します。
3. 最初の設定が完了したら、希望する [License Manager のユースケース](#) に合わせて License Manager の使用を続行できます。

ユーザー、グループ、ロールが License Manager を使用中に使用するアクセス許可の管理の詳細については、以下を参照してください。AWS ベストプラクティスについては、「」を参照してください [License Manager の ID とアクセスの管理](#)。License Manager と統合する Amazon EC2リソースの設定の詳細については、「[Amazon Elastic Compute Cloud ユーザーガイド](#)」の「[Amazon を使用するようにセットアップEC2する](#)」を参照してください。

License Manager の使用

License Manager は、 の混合インフラストラクチャを持つエンタープライズの標準シナリオに適用できます。AWS リソースとオンプレミスリソース。セルフマネージドライセンスの作成、ライセンスを消費するリソースのインベントリの作成、セルフマネージドライセンスとリソースの関連付け、インベントリとコンプライアンスの追跡を行えます。

のライセンス AWS Marketplace 製品

License Manager を使用して、ライセンスルールを に関連付けることができるようになりました。AWS Marketplace BYOL AMI Amazon EC2起動テンプレートを介した 製品、AWS CloudFormation テンプレート、または Service Catalog 製品。いずれの場合も、集中型のライセンス追跡とコンプライアンス遵守によるメリットを得ることができます。

Note

License Manager は、 Marketplace BYOLAMIsから を取得してアクティブ化する方法を変更しません。起動後に、サードパーティソフトウェアをアクティブ化するには、販売者から直接入手したライセンスキーを入力する必要があります。

オンプレミスデータセンターのリソースのライセンスの追跡

License Manager を使用すると、 の外部で実行されているアプリケーションを検出できます。AWS [Systems Manager インベントリ](#) を使用して、ライセンスルールをアタッチします。ライセンスルールがアタッチされたら、とともにオンプレミスサーバーを追跡できます。AWS License Manager コンソールの リソース。

ライセンス込みと の区別 BYOL

License Managerでは、どのリソースが製品に含まれるライセンスを持っているか、どのリソースが自分の所有するライセンスを使用しているかを識別することができます。これにより、BYOLライセンスの使用方法を正確に報告できます。このフィルターにはSSMバージョン 2.3.722.0 以降が必要です。

全体の License Manager AWS アカウント

License Manager を使用すると、全体のライセンスを管理できます。AWS アカウント。ライセンス設定は、 で 1 回作成できます。AWS Organizations 管理アカウント を使用してアカウント間で

共有します。AWS Resource Access Manager または をリンクする AWS Organizations License Manager 設定を使用する アカウント。これにより、クロスアカウント検出を実行して、全体のインベントリを検索することもできます。AWS アカウント。

内容

- [License Manager のセルフマネージドライセンス](#)
- [License Maneger のライセンスルール](#)
- [License Manager の使用状況レポート](#)
- [License Maneger でのライセンスタイプの変換](#)
- [License Manager でリソースグループをホストする](#)
- [License Manager でのインベントリ検索](#)
- [ライセンスマネージャーで付与されたライセンス](#)
- [License Manager で販売者が発行したライセンス](#)
- [サポートされているソフトウェア製品の License Manager ユーザーベースのサブスクリプションを使用する](#)
- [License Manager で Linux サブスクリプションを管理する](#)
- [License Manegerの設定](#)
- [License Manegerのダッシュボード](#)

License Manager のセルフマネージドライセンス

セルフマネージドライセンス (旧ライセンス設定) は License Manager の中核です。セルフマネージドライセンスにはエンタープライズ契約の条項に基づくライセンスルールが含まれています。作成するルールによって、AWS はライセンスを消費するコマンドを処理します。セルフマネージドライセンスを作成する際には、組織のコンプライアンスチームと密接に協力して、お使いのエンタープライズ契約を確認してください。

AWS のサービス License Manager などのサービスクォータは、で使用できるリージョンあたりのリソースまたはオペレーションの最大数を定義します。AWS アカウント そのサービスの。例えば、License Maneger では、リソースごとに最大 個の10セルフマネージドライセンスを持つことができ、どの でも合計 個を超える25セルフマネージドライセンスを持つことはできません。AWS リージョン。License Manager のクォータの詳細については、「」を参照してください。 [AWS License Manager のサービスクォータ](#) AWS 全般のリファレンス。

Note

Systems Manager マネージドインスタンスは、vCPU およびインスタンスタイプのセルフマネージドライセンスに関連付ける必要があります。

内容

- [License Manager のセルフマネージドライセンスパラメータとルール](#)
- [ベンダーライセンスからライセンスマネージャールールを構築する](#)
- [License Manager でセルフマネージドライセンスを作成する](#)
- [License Manager でセルフマネージドライセンスを共有する](#)
- [License Manager でセルフマネージドライセンスを編集する](#)
- [License Manager でセルフマネージドライセンスを非アクティブ化する](#)
- [License Manager でセルフマネージドライセンスを削除する](#)

License Manager のセルフマネージドライセンスパラメータとルール

セルフマネージドライセンスは、基本的なパラメータと、パラメータ値に応じて変化するルールで構成されます。セルフマネージドライセンスにタグを追加することもできます。セルフマネージドライセンスを作成したのち、管理者は、リソースのニーズの変化に合わせてライセンス数や使用制限を変更することができます。

下記を含むパラメータやルールを使用できます。

- セルフマネージドライセンス名 - セルフマネージドライセンスの名前。
- (オプション) 説明 - セルフマネージドライセンスの説明。
- ライセンスタイプ - ライセンスカウントに使用されるメトリック。サポートされている値は、vCPUs、Cores、Sockets、および Instances です。
- (オプション) <option> 数 - リソースによって使用されるライセンスの数。
- ステータス - 設定がアクティブであるかどうかを示します。
- 製品情報 - [自動検出](#)の対象となる製品の名称とバージョン。サポートされている製品は、Windows Server、SQLServer、Amazon RDS for Oracle、Amazon RDS for Db2 です。
- (オプション) ルール - これには次のものが含まれます。使用可能なルールは、カウントタイプによって異なります。

- ホストへのライセンスアフィニティ (日単位) - 指定した日数の間、ライセンスの使用をホストに制限します。範囲は1から180です。カウントタイプはコアまたはソケットでなければなりません。アフィニティ期間が経過すると、24時間以内にライセンスが再利用できるようになります。
- 最大コア - リソースの最大コア数。
- 最大ソケット - リソースの最大ソケット数。
- Maximum vCPUs – vCPUs リソースの最大数。
- 最小コア - リソースの最小コア数。
- 最小ソケット - リソースの最小ソケット数。
- Minimum vCPUs – リソース vCPUs の最小数。
- テナンシー — ライセンスの使用を指定されたEC2テナンシーに制限します。カウントタイプがコアまたはソケットの場合は、Dedicated Host が必要です。共有テナンシー、Dedicated Hosts、Dedicated Instances は、カウントタイプが Instances または の場合にサポートされます vCPUs。コンソール (および API) 名は次のとおりです。
 - 共有EC2-Default
 - ハードウェア専用インスタンス (EC2-DedicatedInstance)
 - Dedicated Host (EC2-DedicatedHost)
 - vCPU 最適化 – License Manager は Amazon [CPUの最適化](#) サポートと統合されておりEC2、インスタンス vCPUs の の数をカスタマイズできます。このルールが True に設定されている場合、License Maneger はカスタマイズされたコア数とスレッド数 vCPUs に基づいてカウントされます。それ以外の場合、License Manegerはインスタンスタイプのデフォルトの の数 vCPUs をカウントします。

次の表は、各カウントタイプでどのライセンスルールが利用できるかを示しています。

コンソール名	API 名前	コア	インスタンス	ソケット	vCPUs
ホストのライセンスアフィニティ(日単位)	licenseAfinityToHost	✓		✓	
最大コア	maximumCores	✓	✓		
最大ソケット	maximumSockets		✓	✓	

コンソール名	API 名前	コア	インスタンス	ソケット	vCPUs
最大 vCPUs	maximumVcpus		✓		✓
最小コア	minimumCores	✓	✓		
最小ソケット	minimumSockets		✓	✓	
最小 vCPUs	minimumVcpus		✓		✓
テナンシー	allowedTenancy	✓	✓	✓	✓
vCPU 最適化	honorVcpu Optimization				✓

ベンダーライセンスからライセンスマネージャールールを構築する

ソフトウェアベンダーライセンスの言語に基づいて、ライセンスマネージャーのルールセットを作成できます。以下の例は、実際のお客様のユースケースのブループリントを意図したものではありません。実際のライセンス契約の適用にあたっては、特定のオンプレミスサーバー環境のアーキテクチャとライセンス履歴に応じて、競合するオプションの中から選択します。オプションは、へのリソースの計画された移行の詳細にも依存します。AWS.

これらの例はできる限りベンダー非依存となるように作成されており、ハードウェアとソフトウェアの割り当てに関する一般的に適用可能な質問に焦点を当てています。ベンダーライセンス条項はとやり取りします AWS の要件と制限。アプリケーションに必要なライセンスの数は、選択したインスタンスタイプやその他の要因によって異なります。

Important

AWS は、ソフトウェアベンダーとの監査プロセスに参加しません。お客様はコンプライアンスに責任を負い、ライセンス契約に基づいてルールを注意深く理解し License Maneger に取り込む責任を負うものとします。

例: オペレーティングシステムライセンスの導入

この例には、サーバーオペレーティングシステムのライセンスが含まれています。ライセンス言語は、CPUコアのタイプ、テナンシー、サーバーあたりの最小ライセンス数に制約を課します。

この例では、ライセンス条項に次の規定が含まれています。

- 物理プロセッサコアによってライセンス数が決まります。
- ライセンスの数はコアの数と等しくなければなりません。
- サーバーでは最低8コアを実行する必要があります。
- オペレーティングシステムは、仮想化されていないホスト上で実行する必要があります。

さらに、お客様は以下の決定を行いました。

- 96コアのライセンスを購入しました。
- ライセンス消費を購入数に制限するために、ハードリミットを設定します。
- 各サーバーには最大16コアが必要です。

次の表ではLicense Managerのルール作成パラメーターと、そのパラメータが捕捉し自動化するベンダーのライセンス要件を関連付けたものです。例示されている値は説明のためのものであり、独自のセルフマネージドライセンスで必要な値を指定することになります。

ライセンスマネージャールール	設定
ライセンスカウントタイプ	[License Type]は Cores に設定されています。
ライセンス数	[Number of cores]は 96 に設定されています。
最小/最大 vCPUs または コア	[最小コア]は 8 に設定されています。 [最大コア]は 16 に設定されています。
ライセンス数のハードリミット	[Enforce license limit] が選択されています。
許可テナンシー	

ライセンスマネージャールール	設定
	テナンシー Dedicated Host に設定されています。

License Manager でセルフマネージドライセンスを作成する

セルフマネージドライセンスは、ソフトウェアベンダーとの契約におけるライセンス条件を表します。セルフマネージドライセンスは、ライセンスのカウント方法 (インスタンス数vCPUs やインスタンス数など) を指定します。また、割り当てられたライセンス数を超えて使用できないように、使用量の制限も指定されています。さらに、テナンシータイプなど、ライセンスに関するその他の制約条件を指定することもできます。

Amazon for RDS Oracle および Amazon RDS for Db2 データベースに関する考慮事項

Amazon RDS for Oracle または Amazon for RDS Db2 データベースの自動検出を設定するための製品情報を追加する場合、次の要件が適用されます。

- サポートされているライセンスカウントタイプはvCPU です。
- ルールはサポートされていません。
- ハードライセンスの制限はサポートされません。
- セルフマネージドライセンスにつき 1 つの製品バージョンを追跡できます。
- 同じセルフマネージドライセンスを使用して Amazon RDS データベースやその他の製品を追跡することはできません。

コンソールを使用してセルフマネージドライセンスを作成するには

1. [License Manager コンソールを開きます](https://console.aws.amazon.com/license-manager/) <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. [セルフマネージドライセンスを作成] を選択します。
4. [Configuration details] パネルで次の情報を入力します。
 - セルフマネージドライセンス名 - セルフマネージドライセンスの名前。
 - 説明 - セルフマネージドライセンスに関する任意の説明。
 - ライセンスタイプ — このライセンスのカウントモデル (vCPUs、コア、ソケット、またはインスタンス)。

- [`<option>` 数 - ライセンスタイプに応じて表示されるオプション。ライセンス制限を超える
と、License Managerが、通知 (ソフト制限) またはリソース使用制限 (ハード制限) のいずれ
かを行います。
 - ライセンス制限を適用します - 選択すると、ライセンス制限がハード制限になります。
 - ルール - 1 つ以上のルール。ルールごとに、ルールタイプを選び、ルール値を入力して、[Add
rule] を選択します。表示されるルールタイプはライセンスタイプにより異なります。具体例
を挙げると、最小値、最大値およびテナンシーなどがあります。テナンシー属性を指定しない
場合は、すべてのタイプを使用できます。
5. (オプション)[Automated discovery rules] (自動検出ルール) パネルで以下の操作を行います。
- a. [\[automated discovery\]](#)(自動検出) を使用して、検出および追跡する各製品の製品名、製品タ
イプ、リソースタイプを選択します。
 - b. [Stop tracking instances when software is uninstalled](ソフトウェアのアンインストール時に
インスタンスの追跡を停止する)を選ぶと、ソフトウェアがアンインストールされ、ライセ
ンスのアフィニティ期間が経過したことをライセンスマネージャーが検出した後、ライセン
スを再利用できるようになります。
 - c. (オプション)お客様のアカウントが組織のライセンス マネージャーの管理アカウントの場
合、自動検出から除外するリソースを定義するオプションがあります。そのためには、除外
ルールの追加 を選択し、フィルタリングするプロパティを選択します。AWS アカウント
IDsとリソースタグがサポートされています。次に、そのプロパティを識別するための情報
を入力します。
6. (オプション) [タグ] パネルを展開し、1 つ以上のタグをセルフマネージドライセンスに追加しま
す。タグはキーと値のペアです。タグごとに次の情報を記入してください。
- キー - 検索可能なキー名。
 - 値 - キーの値。

7. [送信] を選択します。

コマンドラインを使用してセルフマネージドライセンスを作成するには

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

License Manager でセルフマネージドライセンスを共有する

以下を使用できます..。 AWS Resource Access Manager セルフマネージドライセンスを任意の と共有するには AWS アカウントまたは 経由 AWS Organizations。 詳細については、 [「 の共有」を参照してください。](#) [AWS の リソース](#) AWS RAM ユーザーガイド。

サポートされるアカウントのクォータ

でライセンス共有を有効にした場合 AWS License Manager 2023 年 10 月 14 日より前に、 License Manager が組織内でサポートするアカウントの最大数のクォータは、新しいデフォルトの最大数よりも小さくなります。このクォータは、 の APIオペレーションを使用して引き上げることができます。 AWS RAM 次のセクションで説明する 。 License Manager のデフォルトクォータの詳細については、「」の [「ライセンスの使用に関するクォータ」](#)を参照してください。 AWS 全般のリファレンスガイド。

前提条件

以下の手順を完了するには、次のアクセス許可がある組織の管理アカウントのプリンシパルとしてサインインする必要があります。

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

サポートされるアカウントのクォータを増やす

以下の手順を実行することで、Number of accounts per organization for License Manager の現在のクォータを現在のデフォルト最大数まで増やすことができます。

License Manager でサポートされるアカウントのクォータを増やすには

1. [を使用するdescribe-organization](#) AWS CLI オペレーションARNを使用して組織の を決定する コマンド。

```
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. [を使用するget-resource-shares](#) AWS CLI オペレーションARNを使用して組織の を決定する コマンド。

```

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. [aws ram enable-sharing-with-aws-organization](#) AWS CLI とのリソース共有を有効にする コマンド AWS RAM:

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

{
  "returnValue": true
}
```

を使用できます。 [aws organizations list-aws-service-access-for-organization](#) AWS CLI Organizations リストのサービスプリンシパルが License Manager と に対して有効になっていることを確認する コマンド 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

には最大 6 時間かかる場合があります。AWS RAM 組織のこのオペレーションを完了するには、[aws ram enable-sharing-with-aws-organization](#) を使用します。この処理が完了するまでは次に進むことができません。

4. [aws organizations associate-resource-share](#) AWS CLI License Manager リソース共有を組織に関連付ける コマンド :

```
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
    }
  ]
}
```

を使用できます。 [get-resource-share-associations](#) AWS CLI リソース共有の関連付けが status であることを確認する コマンド 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
    }
  ]
}
```

```
}
```

License Manager でセルフマネージドライセンスを編集する

セルフマネージドライセンスの次のフィールドの値を編集できます。

- セルフマネージドライセンス名
- 説明
- <option> 数
- ライセンスタイプの制限を強制

セルフマネージドライセンスを編集するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスを選択します。
4. [Actions]、[Edit] の順に選択します。
5. 必要に応じて詳細を編集し、「更新」を選択します。

コマンドラインを使用してセルフマネージドライセンスを編集するには

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

License Manager でセルフマネージドライセンスを非アクティブ化する

セルフマネージドライセンスを非アクティブ化しても、そのライセンスを使用する既存のリソースは影響を受けず、ライセンスAMIsを使用しても起動できます。ただし、ライセンスの消費は追跡されなくなります。

セルフマネージドライセンスを無効化すると、実行中のインスタンスにアタッチできなくなります。無効化したセルフマネージドライセンスは起動できなくなります。

セルフマネージドライセンスを無効化するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。

2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスを選択します。
4. Action(アクション)、Deactivate(無効化)を選択します。確認を求めるメッセージが表示されたら、[Deactivate (無効化)] を選択します。

コマンドラインでセルフマネージドライセンスを無効化するには

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

License Manager でセルフマネージドライセンスを削除する

セルフマネージドライセンスを削除する前に、すべてのリソースの関連付けを解除する必要があります。新しいライセンスルールでやり直す必要がある場合は、セルフマネージドライセンスを削除できません。ソフトウェアベンダーのライセンス条件が変更された場合は、既存のリソースの関連付けを解除し、セルフマネージドライセンスを削除し、更新した条件が反映された新しいセルフマネージドライセンスを作成して既存のリソースと関連付けることができます。

コンソールを使用してセルフマネージドライセンスを削除するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスの名前を選択し、ライセンスの詳細ページを開きます。
4. 各リソースを (個別または一括で) 選択し、「リソースの関連付けを解除」を選択します。リストが空になるまで繰り返します。
5. [Actions] で、[Delete] を選択します。確認を求めるメッセージが表示されたら、[削除] を選択します。

コマンドラインを使用してセルフマネージドライセンスを削除するには

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

License Manager のライセンスルール

セルフマネージドライセンスルールを作成したら、それを関連する起動メカニズムに添付して、新しいリソースのコンプライアンス違反のデプロイを直接防ぐことができます。組織内のユーザーは、指定された からEC2インスタンスをシームレスに起動できAMI、管理者は組み込みの License Manager ダッシュボードを使用してライセンスインベントリを追跡できます。起動コントロールとダッシュボードアラートによって、容易にコンプライアンス遵守を図ることができます。

Important

AWS は、ソフトウェアベンダーとの監査プロセスに参加しません。お客様はコンプライアンスに責任を負い、ライセンス契約に基づいてルールを注意深く理解しキャプチャして License Manager に取り込むことに責任を負うものとします。

ライセンスの追跡は、インスタンスにルールが添付されてから終了されるまで行われます。使用制限とライセンスルールを定義することにより、License Managerはデプロイメントを追跡して、ルール違反を警告します。ハード制限を設定すると、License Manager によりリソースの起動を妨ぐことができます。

追跡対象のサーバーが停止または終了すると、そのライセンスは解放され、利用可能なライセンスのプールに戻されます。

運用とコンプライアンスへのアプローチは組織によって異なるため、License Manager では複数の起動メカニズムをサポートしています。

- セルフマネージドライセンスと の手動関連付け AMIs — オペレーティングシステムやその他のソフトウェアのライセンスを追跡するには、組織内で広く使用するためにライセンスルールを公開 AMIsする前に、 にライセンスルールをアタッチできます。これらのデプロイAMIは、ユーザーによる追加のアクションを必要とせずに、License Manager で自動的に追跡されます。 [Systems Manager Automation](#)、[VM Import/Export](#)、[Packer](#) などの現在のAMI構築メカニズムにライセンスルールをアタッチすることもできます。 <https://docs.aws.amazon.com/vm-import/latest/userguide/>
- Amazon EC2起動テンプレートと AWS CloudFormation – ライセンスルールを にアタッチするオプションが推奨されていない場合AMIは、 [EC2起動テンプレート](#)または でオプションパラメータとして指定できます。 [AWS CloudFormation テンプレート](#)。これらのテンプレートを使用したデプロイメントはLicense Managerを使って追跡されます。EC2 起動テンプレートまたは にルールを適用できます。AWS CloudFormation セルフマネージドライセンスフィールドに 1 つ以上の IDsセルフマネージドライセンスを指定して テンプレートを作成します。

AWS は、ライセンス追跡データを、AWS 所有する アカウント。AWS はライセンス追跡データにアクセスできません。お客様はライセンス追跡データを管理し、いつでも削除することができます。

セルフマネージドライセンスと の関連付け AMIs

次の手順は、License Manager コンソールAMIsを使用してセルフマネージドライセンスを に関連付ける方法を示しています。この手順では、少なくとも1つの既存のセルフマネージドライセンスがあることを前提としています。自己管理ライセンスは、所有または共有を問わず、アクセスできる任意の AMI に関連付けることができます。が共有AMIされている場合は、現在のアカウントのセルフマネージドライセンスに関連付けることができます。それ以外の場合は、AMI をすべてのアカウントでセルフマネージドライセンスに関連付けるか、現在のアカウントでのみ関連付けるかを指定できます。

をすべてのアカウントでAMIセルフマネージドライセンスに関連付けると、アカウントAMI間でのインスタンスの起動を追跡できます。ハードリミットに達すると、License Manager は追加のインスタンスの起動をブロックします。ソフト制限に達すると、License Manager は追加のインスタンスの起動を通知します。

同じリージョンAMI内で をコピーし、ライセンス設定AMIが関連付けられている場合、それらのライセンス設定は自動的に新しい に関連付けられますAMI。新しい からインスタンスを起動するとAMI、License Manager はそのインスタンスを追跡します。同様に、ライセンス設定が関連付けられている実行中のインスタンスAMIから新しい を作成すると、それらのライセンス設定は自動的に新しい に関連付けられAMI、License Manager は新しい から起動したインスタンスを追跡しますAMI。

Warning

License Manager は、クロスリージョンインスタンスの追跡をサポートしていません。ライセンス設定AMIが関連付けられている を別のリージョンにコピーすると、License Manager は新しい からのすべてのインスタンス起動をブロックしますAMI。

セルフマネージドライセンスと を関連付けるには AMI

1. で License Manager コンソールを開きます<https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスの名前を選択し、ライセンスの詳細ページを開きます。現在関連付けられている を表示するにはAMIs、関連付けられている AMIsを選択します。

4. 関連付け AMI を選択します。
5. 使用可能 AMIs で、1 つ以上の を選択し AMIs、 の関連付け を選択します。
 - アカウントが少なくとも 1 つの を所有している場合 AMIs、所有 AMIs している の AMI 関連付け スコープ を選択するように求められます。別のアカウントから と共有 AMIs された は、お客様のアカウントにのみ関連付けられます。[確認] を選択します。
 - が別のアカウントから共有 AMIs された場合、アカウントのみに関連付けられます。

新しく関連付けられた が、ライセンスの詳細ページの関連付けタブ AMIs に表示される AMIs ようになりました。

セルフマネージドライセンスと の関連付けを解除する AMIs

次の手順は、License Manager コンソール AMIs を使用してセルフマネージドライセンスの関連付けを解除する方法を示しています。登録解除された の関連付けを解除することはできません AMI。License Manager は 8 時間 AMIs ごとに登録解除をチェックし、自動的に関連付けを解除します。

セルフマネージドライセンスと の関連付けを解除するには AMI

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスの名前を選択し、ライセンスの詳細ページを開きます。
4. 関連付けられた AMIs を選択します。
5. AMI を選択し、関連付け解除 AMI を選択します。

License Manager の使用状況レポート

使用 AWS License Manager ライセンス使用状況の定期的なスナップショットをスケジュールすることで、セルフマネージドライセンスの履歴を追跡できます。使用状況レポートを設定することにより、License Manager は、お客様の仕様に基いてセルフマネージドライセンスのレポートを S3 バケットに自動的にアップロードします。使用状況レポートは、以前はレポートジェネレーターと呼ばれていました。複数の使用状況レポートを設定して、環境内の異なるライセンスタイプの設定を効果的に追跡できます。

Note

AWS License Manager はレポートを保存しません。License Manager レポートは S3 バケットに直接発行されます。使用状況レポートを削除すると、レポートは S3 バケットに公開されなくなります。

License Manager で使用状況レポートを作成する

使用状況レポートを作成するときには、License Manager で追跡するセルフマネージドライセンスタイプ、レポートを生成する頻度を定義する頻度間隔、およびレポートタイプを指定します。すべてのレポートは CSV 形式で生成され、S3 バケットに発行されます。使用状況レポートは、次のレポートタイプを 1 つ以上生成できます。

セルフマネージドライセンスの概要レポート

このレポートタイプには、消費されたライセンスの数およびセルフマネージドライセンスの詳細に関する情報が含まれます。追跡されたセルフマネージドライセンスタイプは、ライセンス数、ライセンスルール、および異なるリソースタイプ間のライセンスの配布などの詳細と共にリストされます。

リソース使用状況レポート

このレポートタイプには、追跡されるリソースとそのライセンス消費に関する詳細が示されます。指定されたセルフマネージドライセンスタイプを使用して追跡される各リソースは、ライセンス ID、リソースのステータス、などの詳細とともに一覧表示されます。AWS リソースを所有するアカウント ID。

使用状況レポートを作成するには

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. ナビゲーションパネルで [使用状況レポート] を選択します。
3. [使用状況レポートを作成] を選択し、[使用状況レポートを作成] ペインでレポートのパラメータを定義します。
 - a. 使用状況レポートの [名前] と [説明] (オプション) を入力します。
 - b. ドロップダウンリストから、セルフマネージドライセンスタイプを選択します。これは、使用状況レポートがデータを生成する際のライセンスのタイプです。

- c. 生成するレポートタイプを選択します。
 - d. License Manager がレポートを発行する頻度を選択します。[毎日 1 回]、[毎週 1 回] または [毎月 1 回] を選ぶことができます。
 - e. (オプション) [タグ] を追加して、使用状況レポートリソースを追跡します。
4. [使用状況レポートを作成] を選択します。

新しい使用状況レポートは 60 分以内にレポートの公開を開始します。

アカウントに S3 バケットをまだ関連付けていない場合、使用状況レポートの作成時に、License Manager がアカウントに新しい Amazon S3 バケットを作成します。以前にクロスアカウントインベントリ検索を有効にしたことがある場合、クロスアカウントインベントリ検索が有効化にされたとき License Manager が作成した S3 バケットにレポートが送信されます。

レポートは、次の Amazon S3 URI パターンでバケットに保存されます。

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

License Manager で使用状況レポートを編集する

License Manager コンソールからいつでも使用状況レポートを表示および変更できます。[使用状況レポート] テーブルには、アカウント用に作成されたすべての使用状況レポートがリスト表示されています。テーブルから、さまざまなレポートの概要を確認したり、使用状況レポートに関連付けられた Amazon S3 バケットにピボットし、レポート生成のステータスを表示したりできます。

使用状況レポートを編集するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションパネルで [使用状況レポート] を選択します。
3. テーブルから編集したい使用状況レポートを選択し、[詳細を表示] を選択します。
4. [編集] を選択して、使用状況レポートを変更します。
5. 使用状況レポートに必要な変更を行い、[変更の保存] を選択します。

更新された使用状況レポートは、1 時間以内に新しいレポートを生成します。

Note

使用状況レポートの名前を変更すると、新しい名前を反映した License Manager S3 バケット内の新しいフォルダに、今後のレポートが送信されます。

License Manager で使用状況レポートを削除する

使用状況レポートを削除すると、新しいレポートの生成が停止しますが、Amazon S3 バケットと以前のすべてのレポートは影響を受けません。

Note

セルフマネージドライセンスに使用状況レポートが関連付けられている場合、アカウントからセルフマネージドライセンスを削除することはできません。まず、使用状況レポートを削除する必要があります。

使用状況レポートを編集するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションパネルで [使用状況レポート] を選択します。
3. テーブルから編集したい使用状況レポートを選択し、[詳細を表示] を選択します。
4. [削除] を選択します。この操作は、使用状況レポートを完全に削除します。

License Manager でのライセンスタイプの変換

License Manager を使用すると、ビジネスニーズの変化に応じて、AWS 提供されたライセンスモデルと Bring Your Own License モデル (BYOL) または Bring Your Own Subscription モデル (BYOS) の間でライセンスタイプを変更できます。ライセンスタイプは、既存のワークロードを再デプロイすることなく変更できます。

ライセンスタイプ変換を使用して、次のシナリオでライセンスインベントリを最適化できます。

オンプレミスワークロードを Amazon EC2 に移行する

移行中に、ワークロードを Amazon Elastic Compute Cloud (Amazon EC2) にデプロイし、AWS 提供されたライセンスを使用できます。移行が完了したら、License Manager のライセンスタイ

プ変換を使用して、インスタンスのライセンスタイプを変更します。BYOL または BYOS に変更して、移行中にリリースされたライセンスを使用できます。

ライセンス契約が終了したワークロードの継続実行

License Manager のライセンスタイプ変換を使用して、BYOL または BYOS から AWS 提供されたライセンスに切り替えることができます。この切り替えにより、Flexible pay-as-you Go ライセンスモデルで提供される完全準拠のソフトウェアライセンス AWS でワークロードを引き続き実行できます。オペレーティングシステムのソフトウェアベンダー (Microsoft や Canonical など) とのライセンス契約の有効期限が近づいており、更新する予定がない場合は、この方法を選択できます。

コストの最適化

小規模なワークロードや不規則なワークロードでは、AWS 提供されたライセンス (ライセンス込み) インスタンスの方がコスト効率が良い場合があります。BYOL または BYOS を使用する場合、これらのオプションには長期的なコミットメントが必要になる場合があります。この場合、License Manager のライセンスタイプ変換を使用して、インスタンスを付属のライセンスに切り替え、ライセンス関連のコストを最適化することができます。インスタンスが独自の仮想マシン (VM) イメージから起動された場合は、BYOL または BYOS に切り替えることができます。これは、ワークロードがより安定しているか、予測可能な場合に選択できます。

延長メンテナンス

お使いの Ubuntu オペレーティングシステムの標準サポートが終了した場合は、Ubuntu Pro の有料サブスクリプションを追加できます。Ubuntu Pro にサブスクリプションを追加すると、長期間にわたってセキュリティアップデートが提供されます。詳細については、Canonical のドキュメントの「[Ubuntu Pro](#)」を参照してください。

トピック

- [License Manager でのライセンスタイプ変換の対象となるライセンスタイプ](#)
- [License Manager ライセンスタイプの変換前提条件](#)
- [License Manager でライセンスタイプを変換する](#)
- [License Manager でのテナンシー変換](#)
- [License Manager でのライセンスタイプ変換のトラブルシューティング](#)

License Manager でのライセンスタイプ変換の対象となるライセンスタイプ

License Manager のライセンスタイプ変換は、サポートされているバージョンと Windows Server ライセンスと Microsoft SQL Server ライセンスの組み合わせで使用できます。ライセンスタイプ変換は Ubuntu Linux サブスクリプションでも使用できます。

目次

- [License Manager の Windows および SQL Server の対象となるライセンスタイプ](#)
 - [SQL Server エディション](#)
 - [SQL Server のバージョン](#)
 - [使用オペレーションの値](#)
 - [メディアの互換性](#)
 - [変換パス](#)
- [License Manager での Linux の適格なサブスクリプションタイプ](#)

License Manager の Windows および SQL Server の対象となるライセンスタイプ

Important

Amazon が提供する Amazon マシンイメージ (AMI) から最初に起動されたインスタンスは、ライセンスタイプを BYOL に変換する対象にはなりません。

Windows および SQL Server がライセンスタイプ変換の対象となるには、特定の要件を満たしている必要があります。

トピック

- [SQL Server エディション](#)
- [SQL Server のバージョン](#)
- [使用オペレーションの値](#)
- [メディアの互換性](#)
- [変換パス](#)

SQL Server エディション

License Manager は、次の SQL Server エディションをサポートしています。

- SQL Server Standard エディション
- SQL Server Enterprise Edition
- SQL Server Web エディション

SQL Server のバージョン

License Manager は、次の SQL Server バージョンをサポートしています。

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

使用オペレーションの値

ライセンスタイプ変換によって、インスタンスに関連付けられた使用オペレーションの値が変更されます。次の表に、サポートされているオペレーティングシステムごとの使用オペレーションの値を示します。詳細については、[AMI 請求情報フィールド](#)」を参照してください。

オペレーティングシステムの詳細	使用オペレーション
BYOL としての Windows Server	RunInstances:0800
BYOL としての Windows Server	RunInstances:0800
SQL としての BYOL Server (任意のエディション)	RunInstances:0800

オペレーティングシステムの詳細	使用オペレーション
ライセンスインクルードとしての Windows Server	RunInstances:0002
ライセンスインクルードとしての Windows Server SQL としての BYOL Server (任意のエディション)	RunInstances:0002
ライセンスインクルードとしての Windows Server SQL Server Web as ライセンス込み	RunInstances:0202
ライセンスインクルードとしての Windows Server SQL Server Standard as ライセンス込み	RunInstances:0006
ライセンスインクルードとしての Windows Server SQL Server Enterprise as ライセンス込み	RunInstances:0102

メディアの互換性

次の表は、どのメディアがどのインスタンスライセンスモデルで使用できるかを示しています。

ソース	Target
	BYOL
	ライセンスインクルード

ソース	Target	
AWS が提供する Windows Server イメージ	なし	はい
AWS が提供する SQL Server イメージ	なし	はい
お客様の Windows Server メディア ¹	はい	はい
SQL Server メディア ²	はい	はい

¹ インスタンスがもともと、インポートされた独自の仮想マシン (VM) から起動されたことを示します。[VM Import/Export](#) や [AWS Application Migration Service](#) などのサービスを使用して VM をインポートできます。

² 独自の SQL Server インストールメディア (.iso、.exe) を調達したことを示します。

変換パス

次の表は、ソースライセンスモデルを BYOL とライセンスインクルードの間で別のモデルに変換できるかどうかを示しています。詳細については、「[License Manager でライセンスタイプを変換する](#)」を参照してください。

Important

- Windows Server as BYOL と SQL Server as ライセンス込みの設定はサポートされていません。
- 「必要なし」と指定された変換では、使用オペレーションの値は変更されません。

ソース	Target
-----	--------

ソース	Target					
	BYOL と しての Windows Server	ライセンス インクルー ドとしての Windows Server	BYOL と しての Windows Server	ライセンス インクルー ドとしての Windows Server	BYOL と しての Windows Server	ライセンス インクルー ドとしての Windows Server
			SQL とし ての BYOL サーバー	SQL とし ての BYOL サーバー	ライセンス インクル ードとし ての SQL Server	ライセンス インクル ードとし ての SQL Server
Windows Server as BYOL (メ ディア)	不要	はい	不要	あり ¹	サポートさ れていませ ん	あり ¹
ライセンス インクルー ドとしての Windows Server (お 客様のメ ディア)	あり ²	不要	はい ^{1,2}	不要 ³	サポートさ れていませ ん	あり ¹
ライセン ス込みの Windows Server (AWS 提供 されたイ メージ)	いいえ ^x	不要	いいえ ^x	不要 ³	サポートさ れていませ ん	あり ¹

ソース	Target					
Windows Server as BYOL (メディア)	不要 ⁴	はい	不要	はい	サポートされていません	はい
SQL Server as BYOL (メディア)						
ライセンスインクルードとしての Windows Server (お客様のメディア)	あり ²	不要 ⁴	あり ²	不要	サポートされていません	はい
SQL Server as BYOL (メディア)						

ソース	Target					
ライセンス込みの Windows Server (AWS 提供されたイメージ)	いいえ \times	不要 ⁴	いいえ \times	不要	サポートされています	はい
SQL Server as BYOL (メディア)						
Windows Server as BYOL (メディア)	サポートされています	サポートされています	サポートされています	サポートされています	サポートされています	サポートされています
ライセンスインクルードとしての SQL Server						

ソース	Target					
ライセンス込みの Windows Server (AWS 提供されたイメージまたはメディア)	いいえ ^X	いいえ ^X	いいえ ^X	いいえ ^X	サポートされていません	不要
ライセンス込みの SQL Server (AWS 提供されたイメージ)						
ライセンスインクルードとしての Windows Server (お客様のメディア)	はい ^{2,5,6}	はい ⁵	あり ²	はい	サポートされていません	不要
ライセンスインクルードとしての SQL Server (メディア)						

ソース	Target					
ライセンス込みの Windows Server (AWS 提供されたイメージ)	いいえ ^x	はい ⁵	いいえ ^x	はい	サポートされていません	不要
ライセンスインクルードとしての SQL Server (メディア)						

^x ターゲットライセンスタイプへの変換はサポートされていないため、別の設定で新しいインスタンスをデプロイする必要があります。詳細については、「[メディアの互換性](#)」を参照してください。

他の変換シナリオでは、次の手順を実行してライセンス変換を実行する必要がある場合があります。

¹ SQL Server を Word for BYOL Server に変換する前に、まず SQL Server をインストールする必要があります。

² ライセンスのアクティベーションに独自の KMS サーバーを使用するには、まず Windows 設定を変更する必要があります。詳細については、「[Convert Windows Server from license included to BYOL](#)」を参照してください。

³ SQL Server を使用しないソースから SQL Server を使用するターゲットに変換するときは、まず SQL Server をインストールする必要があります (SQL Server ライセンスタイプに関係なく)。

⁴ SQL Server を使用するソースから SQL Server を使用しないターゲットに変換するときは、まず SQL Server をアンインストールする必要があります (SQL Server ライセンスタイプに関係なく)。

⁵ ライセンス込みの SQL Server に変換する前に、まず SQL Server をアンインストールする必要があります。

⁶ まず、² と ⁵ の手順を実行する必要があります。これらのステップが完了したら、ライセンスタイプをライセンスインクルードとして Windows Server に変換し、ライセンスタイプをもう一度 BYOL として Windows Server に変換する必要があります。

License Manager での Linux の適格なサブスクリプションタイプ

ライセンスタイプ変換は、サポートされている Ubuntu のバージョンで使用できます。サポートされているバージョンには、Ubuntu 18.04.1 LTS などの更新が含まれています。サブスクリプションを Ubuntu Pro に変更すると、セキュリティアップデートがさらに 5 年間提供されます。詳細については、Canonical のドキュメントの「[Ubuntu Pro](#)」を参照してください。

次の Ubuntu バージョンではライセンスタイプ変換を使用できます。

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

オペレーティングシステムの詳細	使用オペレーション
Linux/UNIX	RunInstances
Ubuntu Pro	RunInstances:0g00

Linux の変換パス

Ubuntu

Ubuntu LTS のサポートされている任意のバージョンを Ubuntu Pro に変換できます。Ubuntu Pro から Ubuntu LTS に変換する必要がある場合は、[リクエストを送信する必要があります](#) Support。詳細については、「[サポートケースの作成](#)」を参照してください。

License Manager ライセンスタイプの変換前提条件

License Manager でライセンスタイプを変換するにあたり、一般的な前提条件と、オペレーティングシステムの前件条件があります。

トピック

- [全般](#)
- [Windows](#)
- [Linux](#)

全般

ライセンスタイプ変換を実行するには、以下の一般的な前提条件を満たす必要があります。

- は License Manager にオンボード AWS アカウント する必要があります。「[License Manager の使用を開始する](#)」を参照してください。
- ライセンスタイプを変換する前に、対象となるインスタンスが停止状態になっている必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「[インスタンスの停止と起動](#)」を参照してください。
- ターゲットインスタンスで停止保護が有効になっていると、変換プロセスは失敗します。詳細については、「[License Manager でのライセンスタイプ変換のトラブルシューティング](#)」を参照してください。
- ターゲットインスタンスは Systems Manager Inventory AWS で設定する必要があります。詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager for EC2 インスタンスとインベントリのセットアップ](#)」を参照してください。[AWS Systems Manager](#)
- ユーザーまたはロールに以下のアクセス許可が必要です。
 - `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`

Systems Manager Inventory の詳細については、[AWS Systems Manager Inventory](#)を参照してください。

Windows

Windows インスタンスは、次の前提条件を満たす必要があります。

- Amazon が提供する Amazon マシンイメージ (AMI) から最初に起動されたインスタンスは、ライセンスタイプを BYOL に変換することはできません。元の Amazon EC2 インスタンスは、独自の仮想マシン (VM) イメージから起動する必要があります。VM を Amazon EC2 に変換する方法の詳細については、「[VM Import/Export](#)」を参照してください。
- SQL Server ライセンスを BYOL に変更するには、SQL Server が独自のメディアを使用してインストールされている必要があります。

Linux

Linux インスタンスは、次の前提条件を満たす必要があります。

- インスタンスは Ubuntu LTS を実行している必要があります。
- Ubuntu Pro Client が Ubuntu オペレーティングシステムにインストールされている必要があります。
- Ubuntu Pro Client がインストールされているかどうかを確認するには、次のコマンドを実行します。

```
pro --version
```

- コマンドが見つからない場合や、バージョンをアップデートする必要がある場合は、以下のコマンドを実行して Ubuntu Pro Client をインストールします。

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

- Ubuntu Pro サブスクリプションをアクティベートしてアップデートを受信するには、インスタンスが複数のエンドポイントにアクセスできる必要があります。次のエンドポイントに到達するには、TCP ポート 443 を介したインスタンスからのアウトバウンドトラフィックを許可する必要があります。
 - `contracts.canonical.com` – Ubuntu Pro のアクティベーションに使用されます。
 - `esm.ubuntu.com` – ほとんどのサービスの APT リポジトリアクセスに使用されます。
 - `api.snapcraft.io` – スナップのインストールと実行に使用されます。
 - `dashboard.snapcraft.io` – スナップのインストールと実行に使用されます。
 - `login.ubuntu.com` – スナップのインストールと実行に使用されます。
 - `cloudfront.cdn.snapcraftcontent.com` – コンテンツ開発ネットワーク (CDNs) からのダウンロードに使用されます。
 - `livepatch.canonical.com` – ライブパッチサーバーからパッチをダウンロードするために使用されます。

詳細については、Ubuntu Pro Client ドキュメントの「[Ubuntu Pro Client network requirements](#)」と、Canonical Snapcraft ドキュメントの「[Network requirements](#)」を参照してください。

License Manager でライセンスタイプを変換する

License Manager コンソールまたは を使用して、Windows ライセンス、Microsoft SQL Server ライセンス、Ubuntu Linux サブスクリプションを変換できます AWS CLI。インスタンスのオペレーティングシステムでライセンスまたはサブスクリプションを変換するには、追加の手順を実行する必要があります。

ライセンスタイプの変換は、License Manager コンソールまたは AWS CLI。ライセンスタイプ変換を作成すると、License Manager はインスタンスの課金製品を検証します。これらの予備検証が成功すると、License Manager はライセンスタイプ変換を作成します。 `list-license-conversion-tasks` および `get-license-conversion-task` AWS CLI コマンドを使用して、ライセンスタイプ変換のステータスを確認できます。

License Manager は、ライセンスタイプ変換の一環として、セルフマネージドライセンスに関連付けられているリソースを更新する場合があります。具体的には、タイプ License Included の自動検出ルールを使用するセルフマネージドライセンスの場合、License Manager は、`license`

included の自動検出ルールがリソースを明示的に除外している場合、ライセンスタイプ変換のリソースとライセンスの関連付けを解除します。

たとえば、セルフマネージドライセンスに 2 つの自動検出ルールが含まれており、各ルールにライセンス込みの Windows Server が含まれていない場合、BYOL からライセンス込みの Windows Server へのライセンスタイプの変換により、インスタンスとセルフマネージドライセンスの関連付けが解除されます。ただし、2 つの自動検出ルールのうちの 1 つだけに License Included ルールが含まれていると、インスタンスの関連付けは解除されません。

ライセンスタイプの変換中は、インスタンスを起動または停止しないでください。ライセンスタイプ変換が成功すると、そのステータスは IN_PROGRESS から SUCCEEDED に変わります。ワークフロー中に問題が発生した場合、License Manager はライセンスタイプ変換のステータスを FAILED に更新し、ステータスメッセージをエラーメッセージで更新します。

Note

インスタンスの起動に使用される AMI の請求製品情報は、ライセンスタイプを変換しても変更されません。正確な請求情報を取得するには、Amazon EC2 API [DescribeInstances](#) を使用します。さらに、AMIs から請求情報を検索する既存のワークフローがある場合は、[DescribeInstances](#) を使用するようにそれらのワークフローを更新します。

目次

- [License Manager で Windows および SQL Server のライセンスタイプを変換する](#)
 - [ライセンスタイプ変換制限](#)
 - [License Manager コンソールを使用してライセンスタイプを変換する](#)
 - [を使用してライセンスタイプを変換する AWS CLI](#)
- [License Manager で Linux のライセンスタイプを変換する](#)
 - [ライセンスタイプの変換に関する考慮事項](#)
 - [License Manager コンソールを使用してライセンスタイプを変換する](#)
 - [を使用してライセンスタイプを変換する AWS CLI](#)
 - [Ubuntu Pro サブスクリプションを削除する](#)

License Manager で Windows および SQL Server のライセンスタイプを変換する

License Manager コンソールまたは を使用して AWS CLI 、対象となる Windows および SQL Server インスタンスのライセンスタイプを変換できます。

トピック

- [ライセンスタイプ変換制限](#)
- [License Maneger コンソールを使用してライセンスタイプを変換する](#)
- [を使用してライセンスタイプを変換する AWS CLI](#)

ライセンスタイプ変換制限

Important

マイクロソフトソフトウェアの使用には、マイクロソフトのライセンス条項が適用されます。お客様は、マイクロソフトのライセンス条項を遵守する責任があります。このドキュメントは便宜上のものであり、お客様はこの資料の記述に依存することはできません。このドキュメントは、法的助言を提供するものではありません。お使いの Microsoft ソフトウェアに関するライセンスの権限についてご質問がある場合は、お客様社内の法務部門、Microsoft、Microsoft の販売代理店にお問い合わせください。

License Manager は、Microsoft サービスプロバイダーライセンス契約 (SPLA) に従って作成できるライセンス変換のタイプを制限します。ライセンスタイプの変換には、以下のような制限があります。これは包括的なリストではなく、変更される可能性があります。

- Amazon EC2 インスタンスは、独自の仮想マシン (VM) イメージから起動する必要があります。
- ライセンス込みの SQL Server は Dedicated Host で実行できません。
- ライセンス込みの SQL Server インスタンスには、少なくとも 4 vCPUs が必要です。

License Maneger コンソールを使用してライセンスタイプを変換する

License Manager コンソールを使用してライセンスタイプを変換できます。

Note

停止状態であり、AWS Systems Manager Systems Manager Inventory で関連付けられているインスタンスのみが表示されます。

コンソールでライセンスタイプ変換を開始するには、以下の手順に従います。

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. 左のナビゲーションペインから、[ライセンスタイプの変換] > [ライセンスタイプの変換を作成] を選択します。
3. [ソースオペレーティングシステム] では、変換するインスタンスのプラットフォームを選択します。
 - Ubuntu LTS
 - Windows BYOL
 - Windows ライセンスインクルード
4. (オプション) [インスタンス ID] または [使用オペレーションの値] の値を指定して、使用可能なインスタンスをフィルタリングします。
5. ライセンスを変換したいインスタンスを次を選択します。
6. ライセンスタイプの [使用オペレーションの値] を入力し、変換先のライセンスを選択して、[次へ] 選択します。
7. ライセンスタイプ変換の設定に問題がないことを確認し、[変換を開始] を選択します。

ライセンスタイプ変換パネルから、ライセンスタイプ変換のステータスを表示できます。[変換ステータス] 列には、変換のステータスが [進行中]、[完了]、または [失敗] として表示されます。

Important

Windows Server をライセンスインクルードから BYOL に変換する場合は、Microsoft ライセンス契約に従って Windows をアクティブ化する必要があります。詳細については、「[Convert Windows Server from license included to BYOL](#)」を参照してください。

を使用してライセンスタイプを変換する AWS CLI

AWS CLIでライセンスタイプ変換を開始するには

インスタンスのライセンスタイプを判別する

1. AWS CLIがインストールと設定が完了していることを確認してください。詳細については、「[the AWS CLIのインストール、更新、アンインストール](#)」および「[Configuring the AWS CLI](#)」を参照してください。

Important

を更新 AWS CLI して特定のコマンドを実行し、次のステップで必要な出力をすべて受け取る必要がある場合があります。

2. `create-license-conversion-task-for-resource` AWS CLI コマンドを実行するアクセス許可があることを確認します。このエラーのヘルプについては、「[License Manager のIAMポリシーを作成する](#)」を参照してください。
3. インスタンスに現在関連付けられているライセンスタイプを確認するには、次の AWS CLI コマンドを実行します。インスタンスID を、ライセンスタイプを確認したいインスタンスのIDに置き換えます。

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

4. 次のコードは、`describe-instances` コマンドに対するレスポンスの例です。この `UsageOperation` 値は、ライセンスに関連する請求情報コードであることに注意してください。 `UsageOperationUpdateTime` は請求コードが更新された時刻です。詳細については、「[DescribeInstances](#) Amazon EC2 API リファレンスの」を参照してください。

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

Note

SQL Server Enterprise BYOL を使用した Windows Server の使用オペレーションは、Windows BYOL の使用オペレーションと同じです。これは、同じ料金が請求されるためです。

Windows Server をライセンスインクルードから BYOL に変換する

Windows Server をライセンスインクルードから BYOL に変換しても、License Manager は自動的に Windows をアクティブ化しません。インスタンスの KMS サーバーを AWS KMS サーバーから独自の KMS サーバーに切り替える必要があります。

Important

ライセンス込みから BYOL に変換するには、元の Amazon EC2 インスタンスを独自の仮想マシン (VM) イメージから起動する必要があります。VM を Amazon EC2 に変換する方法の詳細については、[「VM Import/Export」](#) を参照してください。Amazon マシンイメージ (AMI) から最初に起動されたインスタンスは、BYOL へのライセンス変換の対象ではありません。

Microsoft Windows Server のアクティベーションにどのような方法があるかは、Microsoft 社の使用許諾契約書をご確認ください。たとえば、KMS サーバーを使用している場合は、インスタンスの元の KMS 設定から BYOL サーバーのアドレスを取得する必要があります。

1. インスタンスのライセンスタイプを変換するには、次のコマンドを実行し、ARN を変換するインスタンスの ARN に置き換えます。

```
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. ライセンスを変換した後に Windows をアクティブ化するには、オペレーティングシステムの Windows Server KMS サーバーを独自の KMS サーバーにポイントする必要があります。新しい Windows インスタンスにログインし、以下のコマンドを実行します。

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

Windows Server を BYOL からライセンスインクルードに変換する

Windows Server を BYOL からライセンスインクルードに変換すると、License Manager はインスタンスの KMS サーバーを AWS KMS サーバーに自動的に切り替えます。

インスタンスのライセンスタイプを BYOL からライセンスインクルードに変換するには、次のコマンドを実行し、ARN を変換するインスタンスの ARN に置き換えます。

```
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
```

Windows Server と SQL Server の両方を BYOL からライセンスインクルードに変換する

複数の製品を同時に切り替えることができます。たとえば、Windows Server と SQL Server の両方を 1 つのライセンスタイプ変換で変換できます。

Windows Server インスタンスのライセンスタイプを BYOL からライセンスインクルード、SQL Server Standard を BYOL からライセンスインクルードに変換するには、次のコマンドを実行し、ARN を変換するインスタンスの ARN に置き換えます。

```
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
```

License Manager で Linux のライセンスタイプを変換する

License Manager コンソールまたは を使用して AWS CLI 、対象となる Ubuntu LTS インスタンスのライセンスタイプを変換できます。

トピック

- [ライセンスタイプの変換に関する考慮事項](#)
- [License Maneger コンソールを使用してライセンスタイプを変換する](#)
- [を使用してライセンスタイプを変換する AWS CLI](#)
- [Ubuntu Pro サブスクリプションを削除する](#)

ライセンスタイプの変換に関する考慮事項

ライセンスタイプの変換には、以下のような考慮事項があります。これは包括的なリストではなく、変更される可能性があります。

Ubuntu 変換

- ライセンスタイプを Ubuntu Pro に変換するには、インスタンスが Ubuntu LTS を実行している必要があります。
- Ubuntu Pro サブスクリプションではライセンスタイプ変換を使用できません。Ubuntu Pro サブスクリプションを削除するには、「[Ubuntu Pro サブスクリプションを削除する](#)」を参照してください。
- Ubuntu Pro はリザーブドインスタンスとしてはご利用いただけません。オンデマンドインスタンスよりもコストを削減するには、Ubuntu Pro と Savings Plans の併用をお勧めします。詳細については、「[Amazon Word ユーザーガイド](#)」の「[リザーブドインスタンス](#)」および「[Savings Plans ユーザーガイド](#)」の「[Savings Plans とは](#)」を参照してください。 EC2 Savings Plans

License Manager コンソールを使用してライセンスタイプを変換する

License Manager コンソールを使用してライセンスタイプを変換できます。

Note

停止状態であり、AWS Systems Manager Systems Manager Inventory で関連付けられているインスタンスのみが表示されます。

コンソールでライセンスタイプ変換を開始するには、以下の手順に従います。

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. 左のナビゲーションペインから、[ライセンスタイプの変換] > [ライセンスタイプの変換を作成] を選択します。
3. [ソースオペレーティングシステム] では、変換するインスタンスのプラットフォームを選択します。
 - Ubuntu LTS
 - Windows BYOL
 - Windows ライセンスインクルード

4. (オプション) [インスタンス ID] または [使用オペレーションの値] の値を指定して、使用可能なインスタンスをフィルタリングします。
5. ライセンスを変換したいインスタンスを次を選択します。
6. ライセンスタイプの [使用オペレーションの値] を入力し、変換先のライセンスを選択して、[次へ] 選択します。
7. ライセンスタイプ変換の設定に問題がないことを確認し、[変換を開始] を選択します。

ライセンスタイプ変換パネルから、ライセンスタイプ変換のステータスを表示できます。[変換ステータス] 列には、変換のステータスが [進行中]、[完了]、または [失敗] として表示されます。

を使用してライセンスタイプを変換する AWS CLI

でライセンスタイプの変換を開始するには AWS CLI、インスタンスのライセンスタイプが適格であることを確認し、ライセンスタイプの変換を実行して必要なサブスクリプションに変更する必要があります。対象となるサブスクリプションタイプの詳細については、「[License Manager での Linux の適格なサブスクリプションタイプ](#)」を参照してください。

インスタンスのライセンスタイプを判別する

AWS CLIがインストールと設定が完了していることを確認してください。詳細については、「[のインストール、更新、アンインストール](#)」および「[AWS CLI の設定](#)」を参照してください AWS CLI。

Important

を更新 AWS CLI して特定のコマンドを実行し、次のステップで必要な出力をすべて受け取る必要がある場合があります。create-license-conversion-task-for-resource AWS CLI コマンドを実行するアクセス許可があることを確認します。詳細については、「[License Manager の IAM ポリシーを作成する](#)」を参照してください。

インスタンスに現在関連付けられているライセンスタイプを確認するには、次の AWS CLI コマンドを実行します。インスタンス ID を、ライセンスタイプを確認したいインスタンスの ID に置き換えます。

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

```
PlatformDetails, UsageOperation: UsageOperation, UsageOperationUpdateTime:  
UsageOperationUpdateTime}"
```

次のコードは、describe-instances コマンドに対するレスポンスの例です。UsageOperation 値は、ライセンスに関連付けられた請求情報コードです。RunInstances の使用オペレーションの値は、インスタンスが AWS 提供のライセンスを使用していることを示します。UsageOperationUpdateTime は請求コードが更新された時刻です。詳細については、「[」を参照してください](#)[DescribeInstances](#) 「Amazon EC2 API Reference」の「」を参照してください。

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

Ubuntu Pro に変換する

インスタンスを Ubuntu LTS から Ubuntu Pro に変換する前に、正規サーバーからライセンストークンを取得して Ubuntu Pro Client をインストールするようにインスタンスにアウトバウンドインターネットアクセスが設定されている必要があります。詳細については、「[License Manager ライセンスタイプの変換前提条件](#)」を参照してください。

Ubuntu LTS を Ubuntu Pro に変換するには、次の手順に従います。

1. インスタンスの ARN を指定 AWS CLI しながら、 から次のコマンドを実行します。

```
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. インスタンス内から以下のコマンドを実行して、Ubuntu Pro のサブスクリプションステータスに関する詳細を取得します。

```
pro status
```

3. 出力結果から、インスタンスに有効な Ubuntu Pro サブスクリプションがあることを確認します。

```

ubuntu@ip-
SERVICE          pro status
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

```

Ubuntu Pro サブスクリプションを削除する

ライセンスタイプの変換は、Ubuntu LTS から Ubuntu Pro への変換にのみ使用できます。Ubuntu Pro から Ubuntu LTS に変換する必要がある場合は、リクエストを送信する必要があります Support。詳細については、「[サポートケースの作成](#)」を参照してください。

License Manager でのテナンシー変換

お客様のユースケースに合わせて、インスタンスのテナンシーを変更することができます。[modify-instance-placement](#) AWS CLI コマンドを使用して、次のテナンシーを切り替えることができます。

- Shared
- Dedicated Instance
- Dedicated Host
- リソースグループをホストします

お客様のアカウントには、Dedicated Hostのテナンシータイプに変更するために、インスタンスを開始するための利用可能な容量を持つDedicated Hostが必要です。Dedicated Hosts の操作の詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「[Dedicated Hosts の操作](#)」を参照してください。

ホストリソースグループテナンシータイプに移行するには、アカウントに少なくとも1つのホストリソースグループが必要です。ホストリソースグループ内でインスタンスを起動するには、そのインスタンスに、ホストリソースグループに関連付けられているものと同じライセンスセットが必要です。詳細については、「[License Manager でリソースグループをホストする](#)」を参照してください。

テナンシー属性変換制限

テナンシー属性変換には、以下の制限が適用されます。

- Linux 請求コードは、すべてのテナンシータイプで許可されています。
- 共有テナンシーでは、Windows BYOL 請求コードは許可されません。
- Windows Server ライセンスに含まれる請求コードは、すべてのテナンシータイプで許可されています。
- サポートされているすべての SQL Server エディションと SUSE (SLES) ライセンス込みの請求コードは、共有テナンシーおよびハードウェア専有インスタンスで許可されます。ただし、これらの請求コードは、Dedicated Hosts およびホストリソースグループでは許可されません。
- Windows Server 以外のライセンスに含まれる課金コードは、Dedicated Host およびホストリソースグループでは許可されません。

を使用してインスタンスのテナンシーを変更する AWS CLI

テナンシーを変更するには、インスタンスが stopped その状態にある必要があります。

インスタンスを停止するには、次のコマンドを実行します。

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

インスタンスを任意のテナンシーから default または dedicated テナンシーに変更するには、次のコマンドを実行します。

default

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

dedicated

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

インスタンスを任意のテナンシーから自動配置付きの host テナンシーに変更するには、次のコマンドを実行します。

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

```
--tenancy host --affinity default
```

特定の Dedicated Host を対象に、インスタンスを任意のテナンシーから host テナンシーに変更するには、以下のコマンドを実行します。

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

ホストリソースグループを使用してインスタンスを任意のテナンシーから host テナンシーに変更するには、次のコマンドを実行します。

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

License Manager でのライセンスタイプ変換のトラブルシューティング

トラブルシューティングのトピック

- [Windows のアクティベーション](#)
- [インスタンス \[インスタンス\] は Amazon 所有の AMI から起動されます。BYOL Word から最初に起動されたインスタンスを指定しますAMI。](#)
- [インスタンス \[インスタンス\] が BYOL から起動されたことを検証できませんでしたAMI。SSM エージェントがインスタンスで実行されていることを確認します。](#)
- [operationCreateLicenseConversionTaskForResource : InvalidParameterValueException-\[instance\] を呼び出すときにエラー \(ResourceId \) が発生し、ライセンスタイプを変更するために無効な状態になりました。](#)
- [EC2 インスタンス \[instance\] の停止に失敗しました。EC2 のアクセス許可があることを確認する StopInstances.](#)

Windows のアクティベーション

ライセンスタイプ変換には、複数のステップが含まれます。場合によっては、Windows Server インスタンスを BYOL からライセンスインクルードに変換すると、インスタンスの請求製品が正常に更新されます。ただし、KMS サーバーが AWS KMS サーバーに切り替えられない場合があります。

この問題を修正するには、[EC2 Windows インスタンスで Windows アクティベーションが失敗したのはなぜですか？](#) の手順に従って、Systems Manager で Windows をアクティブ化します。

[AWSSupport-ActivateWindowsWithAmazonLicense](#) オートメーションランブック、またはインスタンスにログインし、AWS KMS サーバーに手動で切り替えます。

インスタンス [インスタンス] は Amazon 所有の AMI から起動されます。BYOL Word から最初に起動されたインスタンスを指定しますAMI。

Bring Your Own License モデル (EC2) へのライセンスタイプ変換を実行するには、インポートした AMI から Amazon BYOL Windows インスタンスを起動する必要があります。Amazon 所有の AMI から最初に起動されたインスタンスは、ライセンスタイプを BYOL に変換することはできません。詳細については、「[License Manager ライセンスタイプの変換前提条件](#)」を参照してください。

インスタンス [インスタンス] が BYOL から起動されたことを検証できませんでした AMI。SSM エージェントがインスタンスで実行されていることを確認します。

ライセンスタイプ変換を成功させるには、まずインスタンスがオンラインで、Systems Manager によって管理され、インベントリが収集されている必要があります。AWS Systems Manager エージェント (SSM Agent) は、オペレーティングシステムの詳細を含むインベントリをインスタンスから収集します。詳細については、「[ユーザーガイド](#)」の [SSM エージェントのステータスの確認とエージェントの起動](#)」および [SSM エージェントのトラブルシューティング](#)」を参照してください。

AWS Systems Manager

operation**CreateLicenseConversionTaskForResource** :

InvalidParameterValueException- [instance] を呼び出すときにエラー (ResourceId) が発生し、ライセンスタイプを変更するために無効な状態になりました。

ライセンスタイプを変換するには、対象となるインスタンスが停止状態になっている必要があります。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「[License Manager ライセンスタイプの変換前提条件](#)」および「[インスタンスの停止に関するトラブルシューティング](#)」を参照してください。

EC2 インスタンス [instance] の停止に失敗しました。EC2 のアクセス許可があることを確認する **StopInstances** .

ターゲットインスタンスで StopInstances EC2 APIするアクセス許可が必要です。また、ターゲットインスタンスで停止保護が有効になっていると、変換プロセスは失敗します。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「[実行中または停止したインスタンスに対する停止保護を無効にします](#)」を参照してください。

License Manager でリソースグループをホストする

Amazon EC2 Dedicated Hosts は、お客様専用のEC2インスタンス容量を備えた物理サーバーです。ホストリソースグループは、単一のエンティティとして管理できるDedicated Hostの集合体です。インスタンスを起動すると、License Managerはホストを割り当て、構成した設定に基づいてホストにインスタンスを起動します。既存の Dedicated Hosts をホストリソースグループに追加し、License Managerによる自動ホスト管理を利用できます。詳細については、「[Amazon EC2ユーザーガイド](#)」の「[Dedicated Hosts](#)」を参照してください。

ホストリソースグループを使用して、開発テストホストと製品、組織単位、ライセンス制約など、目的別にホストを分けることができます。Dedicated Host をホストリソースグループに追加した後は、Dedicated Hostで直接インスタンスを起動することはできません。ホストリソースグループを使用してインスタンスを起動する必要があります。

設定

ホストリソースグループには次の設定が可能です。

- ホストを自動的に割り当てる – このホストリソースグループでインスタンスを起動すると EC2、Amazon がユーザーに代わって新しいホストを割り当てることができるかどうかを示します。
- ホストを自動的に解放する — Amazon がユーザーに代わって未使用のホストを解放EC2できるかどうかを示します。未使用のホストには実行中のインスタンスはありません。
- ホストの自動復旧 — Amazon が予期せず失敗したホストから新しいホストにインスタンスを移動EC2できるかどうかを示します。
- 関連付けられたセルフマネージドライセンス - このホストリソースグループ内のインスタンスを起動するために使用できるセルフマネージドライセンス。
- (オプション) インスタンスファミリー - 起動できるインスタンスのタイプ。デフォルトでは、Dedicated Host でサポートされているどのインスタンスタイプでも起動できます。起動した場合[Nitroベース](#)インスタンスを作成すると、同じホストリソースグループ内の異なるインスタンスタイプのインスタンスを起動できます。そうでなければ、同じホストリソースグループ内の同じインスタンスタイプのインスタンスのみを起動する必要があります。

内容

- [License Manager でホストリソースグループを作成する](#)
- [License Manager でホストリソースグループを共有する](#)

- [License Manager で専有ホストをホストリソースグループに追加する](#)
- [License Manager でホストリソースグループでインスタンスを起動する](#)
- [License Manager でホストリソースグループを変更する](#)
- [License Manager でホストリソースグループから Dedicated Hosts を削除する](#)
- [License Manager でホストリソースグループを削除する](#)

License Manager でホストリソースグループを作成する

License Manager が Dedicated Hosts を管理できるようにホストリソースグループを構成します。最も高価なライセンスを最大限に活用するために、1 つ以上のコアベースまたはソケットベースのセルフマネージドライセンスをホストリソースグループに関連付けることができます。ホストの使用率を最適化するために、ホストリソースグループですべてのコアベースまたはソケットベースのセルフマネージドライセンスを許可できます。

ホストリソースグループの作成

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインで、[ホストリソースグループ] を選択します。
3. [リソースグループの作成] を選択します。
4. ホストリソースグループの詳細では、ホストリソースグループの名前と説明を指定します。
5. EC2 Dedicated Host 管理設定 では、必要に応じて次の設定を有効または無効にします。
 - ホストの自動割り当て
 - ホストの自動解放
 - ホストの自動復元
6. (オプション)追加設定で、ホストリソースグループで起動できるインスタンスファミリーを選択します。
7. セルフマネージドライセンスの場合は、1 つ以上のコアベースまたはソケットベースのセルフマネージドライセンスを選択します。
8. (オプション) タグでは、1 つ以上のタグを追加します。
9. [Create] (作成) を選択します。

License Manager でホストリソースグループを共有する

以下を使用できます..。 AWS Resource Access Manager を使用してホストリソースグループを共有するには AWS Organizations。 ホストリソースグループとセルフマネージドライセンスを共有すると、メンバーアカウントは共有ホストリソースグループにインスタンスを起動できます。新しいホストは、ホストリソースグループを所有するアカウントに割り当てられます。メンバーアカウントがインスタンスを所有しています。詳細については、『』を参照してください。[AWS RAM ユーザーガイド](#)。

License Manager で専有ホストをホストリソースグループに追加する

既存のホストを からホストリソースグループに追加できます。 AWS Management Console, AWS CLI、または AWS API。ホストを追加するには、 AWS Dedicated Host とホストリソースグループを作成した アカウント所有者。もしホストリソースグループに許可されたセルフマネージドライセンスとインスタンスタイプがリストされている場合は、追加するホストがこれらの要件を満たしている必要があります。

Note

インスタンスを停止して再起動する場合は、次の 2 つのタスクを実行する必要があります。

- ホストリソースグループを指すようにインスタンスを[変更](#)します。
- ホストリソースグループに一致するセルフマネージドライセンスを[関連付け](#)ます。

Resource Groups の詳細については、「」を参照してください。[AWS Resource Groups ユーザーガイド](#)。

resource group に 1 つ以上の Dedicated Hosts を追加するには、次の手順に従います:

1. で License Manager コンソールにログインします <https://console.aws.amazon.com/license-manager/>。
2. [ホストリソースグループ] を選択します。
3. ホストリソースグループ名の一覧から、Dedicated Hostを追加したいホストリソースグループの名前をクリックします。
4. Dedicated Hosts を選択します。
5. [Add] を選択します。
6. 1 つまたは複数の Dedicated Hosts を選択して、ホストリソースグループに追加します。

7. [追加] を選択します。

ホストの追加には 1 から 2 分かかる場合があります、それは Dedicated Hosts のリストの中に表示されます。

License Manager でホストリソースグループでインスタンスを起動する

インスタンスの起動時に、ホストリソースグループを指定できます。たとえば、次のような [実行インスタンス](#) コマンドを使用できます。コアベースまたはソケットベースのセルフマネージドライセンスをに関連付ける必要がありますAMI。

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

Amazon EC2 コンソールを使用することもできます。詳細については、「Amazon EC2 ユーザーガイド」の [「ホストリソースグループへのインスタンスの起動」](#) を参照してください。

License Manager でホストリソースグループを変更する

ホストリソースグループの設定はいつでも変更することができます。ホスト制限は、ホストリソースグループ内の既存のホスト数より小さく設定することはできません。ホストのリソースグループにそのタイプのインスタンスが動作している場合は、インスタンスタイプを削除することはできません。

ホストリソースグループを変更するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインで、[ホストリソースグループ] を選択します。
3. ホストリソースグループを選択し、アクション、編集を選びます。
4. 必要に応じて設定を変更します。
5. [Save changes] (変更の保存) をクリックします。

License Manager でホストリソースグループから Dedicated Hosts を削除する

ホストリソースグループからホストを削除しても、そのホストで実行されているインスタンスはホスト上に残ります。ホストリソースグループに添付されたインスタンスは、グループに関連付けられた

ままになり、アフィニティによってホストに直接添付されたインスタンスは、同じプロパティを維持します。ホストリソースグループを他のと共有する場合 AWS アカウント、License Manager は共有ホストを自動的に削除し、コンシューマーは 15 日以内にインスタンスをホストから移動するためのエビクション通知を受け取ります。ホストリソースグループから削除された Dedicated Host を操作するには、「Amazon EC2 [ユーザーガイド](#)」の「[Dedicated Hosts](#) の使用」を参照してください。

次の手順に従って、Dedicated Hostをホストリソースグループから削除します。

1. で License Manager コンソールにログインします <https://console.aws.amazon.com/license-manager/>。
2. [ホストリソースグループ] を選択します。
3. Dedicated Hostを削除したいホストリソースの名前をクリックします。
4. Dedicated Hostsを選択します。
5. ホストリソースグループから削除するDedicated Hostを選択します。または、ホストID、ホストタイプ、ホストの状態、またはアベイラビリティゾーンで Dedicated Host を検索することもできます。
6. [削除] を選択します。
7. もう一度確認のために削除を選択します。

License Manager でホストリソースグループを削除する

ホストが存在しない場合は、ホストリソースグループを削除できます。

リソースグループを削除するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインで、[ホストリソースグループ] を選択します。
3. ホストリソースグループを選択し、[アクション]、[削除] を選択します。
4. 確認を求めるメッセージが表示されたら、[削除] を選択します。

License Manager でのインベントリ検索

License Managerでは、[Systems Manager \(SSM\) インベントリ](#)を使ってオンプレミスアプリケーションを検出し、それにライセンスルールをアタッチすることができます。これらのサーバーにライ

センスルールがアタッチされたら、License Manager ダッシュボードで AWS サーバーとともにそれらを追跡できます。

License Manager はこれらのサーバーの起動時または終了時にライセンスルールを検証することはできません。AWS servers up-to-date 以外の情報を保持するには、License Manager コンソールのインベントリ検索セクションを使用してインベントリ情報を定期的に更新する必要があります。

Systems Managerはインベントリデータを30日間保存します。この期間中においては、Ping に応答しない場合であってもLicense Managerが、マネージドインスタンスをアクティブなインスタンスとしてカウントします。Systems Managerからインベントリデータが消去されると、License Managerがそのインスタンスを非アクティブとしてマークし、ローカルインベントリデータを更新します。マネージドインスタンスの正確なカウントを保つには、Systems Managerで登録解除を手動で行い、License Managerがクリーンアップ処理を実行できるようにします。

Systems Manager インベントリをクエリするには、Amazon S3 バケットにインベントリを保存するためのリソースデータ同期、組織アカウントからインベントリデータを集約するための Amazon Athena、および高速なクエリエクスプレッションを提供する AWS Glue ために必要なリソースデータ同期が必要です。詳細については、「[License Manager のサービスにリンクされたロールの使用](#)」を参照してください。

リソースインベントリの追跡は、組織がユーザーが AMI 派生インスタンスを作成したり、実行中のインスタンスに追加のソフトウェアをインストールしたりすることを制限 AWS しない場合にも役立ちます。License Managerには、インベントリ検索を使用してこれらのインスタンスとアプリケーションを簡単に検出するメカニズムが用意されています。これらの検出されたリソースにルールをアタッチし、マネージド AMIs から作成されたインスタンスと同じ方法でルールを追跡および検証できます。

内容

- [License Manager でのインベントリ検索の操作](#)
- [License Manager でのインベントリの自動検出](#)

License Manager でのインベントリ検索の操作

License Managerは[Systems Manager インベントリ](#)を使用して、オンプレミスでのソフトウェアの使用状況を確認できます。セルフマネージドライセンスをオンプレミスサーバーに関連付けると、License Manager は定期的にソフトウェアインベントリを収集し、ライセンス情報を更新し、ダッシュボードを更新して使用状況を報告します。

タスク

- [インベントリ検索のセットアップ](#)
- [インベントリ検索を使用する](#)
- [セルフマネージドライセンスに自動検出ルールを追加する](#)
- [セルフマネージドライセンスをインベントリ検索に関連付ける](#)
- [セルフマネージドライセンスとリソースの関連付けを解除する](#)

インベントリ検索のセットアップ

リソースインベントリ検索を使用する前に、次の要件を完了してください:

- License Manager をアカウントと統合することで、クロス AWS Organizations アカウントインベントリ検出を有効にします。詳細については、「[License Manager の設定](#)」を参照してください。
- 管理するサーバーとアプリケーションのセルフマネージドライセンスを作成します。例えば、Microsoft for SQL Server Enterprise とのライセンス契約の条件を反映するセルフマネージドライセンスを作成します。

インベントリ検索を使用する

リソースインベントリを検索するには、次の手順を実行します。アプリケーションは、名前 (SQL Server) で始まる名前など) と含まれるライセンスのタイプ (SQL Server Web) 用ではないライセンスなど) で検索できます。

リソースインベントリを検索する

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. ナビゲーションペインで [インベントリ検索] を選択します。
3. (オプション) 次のようにフィルターオプションを指定して、検索結果を効率化できます。

Amazon EC2 リソース

フィルター名	説明	論理演算子	サポートされる値
リソース ID	リソースの ID。	Equals, Not equals	

フィルター名	説明	論理演算子	サポートされる値
アカウント ID	リソースを所有する AWS アカウントの ID。	Equals, Not equals	
プラットフォーム名	リソースのオペレーティングシステムプラットフォーム。	Equals, Not equals, Begins with, Contains	
アプリケーション名	アプリケーションの名前。	Equals, Begins with	
ライセンス込みの名前	含まれるライセンスのタイプ。	Equals, Not equals	<ul style="list-style-type: none"> • SQL Server Enterprise • SQL Server Standard • SQL Server Web • Windows Server Datacenter

フィルター名	説明	論理演算子	サポートされる値
タグ	<p>リソースに割り当てられたメタデータタグキーとオプションの値。</p> <p>Not equals 論理演算子は、クロスアカウント検出が有効になっている場合にのみ使用できます。</p>	Equals, Not equals	

Amazon RDS リソース

フィルター名	説明	論理演算子	サポートされる値
エンジンのエディション	データベースエンジンのエディション。	Equals	<ul style="list-style-type: none"> • oracle-ee • oracle-se • oracle-se1 • oracle-se2 • db2-se • db2-ae

フィルター名	説明	論理演算子	サポートされる値
ライセンスパック (Oracle のみ)	Amazon RDS for Oracle ライセンスに関連付けられている管理パック。	Equals	<ul style="list-style-type: none"> Spatial and Graph Active Data Guard Label Security Oracle On-Line Analytical Processing (OLAP) Diagnostic Pack and Tuning Pack

Amazon RDS データベース製品ライセンスの詳細については、「Amazon Word ユーザーガイド」の [RDS for Oracle ライセンスオプション](#) または [RDS for Db2 ライセンスオプション](#) を参照してください。 RDS

セルフマネージドライセンスに自動検出ルールを追加する

セルフマネージドライセンスに製品情報を追加すると、License Manager は、それらの製品がインストールされているインスタンスのライセンス使用状況を追跡できます。詳細については、「[License Manager でのインベントリの自動検出](#)」を参照してください。

セルフマネージドライセンスに自動検出ルールを追加するには

1. <https://console.aws.amazon.com/license-manager/> で [License Manager](#) コンソールを開きます。
2. [インベントリ検索] ページを開きます。
3. リソースを選択し、自動検出ルールの追加を選択します。

4. [セルフマネージドライセンス] で、セルフマネージドライセンスを選択します。
5. 検出して追跡する製品を指定します。
6. (オプション) [ソフトウェアがアンインストールされたときにインスタンスの追跡を停止する] を選択します。License Manager がソフトウェアがアンインストールされ、ライセンスのアフィニティ期間が経過したことを検出した後、ライセンスを再利用できるようにする。
7. (オプション) 自動検出からリソースを除外するには、除外ルールを追加するを選択します。

 Note

除外ルールは、Amazon RDS 製品 (RDS for Oracle や RDS for Db2 など) には適用されません。

- a. フィルタリングしたいプロパティを選択してください。現在アカウントID、およびのタグがサポートされています。
 - b. そのプロパティを識別するための情報を入力します。アカウント ID には、値として 12 桁の AWS アカウント ID を指定します。タグにはキーバリューのペアを入力します。
 - c. ステップ7 を繰り返して、ルールを追加します。
8. [追加] を選択します。

セルフマネージドライセンスをインベントリ検索に関連付ける

管理が必要なアンマネージドリソースを特定した後は、自動検出ではなく、手動でセルフマネージドライセンスと関連付けることができます。

セルフマネージドライセンスをリソースに関連付けるには

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. [インベントリ検索] ページを開きます。
3. リソースを選択し、[セルフマネージドライセンスを関連付ける] を選択します。
4. [セルフマネージドライセンス名] で、セルフマネージドライセンスを選択します。
5. (オプション) [セルフマネージドライセンスをすべてのメンバーアカウントと共有] を選択します。
6. [関連付ける] を選択します。

セルフマネージドライセンスとリソースの関連付けを解除する

ソフトウェアベンダーのライセンス条件が変更された場合は、手動で関連付けられたリソースの関連付けを解除し、セルフマネージドライセンスを削除できます。

セルフマネージドライセンスとリソースの関連付けを解除するには

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスの名前を選択します。
4. [リソース] をクリックします。
5. セルフマネージドライセンスとの関連付けを解除するリソースをそれぞれ選択し、[リソースの関連付けを解除] を選択します。

License Manager でのインベントリの自動検出

License Manager は [Systems Manager インベントリ](#) を使用して、Amazon EC2 インスタンスとオンプレミスインスタンスでのソフトウェア使用状況を検出します。セルフマネージドライセンスに製品情報を追加すれば、License Manager はそれらの製品がインストールされているインスタンスを追跡します。さらに、ライセンス契約に基づいて除外ルールを指定して、除外するインスタンスを決定することもできます。アカウント IDs に属する AWS インスタンスやリソースタグに関連付けられたインスタンスを自動検出の対象から除外できます。

自動検出は、新しいライセンスセット、既存のセルフマネージドライセンス、またはインベントリ内のリソースに追加できます。自動検出のルールは、CLI コマンドを使用して [API UpdateLicenseConfiguration](#) からいつでも編集できます。コンソールでルールを編集するには、既存のセルフマネージドライセンスを削除して新しいセルフマネージドライセンスを作成する必要があります。

自動検出を使用するには、セルフマネージドライセンスに製品情報を追加する必要があります。これは、インベントリ検索を使用してセルフマネージドライセンスを作成するときに行うことができます。

自動検出によって追跡されるインスタンスの関連付けを手動で解除することはできません。デフォルトでは、自動検出では、ソフトウェアのアンインストール後に追跡対象インスタンスの関連付けが解除されません。ソフトウェアのアンインストール時にインスタンスの追跡を停止するように、自動検出を構成できます。

自動検出を構成したら、License Manager ダッシュボードからライセンスの使用状況を追跡できます。

前提条件

- License Manager をアカウントと統合することで、クロス AWS Organizations アカウントインベントリ検索を有効にします。詳細については、「[License Manager の設定](#)」を参照してください。

Note

単一のアカウントで自動検出を設定できますが、除外ルールを追加することはできません。

- インスタンスに Systems Manager インベントリをインストールしてください。

セルフマネージドライセンスの作成時に自動検出を設定するには

セルフマネージドライセンスを作成するときに、自動検出ルールと除外ルールを設定できます。詳細については、「[License Manager でセルフマネージドライセンスを作成する](#)」を参照してください。

既存のセルフマネージドライセンスに自動検出ルールを追加するには

次の手順を使用して、コンソールから既存のセルフマネージドライセンスに自動検出ルールを追加します。またリソース ID を選択し、[自動検出ルールを追加] を選択することで、[インベントリ検索] ペインからも追加できます。

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. 左のナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. セルフマネージドライセンスの名前を選択し、ライセンスの詳細ページを開きます。
4. 検出ルールの自動化] タブで、[自動検出ルールの追加を選択します。
5. 検出して追跡する製品を指定します。

Note

Amazon RDS データベース製品 (Amazon Word for Oracle や Amazon RDS RDS for Db2 など) には、次の制限が適用されます。

- Amazon RDS データベース製品を指定する最大 1 つのルールがサポートされていません。

- Amazon RDS データベース製品ごとに許可されるライセンス設定は 1 つだけです。

6. (オプション) [ソフトウェアがアンインストールされたときにインスタンスの追跡を停止する]を選択します。License Manager がソフトウェアがアンインストールされ、ライセンスのアフィニティ期間が経過したことを検出した後、ライセンスを再利用できるようにする。
7. (オプション) 自動検出から除外するリソースを定義するには、除外ルールの追加を選択します。

Note

- 除外ルールは、RDS データベース製品 (Amazon RDS for Oracle や Amazon RDS for Db2 など) には適用されません。
- 除外ルールは [クロスアカウントリソース検出](#) が有効になっている場合にのみ使用できます。

- a. フィルタリングしたいプロパティを選択してください。現在アカウントID、およびのタグがサポートされています。
 - b. そのプロパティを識別するための情報を入力します。アカウント ID には、値として 12 桁の AWS アカウント ID を指定します。タグにはキーバリューのペアを入力します。
 - c. ステップ 7 を繰り返して、ルールを追加します。
8. 完了したら [追加] を選択し自動検出ルールを適用します。

ライセンスマネージャーで付与されたライセンス

付与されたライセンスは、組織が から購入した製品のライセンスです。 [AWS Marketplace](#)、[AWS Data Exchange](#)、またはソフトウェアをマネージドエンタイトルメントと統合した販売者から直接。ライセンス管理者が使用できる AWS License Manager これらのライセンスの使用を管理し、使用権限と呼ばれる使用権限を特定の に配布するには AWS アカウント。

に配布されるデータライセンス AWS Data Exchange 製品は、 で利用できます。 AWS を通じてアカウント AWS データ交換。 からライセンスを配布する前に AWS Marketplace、サブスクリプション共有を有効にする必要があります。詳細については、 [組織でサブスクリプションを共有する](#) を参照してください。

ライセンス管理者が からエンタイトルメントを配布した後 AWS Marketplace へのライセンス AWS アカウント、受信者が付与されたライセンスを受け入れてアクティブ化すると、サブスクリプションは で利用できます。AWS を通じて アカウント AWS Marketplace。アカウントは製品にもアクセスできます。例えば、ライセンス管理者が から Amazon マシンイメージ (AMI) を購入した場合 AWS Marketplace エンタイトルメントを に配布します。AWS アカウントでは、AMIを使用して から Amazon EC2インスタンスを起動できます。AWS Marketplace および Amazon EC2。

トピック

- [付与されたライセンスを表示する](#)
- [License Manager で付与されたライセンスを管理する](#)
- [License Manager の使用権限を配布する](#)
- [License Manager での許可の承諾とアクティベーション](#)
- [License Manager での許可のライセンスステータス](#)
- [CloudWatch License Manager の購入者アカウントの メトリクス](#)

付与されたライセンスを表示する

License Manager には、認証された権限に基づいて付与されたライセンスを表示および管理するためのタブが表示されます。付与されたライセンスページには以下のタブが表示されます。

マイライセンス

このタブは、License Manager で付与されたライセンスを表示するアクセス権を持つすべてのユーザーが利用できます。このタブには、[ライセンス ID] や [製品名] など、各ライセンスに関する情報が含まれる [自分の付与されたライセンス] セクションがあります。このページでは、各ライセンスに関する追加情報を表示できます。

ライセンスの概要 (組織管理者用)

このタブは組織管理者のみが使用できます。このタブには [合計] セクションがあり、組織内のすべてのアカウントの製品と付与されたライセンスの合計数が表示されます。また、[製品] セクションには、[製品名] や [付与されたライセンスの数] など、各製品のプロパティの詳細を示す表が含まれています。

集約されたライセンス (組織管理者用)

このタブは組織管理者のみが使用できます。このタブには、[ライセンス ID] や [製品名] などの各ライセンスに関する情報が含まれる、[組織に付与されたライセンス] セクションがあります。このページでは、各ライセンスに関する追加情報を表示できます。

License Manager で付与されたライセンスを管理する

付与されたライセンスは、License Manager コンソールに表示されます。受信者は、製品を使用する前に、付与されたライセンスを承諾してアクティベートする必要があります。ライセンスの受け入れとアクティベーションの方法は、ライセンスの発行元かどうかによって異なります。AWS Marketplace アカウントが の組織のメンバーアカウントである場合、AWS Organizations、および組織ですべての機能が有効になっているかどうか。

付与されたライセンスは、ライセンスのメタデータをリージョン間でレプリケーションする必要があります。License Manager は、付与された各ライセンスとその関連情報を他のリージョンに自動的にレプリケートします。AWS リージョン。これにより、ライセンスが付与されているすべてのリージョンを一元的に表示できます。

からのライセンス AWS Marketplace また、AWS Data Exchange

- お客様が購入したサブスクリプションのライセンスは自動的に受け入れられ、アクティブになります。
- もしすべての機能が有効な組織の管理アカウントが、サブスクリプションを購入し、ライセンスをメンバーアカウントに配布すると、ライセンスはメンバーアカウントで自動的に受け入れられます。管理アカウントまたはメンバーアカウントは、後でライセンスをアクティベートできます。
- もし一括請求機能のみ有効な組織の管理アカウントで、サブスクリプションを購入し、ライセンスをメンバーアカウントに配布する場合は、各メンバーアカウントがライセンスを承諾してアクティベートする必要があります。

販売者からのライセンス

- お客様は、License Manager を使用してライセンスを配布する製品のライセンスを承諾してアクティベートする必要があります。
- もしすべての機能が有効になっている組織の管理アカウントが製品を購入し、メンバーアカウントにライセンスを配布すると、そのライセンスはメンバーアカウントで自動的に受け入れられます。管理アカウントまたはメンバーアカウントは、後でライセンスをアクティベートできます。
- もし一括請求機能のみが有効な組織の管理アカウントが、製品を購入し、メンバーアカウントにライセンスを配布する場合は、各メンバーアカウントがそのライセンスを承諾してアクティベートする必要があります。

Console (My licenses)

1 つの について付与されたライセンスを表示および管理できます。AWS アカウント。

アカウントで付与されたライセンスを管理するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、[Granted licenses] (付与されたライセンス)を選択します。
3. 現在選択されていない場合は、[マイライセンス] タブを選択します。
4. (オプション) フィルターオプションを使用して、次のような表示されるライセンスのリストを調べます。
 - 製品 SKU – ライセンスの作成時にライセンス発行者が定義した、このライセンスの製品識別子。同じ製品が複数の に存在するSKU可能性がありますISVs。
 - 受信者 – ライセンス受信者ARNの 。
 - ステータス – ライセンスのステータス。例えば、使用可能。
5. ライセンスに関する追加情報を表示するには、ライセンス ID を選択して [ライセンスの概要] ページを開きます。
6. ライセンス発行者が 以外のエンティティである場合 AWS Marketplaceの場合、最初の許可ステータスは承認保留中 です。次のいずれかを行います。
 - [Accept & activate license(ライセンスの承認とライセンス有効化)]を選択します。その結果権限ステータスは[Active(アクティブ)] になります。
 - [Accept license(ライセンスの承認)]を選択します その結果権限ステータスは[Disabled](無効)になります。ライセンスを使用する準備ができたなら、[Activate license](ライセンスの有効化)を選択します。
 - [Reject license](ライセンスの拒否)を選択します。結果として権限ステータスは[Rejected] (拒否)となります。ライセンスを拒否した後は、ライセンスをアクティブできません。

アクティブ化されたライセンスを引き続き使用したくない場合は、[ライセンスの概要] ページに戻って [ライセンスを非アクティブ化] を選択できます。非アクティブ化されたライセンスを引き続き使用する場合は、[ライセンスの概要] ページに戻り、[ライセンスをアクティブ化] を選択します。

Console (Aggregated licenses)

組織内のすべてのアカウントに付与されたライセンスを集計して表示できます。

Important

付与されたライセンスに組織全体ビューを使用するには、まずリンクする必要があります。AWS Organizations の使用 AWS License Manager コンソールの設定。詳細については、「[License Managerの設定](#)」を参照してください。

でアカウント全体で付与されたライセンスを管理するには AWS Organizations

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、[Granted licenses] (付与されたライセンス)を選択します。
3. 現在選択されていない場合は、[集約されたライセンス] タブを選択します。
4. (オプション) フィルターオプションを使用して、次のような表示されるライセンスのリストを調べます。
 - 製品 SKU – ライセンスの作成時にライセンス発行者が定義した、このライセンスの製品識別子。同じ製品が複数のに存在するSKU可能性がありますISVs。
 - 受益者 - ライセンスが付与されている組織内のアカウント。
5. ライセンスに関する追加情報を表示するには、ライセンスID を選択してライセンスの詳細ページを開きます。
6. ライセンス発行者が 以外のエンティティである場合 AWS Marketplace、次のいずれかを実行します。
 - [ライセンスをアクティブ化] を選択します。その結果権限ステータスは[Active(アクティブ)]になります。
 - [ライセンスを非アクティブ化] を選択します。その結果権限ステータスは [非アクティブ]になります。

アクティブ化されたライセンスを引き続き使用したくない場合は、[ライセンスの概要] ページに戻って [ライセンスを非アクティブ化] を選択できます。非アクティブ化されたライセンスを引き続き使用する場合は、[ライセンスの概要] ページに戻り、[ライセンスをアクティブ化] を選択します。

AWS CLI

を使用できます。AWS CLI は、付与されたライセンスと連携します。

を使用して付与されたライセンスを管理するには 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](#)

License Manager の使用権限を配布する

[すべての機能](#)が有効な組織の管理アカウントでライセンス管理者が操作している場合は、権限を作成することで、付与されたライセンスから組織に使用権限を配布することができます。の詳細については、「」を参照してください。AWS Organizations、「」を参照してください。[AWS Organizations の用語と概念](#)。

権限の受信者を以下のいずれかとして指定できます。

- An AWS アカウント。指定されたアカウントのみが含まれます。
- 組織ルート。組織全体のすべてのアカウントが含まれます。
- 組織単位 (OU) (ネストされていない)。指定した OU と指定した OU のネスト OUs された のすべてのアカウントが含まれます。

Note

1つのライセンスにつき最大2,000個の権限を作成できます。

次のいずれかを使用できます。AWS License Manager コンソールまたは AWS CLI エンタイトルメントを配布する。コンソールで権限を作成するARNときに組織 ID または組織を指定できますが、ARN 形式ではを使用する必要があります。AWS CLI。例えば、ARNsは次のようになります。

組織 ID 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

権限を作成するには (コンソール)

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、[Granted licenses] (付与されたライセンス)を選択します。
3. ライセンス ID を選択して、[ライセンスの概要] ページを開きます。
4. [Grants(権限)]セクションから[Create grant(権限の作成)]を選択します。
5. [Grant details(権限の詳細)]パネルで以下を行います。
 - a. 権限の目的または受信者を特定できるように権限の名前を入力します。
 - b. を入力します。AWS アカウント ID、AWS Organizations OU ID または ARN、または AWS Organizations グラント受信者ARNの ID または。
 - c. [Create grant(権限の作成)]を選択します。
6. [ライセンスの概要] ページの [権限] パネルに権限のエントリが表示されます。権限の初期ステータスは[Pending acceptance(承認保留)] です。受信者が権限を受諾したとき、または受取人が権限を[Rejected(拒否)]したとき、ステータスが [Active(アクティブ)] に変わります。

AWS CLI

を使用できます。AWS CLI エンタイトルメントを配布する。を使用するときは、ARN形式で組織 ID または OU を指定する必要があります。AWS License Manager API.

を使用して許可を作成して一覧表示するには AWS CLI:

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

権限の詳細ページには、エンタイトルメントへのアクセスを権限をつけたアカウントのリストが表示されます。組織にライセンスを配布した後、各アカウントで個別にライセンスを非アクティブ化またはアクティブ化することができます。

License Manager での許可の承諾とアクティベーション

付与されたライセンスに対して権限が作成されると、その権限は受信者に配布されます。権限の受信者が付与されたライセンスを使用するには、ライセンスが承諾され、アクティブになる必要があります。付与アクティベーションプロセスには、 から取得した付与されたライセンスの追加オプションを含めることができます。 AWS Marketplace.

デフォルトでは、付与されたライセンスの [許可の概要] ページのステータスは Pending Acceptance です。許可を [Accept]、[Accept and Activate]、または [Reject] することを選択できます。承認されているが、まだアクティブになっていない権限のステータスは Disabled です。承認済みおよび有効化された権限のステータスは Active です。

権限の受信者が付与されたライセンスを使用するには、ライセンスが承諾され、アクティブになる必要があります。デフォルトでは、付与されたライセンスの権限詳細ページのステータスは [Pending acceptance(承認保留)] となっています。ライセンスを [Accept(承認)]、承認してアクティベート、または 拒否のいずれかを選択することができます。承認されているが、まだアクティブになっていない権限のステータスは無効です。承認済みおよび有効化された権限のステータスはアクティブです。

Tip

組織の管理アカウントからの権限を自動的に承認することができます。グラントの自動承認を有効にするには、 [の設定](#) ページで組織アカウントをリンクします。 AWS License Manager 管理アカウントの コンソール。

から同じ製品に対して 2 つのライセンスをアクティブ化することはできません AWS Marketplace 同時に。 2 つのサブスクリプション (例えば、製品のパブリックオファーとプライベートオファー、製品のサブスクリプションライセンスと同製品の付与されたライセンス) がある場合は、以下のいずれかのアクションを実行できます。

1. 同じ製品に対する既存の権限を無効にしてから、新しい権限を有効化します。
2. 新しい権限を有効化し、既存の有効な権限を無効化して新しい権限に置き換えることを指定します。License Manager コンソールまたは を使用できます。AWS CLI:
 - a. License Manager コンソールを使用して、新しい権限を有効化し、置き換えたい有効な権限の [はい] を選択します。
 - b. を使用してAPI、 に `CreateGrantVersion` を `ALL_GRANTS_PERMITTED_BY_ISSUERActivationOverrideBehavior` で指定して、新しい許可をアクティブ化します `StatusActive`。

Console

License Manager コンソールを使用して、権限を有効化することができます。から取得したグラントをアクティブ化する場合 AWS Marketplace、アクティブな権限を置き換えるかどうかのオプションが表示される場合があります。

- ライセンス管理者は、権限を有効化するときには有効な権限を置き換えるかどうかを指定する必要があります。
- 付与者は、組織内の別のアカウントの権限を有効化するときには、有効な権限を置き換えるかどうかを任意で指定できます。
- 被付与者は、配布された権限を作成した付与者が有効な権限を置き換えるかどうかを指定していない場合、権限を有効化するときには選択する必要があります。

権限を有効化するには (コンソール)

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、[Granted licenses] (付与されたライセンス) を選択します。
3. ライセンス ID を選択して、[ライセンスの概要] ページを開きます。
4. 権限名を選択し、[許可の概要] ページを開きます。
5. 表示されたら、有効な権限を置き換えるかどうかの有効化オプションを選択します。
 - a. いいえ — このオプションは、受信者 (被付与者) の既存の有効な権限を置き換えることなく、権限を有効にします。

- b. はい — このオプションは、同じ製品に対する権限を無効化し、以下の定義された受信者 (被付与者) の新しい権限を有効化します。
 - i. 指定された AWS アカウント。
 - ii. 指定された組織 OU のメンバーアカウント。
 - iii. 組織のすべてのメンバーアカウント。
6. (オプション) 権限を有効化する理由を入力します。
 7. 入力ボックスに **activate** と入力し、[有効化] を選択します。

AWS CLI

を使用できます。AWS CLI は、付与されたライセンスと連携します。

を使用して分散グラントを操作するには AWS CLI:

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

License Manager での許可のライセンスステータス

ライセンスには 2 つのステータスがあります。ライセンスの全体的な可用性と共有性を示すライセンスステータスとライセンスの使用能力を示す権限ステータスです。

次の表に、付与されたライセンスの各ステータスを示します。

ステータス	説明
AVAILABLE	このライセンスは、使用および共有が可能です。
PENDING_AVAILABLE	このライセンスは、まだ処理中のため使用できません。

ステータス	説明
DEACTIVATED	ライセンス発行者によってライセンスが無効化されているため、使用できません。
SUSPENDED	ライセンスは一時停止されているため、使用できません。
EXPIRED	ライセンスは、期限切れのため、使用できません。
PENDING_DELETE	ライセンスは削除中のため使用できません。
DELETED	ライセンス契約がキャンセルされているため、ライセンスは使用できません。

次の表に、権限の各ステータスを示します。

ステータス	説明
PENDING_WORKFLOW	権限は配布中です。
PENDING_ACCEPT	権限が作成されましたが、権限の被付与者がまだ承諾していません。
REJECTED	権限の被付与者によって権限が拒否されました。
ACTIVE	権限が被付与者によって承諾され、使用がアクティブになりました。承諾されたリソースを使用することができます。
FAILED_WORKFLOW	権限の配布に失敗しました。
DELETED	権限が付与者によって削除されました。
PENDING_DELETE	配布された権限は削除中です。

ステータス	説明
DISABLED	権限は権限の被付与者によって承諾されましたが、使用がアクティブになっていません。
WORKFLOW_COMPLETE	組織への権限が配布されたか、リコールされました。権限詳細では、組織内の各アカウントに対する権限付与のステータスが表示されます。

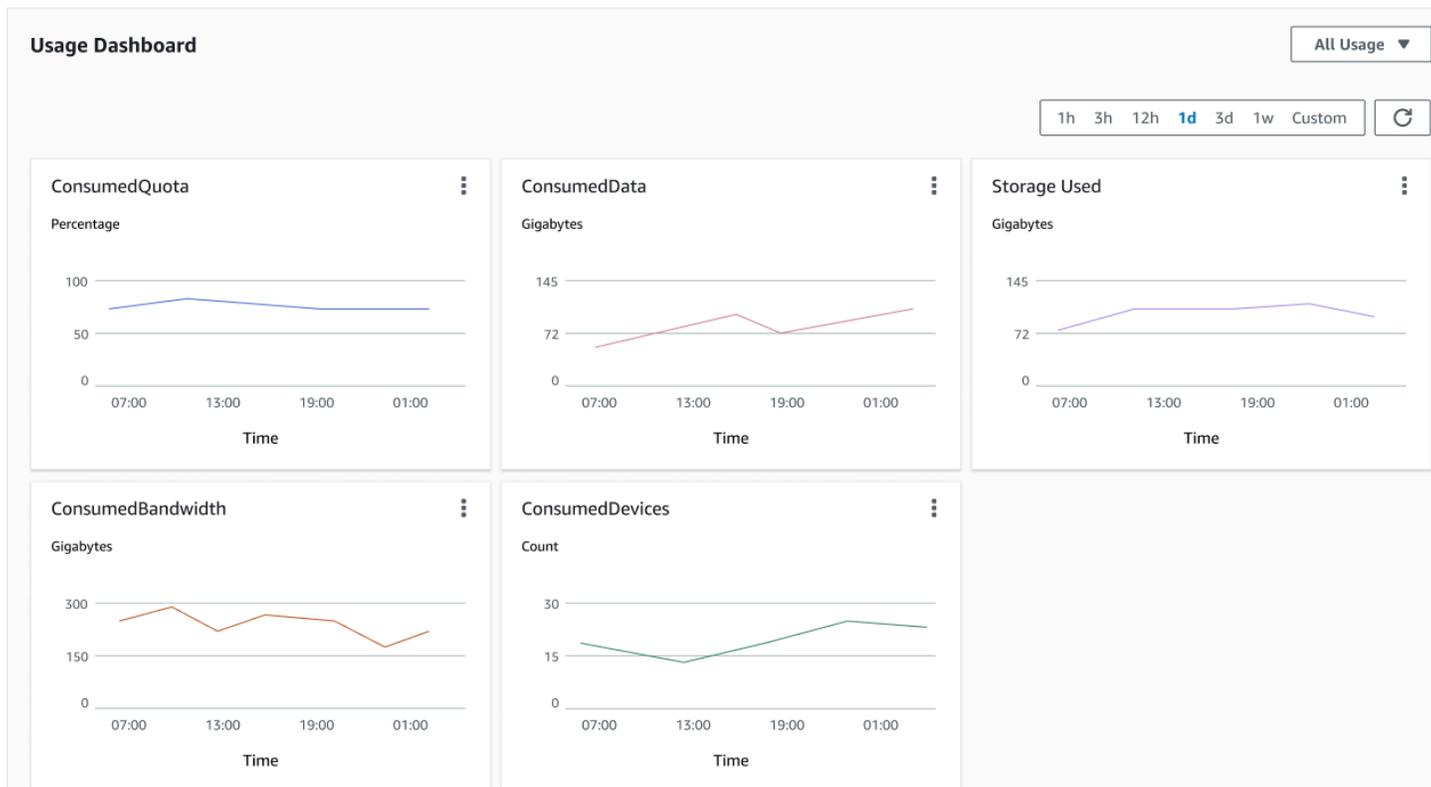
CloudWatch License Manager の購入者アカウントの メトリクス

販売者が発行したライセンスの付与が、選択した使用状況レコードの送信を許可するように設定されている場合、License Manager は、販売者アカウント、ルート購入者アカウント、および使用状況が記録されているアカウントに CloudWatch メトリクスを出力します。購入者アカウントは AWS アカウント 販売者が発行したライセンスを購入または付与されたユーザー。詳細については、「[顧客へのライセンスの付与](#)」を参照してください。

使用状況ダッシュボード

販売者または独立系ソフトウェアベンダー (ISV) アプリケーションが購入者アカウントのライセンスに対する使用状況を記録すると、使用状況が記録されているアカウントとルート購入者アカウントには、License Manager コンソールの使用状況ダッシュボードページに使用状況レコードを含む CloudWatch ウィジェットが表示されます。購入者は、ライセンスを配布したアカウントのメトリクスを確認することもできます。AWS Organizations。使用状況ダッシュボードページのグラフは、使用状況レコードが送信されたすべてのライセンスで使用できます。

以下の画像は、使用状況ダッシュボードの例です。



License Manager で販売者が発行したライセンス

独立系ソフトウェアベンダー (ISVs) が使用できる AWS License Manager は、ソフトウェアライセンスを管理してエンドユーザーに配布します。発行者は、License Manager ダッシュボードを使用して、発行したライセンスの使用状況を一元的に追跡できます。

License Manager は、オープンで安全な業界標準を使用してライセンスを表現し、お客様が信頼性を暗号化して検証することができます。License Manager は、各ライセンスを非対称キーに関連付けます。として ISV、非対称を所有している AWS KMS キーをアカウントに保存します。

販売者が発行したライセンスには、ライセンスメタデータのクロスリージョンレプリケーションが必要です。License Manager は、販売者が発行したライセンスとその関連情報を他のリージョンに自動的に複製します。

License Manager では、次のようなさまざまなライセンスモデルがサポートされています。

- Perpetual - ユーザーがソフトウェアを無期限に使用することができる有効期限のないライフタイムライセンス。
- Floating - アプリケーションの複数のインスタンスで共有可能なライセンス。ライセンスは前払いでき、固定の一連のエンタイトルメントを追加できます。

- Subscription - 有効期限のあるライセンスで、特に無効化されていない限り自動的に更新されます。
- 使用状況ベース – APIリクエスト数、トランザクション数、ストレージ機能など、使用状況に基づく特定の条件を持つライセンス。

License Manager でライセンスを作成し、 を使用して顧客に配布できます。 AWS IAM License Manager によって生成された ID またはベアトークン。 ISV を使用する のお客様 AWS アカウントはライセンス権限を に再配布できます。 AWS それぞれの組織の ID。 配布されたエンタイトルメントを持つお客様は、ソフトウェアとLicense Manegerを統合することで、そのライセンスから必要なエンタイトルメントをチェックアウトしたり、チェックインしたりすることができます。

License Manager で販売者が発行したライセンス使用権限

License Manager は、販売者が発行したライセンス機能をライセンスのエンタイトルメントとしてキャプチャします。エンタイトルメントは、限定または無制限の数量で特徴付けられます。制限されたエンタイトルメントの例は、'40GB のデータ転送'です。数量制限のエンタイトルメントの例は、'Platinum Tier'です。

ライセンスには、付与されたすべてのエンタイトルメント、アクティベーションと有効期限、および発行者の詳細が含まれます ライセンスはバージョン管理されたエンティティであり、各バージョンはイミュータブルです。ライセンスバージョンは、ライセンスが変更されるたびに更新されます。

制限された使用権限をチェックアウトまたはチェックインするには、ISVアプリケーションは制限された各容量の量を指定する必要があります。無制限の使用権限については、ISVアプリケーションは、チェックアウトまたは再チェックインする関連する使用権限を指定するだけです。最後に、制限付き機能では、“オーバーエイジフラグ”もサポートしています。これは、エンドユーザーが最初のエンタイトルメントの使用量を越えることができるかどうかを示すものです。License Manager は、使用状況と超過を に追跡してレポートしますISV。

License Manager で販売者が発行したライセンスの使用

License Manegerでは、チェックアウトされたすべてのエンタイトルメントの数を維持することで、複数のリージョンにわたってライセンスを一元的に追跡できます。また、License Manegerは、各チェックアウトに関連するユーザーのアイデンティティと基礎となるリソース識別子 (使用可能な場合) を、チェックアウトされた日時とともに追跡します。この時系列データは、CloudWatch イベントを通じて追跡できます。

ライセンスは、次に示す状態のいずれかになります。

- Created - ライセンスが作成されます。
- Updated - ライセンスが更新されます。
- Deactivated - ライセンスは非アクティブ化されます。
- Deleted - ライセンスが削除されます。

License Manager で販売者が発行したライセンス使用状況を追跡するために必要なアクセス許可

この機能を使用するには、次の License Manager API アクションを呼び出すアクセス許可が必要です。

```
{
  "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": "*"
    }
  ]
}
```

License Manager と統合して、 を使用しない顧客 AWS アカウントは、 の外部で販売されたライセンスを消費できます。AWS Marketplaceでは、ソフトウェアアプリケーションが License Manager を呼び出せるようにする IAMロールを作成する必要がありますAPI。

を使用する場合 AWS Management Console を使用して、 を使用せずにお客様の一時的な認証情報を配布する AWS アカウント、License Manager はAWSLicenseManagerConsumptionRoleユーザーに代わって を自動的に作成します。詳細については、「[を使用しないISVお客様の一時的な認証情報を取得する AWS アカウント](#)」を参照してください。からこのロールを作成するには AWS CLI、 を使用します。AWS IAM 次の例に示すように、[create-role](#) コマンドを使用します。

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

提供されたtrust-policy-document.jsonファイルは、次の例のようになります。AWS アカウント トークン発行者アカウントとして置き換えられた ID。

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

次に、[attach-role-policy](#) コマンドを使用して を追加します。

AWSLicenseManagerConsumptionPolicy AWS AWSLicenseManagerConsumptionRole ロールへのマネージドポリシー。

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

License Manager で販売者が発行したライセンスを作成する

を使用して顧客に付与するライセンスのブロックを作成するには、次の手順を使用します。AWS Management Console。または、[CreateLicense](#) APIアクションを使用してライセンスを作成することもできます。

コンソールを使用してライセンスを作成するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のメニューで販売者が発行したライセンスを選択します。
3. 選択ライセンスの作成を選択します。
4. ライセンスメタデータで、次の情報を入力します。
 - [ライセンス名] - 購入者に表示する名前 (最大 150 文字)。
 - [ライセンスの説明] - このライセンスを他のライセンスと区別するための、400 文字以内の任意の説明です。
 - 製品 SKU - 製品 SKU。
 - [受取人] - 受取人の名前 (会社または個人)。
 - ホームリージョン - 。AWS ライセンスのリージョン。ライセンスはグローバルに使用できますが、ホームリージョンでのみライセンスを変更できます。ライセンスの作成後にライセンスのホームリージョンを変更することはできません。
 - [ライセンス開始日] - アクティベーションの日付。
 - [ライセンス終了日] - ライセンスの終了日 (該当する場合)。
5. [消費設定] では、以下の情報を指定します。
 - [更新頻度] - 毎週、毎月、またはまったく更新しないかどうか。
 - [消費量設定] - ライセンスを継続的接続に使用する場合は [暫定消費の設定オプション]、オフラインで使用する場合は [借用] を選択します。ライセンスの有効期限を設定するには、Max time to live (minutes) と入力します。
6. [発行者] に、次の情報を入力します。

- を入力する AWS KMS キー – License Manager はこのキーを使用して発行者に署名と検証を行います。詳細については、「[License Manager でのライセンスの暗号化署名](#)」を参照してください。
 - [発行者名] - 販売者の会社名。
 - [販売者レコード] - オプションのビジネス名。
 - 契約 URL – ライセンス契約URLの。
7. Entitlementには、ライセンスが受信者に付与する機能について、次の情報を提供します。
- [名前] - 受取人の名前。
 - [ユニットタイプ] - ユニットタイプを選択し、最大数を指定します。
 - チェック 受信者が更新前にライセンスをチェックインする必要がある場合チェックインを許可します。
 - チェック 受信者が最大数を超過してリソースを使用できる場合には、超過が許可されます。このオプションでは、受信者に追加料金が発生する可能性があります。
8. ライセンスの作成を選択します。

License Manager 販売者が発行したライセンスをISV顧客に付与する

新しいライセンスを追加したら、を使用して顧客にライセンスを付与できます。AWS を使用するアカウント AWS Management Console。受信者は、ライセンスを使用する前に許可を受け入れる必要があります。詳細については、「[ライセンスマネージャーで付与されたライセンス](#)」を参照してください。

または、顧客がを持っていない場合 AWS アカウントでは、License Manager を使用してAPI、お客様が[ライセンスを使用](#)できるようにします。

コンソールを使用してお客様にライセンスを付与するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のメニューで販売者が発行したライセンスを選択します。
3. ライセンスのIDを選択して、詳細ページを開きます。
4. Grantsでは、Create grantを選択します。
5. [Grantの詳細] については、以下の情報を提供してください。
 - [グラント名] - グラント名。これは、検索機能を有効にするために使用されます。

- AWS アカウント ID –。AWS ライセンス受取人の アカウント番号。
 - [ライセンス権]
 - 受信者が付与されたエンタイトルメントを利用できる場合は、[消費] を選択します。
 - 受信者が付与された使用権限を他の に配布できる場合は、Distribution を選択します。AWS アカウント。
 - 選択 オンプレミストークンの生成に を使用せずに共有ライセンスを認証することを許可する AWS ID または認証情報。
 - ライセンス受信者が使用タイプ別の使用記録を発行できるようにするには、[使用記録の提出を許可] を選択します。
 - ホームリージョン –。AWS リージョン ライセンスの。
6. [Create grant(権限の作成)]を選択します。

を使用しないISVお客様の一時的な認証情報を取得する AWS アカウント

を使用しないお客様向け AWS アカウントでは、 を使用して顧客に対して行うのと同じ方法でエンタイトルメントを使用できます。AWS アカウント。一時的な を取得するには、次の手順を使用します。AWS を使用しないお客様の 認証情報 AWS アカウント。API 呼び出しはホームリージョンで行う必要があります。

License Manager の呼び出しに使用する一時的な認証情報を取得するには API

1. [CreateToken](#) API アクションを呼び出して、トークンとしてエンコードされた更新JWTトークンを取得します。
2. 前のステップCreateTokenで から受け取った更新トークンを指定して [GetAccessToken](#)API アクションを呼び出し、一時的なアクセストークンを受け取ります。
3. [AssumeRoleWithWebIdentity](#) API アクションを呼び出し、前のステップGetAccessTokenで から受け取ったアクセストークンと作成したAWSLicenseManagerConsumptionRoleロールを指定して、一時的な を取得します。AWS 認証情報。

からトークンを作成するには AWS License Manager コンソール

1. [License Manager コンソール から](#)、 を使用せずに使用する特定のライセンス使用権限のライセンス詳細ページに移動します。AWS アカウント。
2. トークンの作成を選択して一時アクセストークンを生成します。

Note

一時的なアクセストークンを初めて生成するときには、License Managerがお客様に代わってサービスにアクセスできるように、サービス ロールを作成するように求められます。次のサービスロールが作成されます。AWSLicenseManagerConsumptionRole。

3. token.csvファイルのダウンロード、または生成時にトークン文字列をコピーします。

Important

これは、このトークンを閲覧、ダウンロードできるのはこの時だけです。トークンをダウンロードし、安全な場所に保存することをお勧めします。[サービスの上限](#)まで新しいトークンはいつでも作成できます。

License Manager で販売者が発行したライセンスを確認する

License Managerを使用すると、複数のユーザーが単一のライセンスから限られた機能でエンタイトルメントを同時に使用できます。[CheckoutLicense](#) API アクションを呼び出します。パラメータの説明は以下の通りです。

- [キーフィンガープリント] - 信頼できるライセンス発行者。

例:aws: 123456789012: 発行者:issuer-fingerprint

- 製品 SKU – ライセンスの作成時にライセンス発行者が定義した、このライセンスの製品識別子。同じ製品が複数の に存在するSKU可能性がありますISVs。そのため、信頼できるキー・フィンガープリントが重要な役割を果たします。

例: 1a2b3c4d2f5e69f440bae30eaec9570bb1fb7358824f9ddfa1aa5a0daEXAMPLE

- [エンタイトルメント] - チェックアウトする機能。無制限のケイパビリティを指定した場合、数量はゼロとなります。例:

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

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

- 受益者 – Software as a Service (SaaS) ISVsは、顧客 ID を含めることで、顧客に代わってライセンスをチェックアウトできます。License Manager は、SaaS ISVアカウントで作成されたライセンスのリポジトリへの呼び出しを制限します。

例:user@domain.com

- [ノード ID] - アプリケーションの単一のインスタンスにライセンスをノードロックするための識別子。

例:10.0.21.57

License Manager で販売者が発行したライセンスを削除する

ライセンスを削除したら、再作成することができます。ライセンスとそのデータは6ヶ月間保持され、ライセンス発行者とライセンス付与者は読み取り専用モードで利用できます。

を使用して作成したライセンスを削除するには、次の手順に従います。AWS Management Console。または、[DeleteLicense](#) APIアクションを使用してライセンスを削除することもできます。

コンソールからライセンスを削除するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のメニューで販売者がライセンスを発行を選択します。
3. ライセンスの横にあるラジオボタンを選択して、削除するライセンスを選択します。
4. [削除] を選択します。確認を求められたら、「delete」を入力し、[削除] を選択します。

サポートされているソフトウェア製品の License Manager ユーザーベースのサブスクリプションを使用する

のユーザーベースのサブスクリプションでは AWS License Manager、完全準拠のライセンスソフトウェアサブスクリプションを購入できます。ライセンスは Amazon から提供され、ユーザーごとの

サブスクリプション料金がかかります。Amazon EC2は、サポートされているソフトウェアと共に、事前設定された Amazon マシンイメージ (AMIs) と、ライセンス込みの Windows Server ライセンスを提供します。これらのライセンスは長期間のライセンス契約なしで使用できます。

ユーザーベースのサブスクリプションを使用するには、[AWS Directory Service for Microsoft Active Directory](#) (AWS Managed Microsoft AD) またはセルフマネージド (オンプレミス) ドメインのユーザーを、ソフトウェアを提供するEC2インスタンスに関連付けます。ライセンスされたソフトウェアを利用できるようにするには、ユーザーベースのサブスクリプションを作成し、事前設定されたから起動されたインスタンスに関連付ける必要がありますAMIs。[AWS Systems Manager](#)は、起動するライセンス込みインスタンスを設定して強化します。ユーザーはリモートデスクトップソフトウェアに接続して、ソフトウェアを提供するインスタンスにアクセスする必要があります。

ライセンス込みインスタンスに関連する各ユーザーと [vCPU](#) には料金が発生します。Amazon EC2 リザーブドインスタンスと Savings Plan の料金モデルは、Amazon EC2コストの最適化に役立ちます。詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「[リザーブドインスタンス](#)」を参照してください。ユーザーベースのサブスクリプションは、月の前半から月末までに請求されます。

トピック

- [License Manager でユーザーベースのサブスクリプションを使用する際の考慮事項](#)
- [License Manager でユーザーベースのサブスクリプションを作成するための前提条件](#)
- [License Manager のユーザーベースのサブスクリプションでサポートされているソフトウェア製品](#)
- [その他のソフトウェア](#)
- [License Manager でユーザーベースのサブスクリプションを開始する](#)
- [よりアクティブなリモートユーザーセッションGPO用に Active Directory を設定する](#)
- [含まれているライセンスからインスタンスを起動する AMI](#)
- [を使用してユーザーベースのサブスクリプションインスタンスに接続する RDP](#)
- [Microsoft Office サブスクリプションのファイアウォール設定を変更する](#)
- [License Manager ユーザーベースのサブスクリプションのサブスクリプションユーザーを管理する](#)
- [License Manager の設定から Active Directory の登録を解除する](#)
- [License Manager でのユーザーベースのサブスクリプションのトラブルシューティング](#)

License Manager でユーザーベースのサブスクリプションを使用する際の考慮事項

License Manager でユーザーベースのサブスクリプションを使用する場合、次の考慮事項が適用されます。

- ライセンス込みの Microsoft リモートデスクトップサービス (Win Remote Desktop Services SAL) の AWS Marketplace サブスクリプションには、ユーザーごとの月額料金がかかり、按分はかかりません。
- ユーザーベースのサブスクリプションを提供するインスタンスは、デフォルトで一度に最大 2 つのアクティブなユーザーセッションをサポートします。3 つ以上のアクティブなユーザーセッションを有効にするには、Active Directory グループポリシーオブジェクト (GPO) を設定し、Microsoft RDSライセンスモードを `Per User` に設定します。詳細については、「」の前提条件を参照してください。[よりアクティブなリモートユーザーセッションGPO用に Active Directory を設定する](#)。
- ユーザーベースのサブスクリプションを提供するインスタンスで管理者権限を持つローカルユーザーを作成すると、インスタンスのヘルスステータスが異常に変わる可能性があります。License Manager は、コンプライアンス違反により異常が発生したインスタンスを終了できます。詳細については、「[インスタンスのコンプライアンスに関するトラブルシューティング](#)」を参照してください。
- Microsoft Office 製品で Active Directory を設定する場合、には少なくとも 1 つのサブネットに[VPCエンドポイント](#)がプロビジョニングされているVPC必要があります。License Manager によって作成されたすべてのVPCエンドポイントリソースを削除する場合は、License Manager の設定から設定された Active Directory を削除する必要があります。詳細については、「[License Manager の設定から Active Directory の登録を解除する](#)」を参照してください。
- License Manager によってインスタンスに割り当てられた、値 `UserSubscriptions` を持つ `AWSLicenseManager` のタグキーは変更または削除しないでください。
- サービスが期待どおりに機能するためには、License Manager 用に作成された 2 つのネットワークインターフェイスを変更または削除しないでください。
- License Manager が AWS Managed Microsoft AD ディレクトリのAWS リザーブド組織単位 (OU) で作成するオブジェクトは、変更または削除しないでください。
- ユーザーベースのサブスクリプション用にデプロイされたインスタンスは、AWS Systems Manager によるマネージドノードであり、同じドメインに属する必要があります。Systems Manager によるインスタンスの継続的な管理については、このガイドの「[License Manager でのユーザーベースのサブスクリプションのトラブルシューティング](#)」セクションを参照してください。

- ユーザーのサブスクリプション料金の発生を停止するには、関連付けられているすべてのインスタンスからユーザーの関連付けを解除する必要があります。詳細については、「[ユーザーベースのサブスクリプションを提供するインスタンスからユーザーの関連付けを解除する](#)」を参照してください。

License Manager でユーザーベースのサブスクリプションを作成するための前提条件

ユーザーベースのサブスクリプションを作成する前に、以下の前提条件をご使用の環境に実装する必要があります。

目次

- [IAM ロールとアクセス許可](#)
 - [AWS KMS License Server 認証情報のキーポリシー](#)
- [アクティブディレクトリ](#)
- [セキュリティグループ](#)
- [ネットワーク構成](#)
- [ユーザーベースのサブスクリプション製品を提供するインスタンス](#)
- [Microsoft リモートデスクトップサービス](#)
 - [管理認証情報シークレット](#)

IAM ロールとアクセス許可

AWS アカウント をユーザーベースのサブスクリプションにオンボードするには、License Manager がサービスリンクロールを作成できるようにする必要があります。License Manager コンソールで、ロールがまだ作成されていない場合は、ユーザーベースのサブスクリプションにプロンプトが表示されます。プロンプトに回答し、License Manager がロールを作成することを許可することに同意したら、作成を選択して続行します。詳細については、「[License Manager のサービスにリンクされたロールの使用](#)」を参照してください。

- ユーザーベースのサブスクリプションを作成するには、ユーザーまたはロールに次のアクセス許可が必要です。
 - `ec2:CreateNetworkInterface`
 - `ec2>DeleteNetworkInterface`

- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSubnets`
- `ds:DescribeDirectories`
- `ds:AuthorizeApplication`
- `ds:UnauthorizeApplication`
- `ds:GetAuthorizedApplicationDetails`
- `ds:DescribeDomainControllers`
- Microsoft Office 製品のユーザーベースのサブスクリプションを作成するには、ユーザーまたはロールに次の追加のアクセス許可も必要です。
 - `ec2:CreateVpcEndpoint`
 - `ec2>DeleteVpcEndpoints`
 - `ec2:DescribeVpcEndpoints`
 - `ec2:ModifyVpcEndpoint`
 - `ec2:DescribeSecurityGroups`

AWS KMS License Server 認証情報のキーポリシー

独自のKMSキーを使用して Microsoft RDS License Server の管理認証情報シークレットを暗号化および復号するには、License Manager オペレーションへのアクセスに使用するロールにポリシーをアタッチする必要があります。次の例は、Secrets Manager がKMSキーにアクセスして Microsoft RDS License Server 認証情報シークレットを暗号化および復号するためのアクセス許可を付与するポリシーを示しています。

```
{
  "Version": "2012-10-17",
  "Id": "key-policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/RoleName"
      },
      "Action": [
        "kms:Decrypt"
      ]
    }
  ]
}
```

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

アクティブディレクトリ

License Manager ユーザーベースのサブスクリプションを使用するには、サブスクリプション製品ユーザーのユーザー情報を含む Active Directory (AD) を作成する必要があります。設定に応じて、AWS Managed Microsoft AD、またはセルフマネージド AD を使用できます。

AWS マネージドアクティブディレクトリとセルフマネージドアクティブディレクトリの両方を使用する場合は、ディレクトリ間に双方向のフォレスト信頼を確立する必要があります。詳細については、[「管理ガイド」の「チュートリアル: AWS Managed Microsoft AD とセルフマネージド Active Directory ドメインの間に信頼関係を作成する」](#)を参照してください。AWS Directory Service

Note

ディレクトリ用に設定されたサブネットはすべて、VPCで同じのものである必要があります AWS アカウント。

AWS マネージド Active Directory には以下の制限があります。

- 共有されているディレクトリはサポートされていません。
- 多要素認証はサポートされていません

ディレクトリの作成の詳細については、「AWS Directory Service ユーザーガイド AWS Managed Microsoft AD」の[AWS Managed Microsoft AD 「前提条件」](#)および[AWS Managed Microsoft AD 「ディレクトリの作成」](#)を参照してください。

ユーザーをに関連付けるには AWS Managed Microsoft AD、AWS Managed Microsoft AD ディレクトリにユーザーをプロビジョニングする必要があります。詳細については、「AWS Directory Service 管理ガイド」の[「AWS Managed Microsoft ADのユーザーとグループの管理」](#)を参照してください。

セキュリティグループ

セキュリティグループは、ネットワーク上のリソースとの間で許可されるネットワークトラフィックを制御します。ユーザーベースのサブスクリプション環境のリソースが通信できるようにするには、セキュリティグループが次の基準を満たしている必要があります。

VPC エンドポイントのセキュリティグループ

インバウンドTCPポート1688接続を許可するセキュリティグループを特定または作成します。VPC 設定を構成するときに、このセキュリティグループを指定します。詳細については、「[セキュリティグループの操作](#)」を参照してください。

License Manager は、の設定中にユーザーに代わって作成するVPCエンドポイントにこのセキュリティグループを関連付けますVPC。VPC エンドポイントの詳細については、「AWS PrivateLink ガイド」の[AWS 「インターフェイスVPCエンドポイントを使用して サービスにアクセスする」](#)を参照してください。

Active Directory ドメインコントローラーのセキュリティグループ

AD ドメインコントローラーに使用するセキュリティグループで、各ドメインコントローラーのネットワークインターフェイスIPv4アドレスへのアウトバウンドトラフィックが許可されていることを確認します。

ユーザーベースのサブスクリプションインスタンスのセキュリティグループ

インスタンスとの間で次のアクセスを許可するセキュリティグループを特定または作成します。詳細については、「[セキュリティグループの操作](#)」を参照してください。

- 承認された3389接続ソースからのインバウンドTCPポート接続。
- VPC エンドポイントに到達し、通信するためのアウトバウンドTCPポート1688接続 AWS Systems Manager。

ネットワーク構成

License Manager は、VPC AWS Managed Microsoft AD がプロビジョニングされている のデフォルトのセキュリティグループを使用する 2 つのネットワークインターフェイスを作成します。これらのインターフェイスは、サービスがディレクトリとやり取りするために使用されます。詳細については、「AWS Directory Service 管理ガイド」の「[ステップ 2: License Manager に Active Directory を登録する](#)」および「[作成される対象](#)」を参照してください。

プロビジョニングプロセスが完了したら、License Manager によって作成されたインターフェイスに別のセキュリティグループを関連付けることができます。

DNS 解像度

ユーザーベースのサブスクリプションに登録した Active Directory は、License Manager の設定で設定したすべての VPCs およびサブネットからアクセスできる必要があります。Active Directory ノードにアクセスできるようにするには、次のようにDNS解決を設定します。

- ユーザーベースのサブスクリプションの License Manager 設定で設定された VPCs と Active Directory 間のDNS転送を設定します。DNS転送には Amazon Route 53 または別の DNS サービスを使用できます。詳細については、ブログ記事「[Directory Service のDNS解像度と Amazon Route 53 Resolver の統合](#)」を参照してください。
- DNS のホスト名とDNS解決を有効にしますVPC。詳細については、「[のDNS属性の表示と更新 VPC](#)」を参照してください。

ユーザーベースのサブスクリプション製品を提供するインスタンス

ユーザーベースのサブスクリプションインスタンスを期待どおりに機能させるには、次の前提条件を満たす必要があります。

- 「」の説明に従って、インスタンスのセキュリティグループを設定します [セキュリティグループ](#)。
- Microsoft Office でユーザーベースのサブスクリプションを提供するために起動されたインスタンスに、VPCエンドポイントがプロビジョニングされるサブネットへのルートがあることを確認します。
- ユーザーベースのサブスクリプションを提供するインスタンスは、正常なステータスを得るために AWS Systems Manager によって管理される必要があります。さらに、インスタンスは、ライセンスのアクティベーション後もコンプライアンスを維持するために、ユーザーベースのサブスクリプションライセンスをアクティブ化できる必要があります。

Note

License Manager は異常のあるインスタンスの復旧を試みますが、正常な状態に戻すことができないインスタンスは終了されます。Systems Manager によるインスタンスの継続的な管理とインスタンスのコンプライアンスに関するトラブルシューティング情報については、このガイドの「[License Manager でのユーザーベースのサブスクリプションのトラブルシューティング](#)」セクションを参照してください。

- ユーザーベースのサブスクリプション製品を提供するインスタンスには、インスタンスプロファイルロールをアタッチする必要があり、これによって AWS Systems Manager によるリソースの管理が可能になります。詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。
- インスタンスを終了する [インスタンスからユーザーの関連付けを解除する](#) 前に、インスタンスを終了する必要があります。

Microsoft リモートデスクトップサービス

Microsoft リモートデスクトップサービスのライセンスサーバーには、関連付けられた Active Directory で定義されている管理ユーザーが必要です。そのユーザーは、次のタスクを実行できる必要があります。

- Active Directory ドメインで OU を作成する
- 作成された OU 内のドメイン結合インスタンス (コンピュータの作成)

- Active Directory ドメイン内のターミナルサーバーグループにコンピュータオブジェクトを追加する
- ライセンスサーバーレポートを生成するために、Active Directory ドメイン内のユーザーオブジェクトがターミナルサーバーのライセンスサーバーを読み書きする制御を委任します。

委任の詳細については、[「Active Directory ドメインサービスでの制御の委任」](#)を参照してください。

管理認証情報シークレット

License Manager は AWS Secrets Manager、を使用して、Microsoft Remote Desktop Services ライセンスサーバーでのユーザー管理タスクに必要な認証情報を管理します。ライセンスサーバーをセットアップする前に、ライセンスサーバーでユーザー管理タスクを実行するユーザーの認証情報を含むシークレットを Secrets Manager で作成する必要があります。ライセンスサーバー設定を構成するときは、作成したシークレットの ID を指定する必要があります。

Note

これは、RDSライセンスサーバーレポートの生成用に定義したのと同じユーザーである必要があります。

シークレットを作成するには、Secrets Manager ユーザーガイドの[AWS Secrets Manager 「シークレットの作成」](#)ページの詳細な手順に従い、License Manager に固有の以下の設定を行います。

Important

シークレットを使用するには、License Manager は、次のリストで指定されている正確なキー名、ユーザー名値、および暗号化キーによって異なります。シークレット名はプレフィックスで始まる必要があります `license-manager-user-`。

シークレットタイプの選択ページで、次の操作を行います。

- シークレットタイプ - その他のタイプのシークレットを選択します。
- キーと値のペア - シークレットに保存する次のキーペアを指定します。

ユーザーネーム

- キー: `username`

- 値: Administrator

パスワード

- キー: password

- 値: *The password*

- 暗号化キー – KMSキー以外のaws/secretsmanagerキーを指定するには、License Manager オペレーションへのアクセスに使用するロールにポリシーをアタッチする必要があります。詳細については、「[IAM ロールとアクセス許可](#)」を参照してください。

シークレットの設定ページで、次の操作を行います。

- シークレット名 – License Manager がライセンスサーバーの認証情報シークレットを識別するために使用するプレフィックスで始まるシークレットの名前を指定します。以下に例を示します。

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

これらの手順は、AWS Management Console を使用してシークレットを作成することを前提としています。Secrets Manager ユーザーガイドには、他の方法の詳細な手順も含まれています。Secrets Manager の詳細については、「[Secrets Manager とは](#)」を参照してください。特にコストに関連する詳細については、「Secrets Manager ユーザーガイド」の「[の料金 AWS Secrets Manager](#)」を参照してください。

License Manager のユーザーベースのサブスクリプションでサポートされているソフトウェア製品

AWS License Manager は、Microsoft Visual Studio および Microsoft Office のユーザーベースのサブスクリプションをサポートしています。サポートされているソフトウェア使用率は License Manager によって追跡されます。ユーザーベースのサブスクリプション製品を提供するライセンス込みのインスタンスにアクセスするには、各ユーザーが Windows Server Remote Desktop Services サブスクリバラーアクセスライセンス (RDSSAL) への 1 つのサブスクリプションが必要です。詳細については、「[License Manager でユーザーベースのサブスクリプションを開始する](#)」を参照してください。

サポートされる Windows オペレーティングシステム (OS) プラットフォーム

次の Windows OS プラットフォームのRDSSALライセンスの対象となる製品AMIsを含む Windows があります。

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

ユーザーベースのサブスクリプションでサポートされるソフトウェア

License Manager は、以下のソフトウェアでユーザーベースのライセンスをサポートしています。

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

Microsoft Visual Studio

Microsoft Visual Studio は、デベロッパーがアプリケーションを作成、編集、デバッグ、公開できるようにする統合開発環境 (IDE) です。提供されている Microsoft Visual Studio AMIsには、[AWS Toolkit for](#) が含まれています。[NETリファクタリング](#)と [AWS Toolkit for Visual Studio](#)。

サポートされるエディション

- Visual Studio Professional 2022
- Visual Studio Enterprise 2022

次の表は、License Manager のユーザーベースのサブスクリプションAPIオペレーションに使用されるソフトウェアサブスクリプション名とそれに関連する製品値の詳細を示しています。

ソフトウェアサブスクリプション名	製品値
Visual Studio Enterprise 2022	VISUAL_STUDIO_ENTERPRISE
Visual Studio Professional 2022	VISUAL_STUDIO_PROFESSIONAL

Microsoft Office

Microsoft Office は、ドキュメント、スプレッドシート、スライドショーのプレゼンテーションの操作など、生産性を向上させるさまざまなユースケース向けに Microsoft が開発したソフトウェアのコレクションです。

サポートされるエディション

- Office LTSC Professional Plus 2021

次の表は、License Manager のユーザーベースのサブスクリプションAPIオペレーションに使用されるソフトウェアサブスクリプション名とそれに関連する製品値の詳細を示しています。

ソフトウェアサブスクリプション名	製品価値
Office LTSC Professional Plus 2021	OFFICE_PROFESSIONAL_PLUS

その他のソフトウェア

ユーザーベースのサブスクリプションでは使用できない追加のソフトウェアをインスタンスにインストールできません。追加のソフトウェアインストールは、License Manager では追跡されません。これらのインストールは、Active Directory の管理アカウントを使用して実行する必要があります。を使用する場合 AWS Managed Microsoft AD、管理アカウント (Admin) はデフォルトで ディレクトリに作成されます。詳細については、「AWS Directory Service 管理ガイド」の「[管理者アカウントのアクセス権限](#)」を参照してください。

Active Directory 管理アカウントで追加のソフトウェアをインストールするには、以下を実行する必要があります。

- インスタンスによって提供される製品に管理アカウントをサブスクライブします。
- 管理アカウントをインスタンスに関連付けます。
- 管理者アカウントを使用してインスタンスに接続し、インストールを実行します。

詳細については、「[License Manager でユーザーベースのサブスクリプションを開始する](#)」を参照してください。

License Manager でユーザーベースのサブスクリプションを開始する

次の手順では、ユーザーベースのサブスクリプションを使用して を開始する方法について説明します。これらの手順は、必要な前提条件が既実装されていることを前提としています。詳細については、「[License Manager でユーザーベースのサブスクリプションを作成するための前提条件](#)」を参照してください。

ステップ

- [ステップ 1: 製品をサブスクライブする](#)
- [ステップ 2: License Manager に Active Directory を登録する](#)
- [ステップ 3: RDS ライセンスサーバーを設定する](#)
- [ステップ 4: インスタンスを起動してユーザーベースのサブスクリプションを提供する](#)
- [ステップ 5: ユーザーをユーザーベースのサブスクリプションインスタンスに関連付ける](#)

ステップ 1: 製品をサブスクライブする

Office や Visual Studio などの Microsoft 製品は、Active Directory ユーザーをそれらの製品を含むインスタンスに関連付ける前に、アクティブなサブスクリプションが必要です。Marketplace サブスクリプションステータスが非アクティブで表示されるサブスクリプション製品は、まだサブスクライブされていません。

から Microsoft ユーザーベースのサブスクリプション製品をサブスクライブすると AWS Marketplace、License Manager はアカウントの Microsoft リモートデスクトップサービス (RDS) にサブスクリプションをまだ追加していない場合、自動的に追加します。ライセンス込みの RDS から起動された EC2 インスタンスでグラフィカルデスクトップおよびサブスクリプションベースの Windows アプリケーションにリモートアクセスするには、AMIs が必要です。

次のリンク AWS Marketplace を使用して、で直接製品をサブスクライブできます。

- [Visual Studio Professional](#)
- [Visual Studio Enterprise](#)
- [Office LTSC Professional Plus 2021](#)
- [リモートデスクトップサービスのSALを Win する](#)

License Manager コンソールから製品を検出してサブスクライブする

License Manager コンソールから登録する製品を検出することもできます。

1. <https://console.aws.amazon.com/license-manager/> で [License Manager](#) コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[製品] を選択します。
3. 製品名を選択すると、サブスクリプションの詳細が表示されます。

4. 表示を選択します AWS Marketplace。
5. サブスクリプションの詳細を確認し、[サブスクライブに進む] を選択します。
6. 利用規約を確認し、続行する場合は [条件に同意する] を選択します。

条件に同意する場合は、製品のサブスクリプションを処理する必要があります。サブスクリプションが完了するまで、進行中というメッセージが表示されます。必要な他の設定済み製品でもこの手順を繰り返すことができます。必要なすべての製品のサブスクリプションがアクティブになったら、Active Directory ユーザーを製品にサブスクライブできます。

Note

ユーザー数および関連コストの請求額の見積もりは、でクローズされていない (請求保留中ステータスとマークされている) 請求期間に表示されるまでに 48 時間かかります AWS Billing。詳細については、「AWS Billing ユーザーガイド」の「[月額料金の表示](#)」を参照してください。

ステップ 2: License Manager に Active Directory を登録する

License Manager では、ユーザーをユーザーベースのサブスクリプションに関連付けるために、サブスクリプションユーザーを Active Directory で定義する必要があります。これは、AWS Managed Microsoft AD またはセルフマネージド Active Directory のいずれかです。

ユーザーは設定済み製品のみをサブスクライブできるため、ディレクトリを設定するときは、ユーザーベースのサブスクリプションに必要なすべての製品を選択する必要があります。Active Directory を登録すると、License Manager は 2 つのネットワークインターフェイスを作成して、サービスがディレクトリと通信できるようにします。ネットワークインターフェイスには、LicenseManager 用にAWS 作成されたネットワークインターフェイスと同様の説明が表示されます。<directory_id>.

ユーザーベースのサブスクリプションに登録する追加の DNS に対して VPCs 転送を設定する必要があります。複数のにユーザーベースのサブスクリプションがある場合 AWS リージョン、各リージョンには、次のように設定された DNS 転送を使用する独自の Active Directory が必要です。

ユーザーベースのサブスクリプションで Microsoft Office を使用するには、VPC 設定を更新するアクセス許可を License Manager に付与する必要があります。VPC を設定すると、License Manager はユーザーに代わって [VPC エンドポイント](#) を作成します。これらのエンドポイントは、リソースをアクティブーションサーバーに接続し、コンプライアンスを維持するために必要です。

⚠ Important

続行する前に、License Manager に必要な [サービスリンクロール](#) の作成を許可する必要があります。詳細については、「[License Manager でユーザーベースのサブスクリプションを作成するための前提条件](#)」を参照してください。

コンソールの登録手順は、使用する Active Directory のタイプによって若干異なります。

コンソール登録：AWS Managed Microsoft AD

ユーザーベースのサブスクリプションの Active Directory AWS Managed Microsoft AD として登録するには、次の手順に従います。

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左側のナビゲーションペインの設定で、ユーザーベースのサブスクリプションに移動します。
3. ユーザーベースのサブスクリプションページで、アクティブディレクトリの登録を選択します。
4. ユーザーベースのサブスクリプションのユーザー情報を保存する AWS Managed Directory の名前と ID を選択します。
5. 追加を選択して Active Directory を登録します。

コンソール登録: セルフマネージド Active Directory

ユーザーベースのサブスクリプションにセルフマネージド Active Directory を登録するには、次の手順に従います。

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左側のナビゲーションペインの設定で、ユーザーベースのサブスクリプションに移動します。
3. ユーザーベースのサブスクリプションページで、アクティブディレクトリの登録を選択します。
4. ユーザーベースのサブスクリプションのユーザー情報を保存する AWS Managed Directory の名前と ID を選択します。

からの Active Directory 登録 AWS CLI

Active Directory をユーザーベースのサブスクリプションの ID プロバイダーとしてに登録できます。[RegisterIdentityProvider](#) オペレーション。

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

ユーザーベースのサブスクリプション用に Active Directory と VPC を設定する (AWS CLI)

Active Directory を ID プロバイダーとして登録し、ユーザーベースのサブスクリプション用に VPC を設定できます。 [RegisterIdentityProvider](#) オペレーション。

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

使用可能なソフトウェア製品の詳細については、「[License Manager のユーザーベースのサブスクリプションでサポートされているソフトウェア製品](#)」を参照してください。

ステップ 3: RDS ライセンスサーバーを設定する

Microsoft リモートデスクトップサービス (RDS) ライセンスサーバーは、ユーザーベースのサブスクリプション Microsoft 製品を提供する Word インスタンスにアクセスすると、Active Directory ユーザーにサブスクライバアクセスライセンス (EC2SALs) を発行します。ステップ 1 と 2 を完了したら、次のようにライセンスサーバーを設定できます。

開始する前に、[ユーザーベースのサブスクリプションの前提条件](#) for RDS が完了していることを確認してください。このプロセスでは、Active Directory が既にセットアップされていることを前提としています。

ユーザーベースのサブスクリプション用に RDS ライセンスサーバーを設定する (コンソール)

1. <https://console.aws.amazon.com/license-manager/> で [License Manager](#) コンソールを開きます。
2. 左側のナビゲーションペインの設定で、ユーザーベースのサブスクリプションページに移動します。
3. リモートデスクトップサービス (RDS) タブで、リストに 1 つ以上の Active Directory が表示されます。Active Directory の RDS を設定する必要があることを知らせるプロンプトが表示される場合があります。
4. プロンプトまたはアクションメニューから、RDS License Server の設定を選択します。
5. RDS License Server の設定ダイアログでは、次の設定を構成できます。

Active Directory

このセクションには、設定した RDS ライセンスサーバーに接続されているディレクトリに関する重要な詳細が記載されています。

シークレット

既存のシークレットを選択するか、ライセンスサーバーのユーザー管理タスクに使用される認証情報用に新しいシークレットを作成する必要があります。シークレット名の最初の部分は、「」の「管理認証情報シークレット」セクションで説明されているパターンに従う必要があります [ユーザーベースのサブスクリプションの前提条件](#)。

[タグ]

オプションで、ライセンスサーバーリソースのタグを入力できます。

6. 設定を選択して設定を保存します。

ステップ 4: インスタンスを起動してユーザーベースのサブスクリプションを提供する

製品をサブスクライブしたら、ユーザーが製品を含む AWS Marketplace AMI から に接続するためのインスタンスを起動する必要があります。インスタンスを起動すると、 はインスタンスを Active Directory ドメインに結合し、リソースに対して追加の設定と強化を実行 AWS Systems Manager しようとしています。インスタンスを使用できるようにするための設定が完了には、約 20 分かかることがあります。License Manager コンソールの [ユーザーの関連付け] ページから、インスタンスの [ヘルスステータス] が [アクティブ] であるか確認して、リソースが使用できる状態になっていることを確認できます。

ユーザーベースのサブスクリプションでインスタンスを起動するには、「」を参照してください [含まれているライセンスからインスタンスを起動する AMI](#)。

ステップ 5: ユーザーをユーザーベースのサブスクリプションインスタンスに関連付ける

必要な製品の AWS Marketplace AMI にサブスクライブしたら、ユーザーを製品にサブスクライブし、製品を提供するインスタンスに関連付けることができます。ユーザーを製品に登録し、全員を 1 回の手順でインスタンスに関連付けることも、個別にインスタンスに関連付けることもできます。ユーザーに登録すると、ディレクトリがチェックされ、ユーザー ID が存在することが確認されます。製品に登録するユーザーごとに 1 つのサブスクリプションが作成されます。

Note

各ユーザーには、Windows Server Remote Desktop Services サブスクリバークラスライセンス (SAL) RDS と使用する製品の両方へのサブスクリプションが必要です。アカウントが「」で説明されているように SALRDS にサブスクライブすると [ステップ 1: 製品をサブスクライブする](#)、ユーザーはユーザーベースのサブスクリプション製品をサブスクライブするときに、ユーザーに代わって RDS SAL にサブスクライブされます。

License Manager の [製品] ページにはアクティブなサブスクリプションが表示され、[Marketplace のサブスクリプションステータス] には [アクティブ] と表示されます。License Manager の製品の詳細ページには、[ステータス] が [サブスクライブ済み] のアクティブなユーザーサブスクリプションが表示されます。

Important

Active Directory に製品が設定されていない場合は、コンソールの上部に通知バーが表示され、ディレクトリの設定を調整するよう指示されます。通知バーで [設定を開く] を選択し、License Manager の [設定] ページにアクセスしてディレクトリを編集します。各ユーザーには、RDS SAL使用する製品の両方へのサブスクリプションが必要です。[Marketplace サブスクリプションステータス] が [非アクティブ] の製品にユーザーを登録すると、失敗します。

ユーザーを製品に登録してインスタンスに関連付ける

以下のプロセスにより、ユーザーを製品に登録してインスタンスに関連付けることができます。

ユーザーを製品に登録してインスタンスに関連付けるには

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[ユーザーの関連付け] を選択します。
3. ユーザーを関連付けるインスタンスを選択し、[ユーザーを登録して関連付け] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[登録して関連付け] を選択します。

[ユーザーの関連付け] ページでは、選択したユーザーが [関連付け済み] の [関連付けのステータス] で [ユーザー] の下に表示されているはずですが、[製品] ページでは、[製品名] を選択して製品の詳細ページを確認できます。登録されたユーザーは、[サブスクライブ済み] の [ステータス] で [ユーザー] の下に表示されます。

ユーザーを製品に登録する

次のいずれかの方法を使用して、ユーザーを製品に登録できます。

Console

ユーザーを製品にサブスクライブする (コンソール)

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[製品] を選択します。
3. ユーザーに登録する [Marketplace のサブスクリプションステータス] が [アクティブ] の製品を選択し、[ユーザーに登録] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[サブスクリプション] を選択します。

サブスクリプションを持つユーザーは、[サブスクライブ済み] の [ステータス] で [ユーザー] の下に表示されます。

AWS CLI

ユーザーを製品にサブスクライブする (AWS CLI)

を使用して、ID プロバイダーに登録されている製品にユーザーをサブスクライブできます。
[StartProductSubscription](#) オペレーション。

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

セルフマネージド Active Directory (AWS CLI) を使用してユーザーを製品にサブスクライブする

を使用して、セルフマネージド Active Directory から AWS Managed Microsoft AD ディレクトリに登録されている製品にユーザーをサブスクライブできます。 [StartProductSubscription](#) オペレーション。

```
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>
```

使用可能なソフトウェア製品の詳細については、「[License Manager のユーザーベースのサブスクリプションでサポートされているソフトウェア製品](#)」を参照してください。

サブスクリプションを持つユーザーは、[サブスクライブ済み] の [ステータス] で [ユーザー] の下に表示されます。

ユーザーをインスタンスに関連付ける

次のいずれかの方法を使用して、インスタンスにユーザーに関連付けることができます。

Important

製品をインスタンスに関連付ける前に、まずユーザーを製品に登録する必要があります。

Console

ユーザーをインスタンスに関連付けるには (コンソール)

1. <https://console.aws.amazon.com/license-manager/> で [License Manager](#) コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[ユーザーの関連付け] を選択します。
3. ユーザーを関連付けるインスタンスを選択し、[ユーザーを関連付け] を選択します。
4. ディレクトリに存在するユーザー名を最大 5 つ指定し (信頼できるドメインに存在する場合は [ドメイン名] を含む)、[関連付け] を選択します。

[ユーザーの関連付け] ページでは、選択したユーザーが [関連付け済み] の [関連付けのステータス] で [ユーザー] の下に表示されているはずですが。

AWS CLI

ユーザーをインスタンスに関連付けるには (AWS CLI)

ユーザーベースのサブスクリプションを に提供するために起動したインスタンスにユーザーを関連付けることができます。 [AssociateUser](#) オペレーション。

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

セルフマネージド Active Directory ユーザーをインスタンスに関連付けるには (AWS CLI)

セルフマネージド Active Directory のユーザーを起動されたインスタンスに関連付けて、ユーザーベースのサブスクリプションを に提供できます。 [AssociateUser](#) オペレーション。

```
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>
```

使用可能なソフトウェア製品の詳細については、「[License Manager のユーザーベースのサブスクリプションでサポートされているソフトウェア製品](#)」を参照してください。

[ユーザーの関連付け] ページでは、選択したユーザーが [関連付け済み] の [関連付けのステータス] で [ユーザー] の下に表示されているはずですが、

よりアクティブなリモートユーザーセッションGPO用に Active Directory を設定する

デフォルトでは、Microsoft はユーザーベースのサブスクリプション製品を提供する EC2 Windows インスタンスで最大 2 つのユーザーセッションを同時に RDS 許可します。License Server エンドポイントを設定したら、次のように Active Directory グループポリシーオブジェクト (GPO) で 3 つ以上のユーザーセッションを同時に許可 RDS するように Microsoft を設定できます。

前提条件

環境にライセンスサーバーを作成しておく必要があります。ライセンスサーバーを作成するには、「」を参照してください [ステップ 3: RDS ライセンスサーバーを設定する](#)。

1. の設定に使用するツールは、次のように、実行元の場所GPOによって異なります。

ドメインコントローラーからの中央設定

管理者として Active Directory ドメインコントローラーにログインし、Windows グループポリシーマネージメントコンソールを開きます。

セッションホストでグループポリシーを設定する

管理者として License Server にログインし、ローカルグループポリシーエディタを開きます。

2. 管理コンソールまたはポリシーエディタで、グループポリシーを編集して、Microsoft 経由で接続するセッションホストを指定します。RDS。RDS License Server のエンドポイントアドレスは、License Manager の製品詳細ページ、またはの [list-license-server-endpoints](#) コマンドで確認できます AWS CLI。
3. リモートデスクトップセッションホストのライセンスモードを に設定し Per User、保存します。

License Server for RDS License Manager の設定の詳細については、「開始方法」トピックの「」を参照してください。Microsoft RDSセッションホストの設定の詳細については、[「リモートデスクトップセッションホストのライセンス」](#)を参照してください。

含まれているライセンスからインスタンスを起動する AMI

製品をサブスクライブしたら、ユーザーが製品を含む AWS Marketplace AMIから に接続するためのインスタンスを起動する必要があります。インスタンスを起動すると、 はインスタンスを Active Directory ドメインに結合し、リソースに対して追加の設定と強化を実行 AWS Systems Manager しようとしています。インスタンスを使用できるようにするための設定が完了には、約 20 分かかることがあります。License Manager コンソールの [ユーザーの関連付け] ページから、インスタンスの [ヘルスステータス] が [アクティブ] であるか確認して、リソースが使用できる状態になっていることを確認できます。

Important

起動するインスタンスは、準拠するために必要な前提条件を満たしている必要があります。初期設定を完了できないリソースは終了します。詳細については、「[License Manager でユーザーベースのサブスクリプションを作成するための前提条件](#)」および「[License Manager でのユーザーベースのサブスクリプションのトラブルシューティング](#)」を参照してください。

ユーザーベースのサブスクリプションでインスタンスを起動する

1. で Amazon EC2コンソールにアクセスします <https://console.aws.amazon.com/ec2/>。
2. イメージで、AMIカタログを選択します。
3. AWS Marketplace AMIs を選択します。
4. 検索ボックスに製品名を入力し、Enter キーを押します。例えば、**Visual Studio** を検索します。
5. [パブリッシャー] で [アマゾンウェブサービス] を選択します。
6. ユーザーベースのサブスクリプションを提供するためにインスタンスを起動しようとしている製品で、[選択] を選択します。
7. [続行] を選択して次に進みます。
8. でインスタンスを起動を選択しますAMI。
9. 次の点を確認しながら、ウィザードを完了します。
 - a. Graviton ベースではない Nitro ベースのインスタンスタイプを選択します。
 - b. インスタンスが AWS Managed Microsoft AD ディレクトリに接続できる VPCとサブネットを選択します。
 - c. インスタンスから Active Directory への接続を許可するセキュリティグループを選択します。
 - d. 詳細を展開し、インスタンスの Systems Manager 機能を許可する IAMロールを選択します。
10. Launch instance (インスタンスの起動) を選択します。

からインスタンスを実行している場合は AWS Marketplace AMI、ユーザーを製品にサブスクライブしてインスタンスに関連付ける必要があります。インスタンスは、ユーザーが製品を使用できるように製品を提供します。

特定のオペレーティングシステムのバージョンからインスタンスを起動する AMI

Office LTSC Professional Plus または Microsoft Visual Studio AMIをサポートする からインスタンスを起動すると、起動はデフォルトでの最新の Windows オペレーティングシステムバージョン AMI (Windows Server 2022 など) になります。特定のオペレーティングシステムバージョン で起動するにはAMI、次の手順に従います。

1. <https://console.aws.amazon.com/marketplace> で AWS Marketplace コンソールを開きます。

2. ナビゲーションペインで、[サブスクリプションの管理] を選択します。
3. サブスクリプションの結果を効率化するために、サブスクリプション名の全部または一部を検索できます。例えば、Office LTSC Professional Plus 2021、Visual Studio Enterprise です。
4. サブスクリプションパネルから新しいインスタンスを起動を選択します。これにより、起動設定ページが開きます。
5. Windows OS プラットフォームの以前のバージョンに基づく AMI からインスタンスを起動するには、ソフトウェアバージョンの下にある完全な AWS Marketplace ウェブサイトリンクを選択します。これにより、バージョンのリストから選択できる設定ページに移動します。
6. リストには、サポートされている Windows OS プラットフォームの AMI 最新バージョンが表示されます。起動元の Windows OS バージョンを選択します。

を使用してユーザーベースのサブスクリプションインスタンスに接続する RDP

製品を提供するインスタンスにユーザーを関連付けると、インスタンスの [ヘルスステータス] が [アクティブ] であれば、そのユーザーはインスタンスに接続できます。ユーザーは、関連付けられた ID で製品を使用するには、ドメインのユーザー認証情報を使用して接続する必要があります。

Important

EC2 インスタンスを作成してユーザー用に準備するプロセスには、約 20 分かかる場合があります。インスタンスにアクセスして製品を使用するには、インスタンスの関連付けステータスがアクティブである必要があります。

ユーザーベースのサブスクリプションを備えたインスタンスに接続するには

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[ユーザーの関連付け] を選択します。
3. [ユーザーの関連付け] ページで、インスタンスの [ヘルスステータス] が [アクティブ] であることを確認します。
4. インスタンス ID を書き留めます。これは接続の詳細情報を収集するために必要になります。

5. 「[を使用して Windows インスタンスに接続する RDP](#)」に記載されている手順に従い、関連するユーザーの完全修飾ユーザー名を必ず指定します。

Microsoft Office サブスクリプションのファイアウォール設定を変更する

ファイアウォールは、不正なインバウンドトラフィックまたはアウトバウンドトラフィックからネットワークリソースを保護します。セキュリティグループに対して定義するルールは、EC2 Windows インスタンスで Microsoft Office のユーザーベースのサブスクリプションを提供するために連携する VPC リソースのファイアウォールとして機能します。

次のステップを使用して、サブネットとセキュリティグループを編集できます。License Manager は、この設定を使用して Microsoft Office のエンドポイントをプロビジョニングします AWS PrivateLink。VPC エンドポイントの詳細については、Amazon Virtual Private Cloud ドキュメントの「[What is AWS PrivateLink?](#)」を参照してください。

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. 左側のナビゲーションペインの設定のユーザーベースのサブスクリプションページに移動します。
3. ファイアウォール設定を編集するには、Microsoft Office サブスクリプション製品タブを選択し、ファイアウォールセクションの上部から編集を選択します。ファイアウォールの編集ダイアログが開きます。
4. 設定を変更したら、保存して更新するか、キャンセルを選択して現在の設定を維持します。

License Manager がこれらの設定の変更を完了するまでに数分かかる場合があります。

License Manager ユーザーベースのサブスクリプションのサブスクリプションユーザーを管理する

製品サブスクリプションの請求とレポートの精度を確保し、サブスクリプションリソースへの不正アクセスを防ぐために、License Manager ユーザーベースのサブスクリプションのユーザーアクセスを次のように管理できます。

[インスタンスからユーザーの関連付けを解除する](#)

License Manager ユーザーベースのサブスクリプションをホストするインスタンスからユーザーの関連付けを解除して、リソースへのアクセスを削除します。

ユーザーのサブスクリプションを解除する

のユーザーベースのサブスクリプションからユーザーをサブスクリプション解除 AWS License Manager して、それらのユーザーのサブスクリプション料金の発生を停止します。

Note

Active Directory からユーザーを削除しても、ユーザーの関連付けやサブスクリプションは変更されません。License Manager のユーザーとサブスクリプション製品の詳細ページの関連付けを解除して、インスタンスとの関連付けを解除する必要があります。次に、ユーザーのサブスクリプションを解除する必要があります。

このトピックでは、Active Directory の管理については取り上げません。

サブスクリプション料金

Microsoft Office および Visual Studio サブスクリプションの場合、サブスクリプション製品を提供するすべてのインスタンスからユーザーの関連付けを解除し、製品からサブスクリプションを解除するとすぐに、請求は停止します。

Microsoft RDS はユーザーごとに月単位で請求され、月の一部は按分されません。当月末以降に請求を停止するには、ライセンスサーバー用に設定された Active Directory からユーザーを削除する必要があります。ユーザーが月末に引き続きログインする場合は、ライセンストークンの有効期限が切れるまで自動的に再登録されます。

ユーザーベースのサブスクリプションを提供するインスタンスからユーザーの関連付けを解除する

License Manager のユーザーベースのサブスクリプションを提供するインスタンスへのユーザーアクセスを削除するには、サブスクライブしたユーザーのそのインスタンスとの関連付けを解除します。この変更は、ユーザーのサブスクリプションステータスには影響しません。ユーザーのサブスクリプションを解除し、そのユーザーのサブスクリプション料金を停止するには、「」を参照してください [License Manager でユーザーベースのサブスクリプションからユーザーをサブスクリプション解除する](#)。

インスタンスからサブスクリプションユーザーの関連付けを解除する

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。

2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[ユーザーの関連付け] を選択します。
3. ユーザーの関連付けを解除するインスタンスを選択します。
4. 関連付けを解除するユーザー名を選択し、次に [ユーザーの関連付けを解除] を選択します。

License Manager でユーザーベースのサブスクリプションからユーザーをサブスクリプション解除する

ユーザーベースのサブスクリプション製品のサブスクリプションを解除して、課金を停止する必要があります。

Important

サブスクリプションを解除する前に、まず、現在関連付けられているすべてのインスタンスからユーザーの関連付けを解除する必要があります。

ユーザーベースのサブスクリプションからユーザーの登録を解除するには

1. <https://console.aws.amazon.com/license-manager/> で **License Manager** コンソールを開きます。
2. 左側のナビゲーションペインの [ユーザーベースのサブスクリプション] で、[製品] を選択します。
3. ユーザーの登録を解除する製品を選択します。
4. 登録を解除するユーザー名を選択し、[ユーザーの登録解除] を選択します。

License Manager の設定から Active Directory の登録を解除する

ユーザーベースのサブスクリプションに使用しない場合は、Active Directory を License Manager 設定から登録解除できます。License Manager の設定からディレクトリ設定を登録解除しても、ディレクトリは削除されません。設定からディレクトリを登録解除すると、License Manager のユーザーベースのサブスクリプションのために、そのディレクトリからユーザーを関連付けることができなくなります。

前提条件

License Manager の設定からディレクトリの登録を解除する前に、次のタスクを実行する必要があります。

1. [インスタンスからユーザーの関連付けを解除する](#) 登録解除するディレクトリを参照する各インスタンスから。
2. すべてのサブスクリプションユーザーのインスタンスとの関連付けが解除されたら、インスタンスを終了します。Active Directory を参照するすべてのインスタンスが終了するまで繰り返します。
3. また、変更の発生を停止するには、登録を解除[ユーザーのサブスクリプションを解除する](#)する Active Directory に属する も必要です。

登録解除

License Manager の設定から Active Directory の登録を解除する

前提条件となるタスクをすべて完了したら、で License Manager コンソールを開きます<https://console.aws.amazon.com/license-manager/>。

1. 左のナビゲーションペインの [設定] を選択します。
2. 設定ページの AWS Managed Microsoft AD セクションで、削除を選択します。
3. 必要なテキストを入力してディレクトリを削除することを確認し、削除を選択します。

削除を選択すると、設定ページの AWS Managed Microsoft ADセクションに、設定のステータスを含むディレクトリ ID が表示されます。設定プロセスが完了すると、ディレクトリは AWS Managed Microsoft ADセクションから削除されます。

License Manager でのユーザーベースのサブスクリプションのトラブルシューティング

AWS License Managerのユーザーベースのサブスクリプションで発生する可能性のある問題を解決するために役立つ、トラブルシューティングのヒントを以下に示します。

目次

- [インスタンスコンプライアンスのトラブルシューティング](#)
- [ライセンスコンプライアンスのトラブルシューティング](#)
- [インスタンス接続のトラブルシューティング](#)
- [ドメインへの参加失敗のトラブルシューティング](#)
- [Systems Manager 接続のトラブルシューティング](#)
- [Systems Manager Run Command のトラブルシューティング](#)

インスタンスコンプライアンスのトラブルシューティング

ユーザーベースのサブスクリプションを提供するインスタンスがコンプライアンスを維持するには、正常な状態を維持する必要があります。異常とマークされたインスタンスは、必要な前提条件を満たさなくなります。License Manager はインスタンスを正常な状態に戻すよう試みますが、正常な状態に戻すことができないインスタンスは終了されます。

ユーザーベースのサブスクリプションを提供するために起動され、初期設定を完了できないインスタンスは終了されます。このシナリオでは、設定の問題を修正し、ユーザーベースのサブスクリプションを提供するために新しいインスタンスを起動する必要があります。詳細については、「[License Manager でユーザーベースのサブスクリプションを作成するための前提条件](#)」を参照してください。

ライセンスコンプライアンスのトラブルシューティング

Microsoft Office でユーザーベースのサブスクリプションを提供するように Active Directory を設定した場合は、License Manager が作成する VPC エンドポイントにリソースが接続できることを確認する必要があります。エンドポイントには、ユーザーベースのサブスクリプションを提供するインスタンスからの TCP ポート 1688 でのインバウンドトラフィックが必要です。

[Reachability Analyzer](#) を使用すると、ユーザーベースのサブスクリプションと VPC エンドポイントを提供するインスタンスのネットワーク設定が正しく設定されていることを確認できます。ユーザーベースのサブスクリプションを送信元として提供するサブネットに起動されるインスタンス ID と、Microsoft Office 製品用にプロビジョニングされた VPC エンドポイントを送信先として指定できます。TCP をプロトコルとして指定し、分析するパスの送信先ポートに 1688 を指定します。詳細については、「[ゲートウェイとインターフェイスの VPC エンドポイントを介した接続の問題をトラブルシューティングするにはどうすればよいですか？](#)」を参照してください。

インスタンス接続のトラブルシューティング

ユーザーが RDP を使用して、ユーザーベースのサブスクリプションを提供するインスタンスに接続できる必要があります。インスタンス接続のトラブルシューティングの詳細については、「Amazon EC2 ユーザーガイド」の「[Windows インスタンスへの接続のトラブルシューティング](#)」を参照してください。

ドメインへの参加失敗のトラブルシューティング

ユーザーは、License Manager の設定で設定された Active Directory のユーザー ID を使用して、ユーザーベースのサブスクリプション製品を提供するインスタンスに接続できる必要があります。ドメインに参加できなかったインスタンスは終了されます。

トラブルシューティングを行うには、調査する前にリソースが終了されないように、インスタンスを起動して[手動でドメインに参加させる](#)必要がある場合があります。インスタンスは Systems Manager Run Command を正常に受信して実行する必要があります。オペレーティングシステム内でドメイン参加を完了できる必要もあります。詳細については、「AWS Systems Manager ユーザーガイド」の「[コマンドのステータスについて](#)」および Microsoft Web サイトの「[How to troubleshoot errors that occur when you join Windows-based computers to a domain](#)」を参照してください。

Systems Manager 接続のトラブルシューティング

ユーザーベースのサブスクリプションを提供するインスタンスは、によって管理される必要があります。AWS Systems Manager 管理されない場合、インスタンスは終了します。詳細については、「AWS Systems Manager ユーザーガイド」の[SSM エージェントのトラブルシューティング](#)」および「[マネージドノードの可用性のトラブルシューティング](#)」を参照してください。

Systems Manager Run Command のトラブルシューティング

Systems Manager の機能である Run Command は、ドメインへの参加、オペレーティングシステムの強化、および付属製品のアクセス監査を実行するためのユーザーベースのサブスクリプションを提供するインスタンスで使用されます。詳細については、「AWS Systems Manager ユーザーガイド」の「[コマンドのステータスについて](#)」を参照してください。

License Manager で Linux サブスクリプションを管理する

で AWS License Manager では、Amazon EC2 インスタンスが使用する商用 Linux サブスクリプションを表示および管理できます。の Linux サブスクリプションの使用率を追跡できます。AWS リージョンのアカウントとアカウント AWS Organizations 設定で定義した。License Manager では、Linux サブスクリプションを使用する実行中のインスタンスを包括的に表示できます。また、インスタンスに複数のサブスクリプションが定義されている場合も示します。

License Manager が検出したデータは集約され、License Manager コンソールと Amazon CloudWatch ダッシュボードに表示されます。また、からサブスクリプションデータにアクセスすることもできます。AWS CLI および License Manager Linux サブスクリプション API または関連する SDKs。

Linux ライセンスサブスクリプションは、次のソースから取得できます。

サブスクリプション込み AMIs

- Red Hat Enterprise Linux (RHEL)

- RHEL Red Hat Cloud Access Program による Bring Your Own Subscription モデル (BYOS)
- SUSE Linux エンタープライズサーバー
- Ubuntu Pro サブスクリプション込み AMI

サードパーティーのサブスクリプションプロバイダー

- RHEL Red Hat Subscription Manager からの サブスクリプション (RHSM)

Linux サブスクリプション検出では、結果整合性モデルを使用します。整合性モデルによって、[Linux サブスクリプション] ビューにデータが読み込まれて表示される方法とタイミングが決まります。このモデルでは、License Manager は Linux サブスクリプションデータが リソースから定期的に更新されるようにします。これらの間隔内に一部のデータが取り込まれない場合、情報は次のメトリクスエミッションで配信されます。この動作により、新しく起動されたEC2商用 Linux インスタンスなどのリソースが Linux サブスクリプションダッシュボードに表示されるのを遅らせる可能性があります。

Note

最初のリソース検出が完了するまでに最大 36 時間、新しく起動されたインスタンスが検出されてレポートされるまでに最大 12 時間かかることがあります。リソースが検出されると、Linux サブスクリプションデータに対して Amazon CloudWatch メトリクスが 1 時間ごとに出力されます。

アカウントが [ある場合](#) AWS Organizationsでは、メンバーアカウントを委任管理者として登録できます。詳細については、「[License Manager の委任管理者設定](#)」を参照してください。

重複したサブスクリプションが検出されました

License Manager は、同じEC2インスタンスで 2 つの Linux サブスクリプションを検出すると、重複サブスクリプションアラートを設定します。Linux サブスクリプションデータは、License Manager コンソールのインスタンスページから表示およびフィルタリングできます。

Red Hat Enterprise Linux 7 延長ライフサイクルサポート (RHEL 7 ELS) インスタンス : 7 AMIのサブスクリプションに含まれる からインスタンスを起動してもELS、インスタンスを Red Hat RHEL に登録して使用権限を消費する必要があります。この場合、License Manager は重複するサブスクリプションを報告しますが、それが想定される動作です。

その他の Red Hat Linux インスタンス : [Red Hat Hybrid Cloud Console](#) でサブスクリプションインベントリを検索して、インスタンスが消費するサブスクリプションを確認することをお勧めします。

その他のトピック

- [License Manager で Linux サブスクリプション検出を設定する](#)
- [License Manager で検出されたインスタンスデータを表示する](#)
- [License Manager での Linux サブスクリプションの請求情報](#)
- [License Manager で Linux サブスクリプションの Amazon CloudWatch アラームを管理する](#)

License Manager で Linux サブスクリプション検出を設定する

Linux サブスクリプションの検出は、License Manager コンソール、AWS CLI、License Manager Linux サブスクリプションAPI、または関連する SDKs。の Linux サブスクリプションの検出を有効にする場合 AWS リージョン 指定すると、オプションでのアカウントに検出を拡張できます。AWS Organizations。サブスクリプション使用率を追跡する必要がなくなった場合は、検出を非アクティブ化することもできます。

Note

アカウントごとに最大 5,000 個のリソースを検出して表示できます。AWS リージョン デフォルトでは、です。制限の引き上げをリクエストするには、[制限の引き上げのフォーム](#)を使用してください。

トピック

- [Linux サブスクリプション検出を設定する](#)
- [Red Hat Subscription Manager サブスクリプション検出を有効にする](#)
- [リソース検出のステータス理由](#)
- [Linux サブスクリプションの検出を無効にする](#)

Linux サブスクリプション検出を設定する

License Manager コンソールの設定ページから Linux サブスクリプション検出を設定するには、次の手順に従います。

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで [設定] を選択します。設定ページが開きます。
3. Linux サブスクリプションタブを開き、 の設定を選択します。これにより、Linux サブスクリプション設定の構成パネルが開きます。
4. ソースを選択する AWS リージョン Linux サブスクリプション検出を実行する場所。
5. でアカウント全体のサブスクリプションデータを集約するには AWS Organizations、リンクを選択します。AWS Organizations。このオプションは、 の場合にのみ表示されます。AWS Organizations はアカウント用に設定されています。
6. が付与するオプションを確認して承認する AWS License Manager Linux サブスクリプションのサービスにリンクされたロールを作成する アクセス許可。
7. [設定の保存] を選択します。

Red Hat Subscription Manager サブスクリプション検出を有効にする

ユーザーに代わって Red Hat Subscription Manager (RHSM) からサブスクリプション情報を取得するには、License Manager が Red Hat カスタマーアカウントのAPI認証情報を提供する必要があります。

前提条件

サブスクリプション検出を有効にする前に、次の前提条件を満たしていることを確認してください。

- の Linux サブスクリプションのデフォルト検出を有効にする必要があります AWS アカウント RHSM サブスクリプション検出を設定する前に。デフォルトの検出がアクティブ化されていない場合は、「」を参照してください [Linux サブスクリプション検出を設定する](#)。
- Organization Administrator が提供する企業の Red Hat ログインを使用する場合は、ログイン ID に次のロールとアクセス許可が割り当てられていることを確認します。
 - ロール：サブスクリプションを管理する
 - アクセス許可：View All、または View/Edit All

ログイン ID に必要なロールとアクセス許可がない場合は、Red Hat ポータルの Organization Administrator に連絡して、ログインに追加するようリクエストしてください。Red Hat のロールとアクセス許可の詳細については、「[Red Hat カスタマーポータルのロールとアクセス許可](#)」を参照してください。Red Hat Portal Organization Administrator への連絡方法の詳細については、Red Hat Customer Portal [Knowledgebase](#) の「[Organization Administrator が誰であるかを知る](#)」にはどうすればよいですか？」を参照してください。

- RHSM サブスクリプション検出を有効にするには、Red Hat カスタマーアカウントのAPIオフライントークン、または を指定する必要があります。AWS Secrets Manager オフライントークンを含むシークレット。オフライントークンを取得するには、Red Hat ドキュメントウェブサイトの新しい[オフライントークンの生成](#)で説明されているステップに従います。

Important

お客様のセキュリティは当社にとって重要です。Red Hat のオフラインアクセストークンは Secrets Manager に安全に保存されます。License Manager は、Red Hat にサブスクリプションの詳細をリクエストするたびに、シークレットを使用して一時的なアクセストークンを生成します。

Activation

License Manager コンソールの設定ページからRHSM検出を有効にするには、次の手順に従います。

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで [設定] を選択します。
3. 設定ページで、Linux サブスクリプションタブを開きます。
4. 編集 を選択して Linux サブスクリプション設定を更新します。Linux サブスクリプションの設定検出ページが開きます。
5. アクティベーションプロセスを開始するには、Red Hat Subscription Manager のアクティブ化 (RHSM) 検出チェックボックスを選択します。RHSM アカウントリンクパネルが表示されます。
6. シークレットに適用するシークレット (トークン) オプションを選択し、選択したオプションに応じて残りのステップに従います。
7. オプション: 新しいシークレットを作成する – 推奨

Red Hat オフラインアクセストークンを提供し、ユーザーに代わって License Manager が Secrets Manager にアクセスシークレットを作成できるようにします。

- a. シークレット名 にシークレットの名前を入力します。
- b. Red Hat オフラインアクセストークンをオフライントークンボックスに貼り付けます。トークン値の前後に余分なスペースや改行がないことを確認してください。Red Hat オフラインアクセストークンは、[Red Hat Subscription Manager API トークンページ](#)で生成できます。

オプション: シークレットを選択する

Red Hat オフラインアクセストークンを含む Secrets Manager の既存のシークレットを選択します。

8. (オプション)シークレットにタグを追加します。
9. ページの下部にあるチェックボックスをオンにして、Red Hat Subscription Manager の検出を有効にすると、へのアクセスが付与されることを確認します。AWS License Manager Amazon EC2インスタンスで使用される Red Hat サブスクリプションに関連するデータを収集する サービス。
10. [アクティブ化] を選択します。

リソース検出のステータス理由

AWS License Manager は、各 のステータスと対応するステータスの理由を表示します。AWS リージョン Linux サブスクリプションの検出を有効にすることを選択します。Linux サブスクリプションをにリンクしている場合、ステータスの理由は異なります。AWS Organizations:

- 進行中
- [成功]
- [失敗]

選択したリージョンごとに表示されるステータス理由には、一度に最大 2 つのステータス理由が表示されます。詳細を次の表に示します。

ステータス理由のアクション	説明
アカウントオンボード	1 つのアカウントだけをオンボーディングします。
アカウントオフボード	1 つのアカウントだけをオフボーディングします。
組織オンボード	組織全体をオンボーディングします。
	組織全体をオフボーディングします。

ステータス理由のアクション	説明
組織オフボード	

を呼び出しUpdateServiceSettingsAPIした後、 を呼び出しGetServiceSettingsAPIで、Linuxサブスクリプションの有効化の進行状況をモニタリングできます。各ステータスとステータス理由は複数のリージョンに同時に適用できます。以下の表は、ステータスとステータス理由の詳細を示しています。

ステータス	ステータス理由	説明
進行中	"Region": "Account-Onboard: Pending"	1つのアカウントのLinuxサブスクリプションを有効にしています。
	"Region": "Org-Onboard: Pending"	組織のLinuxサブスクリプションを有効にしています。
	"Region": "Account-Offboard: Pending"	1つのアカウントのLinuxサブスクリプションを無効にしています。
	"Region": "Org-Offboard: Pending"	組織のLinuxサブスクリプションを無効にしています。
[成功]	"Region": "Account-Onboard: Successful"	1つのアカウントのLinuxサブスクリプションの有効化に成功しました。
	"Region": "Org-Onboard: Successful"	組織のLinuxサブスクリプションの有効化に成功しました。
	"Region": "Account-Offboard: Successful"	1つのアカウントのLinuxサブスクリプションの無効化に成功しました。
	"Region": "Org-Offboard: Successful"	組織のLinuxサブスクリプションの無効化に成功しました。

ステータス	ステータス理由	説明
[失敗]	"Region": "Account-Onboard: Failed - Service-linked role not present"	必要なサービスリンクロールが作成されていなかったため、1つのアカウントのLinuxサブスクリプションを有効にできませんでした。必要なロールを作成して、もう一度試してください。
	"Region": "Account-Onboard: Failed - An internal error occurred"	内部エラーのため、1つのアカウントのLinuxサブスクリプションを有効にできませんでした。
	"Region": "Org-Onboard: Failed - Account isn't the management account"	操作を実行するアカウントが組織の管理アカウントではないため、組織のLinuxサブスクリプションを有効にできませんでした。管理アカウントにログインして、もう一度試してください。
	"Region": "Org-Onboard: Failed - Account isn't part of an organization"	操作を実行するアカウントが組織に属していないため、組織のLinuxサブスクリプションを有効にできませんでした。組織内のアカウントから操作を試すか、このアカウントを組織に追加して、もう一度試してください。
	"Region": "Org-Onboard: Failed - Linux subscriptions can't access the organization"	License Manager に組織へのアクセス権限がないため、組織のLinuxサブスクリプションを有効にできませんでした。Linuxサブスクリプションのサービスリンクロールを作成して、もう一度試してください。

Linux サブスクリプションの検出を無効にする

から Linux サブスクリプションの検出を非アクティブ化できます。AWS License Manager 設定ページ。ただし、 の検出を有効にしている場合

Warning

検出を無効にすると、Linux サブスクリプションで以前に検出されたすべてのデータが から削除されます。AWS License Manager.

Linux サブスクリプションの検出を無効にするには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインの [設定] を選択します。
3. [設定] ページで [Linux サブスクリプション] タブを選択し、[Linux サブスクリプション検出を無効にする] を選択します。
4. **Disable** と入力し、[無効化] を選択して無効化を確定します。
5. (オプション) Linux サブスクリプションに使用されているサービスリンクロールを削除します。詳細については、「[License Manager のサービスリンクロールを削除する](#)」を参照してください。
6. (オプション) License Manager と組織間の信頼されたアクセスを無効にします。詳細については、「」を参照してください [AWS License Manager](#) また、 [AWS Organizations](#)。

License Manager で検出されたインスタンスデータを表示する

License Manager が選択した で最初のリソース検出プロセスを完了した後 AWS リージョンコンソールで結果を表示できます。リンクを選択した場合 AWS Organizations、License Manager は組織全体のアカウントからデータを集約します。フィルター条件を満たすサブスクリプションを持つインスタンスのリストを表示するには、 の「インスタンス」セクションに移動します。AWS License Manager console。リストには、次のキーフィールドが表示されます。

- インスタンス ID - インスタンスの ID。
- ステータス - インスタンスのステータス。
- インスタンスタイプ - インスタンスのタイプ。

- サブスクリプション — インスタンスが使用するライセンスサブスクリプションの名前。
- 重複アラート — インスタンス上の同じソフトウェアに対して 2 つの異なるライセンスサブスクリプションがあることを示します。
- アカウント ID - インスタンスを所有するアカウントの ID。
- リージョン – AWS リージョン インスタンスが存在する。
- AMI ID – インスタンスの起動AMIに使用される の ID。
- 使用状況オペレーション – インスタンスのオペレーションと、に関連付けられている請求コード AMI。詳細については、「[使用オペレーションの値](#)」を参照してください。
- 製品コード – インスタンスの起動AMIに使用される に関連付けられた製品コード。詳細については、「[AMI製品コード](#)」を参照してください。
- LastUpdatedTime – 最後の検出でインスタンスの詳細が更新された時刻。

トピック

- [すべてのインスタンスのデータを表示する](#)
- [サブスクリプション別にインスタンスのデータを表示する](#)

すべてのインスタンスのデータを表示する

License Manager がアカウント内のインスタンスについて検出した Linux サブスクリプションデータを表示およびフィルタリングできます。または AWS Organizations、次のように。

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインにある [Linux サブスクリプション] で、[インスタンス] を選択します。これにより、Linux サブスクリプションデータを含むインスタンスのリストが表示されます。
3. (オプション) 次のフィルターを使用して結果を合理化できます。
 - アカウント
 - AMI ID
 - サブスクリプションの複製
 - [インスタンス ID]
 - リージョン
 - 製品コード

- 使用オペレーション
4. (オプション) ビューを にエクスポート CSV を選択して、すべてのインスタンスのデータをカンマ区切り値ファイル () としてエクスポートします CSV。

サブスクリプション別にインスタンスのデータを表示する

選択したリージョン内の組織内アカウント全体で集計されたすべてのインスタンスのデータを表示できます。

特定のサブスクリプションのインスタンスについて検出されたデータを表示するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインにある [Linux サブスクリプション] で、[サブスクリプション] を選択します。
3. [サブスクリプション名] 列で、データを表示したいサブスクリプションを選択します。
4. [インスタンス] タブを選択し、必要に応じてコンソールでデータを確認します。以下でデータをフィルタリングできます。

- [インスタンス ID]
 - アカウント
 - [リージョン]
 - AMI ID
 - 使用オペレーション
 - 製品コード
5. (オプション) ビューを にエクスポート CSV を選択して、このサブスクリプションを持つインスタンスのデータをカンマ区切り値ファイル () としてエクスポートします CSV。

License Manager での Linux サブスクリプションの請求情報

Amazon で実行されている各商用 Linux サブスクリプション EC2 には、Amazon マシンイメージ () に関連付けられた請求情報があります AMI。商用 Linux サブスクリプションには、Amazon EC2 の使用オペレーションがあります。AWS Marketplace 製品コード、またはその両方の組み合わせ。詳細については、Linux インスタンス用 Amazon Elastic Compute Cloud ユーザーガイドの [AMI 請求情報 フィールド](#) と、 [AMI の製品コード](#) を参照してください。AWS Marketplace 販売者ガイド

サブスクリプション名	Amazon EC2 使用状況オペレーション	AWS Marketplace 製品コード	サブスクリプションタイプ
Red Hat Enterprise Linux サーバー BYOS	RunInstances:00g0	x	Bring Your Own Subscription モデル (BYOS)
Red Hat Enterprise Linux Server	RunInstances:0010	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux with High Availability Add-on	RunInstances:1010	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux と SQL Server Standard および High Availability	RunInstances:1014	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux with SQL Server Enterprise および High Availability	RunInstances:1110	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux と SQL Server Standard	RunInstances:0014	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux と SQL Server Web	RunInstances:0210	x	EC2 サブスクリプション込み
Red Hat Enterprise Linux と SQL Server Enterprise	RunInstances:0110	x	EC2 サブスクリプション込み
SUSE Linux エンタープライズサーバー	RunInstances:000g	x	EC2 サブスクリプション込み

サブスクリプション名	Amazon EC2 使用状況オペレーション	AWS Marketplace 製品コード	サブスクリプションタイプ
Red Hat Enterprise Linux for SAP with High Availability and Update Services	RunInstances:0010	✓	AWS Marketplace サブスクリプション 1
SUSE を使用する Linux Enterprise Server SAP	✗	✓	AWS Marketplace サブスクリプション
Ubuntu Pro	RunInstances:0g00	✓	AWS Marketplace サブスクリプション
Red Hat Enterprise Linux Workstation	✗	✓	AWS Marketplace サブスクリプション

1 このサブスクリプションには、Amazon EC2の使用オペレーションと AWS Marketplace 製品コード。

Linux サブスクリプションの使用状況メトリクス

Linux サブスクリプションでは以下のメトリクスとディメンションを使用できます。

メトリクス	説明
RunningInstancesCount	<p>現在のアカウントで実行されているインスタンスのうち、サブスクリプション名、またはサブスクリプション名とリージョンでグループ化されたインスタンスの総数。</p> <p>単位: カウント</p> <p>ディメンション:</p> <p>SubscriptionName : サブスクリプションの名前。</p>

メトリクス	説明
	Region: 商用の Linux サブスクリプションを使用しているリソースが検出されたリージョン。

License Manager で Linux サブスクリプションの Amazon CloudWatch アラームを管理する

License Manager コンソールの Linux サブスクリプションリストページには、License Manager がインスタンスで検出した各 Linux サブスクリプションに対して設定した Amazon CloudWatch アラームなど、次の主要な詳細が表示されます。

- サブスクリプション名
- サブスクリプションタイプ
- サブスクリプションあたりの実行中のインスタンスの数
- 設定された Amazon CloudWatch アラーム

リストから Linux サブスクリプションを選択すると、使用状況メトリクスとアラームタブにそのサブスクリプションのデータが表示されます。このタブでは、選択したサブスクリプションの Amazon CloudWatch ダッシュボードが License Manager コンソールに表示されます。選択した日付から特定の期間、または評価範囲 (時間、日、または 1 週間) が表示されるようにダッシュボードを調整できます。

使用状況メトリクスとアラーム タブでは、各サブスクリプションにアラームセクションがあり、以下の詳細が表示されます。

- アラーム名 - アラームの名前。
- 状態 - アラームの状態。
- デイメンション - アラームのデイメンション。デイメンションには が含まれます。AWS リージョン および定義されたインスタンスタイプ。
- 条件 - アラームの条件。条件には、比較演算子と定義されたアラームしきい値が含まれます。

現在のサブスクリプション使用率に基づいて追跡およびアラートを実行するために定義したデイメンションと条件を使用して CloudWatch アラームを作成できます。Linux サブスクリプションコンソー

ルには、使用中のサブスクリプション名、サブスクリプションタイプ、それぞれの実行インスタンス数、アラームステータスの概要が表示されます。

考えられる CloudWatch アラーム状態は次のとおりです。

- OK - メトリクスや式は、定義されているしきい値の範囲内です。
- ALARM - メトリクスまたは式が定義されたしきい値を超えています。
- INSUFFICIENT_DATA - アラームが開始されたばかりであるか、メトリクスが利用できないか、メトリクスがアラームの状態を判断するのに十分なデータがありません。

トピック

- [Linux サブスクリプションの CloudWatch アラームを作成する](#)
- [Linux サブスクリプションの CloudWatch アラームを変更する](#)
- [Linux サブスクリプションの CloudWatch アラームを削除する](#)

Linux サブスクリプションの CloudWatch アラームを作成する

実行中の EC2 インスタンスで検出した商用 Linux サブスクリプションごとにアラームを作成できます。必要に応じて、サブスクリプションごとにディメンションや条件が異なる複数のアラームを作成できます。

コンソールから Linux サブスクリプションの CloudWatch アラームを作成するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインにある [Linux サブスクリプション] で、[サブスクリプション] を選択します。
3. [サブスクリプション名] 列で、アラームを作成するサブスクリプションを選択し、[アラームの作成] を選択します。
4. アラームの以下の項目を指定します。
 - アラーム名 - 名前を指定します (例: AWS-LM-LS-*AlarmName*)。
 - インスタンスタイプ - 選択したサブスクリプションを使用するインスタンスタイプを選択します。
 - 使用状況のリージョン - アラームを作成するリージョンを選択します。
 - 比較演算子 - アラームしきい値の比較演算子。

- アラームのしきい値 - アラームのしきい値の値。
5. [作成] を選択して、アラームを作成します。

Linux サブスクリプションの CloudWatch アラームを変更する

License Manager コンソールから既存の CloudWatch アラームを変更して、要件の変化に対応できません。

コンソールから Linux サブスクリプションの CloudWatch アラームを変更するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインにある [Linux サブスクリプション] で、[サブスクリプション] を選択します。
3. [サブスクリプション名] 列で、変更するサブスクリプションを選択し、[編集] を選択します。
4. 必要に応じて定義された値を変更します。
5. [編集] を選択してアラームを変更します。

Linux サブスクリプションの CloudWatch アラームを削除する

License Manager コンソールから既存の CloudWatch アラームを削除して、要件の変化に対応できません。

コンソールから Linux サブスクリプションの CloudWatch アラームを削除するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインにある [Linux サブスクリプション] で、[サブスクリプション] を選択します。
3. [サブスクリプション名] 列で、変更するサブスクリプションを選択し、[削除] を選択します。

License Manager の設定

の設定セクション AWS License Manager コンソールには、現在のアカウントの設定が表示されます。関連する機能を有効にするには、設定を構成する必要があります。

Managed licenses

マネージドライセンスでは、以下の設定が可能です。

- 組織へのマネージドエンタイトルメントとセルフマネージドライセンスの配布
- クロスアカウントリソース検出
- Amazon SNS通知

詳細については、「[License Manager のマネージドライセンス設定](#)」を参照してください。

Linux subscriptions

以下の設定は Linux サブスクリプションで設定できます。

- 商用 Linux ライセンスサブスクリプションデータの検出と集約
- Linux サブスクリプションの Red Hat Subscription Manager (RHSM) 検出

詳細については、「[License Manager の Linux サブスクリプション設定](#)」を参照してください。

User-based subscriptions

以下の設定は、ユーザーベースのサブスクリプションに対して設定できます。

- AWS Managed Microsoft AD
- 仮想プライベートクラウド (VPC)

詳細については、「[License Manager のユーザーベースのサブスクリプション設定](#)」を参照してください。

Delegated administration

このタブは、アカウントに組織の管理アクセス権がある場合に表示されます。管理者として、から委任された管理者を登録できます。AWS CLI または AWS Management Console。詳細については、「」を参照してください[License Manager の委任管理者設定](#)。

設定のトピック

- [License Manager の設定を編集する](#)
- [License Manager のマネージドライセンス設定](#)
 - [アカウントの詳細](#)
 - [クロスアカウントリソース検出](#)
 - [Simple Notification Service \(SNS \)](#)
- [License Manager の Linux サブスクリプション設定](#)

- [Linux サブスクリプションの設定](#)
- [Red Hat Subscription Manager の検出](#)
- [License Manager のユーザーベースのサブスクリプション設定](#)
 - [AWS Managed Microsoft AD](#)
 - [仮想プライベートクラウド](#)
- [License Manager の委任管理者設定](#)
 - [委任 License Manager 管理者でサポートされているリージョン](#)
 - [委任 License Manager 管理者を登録する](#)
 - [委任 License Manager 管理者の登録を解除する](#)

License Manager の設定を編集する

License Manager の設定を編集するには、次の手順に従います。

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインの [設定] を選択します。
3. 設定を含むタブを選択します。例えば、[マネージドライセンス] を選択して [アカウントの詳細] を設定します。
4. 設定が完了したら、保存 を選択するか、キャンセル を選択してバックアウトします。

License Manager のマネージドライセンス設定

マネージドライセンスでは次の設定が利用できます。

アカウントの詳細

アカウントの詳細を確認して、アカウントタイプ、アカウントが であるかどうかなどの情報を表示できます。AWS Organizations リンクされている、アカウントの License Manager S3 バケット ARN、および AWS Resource Access Manager を共有しますARN。このセクションでは、 をリンクすることもできます。AWS Organizations アカウント。

マネージドエンタイトルメントまたはセルフマネージドライセンスを組織内に配布するには、リンクを選択します。AWS Organizations アカウント。マネージドエンタイトルメントの配布されたグラントは、すべてのメンバーアカウントによって自動的に受け入れられます。このオプションを選択すると、[管理者](#)アカウントと[メンバー](#)アカウントにサービス連動型のロールが追加されます。

Note

このオプションを有効にするには、管理アカウントにサインインし、すべての機能を有効にする必要があります。AWS Organizations。詳細については、[の「組織内のすべての機能の有効化」](#)を参照してください。AWS Organizations ユーザーガイド。

この選択により、も作成されます。AWS Resource Access Manager 管理アカウントのリソース共有。セルフマネージドライセンスをシームレスに共有できます。詳細については、[『』](#)を参照してください。AWS Resource Access Manager ユーザーガイド。

このオプションを無効にするには、[UpdateServiceSettings](#) を呼び出しますAPI。

クロスアカウントリソース検出

クロスアカウントリソース検出を有効にして、のすべてのアカウントでライセンスの使用を管理できます。AWS Organizations。

組織でクロスアカウントリソース検出を有効にするには、クロスアカウントリソース検出の [有効化] を選択します。クロスアカウントリソース検出を有効にすると、AWS Organizations は、すべてのアカウントでリソース検出を実行するために自動的にリンクされます。

License Managerは[Systems Manager](#)のインベントリを使用してソフトウェアの使用状況を検出します。お客様のすべてのリソース上に、Systems Managerのインベントリが設定されていることを確認します。Systems Manager インベントリを照会するには、次のものが重要です:

- Amazon S3 バケットにインベントリを格納する[リソースデータリンク](#)。
- [Amazon Athena](#) でアカウントからインベントリデータを集約するには AWS Organizations。
- [AWS Glue](#) では高速クエリエクスペリエンスを提供します。

Note

以下ようになります AWS リージョン 不要 Amazon Athena または AWS Glue Systems Manager インベントリのインベントリデータをクエリまたは集計して、ソフトウェアの使用を検出するには :

- アジアパシフィック (ジャカルタ)
- イスラエル (テルアビブ)

Simple Notification Service (SNS)

License Manager から通知とアラートを受信するSNSように Amazon を設定できます。

Amazon SNSトピックを設定するには

1. Simple Notification Service (SNS) の横にある編集を選択します。
2. SNS トピックを次の形式で指定ARNします。

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

3. [Save changes] (変更の保存) をクリックします。

License Manager の Linux サブスクリプション設定

検出プロセス中に、License Manager は で実行されているEC2インスタンスを検索します。AWS アカウント Linux サブスクリプション用の 。インスタンスに複数の Linux サブスクリプションが定義されているかどうかを検出し、データを集約します。

Linux サブスクリプションの設定

Linux サブスクリプションの設定を設定して、License Manager が検出と集約を処理する方法を制御できます。デフォルトの検出設定は、すべてのタイプの Linux サブスクリプションに適用されます。

Linux サブスクリプション検出の設定には、次のアクションを使用できます。

[Edit] (編集)

Linux サブスクリプション検出の設定を変更します。

非アクティブ化

EC2 インスタンスに関連付けられた Linux サブスクリプションの検出と集約を無効にします。Red Hat Subscription Manager でも検出を有効にしている場合、License Manager はまずRHSM登録されたプロバイダーを非アクティブ化し、Linux サブスクリプション検出の非アクティブ化を続行します。

Note

非アクティブ化は、Red Hat Subscription Manager () のアクセスシークレットには影響しませんRHSM。の料金を回避するには AWS 不要になった関連付けられたシークレット

の請求については、[「の削除」](#)を参照してください。AWS Secrets Manager のシークレット AWS Secrets Manager ユーザーガイド。

Linux サブスクリプション検出用の License Manager コンソールには、次の設定が表示されます。

Linux サブスクリプション検出設定

Linux サブスクリプション検出

アカウントの Linux サブスクリプション検出をアクティブ化したかどうかを示します。

ソース AWS リージョン

AWS リージョン License Manager でサブスクリプションデータを検出する場所。

AWS Organizations

オプションで、のアカウント全体でサブスクリプションデータを集約する AWS Organizations.

詳細については、「[License Manager で Linux サブスクリプションを管理する](#)」を参照してください。

Red Hat Subscription Manager の検出

Linux サブスクリプション検出を有効にしている場合は、License Manager のアクセスを設定して、Red Hat Subscription Manager () で管理RHELされるサブスクリプションの追加データを取得できますRHSM。

RHSM サブスクリプション検出の設定には、次のアクションを使用できます。

タグの編集

アクセスシークレットに関連付けられているタグを変更します。

Note

RHSM サブスクリプションに他の変更を加える必要がある場合は、まず現在の登録を非アクティブ化してから、新しい登録を設定する必要があります。

非アクティブ化

RHSM 登録されたプロバイダーを非アクティブ化します。

Note

非アクティブ化は、Red Hat Subscription Manager () のアクセスシークレットには影響しませんRHSM。の料金を回避するには AWS 不要になった関連付けられたシークレットの請求については、[「の削除」を参照してください。AWS Secrets Manager のシークレット](#) AWS Secrets Manager ユーザーガイド。

License Manager コンソールには、RHSM検出のために以下の設定が表示されます。

Red Hat Subscription Manager の検出設定

検出ステータス

RHSM サブスクリプションの検出を有効にしたかどうかを示します。

シークレット名

のRHSMアクセスシークレットへのリンク AWS Secrets Manager Red Hat オフライントークンを含む。License Manager は、このシークレットを使用して新しい一時アクセストークンを生成し、Red Hat Subscription Manager () にサブスクリプションデータをリクエストしますRHSM。

Secrets Manager を使用して、既存のシークレットを変更できます。シークレットのタグやその他のメタデータを更新するには、[「の変更」を参照してください。AWS Secrets Manager のシークレット](#) AWS Secrets Manager ユーザーガイド。シークレット値を更新するには、[「の値を更新する」を参照してください。AWS Secrets Manager シークレット](#)。

に同期された最後のデータ

登録された Red Hat Subscription Manager (RHSM) アカウントからのサブスクリプションデータの最終更新成功からのタイムスタンプ。

タグ

License Manager が Secrets Manager のRHSMアクセスシークレットに割り当てるタグのキーと値のペアを定義できます。RHSM アクセスシークレットを取得および復号するには、License

Manager のサービスにリンクされたロールポリシーに、シークレット、および関連する [タグ](#) が必要です。AWS KMS key、次のタグが割り当てられます。

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

License Manager が登録プロセス中にシークレットを作成した場合、タグは自動的に割り当てられます。オフライントークン用に独自のシークレットを作成する場合は、そのタグをシークレットに割り当て、暗号化されている場合は関連するKMSキーに割り当ててください。タグを追加するには、[「の変更」を参照してください。AWS Secrets Manager のシークレット](#) AWS Secrets Manager ユーザーガイド。

License Manager のユーザーベースのサブスクリプション設定

ユーザーベースのサブスクリプションに必要な製品に応じて、以下の設定が可能です。

AWS Managed Microsoft AD

License Manager には [必要です](#) AWS Managed Microsoft AD ユーザーベースのサブスクリプションを使用する前に設定する必要があります。詳細については、[「サポートされているソフトウェア製品の License Manager ユーザーベースのサブスクリプションを使用する」](#)を参照してください。

仮想プライベートクラウド

License Manager では、[に加えて](#) [を設定VPCする必要がある](#)。AWS Managed Microsoft AD、Microsoft Office でユーザーベースのサブスクリプションを使用する場合。詳細については、[「サポートされているソフトウェア製品の License Manager ユーザーベースのサブスクリプションを使用する」](#)を参照してください。

License Manager の委任管理者設定

委任管理者を登録して、License Manager でマネージドライセンスと Linux サブスクリプションの管理タスクを行うことができます。管理を簡単にするために、License Manager コンソールを使用して、License Manager の各機能に 1 人の委任管理者を登録することをお勧めします。このアプローチを使用すると、License Manager の組織内に 1 人の委任された管理者がいます。

以下を使用 AWS CLI または [ではSDKs](#)、License Manager のサポートされている機能ごとに、組織内の異なるメンバーアカウントを委任管理者として登録できます。これにより、組織内のさまざまなメンバーアカウントがマネージドライセンスと Linux サブスクリプションの管理タスクを実行できるようになります。

⚠ Important

License Manager コンソールの委任管理機能を使用するには、License Manager の各機能に、同じメンバーアカウントを委任管理者として登録する必要があります。委任管理者として複数のメンバーアカウントを登録した場合は、まず既存のメンバーアカウントの登録を解除してから、License Manager の各機能に同じアカウントを登録する必要があります。

委任管理者を登録する前に、組織で信頼できるアクセスを有効にする必要があります。詳細については、「[の招待](#)」を参照してください。[AWS アカウントを組織に参加させ、で信頼されたアクセスを有効にする AWS Organizations.](#)

委任管理者を登録できる機能は次のとおりです。

マネージドライセンス

他のメンバーアカウントとのセルフマネージドライセンスの共有、クロスアカウントリソース検出の実行、マネージドエンタイトルメントの他のメンバーアカウントへの配布などの管理タスクを実行できます。

Linux サブスクリプション

所有および実行する商用 Linux サブスクリプションの表示や管理などの管理タスクを実行できます。AWS リージョン と のアカウント AWS Organizations。Linux サブスクリプションの Amazon CloudWatch アラームを作成および管理することもできます。データを License Manager コンソールに表示するには、まずデータを検出して集計する必要があります。また、設定されている場合、任意のアラームが機能します。

⚠ Important

登録すると、委任管理者は組織内のアカウントが所有するEC2インスタンスを可視化できません。

を使用して、委任された管理者を登録および登録解除できます。[AWS License Manager コンソール](#)、[AWS CLI](#), または [AWS SDKs](#).

委任 License Manager 管理者でサポートされているリージョン

以下のリージョンは License Manager の委任管理者をサポートしています。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- アジアパシフィック (香港)
- 中東 (バーレーン)
- カナダ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 欧州 (ミラノ)
- アフリカ (ケープタウン)
- 南米 (サンパウロ)

委任 License Manager 管理者を登録する

委任された管理者は、 を使用して登録できます。AWS CLI または AWS Management Console.

Console

を使用して委任管理者を登録するには AWS License Manager コンソールで、次の手順を実行します。

1. にサインインする AWS 管理アカウントの管理者として。
2. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。

3. 左のナビゲーションペインから [設定] を選択します。
4. [委任管理] タブを選択します。
5. [Register delegated administrator (委任管理者の登録)] を選択します。
6. メンバーアカウント ID を入力して委任管理者として登録し、License Manager に必要なアクセス許可を付与することを確認して、[登録] を選択します。
7. 指定されたアカウントが License Manager の委任管理者として正常に登録されたことを示すメッセージが表示されます。

AWS CLI

を使用してマネージドライセンスの委任管理者を登録するには AWS CLI、次の手順を実行します。

1. コマンドラインから、以下を実行します。AWS CLI コマンド:

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

2. 次のコマンドを実行して、指定されたメンバーアカウントが委任された管理者として正常に登録されていることを確認します。

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

を使用して Linux サブスクリプションの委任管理者を登録するには AWS CLI、次の手順を実行します。

1. コマンドラインから、以下を実行します。AWS CLI コマンド:

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

2. 次のコマンドを実行して、指定されたメンバーアカウントが委任された管理者として正常に登録されていることを確認します。

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

委任 License Manager 管理者の登録を解除する

委任された管理者の登録は、を使用して解除できます。AWS CLI または AWS Management Console.

Console

を使用して委任された管理者の登録を解除するには AWS License Manager コンソールで、次の手順を実行します。

1. にサインインする AWS 管理アカウントの管理者として。
2. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
3. 左のナビゲーションペインから [設定] を選択します。
4. [委任管理] タブを選択します。
5. [削除] を選択します。
6. License Manager の委任管理者を削除することを確認するテキスト **remove** を入力し、[削除] を選択します。
7. 指定されたアカウントで License Manager の委任管理者が正常に削除されたことを示すメッセージが表示されます。

AWS CLI

を使用してマネージドライセンスの委任管理者の登録を解除するには AWS CLI、次の手順を実行します。

1. コマンドラインから、以下を実行します。AWS CLI コマンド:

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

2. 次のコマンドを実行して、指定したアカウントの委任管理者としての登録が解除されたことを確認します。

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

を使用して Linux サブスクリプションの委任管理者の登録を解除するには AWS CLI、次の手順を実行します。

1. コマンドラインから、以下を実行します。AWS CLI コマンド:

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

2. 次のコマンドを実行して、指定したアカウントの委任管理者としての登録が解除されたことを確認します。

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

登録解除されたアカウントはいつでも再登録できます。

License Managerのダッシュボード

License Manager コンソールの Dashboard セクションには、以下に関連するライセンス消費を追跡するために使用できる使用状況の詳細が表示されます。

- セルフマネージドライセンス
- ライセンス付与資格
- ユーザーベースのサブスクリプションのサブスクライブされたユーザー
- インスタンスの実行

ダッシュボードにはまた、ライセンスルール違反によるアラートも表示されます。

概要

概要セクションには、ライセンスに関する以下の詳細が表示されます。

ライセンスの付与

この地域でこのアカウントに付与されたライセンスの総数。

セルフマネージドライセンス

この地域でこのアカウントに付与されたセルフマネージドライセンスの総数。

販売者が発行したライセンス

この地域でこのアカウントに付与された販売者が発行したライセンスの総数。

製品

[製品] セクションには、ユーザーベースのサブスクリプションに関する以下の詳細が表示されます。

製品名

ユーザーベースのサブスクリプションの製品名。

サブスクライブユーザー

製品のサブスクライブユーザーの数。

ライセンス付与資格

[付与されたライセンス資格] セクションには、以下の詳細が記載されています。

製品名

付与されたライセンスの製品名。

エンタイトルメント

使用権限の名前。

使用方法

使用権限の利用状況。

セルフマネージドライセンス

セルフマネージドライセンスには、以下の詳細が記載されています。

ライセンス名

セルフマネージドライセンスの名前。

エンタイトルメント

使用権限の名前。

使用方法

使用権限の利用状況。

インスタンスの使用状況

[インスタンスの使用状況] セクションには、以下の詳細が記載されています。

実行中のインスタンスの数

この地域内のこのアカウントで実行中のインスタンスの総数。

実行中のインスタンスの集計数

のすべてのアカウントで集計された実行中のインスタンスの合計 AWS Organizations このリージョンの。このグラフは、管理アカウントおよび委任された管理者アカウントにのみ表示されません。

License Manager のモニタリング

で追跡されるライセンスとサブスクリプションの使用状況をモニタリングできます。AWS License Manager Amazon を使用する CloudWatch。CloudWatch は raw データを収集し、読み取り可能なほぼリアルタイムのメトリクスに加工します。特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「[Amazon での License Manager ライセンス使用状況のモニタリング CloudWatch](#)」を参照してください。

によって行われた、または に代わって行われたAPI呼び出しや関連イベントをキャプチャできます。AWS アカウント を使用する AWS CloudTrail。イベントはログファイルとしてキャプチャされ、指定した Amazon S3 バケットに配信されます。が呼び出したユーザーとアカウントを特定できます。AWS、呼び出し元の送信元 IP アドレス、および呼び出しの発生日時。詳細については、「[ログ記録 AWS License Manager API を使用した 呼び出し AWS CloudTrail](#)」を参照してください。

目次

- [Amazon での License Manager ライセンス使用状況のモニタリング CloudWatch](#)
 - [Secrets Manager のメトリクスを監視するアラームを作成する](#)
- [ログ記録 AWS License Manager API を使用した 呼び出し AWS CloudTrail](#)
 - [の License Manager 情報 CloudTrail](#)
 - [ライセンスLicense Managerのログ・ ファイルエントリーについて](#)

Amazon での License Manager ライセンス使用状況のモニタリング CloudWatch

Amazon を使用して License Manager のメトリクス統計をモニタリングできます CloudWatch。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をよりの確に把握できます。特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。例えば、LicenseConfigurationUsagePercentage メトリクスを使用してライセンスの割合を監視し、制限を超える前に対策を講じることができます。詳細については、「[Amazon ユーザーガイド CloudWatch](#)」を参照してください。

License Manager は、AWSLicenseManager/licenseUsage の名前空間で毎時以下のメトリクスを出力します。

メトリクス	説明
RunningInstancesCount	<p>現在のアカウントで実行されているインスタンスのうち、サブスクリプション名でグループ化されたインスタンスの総数。</p> <p>単位: カウント</p> <p>ディメンション:</p> <p>SubscriptionName : サブスクリプションの名前。</p>
AggregateRunningInstancesCount	<p>のすべてのアカウントで実行されているインスタンスの集計合計数 AWS Organizations 現在の の AWS リージョン。</p> <p>単位: カウント</p> <p>ディメンション:</p> <p>SubscriptionName : サブスクリプションの名前。</p>
TotalLicenseConfigurationUsageCount	<p>使用可能なライセンス設定の総数。</p> <p>単位: カウント</p> <p>ディメンション:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : ライセンス設定の Amazon リソースネーム (ARN)。 LicenseConfigurationType : ライセンス設定のタイプ。
LicenseConfigurationUsageCount	<p>この設定の使用済みライセンスの総数。</p> <p>単位: カウント</p> <p>ディメンション:</p> <ul style="list-style-type: none"> LicenseConfigurationArn : ライセンス設定 ARN。 LicenseConfigurationType : ライセンス設定のタイプ。
LicenseConfigurationUsagePercentage	<p>このライセンス設定の使用済みライセンスをパーセンテージで表したものの。</p>

メトリクス	説明
	単位: パーセント
	ディメンション:
	<ul style="list-style-type: none">LicenseConfigurationArn : ライセンス設定 ARN。LicenseConfigurationType : ライセンス設定のタイプ。

Secrets Manager のメトリクスを監視するアラームを作成する

メトリクスの値が変更され、CloudWatch アラームの状態が変化したときに Amazon Simple Notification Service (Amazon SNS) メッセージを送信するアラームを作成できます。アラームは、指定期間にわたって単一のメトリクスを監視し、指定したしきい値に対応したメトリクスの値に基づいて、数期間にわたってアクションを実行します。アラームは、持続する状態変化に対してのみアクションを呼び出します。CloudWatch アラームは、特定の状態にあるという理由だけではアクションを呼び出しません。状態が変更され、指定された期間にわたって維持されている必要があります。詳細については、「[アラームの使用 CloudWatch](#)」を参照してください。

ログ記録 AWS License Manager API を使用した 呼び出し AWS CloudTrail

AWS License Manager は と統合されています。AWS CloudTrail、ユーザー、ロール、またはによって実行されたアクションを記録するサービス AWS License Manager の サービス。License Manager のすべてのAPI呼び出しをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出しには、License Manager コンソールからの呼び出しと、License Manager APIオペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、License Manager の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールのイベント履歴で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、License Manager に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「」を参照してください。 [AWS CloudTrail ユーザーガイド](#)。

トピック

- [の License Manager 情報 CloudTrail](#)
- [ライセンスLicense Managerのログ・ファイルエントリーについて](#)

の License Manager 情報 CloudTrail

CloudTrail が有効になっている AWS アカウント アカウントを作成するとき。License Manager でアクティビティが発生すると、そのアクティビティは他のとともに CloudTrail イベントに記録されます。AWS イベント履歴のサービスイベント。で最近のイベントを表示、検索、ダウンロードできます。AWS アカウント。詳細については、[「イベント履歴で CloudTrail イベントを表示する」](#)を参照してください。

のイベントを継続的に記録するには AWS アカウント License Manager のイベントを含む は、証跡を作成します。証跡により CloudTrail、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべてのに適用されます。AWS リージョン。証跡は、内のすべてのリージョンからのイベントをログに記録します。AWS パーティション分割し、指定した Amazon S3 バケットにログファイルを配信します。さらに、他の AWS は、CloudTrail ログで収集されたイベントデータをさらに分析し、それに基づいて行動するためのサービスです。詳細については、次を参照してください:

- [追跡を作成するための概要](#)
- [CloudTrail がサポートするサービスと統合](#)
- [の Amazon SNS通知の設定 CloudTrail](#)
- [複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信](#)

License Manager のすべてのアクションは によってログに記録 CloudTrail され、 に文書化されます。 [AWS License Manager API リファレンス](#)。例えば、`ListResourceInventory`および `DeleteLicenseConfiguration`アクションへの呼び出しは `CreateLicenseConfiguration`、CloudTrail ログファイルにエントリを生成します。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが root または で行われたかどうか AWS Identity and Access Management (IAM) ユーザー認証情報。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の によって行われたかどうか AWS サービス。

詳細については、[CloudTrail userIdentity 「」要素](#)を参照してください。

ライセンスLicense Managerのログ・ファイルエントリーについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。CloudTrail ログファイルはパブリックAPIコールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、DeleteLicenseConfigurationアクションを示す CloudTrail ログエントリを示しています。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIF2U5EXAMPLEH5AP6",
    "arn": "arn:aws:iam::123456789012:user/Administrator",
    "accountId": "012345678901",
    "accessKeyId": "AKIDEXAMPLE",
    "userName": "Administrator"
  },
  "eventTime": "2019-02-15T06:48:37Z",
  "eventSource": "license-manager.amazonaws.com",
  "eventName": "DeleteLicenseConfiguration",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.83",
  "userAgent": "aws-cli/2.4.6 Python/3.8.8 Linux",
  "requestParameters": {
    "licenseConfigurationArn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
  },
  "responseElements": null,
  "requestID": "3366df5f-4166-415f-9437-c38EXAMPLE48",
  "eventID": "6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

License Manager のセキュリティ

でのクラウドセキュリティ AWS が最優先事項です。として AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、間で共有される責任です。AWS とユーザー。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、が実行するインフラストラクチャを保護する責任があります。AWS の サービス AWS クラウド。AWS は、安全に使用できる サービスも提供します。サードパーティーの監査者は、の一環として、当社のセキュリティの有効性を定期的にテストおよび検証します。[AWS コンプライアンスプログラム](#)。License Manager に適用されるコンプライアンスプログラムの詳細については、「」を参照してください。[AWS コンプライアンスプログラムによる対象範囲内のサービス](#)。
- クラウド内のセキュリティ — お客様の責任は によって決まります。AWS 使用する サービス。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、License Manager 使用時における責任共有モデルの適用法を理解するのに役立ちます。ここでは、セキュリティとコンプライアンスの目標を満たすように License Manager を設定する方法について説明します。また、他の の使用方法についても説明します。AWS License Manager リソースのモニタリングと保護に役立つ のサービス。

内容

- [License Manager でのデータ保護](#)
- [License Manager の ID とアクセスの管理](#)
- [License Manager のサービスにリンクされたロールの使用](#)
- [AWS License Manager の マネージドポリシー](#)
- [License Manager でのライセンスの暗号化署名](#)
- [License Manager のコンプライアンス検証](#)
- [License Manager の耐障害性](#)
- [License Manager のインフラストラクチャセキュリティ](#)
- [を使用した License Manager とインターフェイス VPC エンドポイント AWS PrivateLink](#)

License Manager でのデータ保護

- AWS [責任共有モデル](#)、でのデータ保護に適用されます。AWS License Manager。このモデルで説明されているように、AWS は、すべての を実行するグローバルインフラストラクチャを保護する責任があります。AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツの制御を維持する責任があります。また、 のセキュリティ設定と管理タスクについても責任を負います。AWS のサービス 使用する。データプライバシーの詳細については、「[データプライバシーFAQ](#)」を参照してください。欧州でのデータ保護の詳細については、「」を参照してください。[AWS の責任共有モデルとGDPR](#) ブログ記事 AWS セキュリティブログ。

データ保護の目的で、 を保護することをお勧めします。AWS アカウント 認証情報と を使用して個々のユーザーをセットアップする AWS IAM Identity Center または AWS Identity and Access Management (IAM)。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して と通信する AWS リソースの使用料金を見積もることができます。1TLS.2 が必要で、1.3 TLS をお勧めします。
- で APIとユーザーアクティビティのログ記録を設定する AWS CloudTrail。CloudTrail 証跡を使用してキャプチャする方法については、「」を参照してください。AWS アクティビティ、「」の「[証 CloudTrail 跡の使用](#)」を参照してください。AWS CloudTrail ユーザーガイド。
- 使用アイテム AWS 暗号化ソリューションと 内のすべてのデフォルトのセキュリティコントロール AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- アクセス時に FIPS 140-3 検証済みの暗号化モジュールが必要な場合 AWS コマンドラインインターフェイスまたは を介してAPI、FIPSエンドポイントを使用します。利用可能なFIPSエンドポイントの詳細については、「[連邦情報処理規格 \(FIPS\) 140-3](#)」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これには、License Manager またはその他の を使用する場合も含まれます。AWS のサービス コンソール、API、AWS CLI、または AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

保管中の暗号化

License Managerは、管理アカウントのAmazon S3バケットにデータを保存します。バケットは、Amazon S3 マネージド暗号化キー (SSE-S3) を使用して設定されます。

License Manager の ID とアクセスの管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御するのに役立つ AWS サービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM を使用すると、AWS アカウントの下にユーザーとグループを作成できます。ユーザーが AWS リソースを使用してタスクを実行するために必要なアクセス許可を制御します。追加料金IAMなしで 使用できます。

デフォルトでは、ユーザーには License Manager のリソースおよびオペレーションのための許可がありません。ユーザーに License Manager リソースの管理を許可するには、明示的にアクセス許可を付与するIAMポリシーを作成する必要があります。

ポリシーをユーザーまたはユーザーのグループにアタッチする場合、ポリシーによって特定リソースの特定タスクを実行するユーザーの権限が許可または拒否されます。詳細については、IAM「[ユーザーガイド](#)」の「[ポリシーとアクセス許可](#)」を参照してください。

ユーザー、グループ、ロールを作成する

のユーザーとグループを作成し AWS アカウント、必要なアクセス許可を割り当てることができます。ベストプラクティスとして、ユーザーはIAMロールを引き受けてアクセス許可を取得する必要があります。AWS アカウントのユーザーとグループを設定する方法の詳細については、「[License Manager の使用を開始する](#)」を参照してください。

[IAM ロール](#)は、特定のアクセス許可を持つアカウントで作成できる IAM ID です。IAM ロールは、で AWS ID ができることとできないことを決定するアクセス許可ポリシーを持つ ID であるという点で、IAMユーザーと似ています AWS。ただし、ユーザーは 1 人の特定の人に一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。

IAM ポリシー構造

IAM ポリシーは、1 つ以上のステートメントで構成されるJSONドキュメントです。各ステートメントの構成は以下のとおりです。

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

様々な要素がステートメントを構成しています

- [Effect]:effect は、AllowまたはDenyにすることができます。デフォルトでは、ユーザーにはリソースとAPIオペレーションを使用するアクセス許可がないため、すべてのリクエストは拒否されます。明示的な許可はデフォルトに上書きされます。明示的な拒否はすべての許可に上書きされません。
- アクション:アクションは、アクセス許可を付与または拒否する特定のAPIオペレーションです。
- [リソース]:リソースはアクションの影響を受けます。License Manager APIオペレーションによっては、オペレーションによって作成または変更できる特定のリソースをポリシーに含めることができます。ステートメントでリソースを指定するには、その Amazon リソースネーム () を使用する必要がありますARN。詳細については、[「で定義されるアクション AWS License Manager」](#)を参照してください。
- Condition] (条件): condition はオプションです。ポリシーの発効条件を指定するために使用します。詳細については、[「AWS License Managerの条件キー」](#)を参照してください。

License Manager のIAMポリシーを作成する

IAM ポリシーステートメントでは、をサポートする任意のサービスから任意のAPIオペレーションを指定できますIAM。License Manager では、APIオペレーションの名前で次のプレフィックスを使用します。

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

例:

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

使用可能な License Manager の詳細についてはAPIs、以下のAPIリファレンスを参照してください。

- [AWS License Manager API リファレンス](#)
- [AWS License Manager ユーザーサブスクリプションAPIリファレンス](#)
- [AWS License Manager Linux サブスクリプションAPIリファレンス](#)

単一のステートメントに複数のオペレーションを指定するには、次のようにコンマで区切ります。

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

ワイルドカードを使用して複数のオペレーションを指定することもできます。例えば、次のように、名前が List という単語で始まるすべての License Manager APIオペレーションを指定できます。

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

すべての License Manager APIオペレーションを指定するには、次のように * ワイルドカードを使用します。

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

License Manager ISVを使用する のポリシーの例

ISVs License Manager を介してライセンスを配布するには、次のアクセス許可が必要です。

```
{
  "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": "*"
}
]
```

ユーザー、グループ、およびロールに許可を付与する

必要なIAMポリシーを作成したら、これらのアクセス許可をユーザー、グループ、ロールに付与する必要があります。

アクセス権限を付与するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- のユーザーとグループ AWS IAM Identity Center :

アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「[権限設定を作成する](#)」の手順に従ってください。

- ID プロバイダーIAMを介してで管理されるユーザー :

ID フェデレーションのロールを作成します。IAM ユーザーガイドの「[サードパーティー ID プロバイダー \(フェデレーション\) のロールを作成する](#)」の指示に従います。

- IAM ユーザー :

- ユーザーが担当できるロールを作成します。「[ユーザーガイド](#)」のIAM「[ユーザーのロールを作成する](#)」の手順に従います。IAM

- (お奨めできない方法) ポリシーをユーザーに直接アタッチするか、ユーザーをユーザーグループに追加する。IAM ユーザーガイドの「[ユーザー \(コンソール\) へのアクセス許可を追加する](#)」の手順に従います。

License Manager のサービスにリンクされたロールの使用

AWS License Manager uses AWS Identity and Access Management (IAM) [サービスにリンクされたロール](#)。サービスにリンクされたロールは、License Manager に直接リンクされた一意のタイプのIAMロールです。サービスにリンクされたロールは License Manager によって事前定義されており、サービスが他の を呼び出すために必要なすべてのアクセス許可が含まれています。AWS ユーザーに代わって のサービス。

サービスにリンクされたロールを使用することで、必要なアクセス権限を手動で追加する必要がなくなるため、License Maneger の設定が簡単になります。License Maneger は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、License Maneger のみがそのロールを引き受けることができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

サービスリンクロールは、関連する リソースを削除した後でしか削除できません。これにより、不注意でリソースにアクセスするアクセス許可の削除が防止され、License Manegerリソースは保護されます。

以下のセクションで説明するように、License Maneger の操作は3つのサービスにリンクされた ロールに依存します。

サービスリンクロール

- [License Manager - コアロール](#)
- [License Manager - 管理アカウントのロール](#)
- [License Manager - メンバーアカウントロール](#)
- [License Manager - ユーザーベースのサブスクリプションロール](#)
- [license-manager - Linux サブスクリプションロール](#)

License Manager - コアロール

License Manegerでは、ユーザーに代わってサービスリンクロールが必要です。

コアロールのアクセス許可

という名前のサービスにリンクされたロー

ルAWSServiceRoleForAWSLicenseManagerRoleは、License Manager に へのアクセスを許可します。AWS ユーザーに代わってライセンスを管理する リソース。

AWSServiceRoleForAWSLicenseManagerRole サービスにリンクされたロールは、ロールを継承するために `license-manager.amazonaws.com` のサービスを信頼します。

のアクセス許可を確認するには `AWSLicenseManagerServiceRolePolicy`、「」を参照してください [AWS 管理ポリシー : AWSLicenseManagerServiceRolePolicy](#)。サービスにリンクされたロールのアクセス許可の設定の詳細については、「IAMユーザーガイド」の [「サービスにリンクされたロールのアクセス許可」](#) を参照してください。

License Maneger のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。License Manegerコンソールに初めてアクセスしたときにLicense Manegerの初回実行のエクスペリエンスを完了すると、サービスにリンクされたロールが自動的に作成されます。

IAM コンソールを使用することもできます。AWS CLI、または IAM API を使用して、サービスにリンクされたロールを手動で作成します。詳細については、「IAMユーザーガイド」の [「サービスにリンクされたロールの作成」](#) を参照してください。

Important

このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。2017年1月1日以前にLicense Managerを使用していた場合、サービスリンクロールのサポートが開始された時点で、License Managerが `AWSServiceRoleForAWSLicenseManagerRole` ロールをアカウントに作成済みです。詳細については、[「アカウントに表示される新しいロール」](#) を参照してくださいIAM。

License Manegerコンソールを使用して、サービスにリンクしたロールを作成することができます。

のサービスにリンクされたロールを作成するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. License Maneger の使用開始を選択します
3. アクセスIAM許可 (one-time-setup) フォームで、付与する を選択します。AWS License Manager 必要なアクセス許可 を選択し、続行 を選択します。

IAM コンソールを使用して、License Manager ユースケースでサービスにリンクされたロールを作成することもできます。または、AWS CLI または AWS API、を使用してIAM、サービス名

で `license-manager.amazonaws.com` サービスにリンクされたロールを作成します。詳細については、「IAMユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。

このサービスにリンクされたロールを削除すると、同じIAMプロセスを使用してロールを再作成できます。

License Manager のサービスにリンクされたロールの編集

License Manager は、`AWSServiceRoleForAWSLicenseManagerRole` のサービスリンクロールの編集を許可しません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできます。詳細については、「IAMユーザーガイド」の「[サービスにリンクされたロールの編集](#)」を参照してください。

License Manager のサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスにリンクされたロールのクリーンアップ

IAM を使用してサービスにリンクされたロールを削除する前に、まずそのロールで使用されているすべてのリソースを削除する必要があります。つまり、関連付けられたインスタンスと からセルフマネージドライセンスの関連付けを解除し AMIs、セルフマネージドライセンスを削除します。

Note

リソースを削除する際に License Manager でロールが使用されている場合、削除は失敗することがあります。その場合は、数分待ってから再試行してください。

ロールで使用されている License Manager リソースを削除するには

1. `license-manager` で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、[セルフマネージドライセンス] を選択します。
3. 自分が所有者であるセルフマネージドライセンスを選択し、関連 AMIs および リソースタブ内のすべてのエントリの関連付けを解除します。ライセンス設定ごとにこのプロセスを繰り返します。

4. セルフマネージドライセンスのページを開いたまま、[アクション] を選択し、[削除] を選択します。
5. すべてのセルフマネージドライセンスが削除されるまで、これまでの手順を繰り返します。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API

`AWSServiceRoleForAWSLicenseManagerRole` サービスにリンクされたロールを削除するには、にします。も使用している場合 [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) およびは [AWSLicenseManagerMemberAccountRole](#)、まずこれらのロールを削除します。詳細については、「IAMユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

License Manager - 管理アカウントのロール

License Manager では、ライセンス管理を実行するには、サービスにリンクされたロールが必要です。

管理アカウントロールのアクセス許可

という名前のサービスにリンクされたロー

ル `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` は、License Manager に へのアクセスを許可します。AWS ユーザーに代わって中央管理アカウントのライセンス管理アクションを管理する リソース。

`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` サービスにリンクされたロールは、ロールを継承するために `license-manager.master-account.amazonaws.com` のサービスを信頼します。

のアクセス許可を確認するには `AWSLicenseManagerMasterAccountRolePolicy`、「」を参照してください [AWS 管理ポリシー : AWSLicenseManagerMasterAccountRolePolicy](#)。サービスにリンクされたロールのアクセス許可の設定の詳細については、「IAMユーザーガイド」の「[サービスにリンクされたロールのアクセス許可](#)」を参照してください。

管理アカウントのサービスにリンクされたロールを作成する

サービスにリンクされたこのロールを手動で作成する必要はありません。でクロスアカウントライセンス管理を設定する場合 AWS Management Console、License Manager はサービスにリンクされたロールを作成します。

Note

License Manager でクロスアカウントサポートを使用するには、[AWS Organizations](#) を使用する必要があります。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソールを使用することもできます。AWS CLI、または IAM API を使用して、サービスにリンクされたロールを手動で作成します。詳細については、「IAMユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。

Important

このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。2017年1月1日以前に License Manager を使用していた場合、サービスリンクロールのサポートが開始された時点で、License Manager が `AWSServiceRoleForAWSLicenseManagerMasterAccountRole` をアカウントに作成済みです。詳細については、「[アカウントに表示される新しいロール](#)」を参照してください [IAM](#)。

License Manager コンソールを使用して、このサービスリンクされたロールを作成することができます。

サービスにリンクされたロールを作成するには

1. <https://console.aws.amazon.com/license-manager/> で License Manager コンソールを開きます。
2. [Settings]、[Edit] を選択します。
3. リンクを選択する AWS Organizations アカウント。
4. [Apply] を選択します。

IAM コンソールを使用して、License Manager-Management アカウントのユースケースでサービスにリンクされたロールを作成することもできます。または、AWS CLI または AWS API、を使用して IAM、サービス名で `license-manager.master-account.amazonaws.com` サービスにリンク

されたロールを作成します。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの作成」](#)を参照してください。

このサービスにリンクされたロールを削除すると、同じIAMプロセスを使用してロールを再作成できません。

License Manager のサービスにリンクされたロールの編集

License Manager は、AWSServiceRoleForAWSLicenseManagerMasterAccountRole のサービスリンクロールの編集を許可しません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、を使用してロールの説明を編集することはできますIAM。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの編集」](#)を参照してください。

License Managerのサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API

AWSServiceRoleForAWSLicenseManagerMasterAccountRoleサービスにリンクされたロールを削除するには、にします。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの削除」](#)を参照してください。

License Manager - メンバーアカウントロール

License Managerでは、管理アカウントがライセンスを管理することを許可する、サービスにリンクされたロールが必要です。

メンバーアカウントロールのアクセス許可

という名前のサービスにリンクされたロー

ルAWSServiceRoleForAWSLicenseManagerMemberAccountRoleにより、License Manager はにアクセスできます。AWS ユーザーに代わって、設定された管理アカウントからのライセンス管理アクション用の リソース。

`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` サービスにリンクされたロールは、ロールを継承するために `license-manager.member-account.amazonaws.com` のサービスを信頼します。

のアクセス許可を確認するには `AWSLicenseManagerMemberAccountRolePolicy`、「」を参照してください [AWS 管理ポリシー : AWSLicenseManagerMemberAccountRolePolicy](#)。サービスにリンクされたロールのアクセス許可の設定の詳細については、「IAMユーザーガイド」の [「サービスにリンクされたロールのアクセス許可」](#) を参照してください。

License Manager のサービスにリンクされたロールを作成する

サービスリンクロールを手動で作成する必要はありません。との統合を有効にできます。AWS Organizations 設定ページの License Manager コンソールの管理アカウントから。これを行うには、AWS CLI (を実行 `update-service-settings`) または AWS API (を呼び出し `UpdateServiceSettings`ます)。この操作を行うと、License Manager によって、Organizations メンバーアカウントにサービスにリンクされたロールが作成されます。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソールを使用することもできます。AWS CLI、または AWS API サービスにリンクされたロールを手動で作成する。詳細については、「IAMユーザーガイド」の [「サービスにリンクされたロールの作成」](#) を参照してください。

Important

このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されません。2017年1月1日以前に License Manager サービスを使用していた場合、サービスリンクロールのサポートが開始された時点で、License Manager が `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` ロールをアカウントに作成済みです。詳細については、[「アカウントに表示される新しいロール」](#) を参照してください [IAM](#)。

License Manager コンソールを使用して、サービスにリンクしたロールを作成することができます。

のサービスにリンクされたロールを作成するには

1. にログインする AWS Organizations 管理アカウント。

2. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
3. ナビゲーションペインで、[設定] を選択し、[編集] を選択します。
4. リンクを選択する AWS Organizations アカウント。
5. [Apply] を選択します。これにより、ロールが作成されます。
[AWSServiceRoleForAWSLicenseManagerRole](#) および
[AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) すべての子アカウントの。

IAM コンソールを使用して、License Manager - Member account ユースケースでサービスにリンクされたロールを作成することもできます。または、AWS CLI または AWS API、サービス名で `license-manager.member-account.amazonaws.com` サービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。

このサービスにリンクされたロールを削除すると、同じ IAM プロセスを使用してロールを再作成できます。

License Manager のサービスにリンクされたロールの編集

License Manager は、[AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) のサービスリンクロールの編集を許可しません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、[IAM ユーザーガイド](#)を使用してロールの説明を編集することはできます。IAM。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの編集](#)」を参照してください。

License Manager のサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API

[AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) サービスにリンクされたロールを削除するには、にします。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

License Manager - ユーザーベースのサブスクリプションロール

License Manager には、 を管理するためのサービスにリンクされたロールが必要です AWS ユーザーベースのサブスクリプションを提供する リソース。

ユーザーベースのサブスクリプションロールのアクセス許可

という名前のサービスにリンクされたロー

ル `AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` により、License Manager は を利用できるようになります。 AWS Systems Manager ユーザーベースのサブスクリプションを提供する Amazon EC2 リソースの管理と説明 AWS Directory Service リソースの使用料金を見積もることができます。

のアクセス許可を確認するには `AWSLicenseManagerUserSubscriptionsServiceRolePolicy`、「」を参照してください [AWS 管理ポリシー：AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。サービスにリンクされたロールのアクセス許可の設定の詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールのアクセス許可](#)」を参照してください。

License Manager のサービスにリンクされたロールを作成する

サービスリンクロールは、License Manager コンソールのユーザーベースのサブスクリプションページでロールを作成するように求められるため、手動で作成する必要はありません。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソールを使用することもできます。AWS CLI、または IAM API を使用して、サービスにリンクされたロールを手動で作成します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。

License Manager コンソールを使用して、サービスにリンクしたロールを作成することができます。

のサービスにリンクされたロールを作成するには

1. で License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 左側のナビゲーションペインで、[ユーザーの関連付け] または [製品] を選択します。
3. License Manager の利用規約に同意して、ユーザーベースのサブスクリプションロールを作成します。
4. [Create] (作成) を選択します。これにより、ロールが作成されます。

IAM コンソールを使用して、License Manager - User-based subscriptions ユースケースでサービスにリンクされたロールを作成することもできます。または、AWS CLI または AWS API、サービス名で `license-manager-user-subscriptions.amazonaws.com` サービスにリンクされたロールを作成します。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの作成](#)」を参照してください。

このサービスにリンクされたロールを削除すると、同じ IAM プロセスを使用してロールを再作成できません。

License Manager のサービスにリンクされたロールの編集

License Manager は、`AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` のサービスリンクロールの編集を許可しません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用してロールの説明を編集することはできません。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの編集](#)」を参照してください。

License Manager のサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API

`AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` サービスにリンクされたロールを削除するには、`aws iam delete-role` を使います。詳細については、「IAM ユーザーガイド」の「[サービスにリンクされたロールの削除](#)」を参照してください。

license-manager - Linux サブスクリプションロール

License Manager には、サービスにリンクされたロールが管理に必要です AWS Linux サブスクリプションを提供する リソース。

Linux サブスクリプションロールのアクセス許可

という名前のサービスにリンクされたロー

ール `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` により、License Manager は Linux サブスクリプションに対して次のアクションを実行できます。

- Amazon Elastic Compute Cloud と AWS Organizations リソースの使用料金を見積もることができません。
- "LicenseManagerLinuxSubscriptions": "enabled" から でタグ付けされたシークレットを取得する AWS Secrets Manager は、サードパーティーの Linux サブスクリプションプロバイダーにアクセスしてサブスクリプション情報を取得できます。
- でタグ付けされたKMSキー"LicenseManagerLinuxSubscriptions": "enabled"を使用して、シークレットを復号します。

のアクセス許可を確認するには `AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy`、「」を参照してください[AWS 管理ポリシー : AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。サービスにリンクされたロールのアクセス許可の設定の詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールのアクセス許可」](#)を参照してください。

License Manager のサービスにリンクされたロールを作成する

サービスリンクロールは、License Manager コンソールの Linux サブスクリプションページでロールを作成するように求められるため、手動で作成する必要はありません。

サービスにリンクされたロールを削除したが、再作成する必要がある場合は、同じプロセスで、アカウントにロールを再作成することができます。

IAM コンソールを使用することもできます。AWS CLI、または IAM API を使用して、サービスにリンクされたロールを手動で作成します。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの作成」](#)を参照してください。

License Managerコンソールを使用して、サービスにリンクしたロールを作成することができます。

のサービスにリンクされたロールを作成するには

1. で License Manager コンソールを開きます<https://console.aws.amazon.com/license-manager/>。
2. 左のナビゲーションペインで、[サブスクリプション] または [インスタンス] を選択します。
3. License Manager の利用規約に同意して、Linux サブスクリプションロールを作成します。
4. [Create] (作成) を選択します。これにより、ロールが作成されます。

IAM コンソールを使用して、License Manager - Linux subscriptionsユースケースでサービスにリンクされたロールを作成することもできます。または、AWS CLI または AWS API、サービス名を使用して `license-manager-linux-subscriptions.amazonaws.com` サービスにリン

くされたロールを作成します。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの作成」](#)を参照してください。

このサービスにリンクされたロールを削除すると、同じIAMプロセスを使用してロールを再作成できません。

License Manager のサービスにリンクされたロールの編集

License Manager

は、AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService のサービスリンクロールの編集を許可しません。サービスリンクロールを作成した後は、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、を使用してロールの説明を編集することはできますIAM。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの編集」](#)を参照してください。

License Managerのサービスにリンクされたロールを削除する

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、アクティブにモニタリングやメンテナンスがされているエンティティだけを所有します。ただし、手動で削除する前に、サービスリンクロールをクリーンアップする必要があります。

サービスリンクロールの手動による削除

IAM コンソール、AWS CLI、または AWS API

AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsServiceサービスにリンクされたロールを削除するには、にします。詳細については、「IAMユーザーガイド」の[「サービスにリンクされたロールの削除」](#)を参照してください。

AWS License Manager の マネージドポリシー

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりもAWS 管理ポリシーを使用する方が簡単です。チームに必要なアクセス許可のみを提供する[IAM カスタマー管理ポリシーを作成するには](#)、時間と専門知識が必要です。すぐに開始するには、AWS マネージドポリシーを使用できます。これらのポリシーは一般的なユースケースを対象としており、AWS アカウントで利用できます。AWS 管理ポリシーの詳細については、IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

AWS サービスは、AWS 管理ポリシーを維持および更新します。AWS 管理ポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、AWS マネージド

ポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS 管理ポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

さらに、は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートしています。たとえば、ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、は新しいオペレーションとリソースに読み取り専用アクセス許可 AWS を追加します。職務機能ポリシーのリストと説明については、IAM ユーザーガイド [AWS](#) の「[職務機能用の 管理ポリシー](#)」を参照してください。

AWS 管理ポリシー : AWSLicenseManagerServiceRolePolicy

このポリシーは、License Manager がユーザーに代わってライセンスを管理する API アクションを呼び出すAWSServiceRoleForAWSLicenseManagerRoleことができるように、という名前のサービスにリンクされたロールにアタッチされます。サービスにリンクされたロールの詳細については、「[コアロールのアクセス許可](#)」を参照してください。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを License Manager に許可します。

Action	リソース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/AWSServiceRoleFor</code>

Action	リソースARN
	AWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*

Action	リソースARN
license-manager:GetServiceSettings	*
license-manager:GetLicense*	*
license-manager:UpdateLicenseSpecificationsForResource	*
license-manager:List*	*

でこのポリシーのアクセス許可を表示するには AWS Management Console、「」を参照してください。[AWSLicenseManagerServiceRolePolicy](#).

AWS 管理ポリシー : AWSLicenseManagerMasterAccountRolePolicy

このポリシーは、License Manager がユーザーに代わって中央管理アカウントのライセンス管理を実行する API アクションを呼び出すAWSServiceRoleForAWSLicenseManagerMasterAccountRoleことができるように、という名前のサービスにリンクされたロールにアタッチされます。サービスにリンクされたロールの詳細については、「[License Manager - 管理アカウントのロール](#)」を参照してください。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを License Manager に許可します。

Action	リソースARN
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:GetLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*
s3:PutLifecycleConfiguration	arn:aws:s3:::aws-license-manager-service-*

Action	リソースARN
s3:GetBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:PutBucketPolicy	arn:aws:s3:::aws-license-manager-service-*
s3:AbortMultipartUpload	arn:aws:s3:::aws-license-manager-service-*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*
s3:GetObject	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucketMultipartUploads	arn:aws:s3:::aws-license-manager-service-*
s3:ListMultipartUploadParts	arn:aws:s3:::aws-license-manager-service-*
s3>DeleteObject	arn:aws:s3:::aws-license-manager-service-*/resource-sync/*
athena:GetQueryExecution	*
athena:GetQueryResults	*
athena:StartQueryExecution	*
glue:GetTable	*
glue:GetPartition	*
glue:GetPartitions	*
glue:CreateTable	脚注 ¹ を参照してください。

Action	リソースARN
glue:UpdateTable	脚注 ¹ を参照してください。
glue>DeleteTable	脚注 ¹ を参照してください。
glue:UpdateJob	脚注 ¹ を参照してください。
glue:UpdateCrawler	脚注 ¹ を参照してください。
organizations:DescribeOrganization	*
organizations:ListAccounts	*
organizations:DescribeAccount	*
organizations:ListChildren	*
organizations:ListParents	*
organizations:ListAccountsForParent	*
organizations:ListRoots	*
organizations:ListAWSServiceAccessForOrganization	*
ram:GetResourceShares	*
ram:GetResourceShareAssociations	*
ram:TagResource	*
ram:CreateResourceShare	*
ram:AssociateResourceShare	*
ram:DisassociateResourceShare	*
ram:UpdateResourceShare	*
ram>DeleteResourceShare	*

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

1 AWS Glue アクションに定義されているリソースは次のとおりです。

- `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`

でこのポリシーのアクセス許可を表示するには AWS Management Console、「」を参照してください。[AWSLicenseManagerMasterAccountRolePolicy](#).

AWS 管理ポリシー : AWSLicenseManagerMemberAccountRolePolicy

このポリシーは、License Manager がユーザーに代わって設定された管理アカウントからライセンス管理の API アクションを呼び出す `AWSServiceRoleForAWSLicenseManagerMemberAccountRole` ことができるように、という名前のサービスにリンクされたロールにアタッチされます。詳細については、「[License Manager - メンバーアカウントロール](#)」を参照してください。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを License Manager に許可します。

Action	リソースARN
<code>license-manager:UpdateLicenseSpecificationsForResource</code>	*
<code>license-manager:GetLicenseConfiguration</code>	*
<code>ssm:ListInventoryEntries</code>	*
<code>ssm:GetInventory</code>	*
<code>ssm:CreateAssociation</code>	*
<code>ssm:CreateResourceDataSync</code>	*
<code>ssm>DeleteResourceDataSync</code>	*

Action	リソースARN
ssm:ListResourceDataSync	*
ssm:ListAssociations	*
ram:AcceptResourceShareInvitation	*
ram:GetResourceShareInvitations	*

でこのポリシーのアクセス許可を表示するには AWS Management Console、「」を参照してください。[AWSLicenseManagerMemberAccountRolePolicy](#).

AWS 管理ポリシー：AWSLicenseManagerConsumptionPolicy

IAM ID にAWSLicenseManagerConsumptionPolicyポリシーをアタッチできます。このポリシーは、ライセンスの使用に必要な License Manager API アクションへのアクセスを許可するアクセス許可を付与します。詳細については、「[License Manager で販売者が発行したライセンスの使用](#)」を参照してください。

このポリシーのアクセス許可を表示するには、「」を参照してください。

[AWSLicenseManagerConsumptionPolicy](#) 「」を参照してください AWS Management Console。

AWS 管理ポリシー：

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

このポリシーは、License Manager が API アクションを呼び出してユーザーベースのサブスクリプションリソースを管理できるように

に、AWSServiceRoleForAWSLicenseManagerUserSubscriptionsServiceポリシーという名前のサービスにリンクされたロールにアタッチされます。詳細については、「[License Manager - ユーザーベースのサブスクリプションロール](#)」を参照してください。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを License Manager に許可します。

Action	リソースARN
ds:DescribeDirectories	*

Action	リソースARN
ds:GetAuthorizedApplicationDetails	*
EC2:CreateTags	arn:aws:ec2:*:*:instance/* ¹
EC2:DescribeInstances	*
EC2:DescribeNetworkInterfaces	*
EC2:DescribeSecurityGroupRules	*
EC2:DescribeSubnets	*
EC2:DescribeVpcPeeringConnections	*
EC2:TerminateInstances	arn:aws:ec2:*:*:instance/* ¹
route53:GetHostedZone	*
route53:ListResourceRecordSets	*
secretsmanager:GetSecretValue	arn:aws:secretsmanager:*:*:secret:license-manager-user-*
ssm:DescribeInstanceInformation	*
ssm:GetCommandInvocation	*
ssm:GetInventory	*
ssm:ListCommandInvocations	*
ssm:SendCommand	arn:aws:ssm:*:*:document/AWS-RunPowerShellScript ² arn:aws:ec2:*:*:instance/* ²

¹ License Manager は、製品コード [bz0vcy31ooqlzk5tsash4r1ik](#)、[77yzkpa7kvee1y1tt7wnsdwoc](#)、または [d44g89hc0gp9jdzm99rznthpw](#) のインスタンスでのみタグを作成および終了できます。

2 License Manager は、タグ名が `AWSLicenseManager` 値が のインスタンスでのみ、`AWS-RunPowerShellScript` ドキュメントを使用して SSM Run Command を実行できません `UserSubscriptions`。

でこのポリシーのアクセス許可を表示するには AWS Management Console、「」を参照してください。[AWSLicenseManagerUserSubscriptionsServiceRolePolicy](#)。

AWS 管理ポリシー :

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

このポリシーは、License Manager が API アクションを呼び出して Linux サブスクリプションリソースを管理できるよう

に、`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` ポリシーという名前のサービスにリンクされたロールにアタッチされます。詳細については、「[license-manager - Linux サブスクリプションロール](#)」を参照してください。

ロールのアクセス許可ポリシーは、指定したリソースに対して以下のアクションを実行することを License Manager に許可します。

Action	条件	リソース
<code>ec2:DescribeInstances</code>	該当なし	*
<code>ec2:DescribeRegions</code>	該当なし	*
<code>organizations:DescribeOrganization</code>	該当なし	*
<code>organizations:ListAccounts</code>	該当なし	*
<code>organizations:DescribeAccount</code>	該当なし	*
<code>organizations:ListChildren</code>	該当なし	*
<code>organizations:ListParents</code>	該当なし	*

Action	条件	リソース
<code>organizations:ListAccountsForParent</code>	該当なし	*
<code>organizations:ListRoots</code>	該当なし	*
<code>organizations:ListAWSServiceAccessForOrganization</code>	該当なし	*
<code>organizations:ListDelegatedAdministrators</code>	該当なし	*
<code>secretsmanager:GetSecretValue</code>	StringEquals: 「aws:ResourceTag/LicenseManagerLinuxSubscriptions」 : 「enabled」 「aws:ResourceAccount」 : 「\${aws:PrincipalAccount}」	arn:aws:secretsmanager:*:*:secret:*
<code>kms:Decrypt</code>	StringEquals: "aws:ResourceTag/LicenseManagerLinuxSubscriptions": "enabled" , 「aws:ResourceAccount」 : 「\${aws:PrincipalAccount}」 StringLike: 「kms:ViaService」 : [「secretsmanager.*.amazonaws.com」]	arn:aws:kms:*:*:key/*

でこのポリシーのアクセス許可を表示するには AWS Management Console、「」を参照してください。[AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#).

License Manager の AWS マネージドポリシーの更新

License Manager の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
AWSLicenseManagerUserSubscriptionsServiceRolePolicy - 既存ポリシーへの更新	License Manager は、ライセンスと Active Directory データを管理するために、Route 53 からのルート情報の取得、Amazon EC2 からのネットワーク情報とセキュリティグループルールの取得、Secrets Manager からのシークレットの取得のアクセス許可を追加しました。	2024 年 11 月 7 日
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy - 既存ポリシーへの更新	License Manager は、自分のライセンス使用 (BYOL) サブスクリプションのシークレットを保存および取得し AWS Secrets Manager、AWS KMS キーを使用してアクセストークンシークレットを復号するアクセス許可を追加しました。	2024 年 5 月 22 日
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy - 新しいポリシー	License Manager が、AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService という名前のサービスリンクロールを作成する権限を追加しました。このロー	2022 年 12 月 21 日

変更	説明	日付
	<p>ルは、AWS Organizations および Amazon EC2 リソースを一覧表示するアクセス許可を License Manager に付与します。</p>	
<p>AWSLicenseManagerUserSubscriptionsServiceRolePolicy – 既存ポリシーへの更新</p>	<p>License Manager が <code>ec2:DescribeVpcPeeringConnections</code> 権限を追加しました。</p>	<p>2022 年 11 月 28 日</p>
<p>AWSLicenseManagerUserSubscriptionsServiceRolePolicy - 新しいポリシー</p>	<p>License Manager が、<code>AWSLicenseManagerUserSubscriptionsServiceRolePolicy</code> という名前のサービスリンクロールを作成する権限を追加しました。このロールは、リソースの一覧表示 AWS Directory Service、Systems Manager 機能の使用、ユーザーベースのサブスクリプション用に作成された Amazon EC2 リソースの管理を行うアクセス許可を License Manager に付与します。</p>	<p>2022 年 7 月 18 日</p>
<p>AWSLicenseManagerMasterAccountRolePolicy – 既存ポリシーへの更新</p>	<p>License Manager は、によって管理されるリソースグループの <code>resource-groups:PutGroupPolicy</code> アクセス許可を追加しました AWS Resource Access Manager。</p>	<p>2022 年 6 月 27 日</p>

変更	説明	日付
AWSLicenseManagerMasterAccountRolePolicy - 既存ポリシーへの更新	License Manager は、の AWS マネージドポリシー AWSLicenseManagerMasterAccountRolePolicy 条件キーを の使用から <code>ram:ResourceTag</code> に変更しました <code>aws:ResourceTag</code> 。 AWS Resource Access Manager	2021 年 11 月 16 日
AWSLicenseManagerConsumptionPolicy - 新しいポリシー	License Manager は、ライセンスを消費する権限を付与する新しいポリシーを追加しました。	2021 年 8 月 11 日
AWSLicenseManagerServiceRolePolicy - 既存ポリシーへの更新	License Manager では、委任された管理者の一覧を表示する許可と、 <code>AWSServiceRoleForAWSLicenseManagerMemberAccountRole</code> という名前のサービスリンクロールを作成する権限が追加されていました。	2021年6月16日
AWSLicenseManagerServiceRolePolicy - 既存ポリシーへの更新	License Manager は、ライセンス設定、ライセンス、権限など、すべての License Manager リソースを一覧表示する権限を追加しました。	2021年6月15日

変更	説明	日付
AWSLicenseManagerServiceRolePolicy – 既存ポリシーへの更新	License Manager が、AWSServiceRoleForMarketplaceLicenseManagement という名前のサービスリンクロールを作成する権限を追加しました。このロールは、License Manager でライセンスを作成および管理するためのアクセス許可 AWS Marketplace をに付与します。詳細については、AWS Marketplace 購入者ガイドの Service-linked roles for AWS Marketplace を参照してください。	2021年3月9日
License Manager が変更の追跡を開始	License Manager が AWS マネージドポリシーの変更の追跡を開始しました。	2021年3月9日

License Manager でのライセンスの暗号化署名

License Manager は、ISVまたはによって発行されたライセンスに暗号で署名できます。AWS Marketplace の代わりにを使用しますISV。署名により、ベンダーは、オフライン環境であっても、アプリケーション内でライセンスの整合性と出所を検証できます。

ライセンスに署名するために、License Managerは非対称 AWS KMS key に属し、で保護されている AWS Key Management Service (AWS KMS) 。このカスタマーマネージド型は、数学的に関連するパブリックキーとプライベートキーのペアCMKで構成されます。ユーザーがライセンスをリクエストすると、License Manager はライセンスの使用権を一覧表示するJSONオブジェクトを生成し、このオブジェクトをプライベートキーで署名します。署名とプレーンテキストJSONオブジェクトがユーザーに返されます。これらのオブジェクトを提示した当事者は、公開キーを使用して、ライセンスのテキストが変更されていないこと、およびライセンスがプライベートキーの所有者によって署名されていることを検証できます。キーペアのプライベート部分はを離れません AWS KMS。

での非対称暗号化の詳細については、「」を参照してください。AWS KMS [「対称キーと非対称キーの使用」](#)を参照してください。

Note

License Manager が を呼び出す AWS KMS [Sign](#) ライセンスに署名して検証するときの および [Verify](#) API オペレーション。これらのオペレーションで使用するには、 のキー使用値が [SIGN_VERIFY](#) CMK である必要があります。このさまざまな CMK は、暗号化と復号には使用できません。

以下のワークフローでは、暗号化されたライセンスの発行について説明します。

1. 左 AWS KMS コンソール、API、または では SDK、ライセンス管理者が非対称カスタマーマネージド を作成します。CMK には、署名と検証のキーの使用方法があり、RSASSA-PSS SHA-256 署名アルゴリズムをサポートしている CMK 必要があります。詳細については、「[非対称の作成 CMKs](#)」および [CMK「設定の選択方法」](#)を参照してください。
2. License Manager では、ライセンス管理者は を含む消費設定を作成します。AWS KMS ARN または ID。設定では、Borrow オプションと Provisional オプションのいずれかまたは両方を指定できます。詳細については、「[出品者が発行したライセンスのブロックを作成する](#)」を参照してください。
3. エンドユーザーは、[CheckoutLicense](#) または [CheckoutBorrowLicense](#) API オペレーションを使用してライセンスを取得します。CheckoutBorrowLicense 操作は、Borrow が設定されているライセンスでのみ可能です。レスポンスの一部として、JSON オブジェクトリストの使用権限とともにデジタル署名を返します。プレーンテキストは次の JSON ようになります。

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

```
"nodeId": "100.20.15.10",
"checkoutMetadata": {
  "Mac": "ABCDEFGHJI"
}
}
```

License Manager のコンプライアンス検証

AWS のサービスが特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、「[コンプライアンスAWS のサービス プログラムによる範囲内](#)」「コンプライアンス」を参照して、関心のあるコンプライアンスプログラムを選択してください。一般的な情報については、[AWS 「コンプライアンスプログラム」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「[Downloading AWS Artifact Reports](#)」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービスは、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。は、コンプライアンスに役立つ以下のリソース AWS を提供します。

- [セキュリティのコンプライアンスとガバナンス](#) – これらのソリューション実装ガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする手順を示します。
- [アマゾン ウェブ サービスでの HIPAA セキュリティとコンプライアンスのためのアーキテクチャー](#) – このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

Note

すべての AWS のサービスが HIPAA 対応であるわけではありません。詳細については、[HIPAA 対象サービスリファレンス](#)」を参照してください。

- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解します。このガイドは、ガイダンスを保護し AWS のサービス、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機

構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめたものです。

- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。AWS Config
- [AWS Security Hub](#) – これにより AWS のサービス、セキュリティ状態を包括的に把握できます。AWS Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「[Security Hub のコントロールリファレンス](#)」を参照してください。
- [Amazon GuardDuty](#) – これにより AWS アカウント、不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで DSS、PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

License Manager の耐障害性

- AWS グローバルインフラストラクチャは AWS リージョンとアベイラビリティゾーン。リージョンには、低レイテンシー、高いスループット、そして高度の冗長ネットワークで接続されている複数の物理的に独立および隔離されたアベイラビリティゾーンがあります。アベイラビリティゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

の詳細については、「」を参照してください。AWS リージョンとアベイラビリティゾーンについては、「」を参照してください。[AWS グローバルインフラストラクチャ](#)。

License Manager のインフラストラクチャセキュリティ

マネージドサービスとして、AWS License Manager は によって保護されています AWS グローバルネットワークセキュリティ。参考情報 AWS セキュリティサービスとその方法 AWS インフラストラクチャを保護するには、「」を参照してください。[AWS クラウドセキュリティ](#)。を設計するには

AWS インフラストラクチャセキュリティのベストプラクティスを使用する環境、「セキュリティの柱」の「[インフラストラクチャの保護](#)」を参照してください。AWS Well-Architected フレームワーク。

を使用する AWS は、ネットワーク経由で License Manager にアクセスするためのAPI呼び出しを発行しました。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。1TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリンIAMシパルに関連付けられたシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) リクエストに署名するための一時的なセキュリティ認証情報を生成します。

を使用した License Manager とインターフェイスVPCエンドポイント AWS PrivateLink

仮想プライベートクラウド (VPC) と の間にプライベート接続を確立できます。AWS License Manager インターフェイスVPCエンドポイントを作成します。インターフェイスエンドポイントは、[AWS PrivateLink](#)、インターネットゲートウェイ、NATデバイス、VPN接続、または [AWS Direct Connect](#) を使用 APIせずに License Manager にプライベートにアクセスできるテクノロジー AWS Direct Connect 接続。のインスタンスは、VPC License Manager と通信するためにパブリック IP アドレスを必要としません。VPC と License Manager 間のトラフィックは、Amazon ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ以上の [Elastic Network Interface](#) によって表されます。

詳細については、「[インターフェイスVPCエンドポイント \(AWS PrivateLinkAmazon VPCユーザーガイドの\)](#)」。

License Manager のインターフェイスVPCエンドポイントを作成する

次のいずれかのサービス名を使用して、License Manager用のエンドポイントを作成します。

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

エンドポイントDNSのプライベートを有効にすると、リージョンのデフォルトDNS名を使用して License Manager にAPIリクエストを行うことができます。例えば、`license-manager.region.amazonaws.com` と指定します。

詳細については、「Amazon [ユーザーガイド](#)」の「[インターフェイスエンドポイントの作成](#)」を参照してください。 VPC

License Manager のVPCエンドポイントポリシーを作成する

License Manager へのアクセスを制御するポリシーをVPCエンドポイントにアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できるプリンシパル
- 実行可能なアクション
- アクションが実行されるリソース

以下は、License Managerのエンドポイントポリシーの例です。エンドポイントに接続されている場合、このポリシーは、すべてのリソースのすべてのプリンシパルに対して、指定されたLicense Managerアクションへのアクセスを許可します。

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

詳細については、「Amazon [ユーザーガイド](#)」のVPC「[エンドポイントを使用した サービスへのアクセスの制御](#)」を参照してください。 VPC

License Manager のトラブルシューティング

以下の情報は、 を使用する際の問題のトラブルシューティングに役立ちます。AWS License Manager。 開始する前に、License Manager の設定が に記載されている要件を満たしていることを確認してください[License Manager の設定](#)。

クロスアカウント検出エラー

クロスアカウント検出のセットアップ時には、[インベントリ検索] ページに以下のようなエラーメッセージが表示されることがあります。

Athena 例外:Athenaクエリが失敗した理由-クエリを実行するための権限が不足しています。このデータベースへのアクセスを有効にするには、カタログを移行してください。

これは、Athena サービスが ではなく Athena 管理のデータカタログを使用している場合に発生する可能性があります。AWS Glue Data Catalog。 アップグレード手順については、[「へのアップグレード」](#)を参照してください。 [AWS Glue データカタログのステップバイステップ](#)。

管理アカウントがセルフマネージドライセンスからリソースの関連付けを解除できない

組織のメンバーアカウントがそのアカウント

でAWSServiceRoleForAWSLicenseManagerMemberAccountRoleサービスにリンクされたロール (SLR) を削除し、セルフマネージドライセンスに関連付けられたメンバー所有リソースがある場合、管理アカウントはそれらのメンバーアカウントリソースからライセンスの関連付けを解除できなくなります。つまり、そのメンバーアカウントのリソースが、管理アカウントプールからのライセンスを消費し続けることを意味します。管理アカウントがリソースの関連付けを解除できるようにするには、 を復元しますSLR。

この方法は、マスターアカウントが、メンバーアカウントのリソースに影響を及ぼすいくつかのアクションを管理アカウントに許可しないことをお客様が希望される場合に対応します。

Systems Managerインベントリが古い

Systems Managerはインベントリデータを30日間保存します。この期間中においては、Ping に応答しない場合であってもLicense Managerが、 マネージドインスタンスをアクティブなインスタンスとしてカウントします。Systems Managerからインベントリデータが消去されると、License Manager

がそのインスタンスを非アクティブとしてマークし、ローカルインベントリデータを更新します。マネージドインスタンスの正確なカウントを保つには、Systems Managerで登録解除を手動で行い、License Managerがクリーンアップ処理を実行できるようにします。

登録解除された の見かけ上の永続性 AMI

License Manager は、数時間ごとに、リソースとセルフマネージドライセンスの古い関連付けを消去します。セルフマネージドライセンスAMIに関連付けられた が Amazon を通じて登録解除された場合EC2、 は削除される前に License Manager リソースインベントリに一時的に表示され続けるAMI ことがあります。

リソースインベントリに新しい子アカウントインスタンスが表示されるのが遅い

クロスアカウントサポートが有効になっている場合、License Managerはデフォルトで毎日午後1時にお客様のアカウントを更新します。その日のうちに追加されたインスタンスは、翌日、管理アカウントのリソースインベントリに表示されます。 を編集することで、更新スクリプトの実行頻度LicenseManagerResourceSynDataProcessJobTriggerを変更できます。AWS Glue 管理アカウントの コンソール。

クロスアカウントモード有効にした後、子アカウントのインスタンスが表示されるのが遅い

License Managerでクロスアカウントモードを有効にすると、子アカウント内のインスタンスがリソースインベントリ内に表示されるまで数分から数時間かかります。表示までの時間は、子アカウントの数や、各子アカウント内のインスタンス数に応じて変化します。

クロスアカウント検出を無効化できない

アカウントでクロスアカウント検出を設定すると、シングルアカウント検出に戻すことはできません。

子アカウントのユーザーが、共有セルフマネージドライセンスをインスタンスと関連付けられない

このエラーが発生し、クロスアカウント検出が有効になっている場合は、次の点を確認します:

- 子アカウントが組織から削除されている。
- 子アカウントが、管理アカウントで作成されたリソースシェアから削除されました。
- セルフマネージドライセンスがリソース共有から削除されている。

Linking (リンク中) AWS Organizations アカウントが失敗する

[Settings] ページでこのエラーが生じた場合、下記のいずれかの理由でアカウントが組織のメンバーでなくなっていることが考えられます:

- 子アカウントが組織から削除されている。
- お客様が、アカウントの組織コンソールから License Managerへのアクセスをオフにしました。

License Manager のドキュメント履歴

次の表に、 のリリースを示します AWS License Manager。

変更	説明	日付
Microsoft Remote Desktop Services サブスクライバークセスライセンス (RDSSAL) ユーザーベースのサブスクリプションのサポートを追加	License Manager RDS は、一度に 3 つ以上のリモートデスクトップ接続を設定する機能を含む、SAL ユーザーベースのサブスクリプションの管理と設定のサポートを追加しました。	2024 年 11 月 14 日
ユーザーベースのサブスクリプション SLR 管理ポリシーを更新して、ルートとネットワーク情報を取得	License Manager は、ライセンスと Active Directory データを管理するために、Route 53 からのルート情報の取得、Amazon EC2 からのネットワーク情報とセキュリティグループルールの取得、Secrets Manager からのシークレットの取得のアクセス許可を追加しました。詳細については、「 AWS 管理ポリシー : AWSLicenseManagerUserSubscriptionsServiceRolePolicy 」。	2024 年 11 月 7 日
Red Hat Subscription Manager (BYOL) から RHSM サブスクリプション情報を取得する	License Manager は、Red Hat Enterprise Linux インスタンスの RHSM for BYOL ライセンスからサブスクリプション情報を取得するサポートを追加しました。これには、 の更新が含まれます。 AWSLicens	2024 年 7 月 10 日

変更	説明	日付
	eManagerLinuxSubscriptionsServiceRolePolicy .	
Amazon RDS for Db2 vCPU ベースの BYOL ライセンスのサポートを追加	License Manager は、Amazon RDS for Db2 vCPU ベースの BYOL ライセンスのサポートを追加しました。	2024 年 3 月 20 日
Microsoft Office ユーザーベースのサブスクリプションに対する Windows Server 2019 のサポートを追加しました	AWS は、Amazon Word 上の Microsoft Office AMIs Professional Plus 2021 の Amazon 提供ライセンスを使用して、Amazon マシンイメージ (LTSC) で Windows Server 2019 のサポートを追加しましたEC2。	2023 年 12 月 4 日
セルフマネージド (オンプレミス) ドメインのユーザーは、ユーザーベースのサブスクリプションを利用できます。	License Manager は、AWS Managed Microsoft AD ディレクトリとの信頼が作成されたときに、セルフマネージドアクティブディレクトリドメインのユーザーがユーザーベースのサブスクリプションを利用するためのサポートを追加しました。	2023 年 9 月 6 日
Ubuntu LTS サブスクリプションのライセンスタイプ変換	License Manager は、ライセンスタイプ変換を使用して Ubuntu Pro サブスクリプションを追加するための Ubuntu LTS インスタンスのサポートを追加しました。	2023 年 4 月 20 日

変更	説明	日付
有効なグラントの置き換え	License Manager では、グラントアクティベーション中に、付与されたライセンスに対して有効なグラントを置き換えるオプション機能が追加されました。	2023 年 3 月 31 日
Linux サブスクリプションの委任管理	License Manager で、Linux サブスクリプションの委任管理者のサポートが追加されました。	2023 年 3 月 3 日
Linux サブスクリプション	License Manager で、商用 Linux サブスクリプションの追跡が追加されました。	2022 年 12 月 21 日
Amazon CloudWatch メトリクス	License Manager は、ライセンス設定の使用状況とサブスクリプションに関する CloudWatch メトリクスを出力するようになりました。	2022 年 12 月 21 日
ユーザーベースのサブスクリプション用 Microsoft Office	License Manager で、ユーザーベースのサブスクリプションのサポート対象ソフトウェアとして Microsoft Office が追加されました。	2022 年 11 月 28 日
権限の組織単位への配布	組織内の特定の OU に権限を配布します。	2022 年 11 月 17 日
組織全体のビュー (コンソール)	License Manager コンソール AWS Organizations を使用して、 のアカウント全体で付与されたライセンスを管理します。	2022 年 11 月 11 日

変更	説明	日付
ユーザーベースのサブスクリプション	Amazon EC2 でサポートされているユーザーベースのサブスクリプション製品を使用します。	2022 年 8 月 2 日
ライセンス使用状況データの記録と送信 (コンソール)	License Manager コンソールを使用して、ライセンス使用状況データを記録して送信します。	2022 年 3 月 28 日
ライセンスタイプの変換 (コンソール)	既存のワークロードを再デプロイせずに License Manager コンソールを使用して、ライセンスタイプを AWS が提供するライセンスと Bring Your Own License Model (BYOL) の間で変更します。	2021 年 11 月 9 日
ライセンスタイプ変換 (CLI)	既存のワークロードを再デプロイ AWS CLI することなく、 を使用して、ライセンスタイプを AWS が提供するライセンスと Bring Your Own License モデル (BYOL) の間で変更します。	2021年9月22日
権利の共有	1回のリクエストで、マネージドライセンス権限を組織全体で共有できます。	2021年7月16日

変更	説明	日付
使用状況レポート	License Manager の使用状況レポートで、ライセンスタイプ設定の履歴を追跡します。使用状況レポートは、以前はレポートジェネレーターとライセンスレポートと呼ばれていました。	2021年5月18日
自動検出除外ルール	AWS アカウントの IDs とタグに基づいて License Manager 自動検出からインスタンスを除外します。	2021年3月5日
マネージドエンタイトルメント	License Manager を使用してライセンスを配布する AWS Marketplace および 販売者から購入した製品のライセンス使用権限を追跡して配布します。	2020年12月3日
アンインストールされたソフトウェアの自動会計	ソフトウェアのアンインストール時にインスタンスの追跡を停止するように、自動検出を設定します。	2020年12月3日
タグベースのフィルタリング	タグを使用してリソースインベントリを検索します。	2020年12月3日
AMIの関連付けの範囲	セルフマネージドライセンスと、アカウントと共有されている AMIs を関連付けます AWS。	2020年11月23日

変更	説明	日付
ホストとのライセンスの類似性	特定の日数、専用ハードウェアへのライセンスの割り当てを強制的に行うことができます。	2020年8月12日
Amazon RDS での Oracle デプロイの追跡	Amazon RDS で Oracle データベースエンジンエディションとライセンスパックのライセンス使用状況を追跡します。	2020年3月23日
リソースグループのホスト	ホストリソースグループを設定しLicense Manager が Dedicated Hostsを管理できるようにします。	2019年12月1日
ソフトウェア検出の自動化	新しくインストールされたオペレーティングシステムまたはアプリケーションを検索し、対応するセルフマネージドライセンスをインスタンスにアタッチするように License Manager を設定します。	2019年12月1日
ライセンスインクルードと Bring-Your-Own-License(BYOL)の違い	Amazonが提供するライセンスを使用しているか、独自のライセンスを使用しているかによって、検索結果をフィルタリングします。	2019年11月8日

変更	説明	日付
オンプレミスのリソースにライセンスを添付します	ライセンスをオンプレミスのインスタンスにアタッチすると、License Manager は定期的にソフトウェアインベントリを収集し、ライセンス情報を更新し、使用状況をレポートします。	2019年3月8日
AWS License Manager 初回リリース	初回サービス起動	2018年11月28日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。