



ユーザーガイド

AWS License Manager



AWS License Manager: ユーザーガイド

Copyright © 2026 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
ライセンス管理ワークフローのライセンスアセットグループ	7
既存の License Manager 機能との関係	7
ライセンスアセットグループのユースケースシナリオ	8
はじめに	9
License Manager の使用	10
ライセンスアセットグループ	11
AWS License Manager ライセンスアセットグループについて	11
ライセンスアセットグループの開始方法	13
ライセンスアセットグループの使用	14
ライセンスアセットルールセットの使用	20
セルフマネージドライセンス	28
パラメータとルール	29
ベンダーライセンスからのルールの作成	31
セルフマネージドライセンスを作成する	33
セルフマネージドライセンスを共有する	35
セルフマネージドライセンスを編集する	40
セルフマネージドライセンスを表示する	41
セルフマネージドライセンスを非アクティブ化する	42
セルフマネージドライセンスを削除する	42
セルフマネージドライセンスルール	43
ライセンスの付与	46
付与されたライセンスを表示する	47
付与されたライセンスを管理する	47
使用権限を配布する	51
権限の受理とアクティベーション	52
ライセンスステータス。	55
購入者アカウントのメトリクス	56
ライセンス分析	57
プライマリダッシュボードビュー	57

個々のライセンスアセットグループビュー	58
使用状況レポートを作成する	59
インベントリ検索	62
インベントリ検索の操作	63
インベントリの自動検出	69
ライセンスタイプ変換	71
適格なライセンスタイプ	73
前提条件	83
ライセンスタイプを変換する	86
テナンシー変換	100
トラブルシューティング	102
リソースグループをホストします	104
ホストリソースグループの作成	105
ホストリソースグループの共有	106
ホストリソースグループに Dedicated Hosts を追加する	106
ホストリソースグループのインスタンスを起動する	107
ホストリソースグループの変更	107
ホストリソースグループから Dedicated Hosts を削除する	108
ホストリソースグループを削除します。	108
ユーザーベースのサブスクリプション	109
考慮事項	110
License Manager のサブスクリプション料金	111
ユーザーベースのサブスクリプションの前提条件	116
サポートされているソフトウェアサブスクリプション	126
Active Directory	128
その他のソフトウェア	128
はじめに	129
より多くのセッション用に GPO を設定する	139
クロスアカウント License Manager	140
ライセンス込み AMI からインスタンスを起動する	148
インスタンスへの接続	150
Microsoft Office のファイアウォール設定を変更する	150
サブスクリプションユーザーの管理	151
Active Directory の登録解除	153
トラブルシューティング	154
Linux サブスクリプションを管理する	167

検出を設定する	169
インスタンスデータの表示	175
請求情報	177
CloudWatch アラームの管理	180
販売者が発行したライセンス	182
エンタイトルメント	183
ライセンス使用量	183
必要なアクセス許可	184
販売者が発行したライセンスを作成する	186
販売者に発行されたライセンスを付与する	187
ISV のお客様向けの一時的な認証情報	188
販売者が発行したライセンスを確認する	189
販売者が発行したライセンスを削除する	190
設定	191
License Manager の設定を編集する	192
マネージドライセンス設定	193
Linux サブスクリプション設定	195
ユーザーベースのサブスクリプション設定	198
委任管理者設定	198
License Manager のモニタリング	204
CloudWatch によるモニタリング	204
CloudWatch アラームの作成	206
CloudTrail ログ	207
CloudTrailのLicense Manager情報	207
ライセンスLicense Managerのログ・ ファイルエントリーについて	208
セキュリティ	210
データ保護	211
保管中の暗号化	212
ID とアクセス管理	212
ユーザー、グループ、ロールを作成する	212
IAM ポリシーの構造	213
License Manager の IAM ポリシーを作成する	214
ユーザー、グループ、およびロールに許可を付与する	215
サービスリンクロール	216
コアロール	217
管理アカウントロール	219

メンバーアカウントのロール	222
ユーザーベースのサブスクリプションロール	224
Linux サブスクリプションロール	226
AWS マネージドポリシー	228
AWSLicenseManagerServiceRolePolicy	229
AWSLicenseManagerMasterAccountRolePolicy	231
AWSLicenseManagerMemberAccountRolePolicy	235
AWSLicenseManagerConsumptionPolicy	236
AWSLicenseManagerUserSubscriptionsServiceRolePolicy	236
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy	238
ポリシーの更新	240
ライセンス署名	243
コンプライアンス検証	245
耐障害性	245
インフラストラクチャセキュリティ	246
を使用した VPC エンドポイント AWS PrivateLink	246
License Manager用のインターフェイスVPCエンドポイントの作成	247
License Manager 用のVPCエンドポイントポリシーを作成する	247
トラブルシューティング	249
クロスアカウント検出エラー	249
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	249
Systems Managerインベントリが古い	249
登録解除されたAMIの見かけ上の存続	250
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	250
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	250
クロスアカウント検出を無効化できない	250
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	250
AWS Organizations アカウントのリンクが失敗する	251
ドキュメント履歴	252
.....	cclix

とは AWS License Manager

AWS License Manager を使用すると、組織内の複数の AWS リージョンやアカウントでソフトウェアベンダー (Microsoft、SAP、Oracle、IBM など) からのソフトウェアライセンスを簡単に管理できるため、ソフトウェアライセンスのコンプライアンスを大規模に一元的に可視化し、包括的なレポートを提供できます。これにより、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減らすことができます。

クラウドインフラストラクチャを上に構築すると AWS、Bring Your Own License Model (BYOL) の機会を使用して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、AWS サービス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。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 (vCPU)、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、すべての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。

を使用すると AWS License Manager、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、複数のリージョンで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、CloudWatch メトリクスとイベントを通じて ISV に追跡できます。ISV は、このデータを分析、監査、およびその他の同様の目的で使用できます。

AWS License Manager は、[AWS Marketplace](#) および [AWS Data Exchange](#)、および [AWS Identity and Access Management \(IAM\)](#)、[Service Quotas](#) [AWS Organizations](#)、[CloudFormation](#) AWS リソースタグ付け、および AWS のサービスに統合されています [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) は、を使用して AWS License Manager、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エンドユーザーに管理および配布できます。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。を通じて販売する ISVs 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 AWS Marketplace 恩恵を受けます。ISVs は License Manager を使用してライセンスキーを作成し、AWS アカウントを持た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。

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。

でライセンスを作成し AWS License Manager、IAM ID 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できます AWS License Manager。を使用するエンドユーザー AWS は、ライセンス権限をそれぞれの組織の ID AWS にさらに再配布できます。配布されたエンタイトルメントを持つエンドユーザーは、AWS License Manager と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してチェックインできます。各ライセンスのチェックアウトでは、エンタイトルメント、関連する数量、チェックアウト期間 (**admin-users** 1 時間に 10 個のチェックアウトなど) が指定されています。このチェックアウトは、分散ライセンスの基盤となる IAM ID に基づいて、または AWS License Manager サービス AWS License Manager を通じて 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。

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、単一の AWS アカウント内のセルフマネージドライセンスのライセンスルールを定義するために使用されます。マルチアカウントシナリオでは、一元化されたガバナンスにライセンスアセットグループを使用することを検討してください。

- [ライセンスアセットグループ](#) – 組織内の複数の AWS リージョンとアカウントにわたるライセンスを一元管理および追跡するために使用されます。
- [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 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。ライセンスアセットグループを使用して、単一のアカウント内で個別に管理することも、複数のアカウント間で一元管理することもできます。
- [License Manager でのライセンスタイプの変換](#) – ワークロードを再デプロイせずに AWS、提供されたライセンスと Bring Your Own License Model (BYOL) の間でライセンスタイプを変更するために使用されます。
- [License Manager でのインベントリ検索](#) – AWS Systems Manager インベントリとライセンスルール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。
- [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](#) – AWSで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されます。

関連サービス

License Manager は、Amazon EC2、Amazon RDS AWS Marketplace、AWS Systems Manager および と統合されています 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全体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](#)
- [ハードウェア専有インスタンス](#)
- [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 をと共に使用すると AWS Systems Manager、 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。で License Manager を使用して 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、ソフトウェアを統合した販売者から AWS Marketplace AWS Data Exchange、または販売者から直接購入したライセンスの使用を管理できます AWS License Manager。AWS License Manager を使用して、使用権限と呼ばれる使用権限を特定の に配布できます AWS アカウント。

License Manager は、Amazon RDS for Oracle および Amazon RDS for Db2 vCPU 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、RDS for Oracle および RDS for Db2 DB インスタンスの 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項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](#)

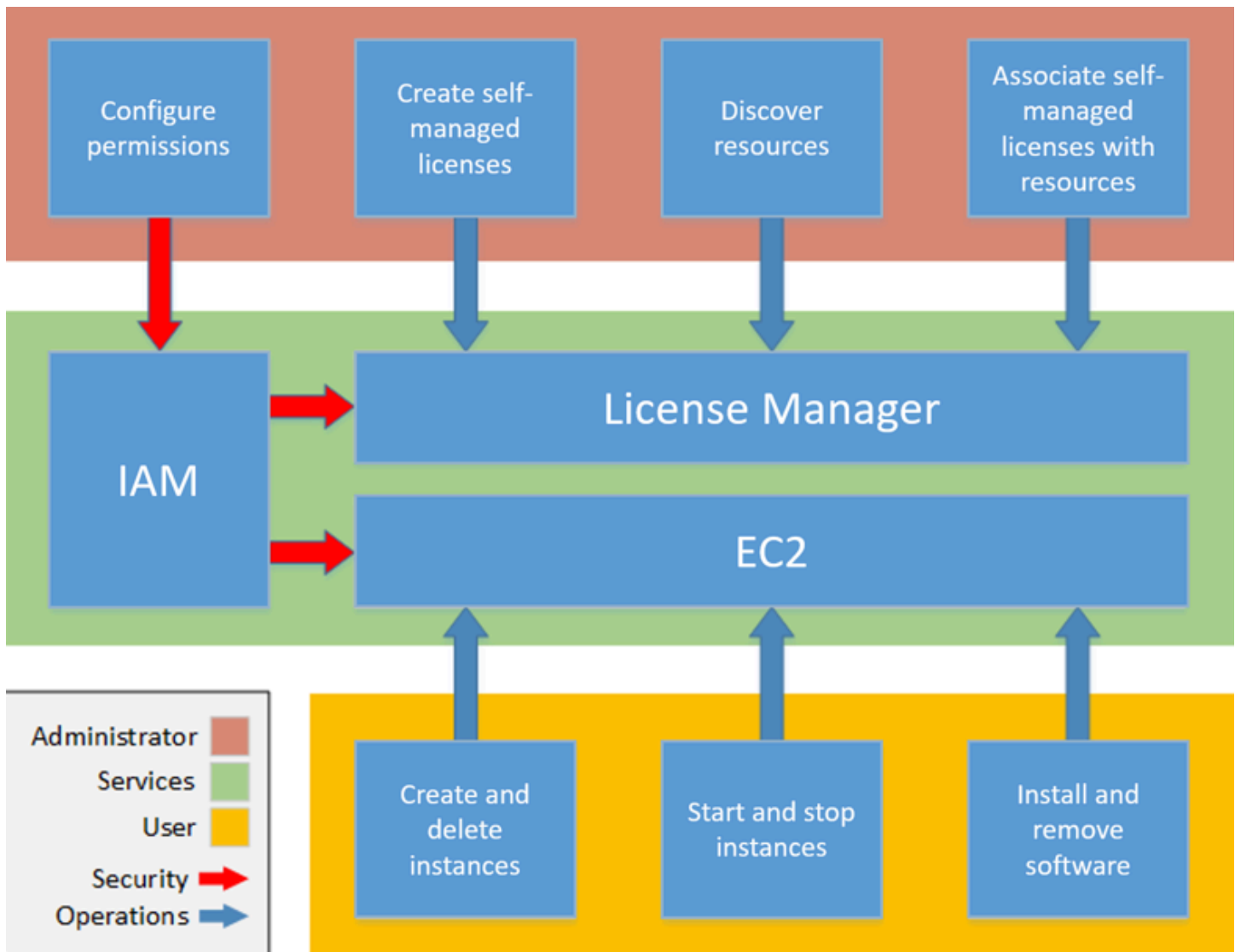
License Manegerの仕組み

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 Maneger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。重要な点として、インスタンスを作成および削除する Amazon EC2 コントロールプレーンなど、AWS サービスとネイティブに統合します。これは、License Maneger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 Manegerを構成するライセンスマネージャーと、Amazon EC2コンソールを使ってリソースの作成、管理、削除を行うユーザーの、異なるが連携し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。

ライセンスアセットグループは、複数の AWS リージョンとアカウントで動作する組織全体のライセンス管理を提供することで、この機能を拡張します。ライセンスアセットグループは、リージョンとアカウントごとにライセンスを個別に管理する代わりに、ライセンス情報を統合ビューに統合し、AWS 組織全体の一元化された監視と自動化されたコンプライアンスモニタリングを可能にします。

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。ライセンスアセットグループを使用すると、ライセンスの専門家は、リージョンやアカウント間でソフトウェアを自動的に検出および追跡する一元的なライセンスグループを作成し、ライセンスを大規模に管理するための管理オーバーヘッドを削減することもできます。実際にはこれは、あるセルフマネージドライセンスを、IT 部門がすべての Amazon EC2 インスタンスデプロイに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。

ライセンス管理ワークフローのライセンスアセットグループ

ライセンスアセットグループは、ライセンス管理ワークフローに組織と自動化のレイヤーを追加します。従来のライセンス設定は個々のライセンスレベルで機能しますが、ライセンスアセットグループは組織レベルで動作し、複数のリージョンとアカウントにわたる統合ビューと自動管理を提供します。

既存の License Manager 機能との関係

ライセンスアセットグループは、既存の License Manager 機能を補完および強化します。

- **ライセンス設定** - ライセンスアセットグループは、セルフマネージドライセンス設定と付与されたライセンスの両方を組み込むことができ、ライセンスが最初に作成または取得された方法に関係なく、統一されたビューを提供します。
- **インベントリ検索** - ライセンスアセットグループはインベントリ検索と同じ検出メカニズムを使用しますが、ルールセットに基づいて検出されたリソースのグループ化と継続的なモニタリングを自動化します。
- **使用状況レポート** - ライセンスアセットグループは、複数のリージョンとアカウントにまたがる包括的なレポートを生成し、個々のライセンスレポートでは達成できない組織全体の可視性を提供します。

- クロスアカウント管理 - ライセンスアセットグループは、マルチアカウントシナリオ専用設計されており、AWS Organizations とシームレスに連携して、一元化されたライセンスガバナンスを提供します。

ライセンスアセットグループのユースケースシナリオ

ライセンスアセットグループは、以下のシナリオで特に重要です。

- マルチリージョンデプロイ - 組織が複数の AWS リージョンでワークロードを実行し、各リージョンを個別に管理せずに統合されたライセンス追跡が必要な場合。
- マルチアカウント組織 - 複数のアカウントで AWS Organizations を使用し、管理アカウントまたは委任された管理者アカウントからの一元的なライセンス監視が必要な場合。
- 自動コンプライアンスモニタリング - AWS 環境全体でプロアクティブなライセンス失効通知と自動コンプライアンス追跡が必要な場合。
- 監査の準備 - ベンダー監査または内部コンプライアンスレビューのために、包括的で組織全体のライセンス使用状況レポートが必要な場合。

License Manager の使用を開始する

を使用するには AWS License Manager、まずオンボーディングステップ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 マネジメントコンソール。

License Manager の使用を開始する

1. 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。

AWS ベストプラクティスに従いながら License Manager を利用するユーザー、グループ、ロールのアクセス許可を管理する方法の詳細については、「」を参照してください[License Manager の Identity and Access Management](#)。License Manager と統合する Amazon EC2 リソースの設定に関する詳細については、「Amazon Elastic Compute Cloud ユーザーガイド」の「[Amazon EC2 を使用するようにセットアップする](#)」を参照してください。

License Manager の使用

License Manager は AWS リソースやオンプレミスリソースの混在するインフラをもつ企業のスタンダードなシナリオに適用できます。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。

AWS Marketplace 製品のライセンス

License Manager を使用して、Amazon EC2 起動テンプレート、AWS CloudFormation テンプレート、または Service Catalog 製品を介してライセンスルールを AWS Marketplace BYOL AMI 製品に関連付けることができるようになりました。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からBYOL AMIを取得してアクティベートする方法を変えるものではありません。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、[Systems Manager インベントリ](#) AWS を使用して の外部で実行されているアプリケーションを検出し、ライセンスルールをアタッチできます。ライセンスルールを設定すると、License Manager コンソール内で、オンプレミスサーバーに伴う AWS リソースを追跡できるようになります。

ライセンスインクルードとBYOLの違い

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ライセンスの使用状況を正確に報告できます。このフィルターを使用するには、SSMのバージョン 2.3.722.0以降が必要です。

AWS アカウント全体の License Manager

License Manager を使用すると、AWS アカウント全体のライセンスを管理できます。ライセンス設定は AWS Organizations 、管理アカウントで一度作成し、 を使用する AWS Resource Access Manager か、License Manager 設定を使用して AWS Organizations アカウントをリンクすること

で、アカウント間で共有できます。これにより、クロスアカウント検出を実行して、AWS アカウント全体のインベントリを検索することもできます。

内容

- [ライセンスアセットグループ](#)
- [License Manager のセルフマネージドライセンス](#)
- [ライセンスマネージャーで付与されたライセンス](#)
- [ライセンス分析](#)
- [License Manager でのインベントリ検索](#)
- [License Manager 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](#)
- [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 Manager で販売者が発行したライセンス](#)
- [License Manager の設定](#)

ライセンスアセットグループ

ライセンスアセットグループは、AWS 環境全体のライセンス使用量を一元的に管理およびモニタリングする方法を提供します。関連アセットをグループ化し、ライセンスルールを適用し、管理アカウントまたは委任管理者アカウントからコンプライアンスを追跡できます。

内容

- [AWS License Manager ライセンスアセットグループについて](#)
- [ライセンスアセットグループの開始方法](#)
- [ライセンスアセットグループの使用](#)
- [ライセンスアセットルールセットの使用](#)

AWS License Manager ライセンスアセットグループについて

のライセンスアセットグループは AWS License Manager、組織内の AWS リージョンとアカウント全体で一元的なライセンス管理を提供し、統合された可視性、自動通知、ソフトウェアライセンスコンプライアンスの包括的なレポートを提供します。

ライセンスアセットグループとは

ライセンスアセットグループは、ユーザー定義ルールに基づいてライセンスと関連する EC2 AWS License Manager インスタンスを統合する 内のコンテナです。これらのグループは、ライセンスとインスタンスが存在するリージョンやアカウントに関係なく、AWS Organizations 全体のソフトウェアライセンスの状態を統一して表示します。

ライセンスアセットグループは、どのライセンスとインスタンスと一緒に属しているかを定義するルールセットを適用することで機能します。たとえば、組織全体で Windows Server を実行するすべての Windows Server ライセンスと EC2 インスタンスを追跡する「Windows Server」ライセンスアセットグループを作成できます。グループは、設定したルールに基づいて、関連するリソースを自動的に検出して含めます。

このシステムは、Microsoft Windows Server、SQL Server、Red Hat Enterprise Linux、Ubuntu Pro、SUSE Enterprise Linux などの一般的なソフトウェア製品の AWS 管理ルールセットと、特定のライセンスニーズに合わせて作成できるカスタムルールセットの両方をサポートしています。

主要な機能とコンポーネント

一元化されたライセンスの可視性

ライセンスアセットグループは、複数の AWS リージョンのライセンス情報を 1 つのビューに集約します。このクロスリージョンの可視性により、各リージョンを個別にチェックして組織のソフトウェアライセンスの状態を把握する必要がなくなります。グループは、AWS Systems Manager エージェントを使用してワークロードで実行されているソフトウェア製品を自動的に検出し、この情報を統合して組織全体を可視化します。

柔軟なルールベースの組織

ライセンスアセットグループは、ルールセットを使用して、追跡および維持するライセンスとインスタンスを定義します。グループとルールセット間のこの柔軟な関係により、ビジネスニーズに合った方法でライセンスを整理できます。AWS マネージドルールセットは、広く採用されている製品に使用したり、特殊なソフトウェアのカスタムルールを作成したりできます。

コンプライアンスの自動モニタリング

ライセンスアセットグループは、Amazon SNS を通じてライセンスの有効期限を自動的に通知するため、ライセンスの更新をプロアクティブに管理できます。ライセンス消費は、vCPU、ソケット、インスタンス、コアメトリクスなど、定義された使用ディメンションに対して追跡されるため、ライセンス義務を確実に認識できます。

既存の AWS サービスとの統合

ライセンスアセットグループは既存の AWS License Manager 機能に基づいて構築され、複数の AWS サービスと統合して包括的なライセンス管理を提供します。この機能は、既に使用しているライセンス設定や自動検出機能と一緒に機能します。

ソフトウェア検出を有効にするには、EC2 インスタンスに AWS Systems Manager エージェントをインストールします。マルチアカウントシナリオでは、クロスアカウント検出を設定し、組織全体の License Manager オペレーションに適切な IAM アクセス許可を確保する必要があります。

ライセンスアセットグループの開始方法

このセクションでは、でライセンスアセットグループの使用を開始する方法について説明します AWS License Manager。前提条件の設定、ソースリージョンの設定、最初のライセンスアセットグループの作成方法について説明します。

前提条件

ライセンスアセットグループの使用を開始する前に、次の前提条件を満たしていることを確認してください。

- AWS Systems Manager EC2 インスタンスにインストールされている (SSM) エージェント
- 複数のアカウントでライセンスを管理する場合に設定されたクロスアカウント検出
- 初めてオンボーディングする場合は、[License Manager 入門ガイド](#)に従って、必要なすべてのアクセス許可を設定します。

ライセンスアセットグループを設定する

ソースリージョンを設定する

ライセンスアセットグループは、AWS License Manager が利用可能なすべての AWS 商用リージョンで使用できます。クロスリージョン検出では、セットアップ中にソース AWS リージョンを選択する必要があります。これにより、License Manager は選択したリージョンのすべてのソフトウェアを検出できます。

コンソールを使用してソースリージョンを設定するには

1. 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、ライセンスアセット検出とルールセットを選択します。
3. License asset discovery セクションで、Edit を選択します。
4. リージョン検出で、製品を検出するリージョンを選択します。
5. 組織の所有者で、すべての組織アカウントでを検出する場合は、有効化 を選択します。
6. [Save changes] (変更の保存) をクリックします。

ライセンスアセットグループの使用

このセクションでは、でライセンスアセットグループを作成、更新、削除、管理する方法について説明します AWS License Manager。ライセンスアセットグループは、AWS リソース全体のライセンスの追跡と管理に役立ちます。

ライセンスアセットグループの作成

ライセンスアセットグループは、AWS リソース全体のライセンスを追跡および管理します。複数のアセットグループを作成して、さまざまなソフトウェア製品を整理し、ライセンスニーズに合わせていつでも設定を変更できます。

Note

ワンクリックテンプレートを使用してライセンスアセットグループをすばやく作成することも、特定のニーズに基づいてさまざまなライセンスルールセットを追加してライセンスアセットグループを手動で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アセットグループを作成するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、ライセンスアセット検出とルールセットを選択します。
3. ライセンスアセット検出セクションで、リージョン検出にリージョンが入力されていることを確認します。
4. ライセンスアセットルールセットセクションで、AWSマネージドルールセット (特定のマネージド製品用に設定されたプリセットルール) AWSまたはカスタムルールセットを選択します。
「[???](#)」を参照してください。
5. ルールセットを使用してライセンスアセットグループを作成するを選択します。

6. ライセンスアセットグループ名には、アセットのグループ化方法を記憶するためのわかりやすい名前を入力します。
7. (オプション) ライセンスアセットグループの説明に、アセットのグループ化方法に関する詳細な説明を入力します。
8. Usage Dimension では、次のオプションのいずれかを選択します: vCPU、ソケット、インスタンス、または Core。このフィールドは、アセットの使用状況の計算を決定します。
9. 新しいルールセットを作成するか、既存のマネージドルールセットまたはカスタムルールセットから追加して、1 つ以上のライセンスアセットルールセットを選択します。 AWS 「[???](#)」を参照してください。
10. (オプション) タグでは、1 つ以上のタグを追加します。
11. ライセンスアセットグループの作成 を選択します。

 Note

ライセンスアセットグループが作成されると、検出は自動的に開始され、通常は 24 時間以内に完了します。この間、License Manager は設定されたリージョンとアカウントをスキャンして、ルールセット条件に一致するすべてのインスタンスを識別します。

CLI を使用してライセンスアセットグループを作成するには

- `create-license-asset-group` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットグループの更新

ライセンスアセットグループを更新して、設定を変更したり、ルールセットを追加または削除したり、タグを更新したりできます。

コンソールを使用してライセンスアセットグループを更新するには

1. 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、ライセンスを選択します。
3. ライセンスアセットグループセクションで、1 つ以上のライセンスアセットグループが使用可能であることを確認します。
4. 編集するライセンスアセットグループを選択するには、チェックボックスをオンにし、アクション、編集を選択します。または、項目自体を選択します。
5. ライセンスアセットグループのページで編集ボタンを選択します。ここから、次のことができます。
 - ライセンスアセットグループ名を編集する
 - ライセンスアセットグループの説明を編集する
 - ライセンスアセットルールセットの追加または削除
 - ライセンスアセットグループタグの追加または削除
6. 変更が完了したら、変更の保存を選択します。

CLI を使用してライセンスアセットグループを更新するには

- `update-license-asset-group` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットグループの削除

不要になったライセンスアセットグループは削除できます。このアクションは元に戻すことができません、ライセンスアセットグループに関連付けられたルールセットは削除されないことに注意してください。

コンソールを使用してライセンスアセットグループを削除するには

1. 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、ライセンスを選択します。
3. ライセンスアセットグループセクションで、1 つ以上のライセンスアセットグループが使用可能であることを確認します。
4. 削除対象のライセンスアセットグループを選択するには、チェックボックスを選択し、アクション、削除を選択します。または、項目自体を選択し、ライセンスアセットグループのページから削除ボタンを選択します。
5. ライセンスアセットグループを完全に削除するには、テキストボックス **confirm** に「削除」と入力し、「削除」を選択します。

Important

このアクションを元に戻すことはできません。このライセンスアセットグループに関連付けられたルールセットは削除されません。

CLI を使用してライセンスアセットグループを削除するには

- `delete-license-asset-group` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットグループの詳細の表示

関連するルールセット、インスタンス、ライセンスなど、ライセンスアセットグループに関する詳細情報を表示できます。

コンソールを使用してライセンスアセットグループの詳細を表示するには

1. 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、ライセンスを選択します。
3. ライセンスアセットグループセクションで、1 つ以上のライセンスアセットグループが使用可能であることを確認します。
4. ライセンスアセットグループの詳細を表示するには、チェックボックスを選択し、アクション、詳細の表示を選択します。または、項目自体を選択します。

CLI を使用してライセンスアセットグループを表示するには

- `get-license-asset-group` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットグループを一覧表示する

アカウント内のすべてのライセンスアセットグループを一覧表示して、ステータスと設定を表示できます。

コンソールを使用してライセンスアセットグループを一覧表示するには

1. 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、ライセンスアセットグループを選択します。
3. ライセンスアセットグループの名前、ステータス、および関連するルールセットのリストを表示します。

CLI を使用してライセンスアセットグループを一覧表示するには

- `list-license-asset-groups` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットグループの検出されたアセットの一覧表示

ライセンスアセットグループに関連付けられたすべてのインスタンス、付与されたライセンス、セルフマネージドライセンスの表示には、最大 24 時間かかります。インスタンス、付与されたライセンス、セルフマネージドライセンスへの変更は 24 時間に反映されます。

コンソールを使用してライセンスアセットグループのアセットを一覧表示するには

1. 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、ライセンスを選択します。
3. チェックボックスを選択し、アクション、ビューの詳細を選択して、ライセンスアセットグループの詳細を表示します。または、項目自体を選択します。
4. ライセンスアセットグループのページから、ライセンスアセットグループに関連付けられたすべてのインスタンス、付与されたライセンス、セルフマネージドライセンスを表示できます。

CLI を使用してライセンスアセットグループのアセットを一覧表示するには

- `list-assets-for-license-asset-group` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ライセンスアセットルールセットの使用

このセクションでは、でライセンスアセットルールセットを作成、更新、削除、管理する方法について説明します AWS License Manager。ライセンスアセットルールセットは、ライセンスアセットグループのリソース検出基準を定義します。

ルールセットについて

ルールセットは、License Manager 内のリソースで、製品のリソース検出基準を定義します。これは、製品検出に使用できる関連ルールの論理グループとして機能し、ルールセットはさまざまな製品で使用できます。

ルールセットには 2 つの異なるタイプがあります。

- AWS マネージドルールセット - License Manager サービスによって作成および保守
- カスタムルールセット - お客様が作成および管理

ルールセットの主な利点は、新しいルールをルールセットに追加でき、それらの変更は、製品の検出に自動的に使用される同じルールセットを使用してすべてのライセンスアセットグループに自動的に反映されることです。

ルールセットタイプ

ライセンスベース

AWS Marketplace 製品を含むセルフマネージドライセンスまたは付与ライセンスの場合
インスタンスベース

特定のプロパティに基づいてインスタンスを検出するには

各ルールセットには、ソフトウェアを検出して追跡する方法を定義する最大 5 つのルールが含まれています。ライセンス、インスタンス、またはその両方を識別するルールを作成し、AND、OR、または完全に一致するロジックを使用して複数の条件を組み合わせて、管理するリソースを正確にターゲットにすることができます。

次の表は、ライセンスアセットルールセットルールの作成時に使用できるキーを示しています。

ライセンスアセットルールセットルールキー

ルールタイプ	Key	オペレーター	値の型	使用できる値
セルフマネージドライセンス	ライセンス設定 ARN	Equals と Not Equals	リスト	有効な ARN
	AWS アカウント ID	Equals と Not Equals	リスト	String
付与されたライセンス	ライセンス ARN	Equals と Not Equals	リスト	有効な ARN
	製品 SKU	Equals と Not Equals	リスト	String
	Issuer	Equals と Not Equals	リスト	String
	受益者	Equals と Not Equals	リスト	String
	ライセンスステータス	Equals と Not Equals	リスト	有効なライセンスステータス
	ホームリージョン	Equals と Not Equals	リスト	有効な AWS リージョン

ルールタイプ	Key	オペレーター	値の型	使用できる値
インスタンス	プラットフォーム	Equals と Not Equals	リスト	Windows、Linux
	EC2 請求製品	Equals と Not Equals	リスト	windows-server-ent erprise、Windows- byol、sql-server- standard、sql-server- enterprise、rhel、rhel -byol、rhel-high- availability、ubuntu- pro、suse-linux
	Marketplace 製品コード	Equals と Not Equals	リスト	String
	AMI ID	Equals と Not Equals	リスト	String
	インスタンスタイプ	Equals と Not Equals	リスト	String
	[インスタンス ID]	Equals と Not Equals	リスト	String
	ホスト ID	Equals と Not Equals	リスト	String

ルールタイプ	Key	オペレーター	値の型	使用できる値
	AWS アカウント ID	Equals と Not Equals	リスト	String

AWSマネージドルールセットの使用

AWS は、一般的なソフトウェア製品用に事前設定されたルールセットを提供します。これらのマネージドルールセットは、によって自動的に更新および管理されます AWS。

AWSマネージドルールセットを使用するには

1. 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、ライセンスアセット検出とルールセットを選択します。
3. ライセンスアセットルールセットセクションで、AWSマネージドルールセットを選択します。
4. 使用可能なマネージドルールセットを参照し、ソフトウェア製品に一致するルールセットを選択します。

使用可能な AWSマネージドルールセットは次のとおりです。

- Microsoft Windows Server データセンター
- Microsoft SQL Server Enterprise Edition
- Microsoft SQL Server Standard Edition
- Red Hat Enterprise Linux
- Ubuntu Pro
- SUSE Enterprise Linux

カスタムルールセットの作成

環境と要件に固有のライセンスとインスタンスの追跡ルールを定義するための独自のルールセットを作成できます。

コンソールを使用してルールセットを作成するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションペインで、ライセンスアセット検出とルールセットを選択します。
3. License asset ruleset セクションで、Create Ruleset を選択します。
4. ルールセット名には、ルールセットのわかりやすい名前を入力します。
5. ルールセットの説明には、ルールセットの目的の説明を入力します。
6. (オプション) ルールセットにタグを追加し、次へを選択します。
7. ステップ 2 (ライセンスの検出を設定する) では、ライセンスに関連するルールを追加できます。これにより、システムはライセンスを使用して、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量を計算できます。ライセンスの検出はオプションですが、ライセンス使用量の計算が必要な場合は追加することをお勧めします。
 - セルフマネージドライセンスを追加し、ARN またはアカウント ID を提供できます
 - 付与されたライセンス (AWS Marketplace から調達されたライセンス) ARN、ProductSKUなどを追加することもできます。
 - ルールの追加を選択して、複数のルールを追加できます。
8. ステップ 3 (インスタンスの検出を設定する) では、さまざまなインスタンスを検出する方法に関するルールを追加できます。これにより、インスタンスは選択基準に基づいて検出され、それらのインスタンスはライセンスアセットグループを設定する製品に考慮されます。次のフィールドを選択して、1 つ以上のルールを追加できます。
 - プラットフォーム (Windows または Linux)
 - EC2 請求製品コード
 - Marketplace 製品コード
 - AMI ID、ホスト ID、インスタンス ID など。
9. 設定を確認し、送信を選択します。
10. 最近作成したルールセットは、マイルールセットで確認できます。

CLI を使用してルールセットを作成するには

- `create-license-asset-ruleset` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ルールセットの更新

カスタムルールセットを更新して、設定の変更、ルールの追加または削除、タグの更新を行うことができます。

コンソールを使用してルールセットを更新するには

1. 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、ライセンスアセット検出とルールセットを選択します。
3. License asset ruleset セクションで、My rulesets に移動します。
4. ルールセットを選択するには、関連するチェックボックスを選択し、アクション、編集を選択します。または、ルールセット名を選択し、ルールセットページの編集ボタンを選択します。
5. ここから、次の更新を行うことができます。
 - ルールセット名を編集する
 - ルールセットの説明を編集する
 - リソースに関連付けられたタグを追加または削除する
6. 変更が完了したら次へを選択します。次の画面から、次のことができます。
 - ルールの追加または削除
 - 既存のルールのライセンスタイプを更新する

- 既存のルールの条件を更新する
7. 変更が完了したら次へを選択します。次の画面から、次のことができます。
 - 包含ルールを追加または削除して、包含するインスタンスを識別する条件を指定する
 8. 前の画面で行われた変更を確認して編集します。送信を選択して変更を確定します。

CLI を使用してルールセットを更新するには

- `update-license-asset-ruleset` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ルールセットの削除

不要になったカスタムルールセットを削除できます。ルールセットは、すべてのライセンスアセットグループから削除されるまで削除できません。

コンソールを使用してルールセットを削除するには

1. 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、ライセンスアセット検出とルールセットを選択します。
3. License asset ruleset セクションで、My rulesets に移動します。
4. 削除対象のルールセットを選択するには、関連するチェックボックスを選択し、アクション、削除を選択します。または、ルールセット名を選択し、ルールセットページの削除ボタンを選択します。
5. ルールセットを完全に削除するには、テキストボックス **confirm** に「削除」と入力し、「削除」を選択します。

⚠ Important

このアクションを元に戻すことはできません。ルールセットは、すべてのライセンスアセットグループから削除されるまで削除できません。

CLI を使用してルールセットを削除するには

- `delete-license-asset-ruleset` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ルールセットの詳細の取得

設定やルールなど、特定のルールセットに関する詳細情報を取得できます。

CLI を使用してルールセットを取得するには

- `get-license-asset-ruleset` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

ルールセットの一覧表示

アカウント内のすべてのルールセットを一覧表示して、使用可能なルールセットの概要を取得できます。

CLI を使用してルールセットを一覧表示するには

- `list-license-asset-rulesets` コマンドを使用します。詳細については、「[AWS CLI コマンドリファレンス](#)」を参照してください。

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

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、がライセンスを消費するコマンド AWS を処理する方法が決まります。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。

セルフマネージドライセンスは、単一、クロス AWS アカウント、AWS アカウント またはライセンスアセットグループと統合して、AWS 組織全体の複数の AWS アカウントとリージョンを一元管理できます。この統合により、エンタープライズ環境のガバナンスとコンプライアンスの追跡が強化されます。

AWS のサービス License Manager などのサービスクォータは、そのサービス AWS アカウントで利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。例えば、License Manager 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、どの場合も合計 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、の[AWS License Manager 「サービスクォータ」](#)を参照してください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表示する](#)
- [License Manager でセルフマネージドライセンスを無効にする](#)
- [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ルール](#)

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。

複数の AWS アカウントでライセンスを管理する組織では、一元化されたガバナンスとポリシーの適用を提供するライセンスアセットグループの使用を検討してください。セルフマネージドライセンスは個々のアカウント内で機能し、組織全体を可視化するためにライセンスアセットグループと統合できます。

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、[vCPU]、[コア]、[ソケット]、および [インスタンス] 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。
- (オプション) 有効期限 - このライセンス設定の有効期限を示します。お客様は、BYOL ライセンスの の条件に基づいて、有効期限に基づいてこの日付を入力できます。
- 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、SQL Server、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。
 - 最大 vCPU - リソースの最大 vCPU 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。
 - 最小 vCPU - リソースの最小 vCPU 数。
- テナンシー - ライセンスの使用を指定した 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。カウントタイプがインスタンスまたは vCPUs の場合、共有テナンシー、Dedicated Hosts、およびハードウェア専有インスタンスがサポートされます。コンソール (および API) の名前は次のとおりです。
 - 共有EC2-Default
 - ハードウェア専有インスタンス (EC2-DedicatedInstance)
 - Dedicated Host (EC2-DedicatedHost)
 - vCPU の最適化 - License Manager は Amazon EC2 の [CPU の最適化](#) サポートと統合されており、インスタンスの vCPU の数をカスタマイズできます。このルールを True に設定すると、License Manager はカスタマイズされたコア数とスレッド数に基づいて vCPUs をカウントします。それ以外の場合は、ライセンスマネージャーはインスタンスタイプのデフォルトの vCPUs 数をカウントします。
- 停止したインスタンスを含める - このルールを True に設定すると、License Manager は停止したインスタンスを追跡し、ライセンス使用量としてカウントします。デフォルト値は False です。False に設定すると、停止したインスタンスはライセンスの使用にはカウントされず、そのライセンスは使用可能なライセンスのプールに解放されます。

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	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)	licenseAffinityToHost	✓		✓	
最大コア	maximumCores	✓	✓		
最大ソケット	maximumSockets		✓	✓	
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の最適化	honorVcpuOptimization				✓
停止したインスタンスを含める	includedStoppedInstances	✓	✓	✓	✓

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。またオプションは AWS へのリソースの移行計画の詳細にも依存します。

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。ベンダーのライセンス条項は、AWS 要件と制限にも影響します。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 Manager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。ライセンス条件には、CPUコアの種類、テナンシー、サーバーあたりの最小ライセンスの数の制約が含まれています。

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。
- インスタンスが停止しても、ライセンスは割り当てられる必要があります。

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。

ライセンスマネージャールール	設定
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	テナンシー Dedicated Host に設定されています。
停止したインスタンスを含める	停止したインスタンスを含める は に設定されます True 。停止したインスタンスは引き続きライセンスを消費します。

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では、ライセンスのカウント方法 (vCPU 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。

Note

セルフマネージドライセンスを作成する前に、組織構造を考慮してください。

- 単一アカウントの使用状況: アカウントで直接セルフマネージドライセンスを作成する
- マルチアカウントの使用: まずライセンスアセットグループを作成し、次にセルフマネージドライセンスを関連付けて一元管理することを検討してください。

Amazon RDS for 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 RDS for 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/>。
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。
 - 有効期限 — セルフマネージドライセンスのオプションの有効期限。
 - ライセンスタイプ - このライセンスのカウントモデル ([vCPU]、[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。これを行うには、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、情報を入力してそのプロパティを識別します。
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. [\[Submit\]](#) を選択してください。

 Note

License Expiry Date が設定されると、License Manager は で設定された Amazon SNS トピックに 120 日、90 日、60 日、30 日、0 日に通知を送信できます [License Manager のセルフマネージドライセンス設定](#)。

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)
- [New-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

を使用して AWS Resource Access Manager、任意の AWS アカウントまたは を通じてセルフマネージドライセンスを共有できます AWS Organizations。詳細については、「AWS RAM ユーザーガイド」の [AWS「リソースの共有」](#) を参照してください。

Organization とセルフマネージドライセンスを共有する AWS

前提条件

この手順を完了するには、AWS Organization を License Manager にリンクする必要があります。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。

ライセンスを共有する

セルフマネージドライセンスを AWS Organization と共有するには、次の手順に従います。

1. 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. アクションメニューから AWS 組織アカウントと共有を選択します。

サポートされるアカウントのクォータ

2023 年 10 月 14 日より AWS License Manager 前に でライセンス共有を有効にした場合、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。次のセクションで説明する の API オペレーションを使用して AWS RAM 、このクォータを増やすことができます。License Manager のデフォルトクォータについて詳しくは、「AWS 全般のリファレンス ガイド」の「[ライセンスで使用するクォータ](#)」を参照してください。

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. [describe-organization](#) AWS CLI コマンドを使用して、オペレーションを使用して組織の ARN を決定します。

```
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. [get-resource-shares](#) AWS CLI コマンドを使用して、オペレーションを使用して組織の ARN を決定します。

```
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. [enable-sharing-with-aws-organization](#) AWS CLI コマンドを使用して、以下とのリソース共有を有効にします AWS RAM。

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

{
  "returnValue": true
}
```

[list-aws-service-access-for-organization](#) AWS CLI コマンドを使用して、Organizations リストのサービスプリンシパルが License Manager で有効になっていること、および以下を確認できます 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

が組織のこのオペレーションを完了する AWS RAM までに最大 6 時間かかる場合があります。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. [associate-resource-share](#) AWS CLI コマンドを使用して、License Manager リソース共有を組織と関連付けます。

```
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
    }
  ]
}
```

[get-resource-share-associations](#) AWS CLI コマンドを使用して、リソース共有の関連付けstatusがであることを確認します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
- 有効期限
- <option> 数
- ライセンスタイプの制限を強制
- 停止したインスタンスを含める

セルフマネージドライセンスを編集するには

1. 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。

Note

License Expiry Date が設定されると、License Manager は で設定された Amazon SNS トピックに 120 日、90 日、60 日、30 日、0 日に通知を送信できます [License Manager のセルフマネージドライセンス設定](#)。

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)
- [Update-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

License Manager でセルフマネージドライセンスを表示する

License Manager コンソールを使用してセルフマネージドライセンスを表示し、AWS 環境全体の使用状況、コンプライアンス、およびディストリビューションをモニタリングできます。

1 つのアカウントでライセンスを表示する

現在のアカウント内のセルフマネージドライセンスを表示するには:

1. 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、**[Self-managed licenses]** を選択します。
3. ライセンスのリスト、ステータス、現在の使用状況を確認します。
4. ライセンス名を選択すると、関連するリソースやコンプライアンスステータスなどの詳細情報が表示されます。

集約ライセンスを表示する (組織管理者または委任管理者の場合)

組織管理者と委任管理者は、一元管理された場所から組織内のすべての AWS アカウントのセルフマネージドライセンスを表示できます。これにより、ライセンスコンプライアンスのための組織全体の可視性と管理機能が提供されます。

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. 組織管理者または委任管理者としてサインインしていることを確認します。
3. 左側のナビゲーションペインで、**[Self-managed licenses]** を選択します。
4. **Organization license configuration** タブを選択して、集約されたライセンスビューを表示します。
5. 組織のアカウント全体のすべてのセルフマネージドライセンスの集約ビューを確認します。

この集約ビューは、一元化されたライセンスガバナンスを可能にし、AWS 組織全体のコンプライアンスを確保するのに役立ちます。

コマンドラインを使用して集約ライセンスを表示するには

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

License Manager でセルフマネージドライセンスを無効にする

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している既存のリソースは影響を受けず、そのライセンスを使用している AMI は引き続き起動することができます。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. 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)
- [Update-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す。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. 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)
- [Remove-LICMLicenseConfiguration](#) (AWS Tools for PowerShell)

License Manager のセルフマネージドライセンスルール

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AMIからシームレスに EC2 インスタンスを起動でき、管理者は組み込みのLicense Manager ダッシュボードを介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げることができます。

追跡対象サーバーが終了すると、そのライセンスは解放され、使用可能なライセンスのプールに戻されます。デフォルトでは、追跡対象サーバーが停止すると、そのライセンスもリリースされ、プールに戻されます。ただし、停止したインスタンスを含めるルール (includedStoppedInstances) が True に設定されている場合、停止したインスタンスは引き続き追跡され、ライセンス使用量として

カウントされます。これは、実行中の状態に関係なく、ライセンスがインスタンスに割り当てられ続けることをライセンス条件が要求する場合に便利です。

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。

- 手動でのセルフマネージドライセンスと AMI の関連付け - オペレーティングシステムや他のソフトウェアのライセンスを追跡する場合、それらを公開して組織内で広く使用できるようにする前に、ライセンスルールを AMI に添付することができます。これらのAMIからのデプロイメントは、ユーザーによる追加のアクションを必要とせずに、License Manager によって自動的に追跡されます。[Systems Manager Automation](#)、[VM Import/Export](#) および [Packer](#) といった現在お使いの AMI 作成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。
- Amazon EC2 起動テンプレートと AWS CloudFormation – AMIs にライセンスルールをアタッチすることが推奨されない場合は、[EC2 起動テンプレート](#) または [CloudFormation テンプレート](#) でオプションパラメータとして指定できます。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。セルフマネージドライセンスフィールドに 1 つ以上のセルフマネージドライセンス IDs を指定することで、EC2 起動テンプレートまたは CloudFormation テンプレートにルールを適用できます。

AWS は、ライセンス追跡データを、ライセンス追跡データを所有する AWS アカウントを介してのみアクセス可能な機密データとして扱います。は、ライセンス追跡データにアクセス AWS 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 AMI の関連付け

以下の手順では、License Manager コンソールを使用して、セルフマネージドライセンスを AMI に関連付ける方法を示します。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。所有または共有されている、アクセス可能な任意の AMI に、セルフマネージドライセンスを関連付けることができます。AMI がユーザーと共有されている場合は、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の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。

すべてのアカウントのセルフマネージドライセンスに AMI を関連付けると、アカウント間で AMI から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。

同じリージョン内で AMI をコピーし、その AMI にライセンス設定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 AMI に関連付けられます。新しい AMI からインスタンスを起動すると、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から新しい AMI 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 AMI に関連付けられ、License Manager は新しい AMI から起動したインスタンスを追跡します。

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。ライセンス設定が関連付けられている AMI を別のリージョンにコピーすると、License Manager は新しい AMI からのすべてのインスタンス起動をブロックします。

セルフマネージドライセンスと AMI を関連付けるには

1. 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AMIを表示するには、関連付けられているAMIを選択します。
4. [Associated AMI] を選択します。
5. [Available AMIs] で、1 つまたは複数のAMIを選択し、[Associate]を選択します。
 - アカウントが少なくとも AMIs の1 つのを所有している場合は、所有しているAMIsのAMIアソシエーション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共有されたAMI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。
 - AMIが別のアカウントからユーザーと共有されている場合、AMIはお客様のアカウントにのみ関連付けられます。

新しく関連付けられたAMIは [ライセンスの詳細] ページの関連付けられているAMIsタブに表示されます。

セルフマネージドライセンスと AMI の関連付けの解除

以下の手順では、License Manager コンソールを使用して、セルフマネージドライセンスと AMI の関連付けを解除する方法を説明します。登録解除されたAMIの関連付けを解除することはできません。License Manager は 登録解除されたAMIを8時間ごとにチェックし、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 AMI の関連付けを解除するには

1. 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. [Associated AMIs] を選択します。
5. AMIを選択し、AMI関連付け解除を選択します。

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とは、組織が [AWS Marketplace](#)、[AWS Data Exchange](#) から購入した製品のライセンス、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購入した製品のライセンスです。ライセンス管理者は AWS License Manager、を使用して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 AWS アカウントに配布できます。

AWS Data Exchange 製品に配布されるデータライセンスは、AWS AWS Data Exchange を通じてアカウントで利用できます。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 AWS Marketplace ライセンスからアカウントにエンタイトルメントを AWS 配布し、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を通じて AWS アカウントで使用できます AWS Marketplace。アカウントには、製品へのアクセス権もあります。たとえば、ライセンス管理者が から Amazon マシンイメージ (AMI) を購入 AWS Marketplace し、エンタイトルメントを AWS アカウントに配布する場合、AWS Marketplace と Amazon EC2 を使用して AMI から Amazon EC2 インスタンスを起動できます。

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 で承諾とアクティベーションを付与する](#)
- [License Manager での許可のライセンスステータス](#)
- [License Manager の購入者アカウントの CloudWatch 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。ライセンスを承諾してアクティブ化する方法は、ライセンスの送信元かどうか AWS Marketplace、アカウントが組織のメンバーアカウントかどうか AWS Organizations、組織ですべての機能が有効になっているかどうかによって異なります。

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 AWS リージョンに自動的にレプリケートします。これにより、お客様にライセンスが付与されたすべてのリージョンを一元的に把握することができます。

AWS Marketplace および AWS Data Exchange からのライセンス

- 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ブ化する必要があります。

Console (My licenses)

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

アカウントで付与されたライセンスを管理するには

1. 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 - ライセンスを作成する際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。同じ商品SKUが複数のISVにわたって存在する場合があります。

- 受信者 - ライセンス受信者の ARN。
 - 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の場合 AWS Marketplace、最初の付与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 AWS License Manager コンソール設定 AWS Organizations を使用してリンクする必要があります。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. 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 - ライセンスを作成する際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。同じ商品SKUが複数のISVにわたって存在する場合があります。
 - 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は 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

を使用して AWS CLI、付与されたライセンスを操作できます。

AWS CLIを使用して付与されたライセンスを管理するには

- [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。詳細については AWS Organizations、[AWS Organizations 「の用語と概念」](#)を参照してください。

権限の受信者を以下のいずれかとして指定できます。

- AWS アカウント指定されたアカウントのみを含む。
- 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。
- 指定された組織単位 (OU) と、指定された OU の下にあるネストされた OU 内のすべてのアカウントを含む、ネストされていない OU。

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。

AWS License Manager コンソールまたは を使用して、使用権限 AWS CLI を配布できます。コンソールで許可を作成するときに組織 ID または組織 ARN を指定できますが、AWS CLIでは ARN 形式を使用する必要があります。例えば、ARN は次のようになります。

組織 ID の ARN

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

組織 OU の 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. 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. 許可受信者の AWS アカウント ID、AWS Organizations OU ID または ARN、または AWS Organizations ID または ARN を入力します。
 - 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

を使用してエンタイトルメントを AWS CLI 配布できます。AWS License Manager API を使用する場合は、組織 ID または OU を ARN 形式で指定する必要があります。

AWS CLIを使用して権限を作成し、一覧表示するには

- [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 で承諾とアクティベーションを付与する

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。権限のアクティベーションプロセスには、AWS Marketplaceから取得された、付与されたライセンスの追加オプションが含まれる場合があります。

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

拒できます。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。グラントの自動承諾を有効にするには、管理アカウントから AWS License Manager コンソール [の設定](#) ページで組織アカウントをリンクします。

から同じ製品に対して AWS Marketplace 2 つのライセンスを同時にアクティブ化することはできません。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 AWS CLI を使用できます。
 - 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. CreateGrantVersion API を使用して、Status が Active の ActivationOverrideBehavior に ALL_GRANTS_PERMITTED_BY_ISSUER を指定して新しい権限を有効化します。

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。から取得された許可をアクティブ化すると AWS Marketplace、アクティブな許可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、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を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. 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

を使用して AWS CLI、付与されたライセンスを操作できます。

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。
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。

ステータス	説明
拒否	権限の被付与者によって権限が拒否されました。
アクティブ	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。
無効	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。

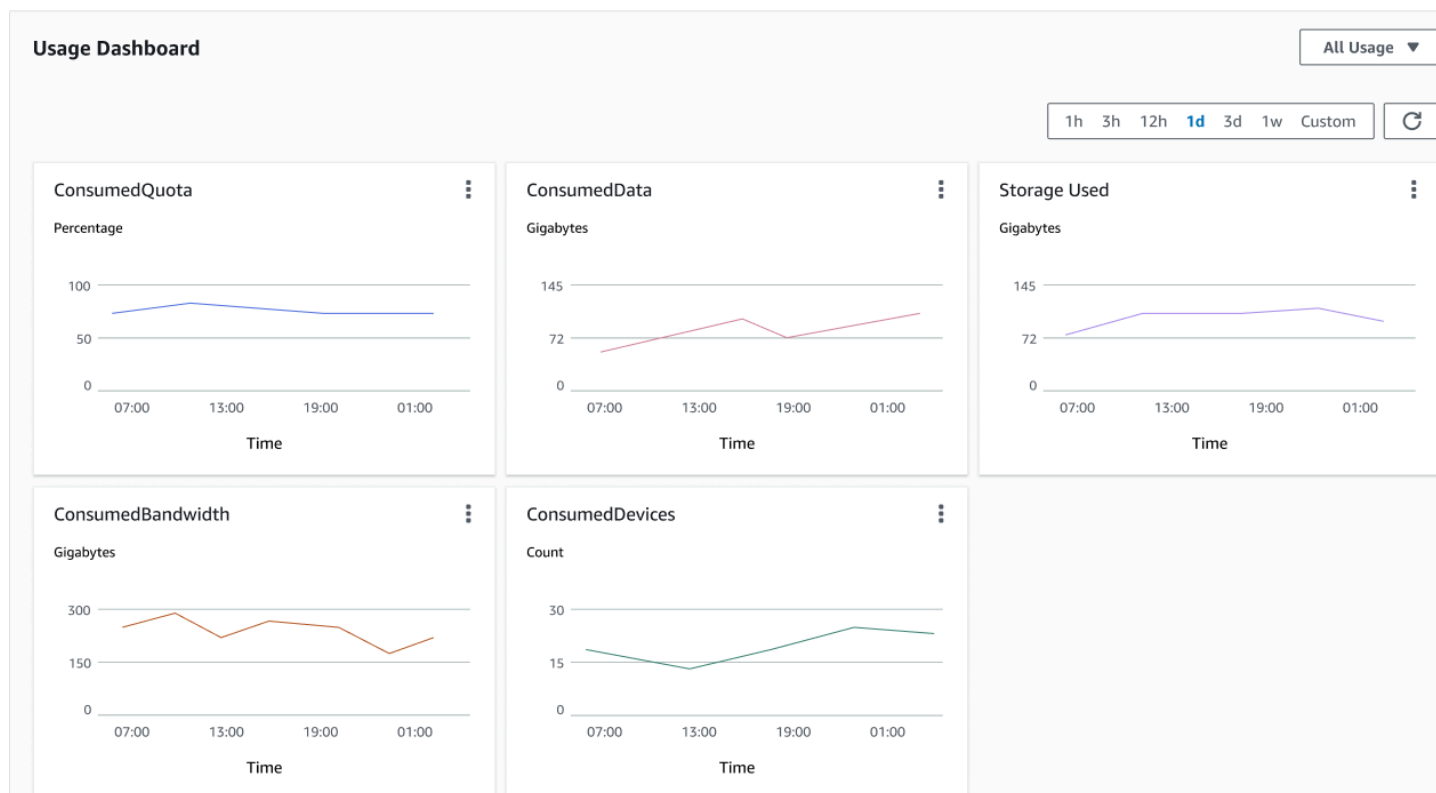
License Manager の購入者アカウントの CloudWatch メトリクス

販売者が発行したライセンスの権限が [使用状況レコードの送信を許可] 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、および使用状況の記録対象となるアカウントに CloudWatch メトリクスを出力します。購入者アカウントは、販売 AWS アカウント 者が発行したライセンスを購入または付与した です。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の使用状況を記録する場合、使用状況が記録されるアカウントとルート購入者アカウントの License Manager コンソールの [使用状況ダッシュボード] ページには、CloudWatch ウィジェットが表示され、そこで使用状況レコードを確認できます。購入者は、AWS Organizationsでライセンスを配布したアカウントのメトリクスも確認できます。[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について表示されます。

以下の画像は、使用状況ダッシュボードの例です。



ライセンス分析

ライセンスアセットグループは、包括的なダッシュボードと視覚化機能を提供し、組織内のすべての AWS リージョンとアカウントでソフトウェアライセンスポートフォリオを可視化できます。

内容

- [プライマリダッシュボードビュー](#)
- [個々のライセンスアセットグループビュー](#)
- [使用状況レポートを作成する](#)

プライマリダッシュボードビュー

ライセンスアセットグループダッシュボードには、インスタンス数に基づいて上位 5 つのライセンスアセットグループが、リアルタイムの消費追跡とともに表示されます。

時間範囲の選択

- 過去 1、3、6、12 か月、またはカスタム日付範囲から選択

- 柔軟な日付範囲を使用して季節的なパターンを特定し、成長傾向を追跡する

インタラクティブビジュアライゼーション

- グラフにカーソルを合わせると、詳細なインスタンス数が表示されます。
- ライセンスタイプの使用状況の傾向を表示します。
 - セルフマネージドライセンス - ソフトウェアベンダーからの BYOL
 - 付与されたライセンス - AWS Marketplace またはサードパーティーの調達および AWS提供ライセンス

個々のライセンスアセットグループビュー

ドロップダウンメニューからライセンスアセットグループを選択すると、詳細情報が表示されます。

概要タブ

詳細

- ライセンスアセットグループ内で追跡されるインスタンスの合計数
- ライセンスアセットグループ内で追跡される付与されたライセンス
- ライセンスアセットグループ内で追跡されるセルフマネージドライセンス

今後の更新

ライセンスアセットグループ内で追跡される、今後 7、30、または 100 日間に更新されるライセンスのリスト

Note

今後の更新を表示するには、ライセンスの有効期限を設定する必要があります。「[License Manager でセルフマネージドライセンスを編集する](#)」を参照してください。

使用状況の傾向

インスタンスとライセンスの傾向には、ライセンスアセットグループ内で追跡された選択した期間におけるセルフマネージドライセンスと付与されたライセンスの両方のライセンス消費パターンが表示されます。

ライセンスアセットグループによって提供されるメトリクスの詳細については、「」を参照してください [Amazon CloudWatch による License Manager のモニタリング](#)。

使用状況レポートを作成する

AWS License Manager は、セルフマネージドライセンスとライセンスアセットグループの両方に包括的な使用状況レポート機能を提供します。セルフマネージドライセンスの定期レポートまたはライセンスアセットグループのオンデマンドレポートを生成して、組織全体のライセンスの使用状況、コンプライアンス、リソースインベントリを追跡できます。

セルフマネージドライセンスレポート

セルフマネージドライセンスレポートは、ライセンス使用状況の定期的なスナップショットを提供します。Amazon S3 バケットへの自動発行を使用して、環境内のさまざまなライセンスタイプを追跡するように複数の使用状況レポートを設定できます。

セルフマネージドライセンスの概要レポート

消費されたライセンスの数に関する情報と、ライセンス数、ライセンスルール、リソースタイプ間の配布など、セルフマネージドライセンス設定に関する詳細が含まれています。

リソース使用状況レポート

追跡されたリソースとそのライセンス消費に関する詳細を提供し、各リソースをライセンス ID、ステータス、AWS アカウント ID 情報とともに一覧表示します。

セルフマネージドライセンス使用状況レポートを作成するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションパネルから、使用状況レポート (ライセンス分析の下) を選択します。
3. 使用状況レポートの作成を選択し、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。

- c. 生成するレポートタイプを選択します。
 - d. 頻度を選択します: 24 時間に 1 回、7 日に 1 回、または 30 日に 1 回。
 - 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。

CLI を使用してセルフマネージドライセンスレポートを作成するには

- `create-license-manager-report-generator` コマンドを使用します。

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

ライセンスアセットグループレポート

ライセンスアセットグループレポートは、組織内の複数の AWS リージョンとアカウントにわたるソフトウェアライセンスコンプライアンスに関するオンデマンドの包括的なレポートを提供します。これらのレポートは、検出され、ライセンスアセットグループにマッピングされたすべてのリソースの詳細なインベントリを提供します。

ライセンスアセットグループレポートを作成するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. ナビゲーションパネルから、使用状況レポート (ライセンス分析の下) を選択します。
3. ライセンスアセットグループレポートの作成を選択し、パラメータを定義します。
 - a. レポートの名前とオプションの説明を入力します。

- b. ドロップダウンリストからライセンスアセットグループを選択します。
 - c. 日付範囲を選択して、その範囲内のすべてのリソースを一覧表示します。
 - d. (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。

CLI を使用してライセンスアセットグループレポートを作成するには

- 特定の時間範囲のオンデマンドレポートには、`create-license-manager-report-generator` コマンドを使用します。

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

Note

ライセンスアセットグループレポートは、指定された時間範囲でオンデマンドで生成され、定期的なスケジューリングはサポートされていません。--report-frequency のパラメータは省略します。

レポートストレージ

使用状況レポートは 60 分以内に公開されます。アカウントに Amazon S3 バケットがまだ関連付けられていない場合、License Manager は使用状況レポートの作成時に新しい Amazon S3 バケットを作成します。レポートは、次の Amazon S3 URI パターンで保存されます。

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

CLI コマンドの詳細については、[create-license-manager-report-generator \(\)](#)」を参照してください
AWS CLI。

 Note

AWS License Manager はレポートを保存しません。レポートは Amazon 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 Amazon S3 バケットに発行されなくなります。

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。

ライセンスアセットグループを使用している組織の場合、インベントリの検索結果を AWS Organizations 内の複数の AWS リージョンとアカウントに統合できるため、検出されたリソースがどのリージョンまたはアカウントに存在するかに関係なく、統合されたビューが提供されます。

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 サーバー以外の情報を up-to-date 状態に保つには、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。

あなたの組織が AWS ユーザーに AMI 派生インスタンスの作成や実行中のインスタンスへの追加ソフトウェアのインストールを制限していない場合にも、リソースインベントリの追跡は役立ちます。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て、管理された AMI から作成されたインスタンスと同じように、追跡と検証を行うことができます。

内容

- [License Manager でインベントリ検索を操作する](#)
- [License Manager でのインベントリの自動検出](#)

License Manager でインベントリ検索を操作する

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](#)
- [自動検出ルールをセルフマネージドライセンスに追加する](#)
- [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 との SQL Server Enterprise のライセンス契約の条件を反映した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) と含まれているライセンスの種類 (たとえば、「SQL Server Web」のライセンスでないもの) で検索できます。

リソースインベントリを検索する

1. 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 [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、検索結果を合理化できます。

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
Resource ID (リソース ID)	リソースの ID。	Equals, Not equals	
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	• SQL Server Enterprise • SQL Server Standard •

フィルター名	説明	論理演算子	サポートされる値
			SQL Server Web • Windows Server Datacenter
タグ	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。 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。	Equals, Not equals	

「Amazon RDS のリソース」

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エディション。	Equals	- 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
License Pack (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	- 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 RDS 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。

自動検出ルールをセルフマネージドライセンスに追加する

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. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
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. [Add] (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. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
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に関連付ける] 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 を選択してください。

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. 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 のインベントリ](#) を使用して Amazon EC2 インスタンスやオンプレミスインスタンス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。AWS アカウントID、または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することができます。

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。自動検出のためのルールは、API コマンド「[UpdateLicenseConfiguration](#)」を使って CLI 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. 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. 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 RDS for Oracle や Amazon 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す。

- 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。

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と Bring Your Own License Model (BYOL) 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。

オンプレミスのワークロードを Amazon EC2 に移行してください

移行中、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。移行中にリリースされたライセンスを使用できるように、BYOL に変更できます。

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 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、柔軟なpay-as-youのライセンスモデルを使用して、が提供す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

小規模または不規則なワークロードの場合、AWS 提供されたライセンス (ライセンスを含む) 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 を使用する場合は、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 に戻すことができます。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 on Pro にサブスクリプションを追加すると、セキュリティ更新プログラムが長期間提供されます。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。

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、Windows Server ライセンスと Microsoft SQL Server ライセンスのサポートされているバージョンおよび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 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 Linux の対象となるサブスクリプションタイプ](#)
 - [ライセンスタイプの変換に関する考慮事項](#)

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 提供の Amazon マシンイメージ (AMI) から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。

Windows と SQL Server がライセンスタイプの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 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スタンダード版
- SQL Server Enterprise Edition版
- SQL Serverウェブ版

SQL Server 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
BYOL としての SQL Server (任意のエディション)	

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 BYOL としての SQL 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 ライセンスインクルードとしての SQL Server Web	RunInstances:0202
ライセンスインクルードとしての Windows Server SQL Server Standard (ライセンスインクルード)	RunInstances:0006
ライセンスインクルードとしての Windows Server SQL Server Enterprise (ライセンスインクルード)	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利用できるかを示しています。

ソース	ターゲット	
	BYOL	ライセンスインクルード
AWS が提供する Windows Server イメージ	いいえ	はい
AWS が提供する SQL Server イメージ	いいえ	はい
お客様の Windows Server メディア ¹	はい	はい
お客様の 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) を使用していることを示します。

変換パス

次の表は、BYOL とライセンスインクルードの間でソースライセンスモデルを別のライセンス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

- BYOL としての Windows Server とライセンスインクルードとしての SQL Server という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	ターゲット					
	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 BYOL とし ての SQL Server	ライセンス インクルー ドとしての Windows Server BYOL とし ての SQL Server	BYOL と しての Windows Server 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 Windows Server ライセンス インクル ードとし ての SQL Server
BYOL と しての Windows サーバー (お客様の メディア)	Not needed	Yes	Not needed	Yes ¹	Unsupport ed	Yes 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)	Yes ²	Not needed	Yes ^{1、2}	Not needed ³	Unsupport ed	Yes ¹
ライセン ス込みの Windows Server (AWS 提供	NoX	Not needed	NoX	Not needed ³	Unsupport ed	Yes ³

ソース	ターゲット					
されたイメージ)						
BYOL としての Windows サーバー (お客様のメディア)	Not needed ⁴	Yes	Not needed	Yes	Unsupported	Yes
BYOL としての SQL サーバー (お客様のメディア)						
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)	Yes ²	Not needed ⁴	Yes ²	Not needed	Unsupported	Yes
BYOL としての SQL サーバー (お客様のメディア)						

ソース	ターゲット					
ライセンス込みの Windows Server (AWS 提供されたイメージ)	NoX	Not needed ⁴	NoX	Not needed	Unsupported	Yes
BYOL としての SQL サーバー (お客様のメディア)						
BYOL としての Windows サーバー (お客様のメディア)	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported	Unsupported
ライセンスインクルードとしての SQL Server						

ソース	ターゲット					
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)	NoX	NoX	NoX	NoX	Unsupported	Not needed
ライセンス込みの SQL Server (AWS 提供イメージ)						
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)	Yes ^{2, 5, 6}	Yes ⁵	Yes ²	Yes	Unsupported	Not needed
ライセンスインクルードとしての SQL Server (お客様のメディア)						

ソース	ターゲット					
	No ^x	Yes ⁵	No ^x	Yes	Unsupported	Not needed
ライセンス込みの Windows 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 SQL Server (お客様のメディア)						

^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 用の BYOL 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 まず、ライセンスアクティベーションに独自の KMS サーバーを使用するように Windows の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 がインストールされていないソースから SQL Server がインストールされているターゲットに変換する場合は、SQL Server のライセンスタイプにかかわらず、まず SQL Server をインストールする必要があります。

⁴ SQL Server がインストールされているソースから SQL Server がインストールされていないターゲットに変換する場合は、SQL Server のライセンスタイプにかかわらず、まず SQL Server をアンインストールする必要があります。

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。これらの手順が完了したら、ライセンスタイプをライセンスインクルードとしての Windows Server に変換し、そのライセンスタイプをもう一度 BYOL としての Windows Server に変換する必要があります。

License Manager で Linux の対象となる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 などのアップデートが含まれます。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。

ライセンスタイプ変換は、Ubuntu、RHEL、RHEL for SAP の長期サポート (LTS) バージョンに使用できます。サブスクリプションは、が提供するオプションと Red Hat AWSが提供するオプションの間で切り替えることができます AWS Marketplace。

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。

RHEL と RHEL for SAP の変換

- Red Hat が AMI 出品として販売するサブスクリプションに変換する場合は AWS Marketplace 、ライセンス変換を開始する前に、まず Marketplace AMI 出品にサブスクライブする必要があります。
- の Red Hat Subscriptions SaaS リストに移行する AWS Marketplace には、変換前に Red Hat からサブスクリプションを購入する必要があります。
- から年間 Red Hat 契約を結 AWS Marketplace んでいる場合、別のサブスクリプションタイプに変換しても、未使用の月については返金されません。
- で Red Hat によって販売された RHEL for SAP から によって販売された RHEL for SAP AWS に変換 AWS Marketplace するには、にリクエスト AWS Marketplace を送信します サポート。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。

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にライセンスタイプ変換を使用することはできません。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 EC2 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。Amazon EC2 Savings Plans
- Ubuntu Pro から Ubuntu LTS に変換するには、にリクエストを送信します サポート。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提条件があります。

トピック

- [General](#)
- [Server](#)
- [Linux](#)

General

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。
- ターゲットインスタンスは で実行する必要があります AWS。オンプレミスインスタンスはサポートされていません。
- 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 の EC2 インスタンスのセットアップ](#)」と「[AWS Systems Manager インベントリ](#)」を参照してください。
- 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。

Server

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 提供の Amazon マシンイメージ (AMI) から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。オリジナルの 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。

RHEL

- AWSが提供するサブスクリプションから、Red Hat が AMI 出品として販売するサブスクリプションに変換する場合は AWS Marketplace、ライセンス変換を開始する前に、まず Red Hat から Marketplace AMI 出品にサブスクライブする必要があります。
- AWSが提供するサブスクリプションからの Red Hat Subscriptions SaaS リストに移行する AWS Marketplace には、変換前に Red Hat からサブスクリプションを購入する必要があります。

RHEL for SAP

- RHEL for SAP および Update Services の変換の場合、インスタンスは RunInstance:0010 の使用オペレーションとアタッチされた AWS Marketplace 製品コード AWS Marketplace を使用してから起動する必要があります。
- AWSが提供するサブスクリプションから、Red Hat が AMI 出品として販売するサブスクリプションに変換する場合は AWS Marketplace、ライセンス変換を開始する前に、まず Red Hat から Marketplace AMI 出品にサブスクライブする必要があります。
- AWSが提供するサブスクリプションからの Red Hat Subscriptions SaaS リストに移行する AWS Marketplace には、変換前に Red Hat からサブスクリプションを購入する必要があります。

Ubuntu

- 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。インスタンスからの TCP ポート 443 経由のアウトバウンドトラフィックが、以下のエンドポイントに到達すること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 リポジトリへの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 (CDN) 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

Windows ライセンス、Microsoft SQL Server ライセンス、および Ubuntu Linux サブスクリプションは、License Manager コンソールまたは AWS CLIを使用して変換できます。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。

ライセンスタイプを変換する

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。

例えば、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あり、各ルールでライセンスインクルードの Windows Server が除外されている場合、BYOL からライセンスインクルードの Windows Server にライセンスタイプを変更すると、セルフマネージドライセンスからインスタ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

ライセンスタイプを変更しても、インスタンスの起動に使用する AMI の請求製品情報は変わりません。正確な請求情報を取得するには、Amazon EC2 [DescribeInstances](#) API を使用します。さらに、AMI 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、これらのワークフローを更新して DescribeInstances を使用してください。

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](#)

- [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](#)
 - [Red Hat でサポートされている変換](#)
 - [HA および更新サービスを使用した RHEL for SAP \(AWS で販売 AWS Marketplace\) から HA および更新サービスを使用した RHEL for SAP \(で Red Hat で販売 AWS Marketplace\) に変換する](#)
 - [HA および更新サービス \(AWS で販売 AWS Marketplace\) を使用した RHEL for SAP から Red Hat サブスクリプション \(で Red Hat で販売 AWS Marketplace\) に変換する](#)
 - [Red Hat License-Included \(LI\) から RHEL \(Red Hat で販売 AWS Marketplace\) に変換する](#)
 - [の Red Hat Enterprise Linux \(RHEL\) から Red Hat License-Included \(LI\) に変換 AWS する](#)
 - [Red Hat サブスクリプション \(Red Hat で販売 AWS Marketplace\) から Red Hat ライセンス込み \(LI\) に変換する](#)
 - [その他の要件](#)
 - [Ubuntu Pro に変換する](#)
- [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 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](#)

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、

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 では、マイクロソフト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タイプ変換が制限されています。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 SQL Server は、Dedicated Host では実行できません。
- ライセンス込みの SQL Server インスタンスには、少なくとも 4 つの vCPU が必要です。

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. 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。
 - RHEL
 - RHEL for SAP
 - 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 を付属のライセンスからBYOLに変換する場合は、マイクロソフトのライセンス契約に従って Windows をライセンスをアクティベート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すべての出力を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, ProductCode: ProductCode, 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、「Amazon EC2 API リファレンス」の「[DescribeInstances](#)」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

Windows Server with SQL Server Enterprise BYOL 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。なぜなら同一の請求となるためです。

Windows Server を付属のライセンスから BYOL に変換する

Windows Server をライセンス付きから BYOL に変換した場合、License Manager は Windows を自動的にアクティブ化しません。インスタンスの KMS サーバーを KMS AWS 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

付属ライセンスから BYOL に変換するには、オリジナルの 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 に変換する方法については、「[VM Import/Export](#)」を参照してください。Amazon Machine Image (AMI) から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外となります。

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 BYOL 設定からKMS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. ライセンスの変換後に Windows をアクティブ化するには、お客様がお使いの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サーバーに指定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からライセンス付に変換する

Windows Server を BYOL からライセンス込みに変換すると、License Manager はインスタンスの KMS サーバーを KMS AWS 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、以下のコマンドを実行し、ARN を変換したいインスタンスの 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 からライセンス込みに変換する

複数の製品を同時に切り替えることができます。例えば、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に、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 を変換したいインスタンスの 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、RHEL、RHEL for SAP 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

- [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 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. 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。
 - RHEL
 - RHEL for SAP
 - 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 Linux の対象となる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すべての出力を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 の値は、ライセンスに関連する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、「Amazon EC2 API リファレンス」の「[DescribeInstances](#)」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"
```

Red Hat でサポートされている変換

Red Hat Enterprise Linux (RHEL) 製品では、次の変換がサポートされています。各変換には、特定の送信元および送信先のライセンスコンテキストが必要であり、追加の要件がある場合があります。

HA および更新サービスを使用した RHEL for SAP (AWS で販売 AWS Marketplace) から HA および更新サービスを使用した RHEL for SAP (Red Hat で販売 AWS Marketplace) に変換する

CLI コマンドの例:

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

注記:

- RHEL for SAP with HA and Update Services (AWS で販売 AWS Marketplace) には、製品のサブスクリプションに応じてさまざまな製品コード IDs (別名 Marketplace コード) があります AWS Marketplace。EC2 describe-instances レスポンスで、インスタンスの正しい製品コード ID を確認してください。
- RHEL for SAP with HA and Update Services (Red Hat で販売 AWS Marketplace) には、du6111oq9lwrc996awt04qyql (NA & Global) と 952qwcsxkm430zxhpy32i7w8g (EMEA) の

2 つの異なる製品コード IDs があります。どの を使用するかは、リージョンによって異なります。Marketplace で RHEL for SAP with HA と更新サービスのサブスクリプションをチェックして、どちらであるかを確認してください。

変換されると、サポート リクエストが必要なこのプライベート機能の許可リストに登録されていない限り、HA および更新サービス (AWS で販売 AWS Marketplace) を使用してインスタンスを RHEL for SAP に戻すことはできません。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。

HA および更新サービス (AWS で販売 AWS Marketplace) を使用した RHEL for SAP から Red Hat サブスクリプション (で Red Hat で販売 AWS Marketplace) に変換する

Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace) とは、顧客が購入できる SaaS サブスクリプションを指します AWS Marketplace。現時点では 2 つのリストもあります。

CLI コマンドの例:

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

注記:

- RHEL for SAP with HA and Update Services (AWS で販売 AWS Marketplace) には、AWS Marketplace 製品のサブスクリプションに応じてさまざまな製品コード IDs (別名 Marketplace コード) があります。EC2 describe-instances レスポンスで、インスタンスの正しい製品コード ID を確認してください。
- Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace) には、インスタンスに追加する製品コードはありません。
 - 説明: SaaS 製品コードは EC2 インスタンスにアタッチされないため、create-license-conversion-task-for-resource CLI コマンドを呼び出すときに、送信先製品コードを含めないことが想定されます。

変換されると、サポート リクエストが必要なこのプライベート機能の許可リストに登録されていない限り、HA および更新サービス (AWS で販売 AWS Marketplace) を使用してインスタンスを RHEL

for SAP に戻すことはできません。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。

Red Hat License-Included (LI) から RHEL (Red Hat で販売 AWS Marketplace) に変換する

CLI コマンドの例:

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

注記:

- RHEL (Red Hat で販売 AWS Marketplace) には、6cd5fxzrad0cu2j23p692xytz (NA & Global) と 6t1yup6mik9ng3ge36n33xqhw (EMEA) の 2 つの異なる製品コード IDs があります。どのを使用するかは、リージョンによって異なります。Marketplace で RHEL for SAP with HA and Update Services サブスクリプションをチェックして、どちらであるかを確認してください。

の Red Hat Enterprise Linux (RHEL) から Red Hat License-Included (LI) に変換 AWS する

CLI コマンドの例:

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

または、次のようになります。

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

注記:

- Red Hat Enterprise Linux (RHEL) for AWS には、6cd5fxzrad0cu2j23p692xytz (NA & Global) と 6t1yup6mik9ng3ge36n33xqhw (EMEA) の 2 つの異なる製品コード IDs があります。どのを使用するかは、リージョンによって異なります。EC2 describe-instances レスポンスで、インスタンスの正しい製品コード ID を確認してください。
- AWS インスタンスの Red Hat Enterprise Linux (RHEL) には、RunInstances または RunInstances:00g0 の使用オペレーションがあります。これは、インスタンスが AWS 製品 AMI の Red Hat Enterprise Linux (RHEL) から最初に起動されたか、後でこのサブスクリプションに変換されたかによって異なります。EC2 describe-instances レスポンスで、インスタンスの正しい使用オペレーションを確認してください。

CLI コマンドの例:

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

注記:

- Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace) には、インスタンスに追加する製品コードはありません。
 - 説明: SaaS 製品コードは EC2 インスタンスにアタッチされないため、create-license-conversion-task-for-resource CLI コマンドを呼び出すときに、送信先製品コードを含めないことが想定されます。
- Red Hat サブスクリプション (Red Hat が で販売 AWS Marketplace) は、CLI コマンドの呼び出し元によって にサブスクライブする必要があります。同じ組織内の他のアカウントのサブスクリプションはまだサポートされていません。

Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace) から Red Hat ライセンス込み (LI) に変換する

CLI コマンドの例:

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

注記:

- Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace) には、インスタンスに追加される製品コードはありません。

その他の要件

インスタンスは、ライセンス変換タスクを作成する前に停止状態である必要があります。ライセンス変換タスクが完了または失敗する前に、インスタンスを開始または終了しようとししないでください。これは、すべてのライセンスタイプの変換で同じ要件です。

送信先がこれらの Marketplace 製品の 1 つである場合:

- RHEL for SAP with HA and Update Services (Red Hat で販売 AWS Marketplace)
- RHEL (Red Hat で販売 AWS Marketplace)
- Red Hat サブスクリプション (Red Hat で販売 AWS Marketplace)

次に、顧客は CLI コマンドを呼び出す前に Marketplace でアクティブなサブスクリプションを持っている必要があります。そうしないと、変換リクエストが拒否されるか、失敗する可能性があります。コンソールとは異なり、CLI からライセンス変換タスクを作成する場合、License Manager は顧客を送信先製品に自動的にサブスクライブしようとしません。

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 クライアント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を設定する必要があります。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、サポートにリクエストを送信する必要があります。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。

- 共有済み
- 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

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。
- Windows BYOL 請求コードは、共有テナンシーでは使用できません。
- 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 --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](#)
- [Instance \[instance\] is launched from an Amazon owned AMI. Provide an instance launched originally from a BYOL AMI.](#)
- [Failed to validate that instance \[instance\] was launched from a BYOL AMI. Ensure that the SSM Agent is running on your instance.](#)
- [An error occurred \(InvalidParameterValueException\) when calling the CreateLicenseConversionTaskForResource operation: ResourceId - \[instance\] is in an invalid state for changing license type.](#)
- [EC2 instance \[instance\] failed to stop. Ensure that you have permissions for EC2 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、インスタンスの課金製品が正常に更新されます。ただし、KMSサーバーが AWS KMSサーバーには切り替わらない場合があります。

この問題を解決するには、「[EC2 Windows インスタンスで Windows ライセンス認証が失敗したのはなぜですか](#)」の手順を実行し、Systems Manager で [AWSsupport-ActivateWindowsWithAmazonLicense](#) Automation ランプックを使用するか、またはインスタンスにログインし、手動で AWS KMS サーバーに切り替えることで、Windows をアクティブ化します。

Instance [instance] is launched from an Amazon owned AMI. Provide an instance launched originally from a BYOL AMI.

ライセンスタイプを Bring Your Own License model (BYOL) に変換するには、インポートした AMI から Amazon EC2 Windows インスタンスを起動する必要があります。もともと Amazon 所有の AMI から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。

Failed to validate that instance [instance] was launched from a BYOL AMI. Ensure that the SSM Agent is running on your instance.

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 エージェント) は、オペレーティングシステムに関する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、「AWS Systems Manager ユーザーガイド」の「[SSM エージェントステータスを確認し、エージェントを起動する](#)」と「[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。

An error occurred (InvalidParameterValueException) when calling the **CreateLicenseConversionTaskForResource** operation: ResourceId - [instance] is in an invalid state for changing license type.

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 instance [instance] failed to stop. Ensure that you have permissions for EC2 **StopInstances**.

ターゲットインスタンスで StopInstances EC2 API アクションを実行するための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、EC2 インスタンス容量を利用したお客様専用の物理サーバーです。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 Host](#)」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内でインスタンスの起動が利用可能な容量を超える場合、Amazon EC2 がお客様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 EC2 がお客様に代わって未使用のホストを解放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。
- ホストを自動的に復旧する - Amazon EC2 が、予期せず障害が発生したホストから新しいホストにインスタンスを移動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 でホストリソースグループに Dedicated Hosts を追加する](#)
- [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. 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

を使用して AWS Resource Access Manager ホストリソースグループを共有できます 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した後、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、[AWS RAM ユーザーガイド](#)をご参照ください。

License Manager でホストリソースグループに Dedicated Hosts を追加する

既存のホストは AWS マネジメントコンソール、AWS CLI、または AWS API からホストリソースグループに追加できます。ホストを追加するには、Dedicated Host および Host リソースグループを作成した AWS アカウント所有者である必要があります。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。

ホストリソースグループに追加できる Dedicated Hosts の数に制限はありません。リソースグループの詳細については、[AWS Resource Groups ユーザーガイド](#)を参照してください。

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:

- License Manager コンソールにログインします<https://console.aws.amazon.com/license-manager/>。
- [ホストリソースグループ] を選択します。
- 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。
- Dedicated Hostsを選択します。
- [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 AMI に関連付ける必要があります。

```
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にインスタンスを作成する](#)」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. 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 AWS アカウントと共有する場合、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 の操作](#)」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. 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] を選択してください。
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. 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] を選択してください。

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

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、サポート対象のソフトウェアを含む事前設定済みの Amazon マシンイメージ (AMI) 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。ライセンス取得済み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 AMI 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。[AWS Systems Manager](#) は、起動させるライセンス込みのインスタンスを設定し、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。

ライセンス込みのインスタンスに関連付けられたユーザーと [vCPU](#) にはそれぞれ料金が発生します。Amazon EC2 のリザーブドインスタンスと Savings Plans の料金モデルは、Amazon EC2 のコストを最適化するのに役立ちます。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 のサブスクリプション料金](#)
- [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](#)
- [Active Directory](#)
- [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の使用を開始する](#)
- [よりアクティブなリモートユーザーセッション用に Active Directory GPO を設定する](#)
- [共有 AWS License Manager を使用してクロスアカウントの使用を開始する AWS Managed Microsoft AD](#)
- [ライセンス込み AMI からインスタンスを起動する](#)

- [RDP 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](#)
- [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 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 に設定します Per User。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用に Active Directory GPO 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、VPC 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 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AWS の予約済み組織単位 (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 Microsoft Office または Visual Studio 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、「[License Manager 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 のサブスクリプション料金

License Manager のサブスクリプションと請求は、使用されているサブスクリプション製品によって異なります。

Microsoft Office および Visual Studio サブスクリプション

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、請求は直ちに停止します。

Microsoft リモートデスクトップサービス (RDS) サブスクリプション

Microsoft RDS は、ユーザーが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するときにライセンスサーバーから発行されたユーザーサブスクリプションとクライアントアクセスライセンス (CAL) トークンの組み合わせに基づいて、ユーザーごとに月単位で請求されます。

License Manager での Microsoft RDS の請求

Microsoft RDS の請求は、Active Directory ユーザーが License Manager を通じてサブスクライブされたときに開始され、クライアントアクセスライセンス (CAL) トークンの有効期限が切れた後、発行日から 60 日後に終了します。一部の月は按分されません。ユーザーのサブスクリプションを解除しても、トークンの有効期限が切れるまで請求は継続されます。

サブスクライブしていないユーザーがライセンストークンの有効期限が切れた後もログインを続けると、自動的に再サブスクライブされ、再びサブスクライブが解除されてトークンの有効期限が切れるまで請求が続行されます。

同様に、一度もサブスクライブしたことがないが、ライセンスサーバーに関連付けられているインスタンスにログインすると、License Manager は自動的にサブスクライブし、RDS 請求を開始します。請求は、サブスクリプションが解除され、トークンの有効期限が切れるまで続行されます。

今月末にユーザーの請求を停止するには、サブスクリプションを解除する前に、ライセンスサーバー用に設定された Active Directory からそのユーザーを削除する必要があります。

Warning

アクティブな Microsoft Office または Visual Studio サブスクリプションを保持している Active Directory ユーザーを削除すると、そのユーザーは関連付けられているインスタンスにアクセスできなくなります。

次のシナリオ例は、RDS 請求の仕組みを示しています。

シナリオ 1: 標準サブスクリプションと請求

次のシナリオは、12/15/2024 にサブスクライブされているが、サブスクリプションインスタンスにアクセスしない Active Directory (AD) ユーザーの請求に影響する標準的なアクションのセットを示しています。

アクション: ユーザーがサブスクリプションを解除しない場合、請求は無期限に続行されます。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
12/15/2024	12/15/2024	--	該当なし	--	--	--

アクション: ユーザーは 1/15/2025 にサブスクリプション解除されます。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
12/15/2024	12/15/2024	--	該当なし	1/15/2025	No	1/31/2025

シナリオ 2: ライセンストークンがユーザーのサブスクリプションと請求にどのように影響するか

次のシナリオは、ライセンストークンの有効期限が、9/15/2024 にサブスクライブし、ドメインに参加しているサブスクリプション製品インスタンスに同じ日にログインする Active Directory (AD) ユーザーのユーザーサブスクリプションにどのように影響するかを示しています。

アクション: AD ユーザーの初回サブスクリプションとログイン。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

アクション: 同じ AD ユーザーが 10/19/2024 にサブスクリプション解除されました。ただし、ユーザーがディレクトリから削除されなかったため、請求はライセンストークンの有効期限が切れる月末まで継続されます。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
---------------------	------	--------	---------------	------------------	----------------	------

代替アクション: AD 管理者は 10/20/2024 にディレクトリからユーザーを削除し、翌日にユーザーのサブスクリプションを解除します。この場合、ユーザーがディレクトリから削除された月の月末に請求が停止します。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/21/2024	10/20/2024	10/31/2024

シナリオ 3: サブスクリプション解除されたユーザーが再サブスクライブされる

次のシナリオは、ライセンストークンの有効期限が切れたサブスクリプション解除された Active Directory (AD) ユーザーが、ドメインに参加しているサブスクリプション製品インスタンスにアクセスすると、自動的に再サブスクリプションされる方法を示しています。

アクション: AD ユーザーの初期サブスクリプションとログイン。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024	9/15/2024	9/15/2024	11/15/2024	--	--	--

アクション: 同じ AD ユーザーが 10/19/2024 にサブスクリプション解除されました。ただし、ユーザーがディレクトリから削除されなかったため、請求はライセンストークンの有効期限が切れる月末まで継続されます。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024	9/15/2024	9/15/2024	11/15/2024	10/19/2024	--	11/30/2024

アクション: 前のライセンストークンの有効期限が切れた後、請求が終了する前に、同じ AD ユーザーがドメインに参加しているサブスクリプション製品インスタンスにアクセスします。請求は、ユーザーが再度サブスクリプションを解除され、新しいトークンの有効期限が切れるまで続きます。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
11/20/2024 (re-subscribed)	billing continues	11/20/2024	1/20/2025	--	--	--

シナリオ 4: インスタンスアクセス時の自動サブスクリプション

次のシナリオは、RDS SAL にサブスクライブしたことがない Active Directory (AD) ユーザーが、ドメインに参加しているサブスクリプション製品インスタンスにログインしたときに自動的にサブスクライブされる方法を示しています。

アクション: RDS SAL にサブスクライブしたことがない AD ユーザーは、9/15/2024 にドメインに参加しているサブスクリプション製品インスタンスにログインし、自動サブスクライブされます。請求

が開始され、ユーザーがサブスクリプションを解除され、新しいトークンの有効期限が切れるまで継続します。

AD ユーザーがサブスクライブしました	請求開始	CAL 発行	CAL の有効期限が切れる	サブスクライブ解除されたユーザー	AD から削除されたユーザー	請求終了
9/15/2024 (自動サブスクライブ)	9/15/2024	9/15/2024	11/15/2024	--	--	--

ユーザー CALs [「リモートデスクトップデプロイのライセンス CALs あたりの」](#) セクション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 ロールおよび許可](#)
 - [AWS KMS License Server 認証情報のキーポリシー](#)
- [Active Directory](#)
- [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 ロールおよび許可

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 コンソールでは、ロールがまだ作成されていない場合、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。プロンプトに応答し、License Manager にロールの作成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。

- Amazon EC2 – ネットワークインターフェイスとサブネットを使用します。

- `ec2:CreateNetworkInterface`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSubnets`

- Directory Service – アクティブディレクトリを管理します。

- `ds:DescribeDirectories`
- `ds:AuthorizeApplication`
- `ds:UnauthorizeApplication`
- `ds:GetAuthorizedApplicationDetails`
- `ds:DescribeDomainControllers`

- Route 53 – ルーティングを設定します。

- `route53:DeleteHealthCheck`
- `route53:ChangeResourceRecordSets`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZones`
- `route53:ListHostedZonesByVPC`
- `route53>CreateHostedZone`

- `route53:DeleteHostedZone`

- `route53:ListResourceRecordSets`
- `route53:GetHealthCheckCount`
- `route53:AssociateVPCWithHostedZone`

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。

JSON

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

```

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

```

Active Directory

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、ディレクトリ間で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、 の同じ VPC からのものである必要があります AWS アカウント。共有サブネットはサポートされていません。

AWS マネージドアクティブディレクトリ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、ディレクトリが最初にプライマリアカウントでオンボーディングされている場合にのみサポートされ、共有アカウントでオンボーディングできます。
- 多要素認証はサポートされていません

タグベースのフィルターの前提条件

Active Directory にタグベースのフィルターを使用する場合は、まず次のように AWS Resource Explorer サービスにオンボードする必要があります。

1. <https://resource-explorer.console.aws.amazon.com/resource-explorer> で Resource Explorer コンソールを開きます。
2. [Resource Explorer を有効にする] を選択します。
3. Resource Explorer のセットアップページで、次のようにセットアップオプションを選択します。

Quick Setup

基本設定の場合は、このオプションを選択します。

詳細設定

カスタム設定の場合は、このオプションを選択します。少なくとも Active Directory が存在するリージョンのインデックスを作成してください。

4. アグリゲータインデックスリージョンのリージョンを選択します。
5. Resource Explorer をオンにして設定を保存します。
6. ナビゲーションペインで、ビューを選択し、ビューの作成を選択します。

Note

ナビゲーションペインが表示されない場合は、メニューアイコン (3 つの水平バー) を選択します。

7. a. ビューの作成ページで、名前 **license-manager-user-subscriptions-view** に と入力します。
b. リソースフィルターがすべてのリソースを含めるに設定されていることを確認します。
c. 「リソース属性の追加」セクションで、タグチェックボックスが選択されていることを確認します。
8. ビューの作成を選択して終了します。

ディレクトリの作成 AWS Managed Microsoft AD の詳細については、「AWS Directory Service ユーザーガイド」の [AWS Managed Microsoft AD 「前提条件」](#) と [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は、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、VPC 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 エンドポイントの詳細については、「AWS PrivateLink ガイド」の「[インターフェイス VPC エンドポイントを使用して AWS の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が、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 IP アドレスへのアウトバウンドトラフィックを許可していることを確認します。さらに、ドメインコントローラーセキュリティグループは、TCP 9389 を含むすべての Active Directory 関連ポートでの通信を許可する必要があります。Active Directory PowerShell モジュールやその他の管理ツールがドメインコントローラーと通信するために使用する Active Directory Web Services (ADWS) には、ポート 9389 が必要です。

「アクティブディレクトリを登録する」ステップのセキュリティグループの要件

Active Directory を License Manager にオンボーディングするときに、指定されたサブネットにネットワークインターフェイスが作成され、VPC のデフォルトのセキュリティグループでタグ付けされます。このセキュリティグループが Active Directory ドメインコントローラーへのアクセスを許可されていることを確認してください。これは、オンボーディングが完了した後も任意のグループに置き換えることができますが、ドメインコントローラーへのネットワークアクセスは引き続き必要です。

「RDS ライセンスサーバーの設定」ステップのセキュリティグループ要件

ライセンスサーバーの設定中に、License Manager は指定したサブネットに 2 つのネットワークインターフェイスを作成します。これらのネットワークインターフェイスには、必要なすべてのポート設定を含む新しく作成されたセキュリティグループが自動的にタグ付けされます。Active Directory ドメインコントローラーのセキュリティグループが、TCP ポート 9389 を含むすべての Active Directory 関連ポートのサブネット CIDRs からの双方向トラフィックを許可していることを確認します。Active Directory PowerShell モジュールやその他の管理ツールがドメインコントローラーと通信するために使用する Active Directory Web Services (ADWS) には、ポート 9389 が必要です。

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以下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、AWS Managed Microsoft AD がプロビジョニングされている VPC 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 解決

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 VPCs と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、DNS 解決を次のように設定します。

- 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 とアクティブディレクトリ間の 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「[Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolvers](#)」を参照してください。
- VPC で [DNS 解決] と [DNS ホスト名] を有効にします。詳細については、「[VPC の DNS 属性の表示と更新](#)」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が期待どおりに機能するには、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てい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、ライセンスのアクティベーション後もインスタンスがコンプライアンスを維持するには、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ます。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、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 Remote Desktop Services 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の設定を行うときは、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、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-`。

[シークレットのタイプを選択] ページで以下を行います。

- 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。

ユーザー名

- キー: `username`
- 値: `Administrator`

[パスワード]

- キー: `password`
- 値: `####`

- 暗号化キー – キー以外の KMS `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 ロールおよび許可](#)」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。例えば、次のようになります。

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

この手順では、を使用してシークレットを作成することを前提 AWS マネジメントコンソールとしています。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情報については、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各ユーザーがアクセスするには、Windows Server Remote Desktop Services のサブスクライバーアクセスライセンス (RDS SAL) の単一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の使用を開始する」](#)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 RDS SAL ライセンスの対象となる製品を含む Windows AMIs があります。

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

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、開発者がアプリケーションを作成、編集、デバッグ、および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 AMI には、[AWS Toolkit for .NET Refactoring](#) と [AWS Toolkit for Visual Studio](#) が含まれています。

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の 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価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
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
- Office LTSC Professional Plus 2024
- Office LTSC Professional Plus 2021 32 ビット (x86)
- Office LTSC Professional Plus 2024 32 ビット (x86)

次の表は、License Manager のユーザーベースのサブスクリプションの 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価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
Office LTSC Professional Plus 2024	OFFICE_PROFESSIONAL_PLUS

Active Directory

License Manager は、Microsoft Visual Studio、Microsoft Office、リモートデスクトップサービスサブスクリバークアクセスマイセン (RDS SAL) 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。製品は、AWS Managed Microsoft AD 環境内にデプロイされているか、AWS 環境内の VPC へのネットワーク接続を持つ、またはセルフマネージドアクティブディレクトリのいずれかをサポートする場合があります AWS。

この表は、ユーザーベースのサブスクリプションで使用すると、各ソフトウェア製品でサポートされている Active Directory のタイプを示しています。

ソフトウェア製品	AWS Managed Microsoft AD	セルフマネージド AD
Microsoft Visual Studio	サポート	サポートされていません
Microsoft Office	サポート	サポートされていません
RDS SAL 製品	サポート対象	サポート

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す。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、「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 管理アカウントを使用して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。

- インスタンスが提供す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の使用を開始する](#)」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の使用を開始する

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詳しく説明します。これらの手順は、必要な前提条件が既に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。

Steps

- [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 製品では、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列の AWS Marketplace にサブスクリプションボタンを表示す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自動的に追加します。RDS は、ライセンス込み AMIs 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と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ために必要です。

以下のリンク AWS Marketplace を使用して、で製品に直接サブスクライブできます。

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

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. 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. 製品名を選択するか、AWS Marketplace のサブスクリプションボタンを選択してサブスクリプションの詳細を表示します。
4. リストされている Marketplace 製品ごとに、サブスクリプションオプションの表示を選択します。条件を確認し、サブスクライブを選択して続行します。

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 を製品に登録できます。

Note

ユーザー数および関連コストの推定請求額は、でクローズされていない請求期間 (保留中の請求ステータスとしてマークされている) 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が Active Directory で定義されている必要があります。これは、サブスクリプションに応じて、AWS Managed Microsoft AD またはセルフマネージド Active Directory のいずれかになります。

- スタンドアロンの Microsoft Office または Visual Studio 製品のみサブスクライブする場合は、を設定する必要があります AWS Managed Microsoft AD。
- [Win Remote Desktop Services SAL](#) にサブスクライブする場合は、AWS Managed Microsoft AD またはセルフマネージド Active Directory を使用できます。

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ベ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。

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 VPCs に対して DNS 転送を設定する必要があります。複数の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 DNS 転送で独自の Active Directory が設定されている必要があります。

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。

登録手順は、サブスクライブしている製品に応じてコンソールによって異なります。にサブスクライブしている場合は Win Remote Desktop Services SAL、Microsoft RDS SAL タブを選択します。Microsoft Office または Visual Studio にサブスクライブしていて、RDS SAL にサブスクライブしていない場合は、スタンドアロン MSO サブスクリプションタブを選択します。

Microsoft RDS SAL

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. 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のリモートデスクトップサービス (RDS) タブで、アクティブディレクトリの登録を選択します。
4. AWS Managed Active Directory オプションを選択して詳細を入力します。
5. AWS Active Directory リストからマネージドディレクトリを選択するか、新しいマネージドディレクトリを作成してから戻って選択します。
6. 登録を選択して AWS Managed Active Directory を登録します。

セルフマネージド Active Directory を登録する

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. 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のリモートデスクトップサービス (RDS) タブで、アクティブディレクトリの登録を選択します。
4. セルフマネージド Active Directory オプションを選択して詳細を入力します。
5. Active Directory ドメインを入力します。
6. Active Directory IP アドレスのバージョンを選択し、ディレクトリのプライマリ IP アドレスとセカンダリ IP アドレスを入力します。
7. ネットワークセクションで、Active Directory が存在する VPC と 2 つのサブネットを選択します。
8. Microsoft RDS サブスクリプションの前提条件の一部として作成した管理者認証情報を選択します。

Stand-alone MSO subscriptions

登録 AWS Managed Microsoft AD

ユーザーベースの Microsoft Office および Visual Studio 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. 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、登録する Microsoft Office または Visual Studio サブスクリプション製品のタブを選択し、アクティブディレクトリの登録を選択します。
4. AWS Active Directory リストからマネージドディレクトリを選択するか、新しいマネージドディレクトリを作成してから戻って選択します。
5. 登録 を選択して AWS Managed Active Directory を登録します。

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、AWS LicenseManager *<directory_id>* 用に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あります。

からの Active Directory 登録 AWS CLI

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 Active Directory を [RegisterIdentityProvider](#) オペレーションに登録できます。

```
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、[RegisterIdentityProvider](#) オペレーションで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。

```
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 EC2 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ーアクセスライセンス (SALs) 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、RDS [ユーザーベースのサブスクリプションの前提条件](#)の 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. 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) タブには、1 つ以上のアクティブディレクトリがリストに表示されます。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 ライセンスサーバーの設定を選択します。
5. RDS License Server の設定ダイアログでは、次の設定を行うことができます。

Active Directory

このセクションでは、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の主要な詳細について説明します。

シークレット

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には、既存のシークレットを選択するか、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 しようします。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[ライセンス込み AMI からインスタンスを起動する](#)。

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

必要な製品の AMI AWS Marketplace 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。製品をサブスクライブ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。

各ユーザーは、Windows Server Remote Desktop Services サブスクライバークセスライセンス (RDS SAL) と使用する製品の両方のサブスクリプションを持っている必要があります。

アカウントが「」で説明されているように RDS SAL 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](#)、License Manager 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、Active Directory 内のユーザーを RDS SAL に自動的にサブスクライブします。

Note

サブスクライブしたことがないユーザーが RDS SAL に関連付けられたインスタンスにログインすると、License Manager は自動的にサブスクライブし、Microsoft RDS の請求を開始します。請求は、サブスクリプションが解除され、RDS SAL ライセンスサーバーによって発行されたライセンストークンの有効期限が切れるまで継続されます。

同様に、以前にサブスクライブしたユーザーがサブスクライブを解除しても、RDS SAL ライセンストークンの有効期限が切れた後もログインを続けると、自動的に再サブスクライブされ、再びサブスクライブ解除されてトークンの有効期限が切れるまで請求が続行されます。

サブスクリプション料金と請求の詳細については、「」を参照してください[License Manager のサブスクリプション料金](#)。

License Manager の製品ページには、マーケットプレイスのサブスクリプションステータスをアクティブとして一覧表示して、アクティブなサブスクリプションが表示されます。製品詳細ページに、License Manager はステータスが Subscribed のアクティブなユーザーサブスクリプションを表示します。

Important

Active Directory が製品で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、ディレクトリ設定を調整するように指示されます。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。各ユーザーは、RDS SAL と使用する製品の両方のサブスクリプションを持っている必要があります。[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

ユーザーに関連付けるインスタンスを選択すると、ユーザーがまだサブスクライブしていない場合は、オプションでインスタンスが提供する製品にサブスクライブできます。次のいずれかの方法を使用して、ユーザーをサブスクライブして関連付けます。

Console

ユーザーをインスタンスに関連付けるには、次の手順に従います。

1. 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. ユーザーに関連付けるインスタンスを選択し、次のいずれかのオプションを選択します。

ユーザーに関連付ける

ディレクトリに存在するユーザー名を最大 5 つ指定し、信頼されたドメインに存在する場合はドメイン名を含めて、関連付けを選択します。この方法を使用する場合、ユーザーはインスタンスが提供する製品を既にサブスクライブしている必要があります。

ユーザーをサブスクライブして関連付ける

ディレクトリに存在するユーザー名を最大 5 つ指定し、信頼されたドメインに存在する場合はドメイン名を含めて、サブスクライブと関連付けを選択します。

(オプション) ユーザー関連付けを確認する

ユーザー関連付けページで、選択したユーザーが関連付けステータスが関連付けられているユーザーの下に表示されます。

(オプション) サブスクライブしているユーザーを確認する

製品ページで、製品名を選択します。サブスクライブされたユーザーは、ステータスがサブスクライブされたユーザーの下に表示されます。

AWS CLI

起動したインスタンスにユーザーを関連付けることで、ユーザーベースのサブスクリプションに [AssociateUser](#) オペレーションを提供できます。

```
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)

起動したインスタンスにセルフマネージド Active Directory のユーザーを関連付けることで、ユーザーベースのサブスクリプションに [AssociateUser](#) オペレーションを提供できます。

```
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. 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. Marketplace サブスクリプションステータスがアクティブであるユーザーをサブスクライブする製品を選択します。
4. 製品が Microsoft RDS の場合は、サブスクライブするユーザーを含む登録済み Active Directory を選択します。
5. 続行するには、サブスクライブユーザーを選択します。
6. ディレクトリに存在するユーザー名を最大 20 個指定し、信頼されたドメインに存在する場合はドメイン名を含めて、Subscribe を選択します。

サブスクリプションを持つユーザーは、ステータスがサブスクライブされている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)

[StartProductSubscription](#) オペレーションを使用して、ID プロバイダーに登録されている製品にユーザーを登録できます。

```
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 を使用して製品をサブスクライブする (AWS CLI)

[StartProductSubscription](#) オペレーションを使用して、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。

```
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。

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

デフォルトでは、Microsoft RDS 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許可します。RDS 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) で複数のユーザーセッションを同時に許可するように Microsoft RDS 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. GPO の設定に使用するツールは、次のように、GPO の実行元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 グループポリシー管理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 RDS を介して接続するセッションホストを指定します。RDS License Server のエンドポイントは、License Manager 製品の詳細ページ、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。

RDS License Server for License Manager の設定の詳細については、「開始方法」トピック [the section called “ステップ 3: RDS を設定する”](#) 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。

共有 AWS License Manager を使用してクロスアカウントの使用を開始する AWS Managed Microsoft AD

AWS License Manager は、共有 を使用したクロスアカウント機能をサポートしているため AWS Managed Microsoft AD、組織は複数のアカウントにインスタンスをデプロイしながら、ディレクトリ所有者アカウントからのユーザーサブスクリプションを一元管理できます。

用語

- ディレクトリ所有者アカウント - マネージド AD が存在し、サブスクリプションの管理も担当するライセンス管理者アカウント。
- ディレクトリコンシューマーアカウント - 共有 AD を使用してユーザーサブスクリプションインスタンスを起動する AWS アカウント。

前提条件

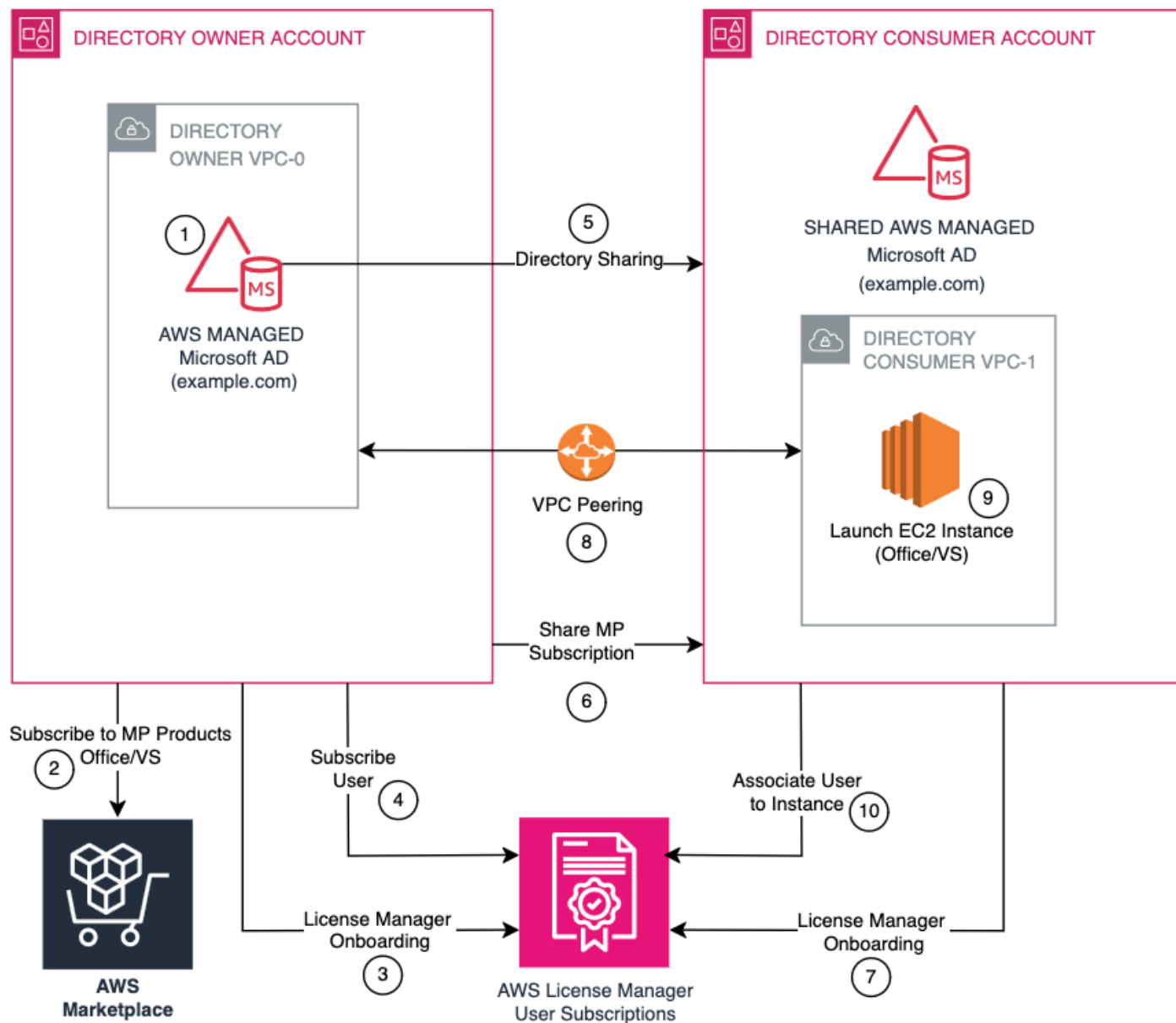
開始する前に、以下を確認してください。

- AWS Managed Microsoft AD ディレクトリ所有者アカウントの - サブスクリプションを制御するディレクトリ所有者アカウント/ライセンス管理者アカウントに設定されます。
- ディレクトリ所有者アカウントとすべてのディレクトリコンシューマーアカウント間のネットワーク接続。
- 必要な IAM アクセス許可 - [ユーザーベースのサブスクリプション IAM ロール](#) を参照してください。
- ディレクトリ所有者アカウントの AWS Marketplace で必要な License Manager 製品のサブスクリプション:
 - [Visual Studio Professional 2022](#)
 - [Visual Studio Enterprise 2022](#)
 - [Office LTSC Professional Plus](#)

制限事項

- ユーザーサブスクリプションの管理は、ディレクトリ所有者アカウントに制限されます。
- クロスリージョン共有はサポートされていません。
- ディレクトリ所有者アカウントによる一括請求 - すべてのサブスクリプションコストはディレクトリ所有者アカウントに請求されますが、サブスクリプションは複数のアカウントに存在する可能性があります。
- アカウント間のネットワーク接続が必要です。

ネットワークアーキテクチャ



クロスアカウント License Manager 機能を設定する方法

クロスアカウント License Manager 機能を設定するには:

1. ディレクトリ所有者アカウント/ライセンス管理者アカウントを設定します。
2. ディレクトリコンシューマーアカウントを設定します。
3. ネットワーク接続を確立します。
4. インスタンスをデプロイし、ユーザーの関連付けを管理します。

ステップ 1: ディレクトリ所有者/ライセンス管理者アカウントを設定する

を作成して共有する AWS Managed Microsoft AD

1. 存在しない場合は、VPC AWS Managed Microsoft AD に [作成](#)します。
2. ディレクトリの共有で説明されているように、ディレクトリをディレクトリコンシューマーアカウントと共有[します](#)。
3. ディレクトリが必要なユーザーとグループで正しく設定されていることを確認します。

製品をサブスクライブする

1. [こちら](#)に移動します AWS Marketplace。
2. 必要な製品、Visual Studio または Office と RDS SAL を見つけてサブスクライブします。
3. License Manager Create Grants を使用して、Visual Studio または Office サブスクリプションをディレクトリコンシューマーアカウントと共有します。または、請求には影響しないため、これらのアカウントの AWS Marketplace 製品をサブスクライブすることもできます。[「付与されたライセンス」](#)を参照してください。
4. サブスクリプションステータスがアクティブであることを確認します。

License Manager に登録する

1. License Manager コンソールを開きます。
2. ユーザーベースのサブスクリプション設定に移動します。
3. ID プロバイダーの登録を選択します。
4. [こちら](#)を選択します AWS Managed Microsoft AD。
5. 登録プロセスを完了します。

ステップ 2: ディレクトリコンシューマーアカウントを設定する - 共有 AD を持つアカウント

共有ディレクトリを受け入れる

1. AWS Directory Service コンソールを開きます。
2. 共有ディレクトリに移動します。
3. 共有ディレクトリの招待を見つけて受け入れます。
4. アカウントに割り当てられた新しいディレクトリ ID を書き留めます。

MP サブスクリプションを受け入れる

License Manager Grants では、AWS Marketplace 製品の許可を受け入れます。または、製品をサブスクライブします AWS Marketplace 。詳細については、[CreateGrant API](#)」を参照してください)。

License Manager に登録する

1. License Manager コンソールを開きます。
2. ユーザーベースのサブスクリプションに移動し、製品を選択します。
3. 共有ディレクトリ ID と製品を使用して登録します。
4. 登録ステータスを確認します。

ステップ 3: VPCs 間のネットワーク接続を確立する

Amazon EC2 インスタンスをディレクトリにドメイン結合するには、VPCs 間のネットワーク接続を確立する必要があります。2 つの VPCs 間のネットワーク接続を確立するには、いくつかのオプションがあります。このセクションでは、Amazon VPC ピアリングを使用する方法について説明します。

VPC ピアリング接続のセットアップ

1. ディレクトリ所有者 [VPC-0 とディレクトリコンシューマー VPC-1 の間に 1 つの VPC ピアリング接続](#)を作成し、ディレクトリ所有者 VPC-0 とディレクトリコンシューマー VPC-2 の間に別の接続を作成します。VPC-0 VPC-1
2. [VPCs ピアリング接続を指す VPC ルートテーブルにルートを追加して、ピアリング接続内の他の VPC にトラフィックをルーティング](#)することで、ピア接続された VPC 間のトラフィックルーティングを有効にします。
3. ディレクトリ所有者 VPC-0 とのピアリング接続を追加して、各ディレクトリコンシューマー VPC ルートテーブルを設定します。必要に応じて、インターネットゲートウェイを作成してディレクトリコンシューマー VPCs にアタッチすることもできます。これにより、ディレクトリコンシューマー VPCs のインスタンスは、ドメイン結合を実行する Amazon EC2 Systems Manager エージェントと通信できるようになります。

セキュリティグループの設定

アウトバウンドルールテーブルに[AWS Managed Microsoft AD プロトコルとポート](#)を追加して、アウトバウンドトラフィックを有効にするようにディレクトリコンシューマー VPCs [のセキュリティグ](#)

ループを設定します。また、ディレクトリドメインコントローラー VPCs のセキュリティグループを設定して、インバウンドルールテーブルに AWS Managed Microsoft AD プロトコルとポートを追加してインバウンドトラフィックを有効にし、ディレクトリコンシューマーアカウントからのトラフィックを許可します。

セキュリティグループの要件

コンシューマーアカウント VPCs:

- ディレクトリ所有者 VPC へのアウトバウンドトラフィックを有効にする
- 必要な AD ポートでの通信を許可する

ディレクトリ所有者 VPC:

- コンシューマー VPCs からのインバウンドトラフィックを設定する
- 以下を含む必要な AWS Managed Microsoft AD プロトコルとポートを追加します。
 - TCP 53 (DNS)
 - UDP 53 (DNS)
 - TCP 88 (Kerberos)
 - UDP 88 (Kerberos)
 - TCP 135 (RPC)
 - TCP 389 (LDAP)
 - UDP 389 (LDAP)
 - TCP 445 (SMB)
 - TCP 464 (Kerberos パスワード)
 - UDP 464 (Kerberos パスワード)
 - TCP 636 (LDAPS)
 - TCP 9389 (Active Directory Web Services)
 - TCP 3268-3269 (グローバルカタログ)
 - TCP 1024-65535 (動的 RPC)

Active Directory PowerShell モジュールやその他の管理ツールがドメインコントローラーと通信するために使用する Active Directory Web Services (ADWS) には、ポート 9389 が必要です。

ステップ 4: インスタンスをデプロイし、ユーザー関連付けを管理する

ユーザーをサブスクライブする (ディレクトリ所有者アカウントのみ)

1. License Manager コンソールを開きます。
2. ユーザーベースのサブスクリプションに移動します。
3. ユーザーをサブスクライブするを選択する
4. AWS Managed Microsoft AD ユーザー識別子を入力する
5. 製品を選択し、サブスクリプションを確認します。

インスタンスの起動

任意のアカウントでこのステップを実行します。

1. Amazon EC2 コンソールに移動します。
2. [インスタンスの作成] を選択してください。
3. 適切な License Manager AMI を選択します。
4. ネットワーク設定を構成します。
5. を確認して起動します。

ユーザーをインスタンスに関連付ける

インスタンスが存在する任意のアカウントでこのステップを実行します。

1. License Manager コンソールを開きます。
2. ユーザー関連付けに移動します。
3. ターゲットインスタンスを選択します。
4. ユーザーの関連付けを選択します。
5. AWS Managed Microsoft AD ユーザー名を入力します。
6. 関連付けを確認します。

トラブルシューティング

一般的な問題と解決策:

ドメイン結合の失敗

1. アカウント間のネットワーク接続を確認します。
2. セキュリティグループの設定を確認します。
3. DNS 解決が機能していることを確認します。
4. ルートテーブルエントリを検証します。

ユーザーサブスクリプションの問題

1. ユーザーが存在することを確認します AWS Managed Microsoft AD。
2. ディレクトリ所有者アカウントのサブスクリプションステータスを確認します。
3. ネットワーク接続を確認します。
4. エラーログを確認します。

ネットワーク接続の問題

1. VPC ピアリング接続ステータスをテストします。
2. ルートテーブルの設定を確認します。
3. セキュリティグループルールを確認します。
4. DNS 解決を確認します。

DNS 解決に問題がある

1. DHCP オプションセットを確認します。
2. DNS サーバー設定を確認します。
3. コンシューマーインスタンスからのテスト名解決。

その他のリソース

- [AWS License Manager ユーザーガイド](#)
- [AWS Directory Service のドキュメント](#)
- [ディレクトリの共有](#)
- [Amazon EC2 インスタンスを複数のアカウントと VPC の AWS Managed Microsoft AD ディレクトリにドメイン結合する方法 VPCs](#)

- [付与されたライセンス](#)

ライセンス込み AMI からインスタンスを起動する

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を使用してインスタンスを起動する

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) にアクセスします。
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. [AMI でインスタンスを起動] を選択します。
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. [詳細設定] 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. [インスタンスを起動] を選択します。

AWS Marketplace AMI からインスタンスを実行している場合は、ユーザーを製品にサブスクライブし、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バージョン AMI からインスタンスを起動する

Office LTSC Professional Plus または Microsoft Visual Studio をサポートする AMI からインスタンスを起動すると、起動はデフォルトで AMI の最新の Windows オペレーティングシステムバージョン (Windows Server 2025 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 AMI でを起動するには、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には、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、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. このリストには、サポートされている Windows OS プラットフォームの最新の AMI 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。

RDP 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

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は、約 20 分かかります。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. 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. 「[RDP を使用した Windows インスタンスへの接続](#)」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てください。

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。

次の手順を使用して、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、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. 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. 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。これにより、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

License Manager の Microsoft Office および Visual Studio 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、次のようにユーザーアクセスを管理できます。

[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 Microsoft Office または Visual Studio 製品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 Microsoft Office または Visual Studio 製品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、Microsoft Office および Visual Studio 製品のユーザー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削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。

内容

- [License Manager 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 でユーザーベースの製品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](#)

License Manager 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 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、そのインスタンスからサブスクライブしているユーザーの関連付けを解除できます。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製品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. 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製品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

料金の発生を停止するには、Microsoft Office または Visual Studio ユーザーベースのサブスクリプション製品から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。Microsoft RDS は、ユーザーサブスクリプションと、ユーザーが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するときにライセンスサーバーから発行されたクライアントアクセスライセンス (CAL) トークンの組み合わせに基づいて、ユーザーごとに月単位で請求されます。詳細については、「[License Manager で Microsoft RDS の請求](#)」を参照してください。

⚠ Important

Microsoft Office または Visual Studio ユーザーベースのサブスクリプション製品の場合、サブスクリプションを解除する前に、まず、Active Directory ユーザーと現在関連付けられているすべてのインスタンスとの関連付けを解除する必要があります。

ユーザーベースの製品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

1. 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 Active Directory を使用しない場合は、License Manager 設定から Active Directory の登録を解除できます。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の登録を解除すると、License Manager でそのディレクトリから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の。
2. すべてのサブスクリプションユーザーの関連付けがインスタンスから解除されたら、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

⚠ Important

Active Directory を Microsoft RDS SAL ユーザーに使用する場合は、AD の登録を解除して削除する前に、関連するライセンスサーバーエンドポイントを削除する必要があります。

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

1. 左側のナビゲーションペインで [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 ディレクトリ ID と設定のステータスが表示されます。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](#)
- [ユーザーサブスクリプション製品設定の失敗のトラブルシューティング](#)
- [ユーザーサブスクリプションインスタンスの起動失敗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](#)

- [Microsoft RDS ライセンスの失敗のトラブルシューティング](#)
- [Microsoft Office のアクティベーションの失敗のトラブルシューティング](#)
- [Active Directory を削除できないときのトラブルシューティング](#)
- [AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service リンクロール \(SLR\) を削除できない問題のトラブルシューティング](#)
- [RDS SAL 製品のサブスクリプションが存在しないエラーのトラブルシューティング](#)
- [ライセンス数が正しく表示されないトラブルシューティング](#)
- [RDS License Diagnoser の問題のトラブルシューティング](#)
- [信頼のトラブルシューティング](#)
- [ユーザーサブスクリプションの請求に関する問題のトラブルシューティング](#)
- [非アクティブなマーケットプレイスサブスクリプションステータスのトラブルシューティング](#)
- [インスタンスあたりのユーザー制限のトラブルシューティング](#)
- [RDS SAL への移行後に CAL トークンが供給されなかった場合のトラブルシューティング](#)
- [ユーザーサブスクリプション製品を使用する EC2 インスタンスでシームレスなドメイン結合が機能しない](#)
- [VPC エンドポイントがアカウントに作成された](#)
- [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](#)
- [Managed Active Directory のユーザー名を変更する](#)
- [終了したインスタンスからユーザーの関連付けを解除する](#)
- [ユーザーサブスクリプションインスタンスに追加のソフトウェアをインストールする](#)
- [ユーザーサブスクリプションインスタンスの日本語言語パック](#)
- [ユーザーサブスクリプションインスタンスのローカル管理者ユーザー](#)
- [ユーザーサブスクリプションインスタンスに RDP を実行できるユーザーの数](#)
- [Office および Visual Studio 製品のセルフマネージド AD のユーザー](#)
- [サポートされている Windows オペレーティングシステム](#)
- [Office および Visual Studio でサポートされているバージョン](#)
- [古い Windows Server バージョンでのユーザーサブスクリプションの使用](#)
- [アカウントまたはリージョン間で License Manager ユーザーサブスクリプションを使用する](#)
- [AWS サポートに連絡するためのヒント](#)

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。

ユーザーサブスクリプション製品設定の失敗のトラブルシューティング

アウトバウンドネットワークアクセスの問題により、製品設定が失敗している可能性があります。これに対処するには、デフォルトのセキュリティグループが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と SSM の IP アドレスへのアウトバウンドトラフィックを許可していることを確認します。

- デフォルトのセキュリティグループ設定が、ドメインコントローラーネットワークインターフェイスの IP アドレスへのアウトバウンドトラフィックを容易にすることを確認します。
- License Manager は、AWS Managed Microsoft AD がプロビジョニングされている VPC 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、ディレクトリに必要なサービス機能に使用されます。デフォルトの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 IP アドレス、またはドメインコントローラーが使用するセキュリティグループ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。詳細については、「[管理ガイド](#)」の「[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「[作成される内容](#)」を参照してください。 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_what_gets_created.html Directory Service
- ユーザーベースのサブスクリプションまたは VPC エンドポイントを提供するインスタンスからのアウトバウンドインターネットアクセスを設定します。
- ユーザーベースのサブスクリプションまたは VPC エンドポイントを提供するインスタンスからのアウトバウンドインターネットアクセスは、インスタンスが SSM と通信するように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[EC2 インスタンス用の Systems Manager のセットアップ](#)」を参照してください。

プロビジョニングプロセスが完了すると、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。また、選択するセキュリティグループでは、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の IPv4 アドレスまたはセキュリティグループに必要なトラフィックを許可する必要があります。詳細については、Amazon Virtual Private Cloud [ユーザーガイド](#) の「[セキュリティグループの操作](#)」を参照してください。

ユーザーサブスクリプションインスタンスの起動失敗のトラブルシューティング

インスタンスの起動は、複数の理由で失敗する可能性があります。インスタンスの起動が失敗する一般的な問題のいくつかを次に示します。

- インスタンスが SSM によって検出可能であることを確認します。「」を参照してください [the section called “インスタンス接続のトラブルシューティング”](#)。
- インスタンスがドメインに参加できることを確認します。「」を参照してください [the section called “ドメインへの参加失敗のトラブルシューティング”](#)。
- Route53 アウトバウンドリゾルバーエンドポイントルールが設定されていることを確認します。詳細については、ブログ記事「[Integrating your Directory Service's DNS resolution with Amazon Route 53 Resolver](#)」を参照してください。
- ユーザーサブスクリプション AMIs 上に作成されたカスタム AMIs からインスタンスを起動する場合は、カスタム AMIs からインスタンスを作成および起動するときに、Sysprep を実行し、一意のコンピュータ名を確認してください。

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を提供するインスタンスのネットワーク設定と VPC エンドポイント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提供するサブネットで起動されたインスタンス ID を送信元、Microsoft Office 製品用にプロビジョニングされた VPC エンドポイントを宛先として指定できます。分析するパスのポートとして TCP を指定し、宛先ポートに 1688 を指定します。詳細については、「[How can I troubleshoot connectivity issues over my gateway and interface VPC endpoints?](#)」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

ユーザーが製品を使用するには、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 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、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。

ユーザーベースのサブスクリプション製品 AMI をベースイメージとして使用するカスタム AMI からインスタンスを起動する場合は、カスタム AMI で Sysprep ステップを実行して、起動時に一意のコンピュータ名を確保する必要があります。/generalize で Sysprep を実行する前に、マシンがドメインから削除されていることを確認してください。

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](#)」と「[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。

Microsoft RDS ライセンスの失敗のトラブルシューティング

CAL (クライアントアクセスライセンス) の発行で問題が発生した場合は、サーバーファームまたはターミナルサーバーグループに追加の Microsoft RDS ライセンスサーバーが存在するかどうかを確認します。CAL の発行を妨げ、ライセンスの複雑さにつながる可能性があるため、これらの場所に追加のライセンスサーバーを配置することはお勧めしません。

この問題を解決するには、目的の Microsoft RDS サーバーのみがサーバーファームとターミナルサーバーグループに残っていることを確認します。

ライセンスの問題をトラブルシューティングするときは、/admin フラグを使用して接続すると、標準のライセンスチェックがバイパスされることに注意してください。このフラグは管理目的で使用され、CAL は消費されないためです。これにより、基盤となるライセンスの問題がマスクされる可能性があります。ライセンスの問題を診断するには、ライセンス管理のために標準ユーザー接続 (/admin フラグなし) が正しく機能していることを確認します。

Microsoft Office のアクティベーションの失敗のトラブルシューティング

Microsoft Office のアクティベーションが失敗した場合、インスタンスが License Manager に定義されている VPC にアクセスできることを確認します。次のいずれかのオプションがこの要件を満たしています。

- インスタンスが License Manager でオンボードされている VPC で実行されている (VPC エンドポイント経由)
- インスタンスは、License Manager オンボード VPC とピア接続されている VPC で実行されています。

この問題を解決するには、インスタンスが正しい VPC に移動されていることを確認するか、License Manager オンボード VPC との VPC ピアリングを確立します。

Active Directory を削除できないときのトラブルシューティング

License Manager は、設定中に Directory Service で承認されたアプリケーションとして登録されるため、設定後にアクティブなディレクトリが削除されないように保護されます。標準手順の一環として、お客様はまずすべてのインスタンス、インスタンスの関連付け、およびユーザーサブスクリプションを削除する必要があります。その後、License Manager からアクティブディレクトリを削除し、その後ディレクトリ自体を削除できます。

AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService Service リンク ロール (SLR) を削除できない問題のトラブルシューティング

License Manager では、ユーザーベースのサブスクリプションを提供する AWS リソースを管理するために、AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService サービスにリンクされたロールが必要です。サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、License Manager の設定が簡単になります。License Manager 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 Manager のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他の IAM エンティティに添付することはできません。

詳細については、[the section called “ユーザーベースのサブスクリプションの前提条件”](#)「」および「[License Manager – ユーザーベースのサブスクリプションロール](#)」および「[サービスにリンクされたロール](#)」を参照してください。

RDS SAL 製品のサブスクリプションが存在しないエラーのトラブルシューティング

アカウントには Windows Server Remote Desktop Services サブスクライバーアクセスライセンス (RDS SAL) のサブスクリプションが必要です。ユーザーベースのサブスクリプション製品を提供するインスタンスに関連付けられたすべてのユーザーは、使用する他の製品に加えて、このライセンスに対するアクティブなサブスクリプションを 1 つ持っている必要があります。ユーザーがユーザーベースのサブスクリプション製品に登録すると、ユーザーに代わって RDS SAL に登録されることになります。

ただし、他のコンプライアンス上の理由でこれがサブスクリプション解除または削除された場合は、再サブスクリプションが必要になる場合があります。すでにサブスクライブしている場合は、サブスクライブ解除と再サブスクライブを試すことができますが、License Manager ユーザーサブスクリプションには影響しません。

ライセンス数が正しく表示されないトラブルシューティング

初期セットアップまたは設定の変更後、ライセンスサーバーが License Diagnoser のすべてのライセンスタイプの正確なライセンス数を表示するまでに最大 24 時間かかる場合があります。

対応方法:

- 正確なライセンス数レポートが予想されるまで、セットアップ後最大 24 時間待機します。

この遅延は正常であり、ライセンスサーバーがさまざまなライセンスタイプ間ですべてのライセンス情報を適切に同期および更新するのに十分な時間を確保できます。エラーが発生した場合は、「」を参照してください [the section called “RDS License Diagnoser の問題のトラブルシューティング”](#)。

RDS License Diagnoser の問題のトラブルシューティング

これらのエラーは通常、認証情報またはアクセス許可の問題によって発生します。解決するには:

1. ユーザー認証情報の検証: オンボーディング中に License Manager に提供されたのと同じユーザーアカウントを使用していることを確認します。
2. セッション認証情報を確認する: 概要セクションでサーバーに対して「認証情報が利用不可」と表示される場合:
 - a. 「認証情報は利用できません」と表示されている概要セクションのライセンスサーバーをクリックします。
 - b. 開いた右側のサイドメニューで、License Manager にオンボードされたユーザーの認証情報を追加します。
 - c. 「更新」をクリックします。

問題が解決しない場合は、Microsoft のドキュメントで説明されている追加のトラブルシューティング手順に従います。 [RDS に接続できない - ライセンスサーバーがない](#)

これにより、License Diagnoser の認証情報とアクセス許可に関連するほとんどの問題が解決されます。

信頼のトラブルシューティング

多くのお客様との作業経験に基づいて、信頼設定の問題の大部分は DNS 解決エラーまたはネットワーク接続エラーです。以下は、一般的な問題の解決に役立つトラブルシューティング手順です。

- でアウトバウンドネットワークトラフィックを許可したかどうかを確認します AWS Managed Microsoft AD。
- DNS サーバーまたはオンプレミスドメインのネットワークがパブリック (RFC 1918 以外) IP アドレス空間を使用している場合は、次の手順に従います。
 - コンソールで Directory Service 、ディレクトリの IP ルーティングセクションに移動し、アクションを選択し、ルートの追加を選択します。
 - CIDR 形式を使用して、DNS サーバーまたはオンプレミスネットワークの IP アドレスブロックを入力します。例: 203.0.113.0/24。

- DNS サーバーとオンプレミスネットワークの両方が RFC 1918 プライベート IP アドレススペースを使用している場合、このステップは必要ありません。
- セキュリティグループを検証し、該当するルートが必要かどうかを確認したら、Windows Server インスタンスを起動して AWS Managed Microsoft AD ディレクトリに結合します。インスタンスが起動すると、次のようになります。
- DNS 接続をテストするには、次の PowerShell コマンドを実行します。

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

また、ドキュメントの [「信頼作成ステータスの理由」ガイド](#) の Directory Service メッセージの説明を確認する必要があります。

ユーザーサブスクリプションの請求に関する問題のトラブルシューティング

AWS は、ライセンスに含まれる Microsoft Office または Visual Studio インスタンスに関連付けられたユーザーの数に基づいて、月額サブスクリプションを通じて請求します。これらのユーザーあたりの料金は暦月ごとに請求され、請求は製品をサブスクライブした時点から開始されます。既存の月にユーザーへのアクセスを削除すると、その月の残りの期間に対してユーザーに請求されます。翌月にユーザーの料金が発生しなくなります。

さらに、次のことを行います。

- 請求は、ユーザーサブスクリプション内のユーザーごとに基づきます。アクティブディレクトリ内のすべてのユーザーではなく、製品にサブスクライブしているユーザーのみが料金が発生します。
- 請求は、各暦月の最初の日から毎月のサイクルで行われます。料金は、サブスクリプションのアクティベーションの具体的な日付に関係なく、1 か月間にわたって課金されます。
- Office/VS インスタンスにアクセスする必要があるユーザーごとに RDS SAL が必要です。
- ユーザーベースのサブスクリプションに課金されないようにするには、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。Active Directory からユーザーを削除しても、インスタンスからのユーザーの関連付けは解除されません。詳細については、[「the section called “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。
- ユーザーは 1 回だけカウントされます。ユーザーが接続する EC2 インスタンスの数に関係なく、Microsoft Office と Visual Studio に対してユーザーごとに課金されます。ユーザーは、複数のインスタンスの使用に関係なく、サブスクリプションに対して 1 回課金されます。

非アクティブなマーケットプレイスサブスクリプションステータスのトラブルシューティング

必要な製品でディレクトリを設定したら、必要な製品をサブスクライブする必要があります。

[Marketplace のサブスクリプションステータス] が [非アクティブ] の製品では、ユーザーをインスタンスに関連付けて利用する前に、登録する必要があります。

インスタンスあたりのユーザー制限のトラブルシューティング

ユーザーあたり 25 個のインスタンスに制限があります。調整が必要な場合は、AWS サポートにお問い合わせください。ユーザーは、複数のインスタンスの使用に関係なく、サブスクリプションに対して 1 回課金されます。

RDS SAL への移行後に CAL トークンが供給されなかった場合のトラブルシューティング

独自の Microsoft RDS ライセンスサーバーを使用する場合、既に発行されたクライアントアクセスライセンス (CAL) トークンは、有効期限が切れるまで有効です。この期間中、有効な CAL トークンを持つユーザーは RDS SAL 製品に自動的にサブスクライブされません。License Manager が設定されていても、新しいユーザーセッションは自動的に RDS SAL にサブスクライブされません。License Manager は、独自のライセンスサーバーによって発行された既存の CAL トークンを上書きしません。サービスマネージドライセンスサーバーは、既存の CAL トークンの有効期限が切れた後のみ、トークンの発行と新しいリクエストの処理を開始します。現在発行された CAL トークンの有効期限に達すると、新しいトークンリクエストはサービスマネージドライセンスサーバーによって処理され、ユーザーは必要に応じて RDS SAL 製品に自動的にサブスクライブされます。

ユーザーサブスクリプション製品を使用する EC2 インスタンスでシームレスなドメイン結合が機能しない

License Manager は、SSM を使用してこれらのインスタンスでドメイン結合を実行し、製品をサブスクライブしているユーザーのみに許可されたアクセスを許可する必要があります。その結果、シームレスなドメイン結合機能は非アクティブ化されます。

VPC エンドポイントがアカウントに作成された

License Manager は、リソースがアクティベーションサーバーに接続し、VPC を設定するときにコンプライアンスを維持するために必要な VPC エンドポイントを作成します。

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

VPC エンドポイントリソースを削除するには、次のアクションを実行する必要があります。

- すべてのユーザーとユーザーベースのサブスクリプションとの関連付けを解除します。詳細については、「[the section called “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 設定から設定されているディレクトリをすべて削除します。詳細については、「[the section called “Active Directory の登録解除”](#)」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すべてのインスタンスを終了します。詳細については、「[the section called “ライセンス込み AMI からインスタンスを起動する”](#)」を参照してください。

Managed Active Directory のユーザー名を変更する

ユーザー名を変更しても、関連するインスタンスへの RDP 機能には影響しません。関連付けられたユーザーは、更新された RDP へのログインの詳細をユーザーサブスクリプションインスタンスで使用する必要があります。

終了したインスタンスからユーザーの関連付けを解除する

ユーザーサブスクリプションインスタンスが終了するたびに、インスタンスに関連付けられているすべてのユーザーの関連付けが解除されます。ユーザーの関連付けを手動で解除する必要はありません。

Note

インスタンスが停止しても、ユーザーの関連付けは解除されません。

ユーザーサブスクリプションインスタンスに追加のソフトウェアをインストールする

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す。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、AWS Managed Microsoft AD ディレクトリにデフォルトで作成される管理者アカウントを使用して実行する必要があります。詳細については、「[管理ガイド](#)」の「[管理者アカウント](#)」を参照してください。Directory Service

管理者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、次のことを行う必要があります。

- 管理者アカウントをインスタンスが提供する製品に登録します。
- 管理者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、「[the section called “はじめに”](#)」を参照してください。

ユーザーサブスクリプションインスタンスの日本語言語パック

日本語パックのインストールは、ユーザーサブスクリプションインスタンスでサポートされています。

ユーザーサブスクリプションインスタンスのローカル管理者ユーザー

これらの Microsoft 製品への不正アクセスを防ぐために、ユーザーマネージド Active Directory ドメインのユーザーのみをユーザーサブスクリプションインスタンスに関連付けることができます。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ります。

ユーザーサブスクリプションインスタンスに RDP を実行できるユーザーの数

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、[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](#)で説明されているように、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。デフォルトでは、Windows では、Windows サーバーのすべてのエディションで、管理者接続を含め、いつでも最大 2 つのリモートデスクトップ接続が許可されます。2 人以上の同時ユーザーを使用するには、RDS Licensing サーバーを設定する必要があります。

Office および Visual Studio 製品のセルフマネージド AD のユーザー

セルフマネージドディレクトリにユーザーを関連付けるには、セルフマネージドディレクトリと AWS Managed Microsoft AD ディレクトリの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](#) Directory Service」を参照してください。

サポートされている Windows オペレーティングシステム

サポートされている Windows オペレーティングシステムプラットフォームの詳細については、「」を参照してください [the section called “サポートされているソフトウェアサブスクリプション”](#)。

Office および Visual Studio でサポートされているバージョン

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の詳細については、「」を参照してください [the section called “対応ソフトウェア”](#)。

古い Windows Server バージョンでのユーザーサブスクリプションの使用

Office LTSC Professional Plus または Microsoft Visual Studio をサポートする AMI からインスタンスを起動すると、起動はデフォルトで最新の Windows OS プラットフォームバージョンの AMI (Windows Server 2022 など) になります。以前の OS プラットフォームバージョンで を起動するには、次の手順に従います。

1. で AWS Marketplace コンソールを開きます <https://console.aws.amazon.com/marketplace>。
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には、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 や Visual Studio Enterprise などです。
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. このリストには、サポートされている Windows OS プラットフォームの最新の AMI 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。

アカウントまたはリージョン間で License Manager ユーザーサブスクリプションを使用する

これらのシナリオがサポートされています。

- アカウント間で License Manager ユーザーサブスクリプションを使用する
- 共有 Active Directory での License Manager ユーザーサブスクリプションの使用

これらのシナリオはサポートされていません。

- リージョン間で License Manager ユーザーサブスクリプションを使用する

AWS サポートに連絡するためのヒント

- AWS サポートに連絡するときは、終了したインスタンスと同じ設定のインスタンスを作成し、インスタンスの終了保護を有効にして、迅速な対応を行ってください。
- RDP 関連の問題については、これらの問題のデバッグに役立つ RDP 関連のログが必要になります。インターネットアクセスがある環境には、「AWSsupport-RunEC2RescueForWindowsTool」を使用してください。詳細については、[EC2Rescue for Windows Server](#) を参照してください。
- Office インスタンスを作業インスタンスとして使用し、元のインスタンスのボリュームのスナップショットから復元されたボリュームをマウントすることで、インターネットアクセスのない環境でもデータを収集できます。
- バックアップ AMIs からのインスタンス起動のトラブルシューティング: バックアップ AMI からインスタンスを起動する場合は、元のインスタンスを終了する必要があります。

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

を使用すると AWS License Manager、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。設定で AWS Organizations 定義した および AWS リージョンアカウントの Linux サブスクリプションの使用率を追跡できます。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、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 を使用して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。

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に含まれる AMIs

- Red Hat Enterprise Linux (RHEL)
- Red Hat Cloud Access プログラムによる RHEL Bring Your Own Subscription モデル (BYOS)
- SUSE Linux Enterprise Server

- Ubuntu Pro サブスクリプションに含まれる 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

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

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。これらの間隔で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の放出時に配信されます。この動作により、新しく起動した 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までに時間がかかる場合があります。

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の 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は AWS Organizations、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 Extended Lifecycle Support (RHEL 7 ELS) インスタンス: RHEL 7 ELS のサブスクリプション込み AMI からインスタンスを起動しても、インスタンスを Red Hat に登録し、使用権限を使用する必要があります。この場合、License Manager はサブスクリプションの重複を報告しますが、これが予想される動作です。

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 を使用して設定できます。AWS リージョン指定した の Linux サブスクリプションの検出を有効にすると、オプションで検出を のアカウントに拡張できます 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

デフォルトでは、アカウントごとに あたり最大 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。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アクティブ化する](#)
- [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. 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、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. Linux サブスクリプション検出を実行するソース AWS リージョンを選択します。
5. 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には AWS Organizations、リンク AWS Organizationsを選択します。このオプションは AWS Organizations 、 がアカウントに設定されている場合にのみ表示されます。
6. 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 AWS License Manager アクセス許可を付与するオプションを確認して確認します。
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アクティブ化する

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 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。

- RHSM サブスクリプション検出を設定する AWS アカウント 前に、 で 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。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 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 に連絡する方法の詳細については、Red Hat Customer Portal ナレッジベースの「[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 API オフライントークン、またはオフライントークンを含む AWS Secrets Manager シークレットを指定する必

必要があります。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 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. 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の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 (RHSM) 検出のアクティブ化チェックボックスをオンにします。Link RHSM アカウント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依存する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、License Manager がユーザーに代わって Secrets Manager で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 Subscription [Manager API トークンページで Red Hat オフラインアクセストークン](#)を生成できます。

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 検出をアクティブ化することで、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ための AWS License Manager サービスへのアクセスを許可することを確認します。
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、Linux サブスクリプションの検出を有効にするために選択した各 AWS リージョン 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。Linux サブスクリプションを以下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。
組織オフボード	組織全体をオフボーディングします。

UpdateServiceSettings API を呼び出してから GetServiceSettings API を呼び出すことで、Linux サブスクリプションの有効化の進捗状況を監視できます。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。
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

ステータス	ステータス理由	説明
		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

AWS License Manager 設定ページから 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。ただし、 の検出を有効にした場合

⚠ 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. 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 [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、[AWS License Manager 「」 および AWS Organizations 「」](#)を参照してください。

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すると 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、AWS License Manager コンソールのインスタンスセクションに移動します。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 - インスタンス AWS リージョン が存在する。

- AMI ID - インスタンスの起動に使用される AMI の ID。
- 使用オペレーション - インスタンスのオペレーション、および AMI に関連付けられている請求コード。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に使用される AMI に関連付けられている製品コード。詳細については、「[AMI 製品コード](#)」を参照してください。
- LastUpdatedTime - 最後の検出がインスタンスの詳細を更新した時刻。

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 AWS Organizations。

1. 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) 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 (CSV) としてエクスポートするには、[ビューを CSV にエクスポート] を選択します。

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. 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) このサブスクリプションを含むインスタンスのデータをカンマ区切り値ファイル (CSV) としてエクスポートするには、[ビューを CSV にエクスポート] を選択します。

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

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

サブスクリプション名	Amazon EC2 の使用オペレーション	AWS Marketplace 製品コード	サブスクリプションタイプ
Red Hat Enterprise Linux Server 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を含む
Red Hat Enterprise Linux with High Availability Add-on	RunInstances:1010	x	EC2 サブスクリプションを含む
Red Hat Enterprise Linux with SQL Server Standard および High Availability	RunInstances:1014	x	EC2 サブスクリプションを含む
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を含む
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014	x	EC2 サブスクリプションを含む
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210	x	EC2 サブスクリプションを含む
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110	x	EC2 サブスクリプションを含む
SUSE Linux Enterprise Server	RunInstances:000g	x	EC2 サブスクリプションを含む

サブスクリプション名	Amazon EC2 の使用オペレーション	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 Linux Enterprise Server with SAP	✗	✓	AWS Marketplace サブスクリプション
Ubuntu Pro	RunInstances:00g0	✓	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 使用オペレーションと AWS Marketplace 製品コードの両方があります。

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	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。 単位: カウント ディメンション: SubscriptionName : サブスクリプションの名前。 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。このタブには、License Manager コンソール内で選択したサブスクリプションの Amazon CloudWatch ダッシュボードが表示されます。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次の詳細を含むアラームセクションがあります。

- 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、定義された AWS リージョンとインスタンスタイプが含まれます。
- 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。

定義したデイメンションと条件を使用して CloudWatch アラームを作成し、サブスクリプションの現在の使用状況に基づいて追跡および警告することができます。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。

CloudWatch アラームの状態には以下のものがあります。

- 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。
- アラーム – メトリクスまたは式が、定義されているしきい値を超えています。

- データ不足 - アラームが開始されたか、メトリクスが利用可能でないか、またはメトリクスがアラームの状態を決定するためのデータが不足しています。

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. 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 アラームを変更するには

1. 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 アラームを削除するには

1. 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 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) は AWS License Manager を使用してソフトウェアライセンスを管理し、エンドユーザーに配布できます。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。ISV は、非対称 AWS KMS キーを所有し、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。
- Usage-based - API リクエスト数、トランザクション数、ストレージ容量など、使用状況に応じて特定の条件が設定されるライセンス。

License Manager でライセンスを作成し、IAM ID AWS または License Manager によって生成されたベアラートークンを使用して顧客に配布できます。AWS アカウントを持つ ISV のお客様は、ライセンス権限をそれぞれの組織の ID AWS に再配布できます。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 Manager 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。

制限付きエンタイトルメントをチェックアウトまたはチェックインするには、ISV アプリケーションで各制限されたキャパシティの量を指定する必要があります。無制限のエンタイトルメントの場合、ISV アプリケーションは、チェックアウトまたは再度チェックインする関連するエンタイトルメント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超えることができるかどうかを示すものです。License Manager は、ISV の使用状況と超過状況を追跡し、レポートします。

License Manager で販売者が発行したライセンスの使用

License Manager 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 Manager 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。CloudWatch Eventsを通じて、この時系列データを追跡できます。

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ためのアクセス許可が必要です。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "license-manager:CreateLicense",
        "license-manager:CreateLicenseVersion",
        "license-manager:ListLicenses",
        "license-manager:ListLicenseVersions",
        "license-manager:GetLicense",
        "license-manager>DeleteLicense",
        "license-manager:CheckoutLicense",
        "license-manager:CheckInLicense",
        "license-manager:ExtendLicenseConsumption",
        "license-manager:GetLicenseUsage",
        "license-manager:CreateGrant",
        "license-manager:CreateGrantVersion",
        "license-manager>DeleteGrant",
        "license-manager:GetGrant",
        "license-manager:ListDistributedGrants"
      ]
    }
  ]
}
```

```
    ],
    "Resource": "*"
  }
]
}
```

AWS アカウントを持たないお客様が、の外部で販売されたライセンスを使用できるように License Manager と統合する場合は AWS Marketplace、ソフトウェアアプリケーションが License Manager API を呼び出すことを可能にする IAM ロールを作成する必要があります。

を使用して のないお客様に一時的な認証情報を AWS マネジメントコンソール 配布する場合 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、「[AWS アカウントを持たない ISV 顧客の一時的な認証情報を取得する](#)」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、次の例に示すように、AWS IAM [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、トークン発行者アカウントとして置き換えられた独自の AWS アカウント ID を持つ次の例のようになります。

JSON

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

```

    }
  }
}

```

次に、[attach-role-policy](#) コマンドを使用して、AWSLicenseManagerConsumptionPolicy AWS 管理ポリシーを AWSLicenseManagerConsumptionRole ロールに追加します。

```

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

AWS マネジメントコンソール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、次の手順に従います。また、[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. 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] - 製品の 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 - ライセンスの AWS 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。

- AWS KMS キーの入力 - License Manager はこのキーを使用して発行者に署名して検証します。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] - ライセンス契約への URL。

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。

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

新しいライセンスを追加した後、AWS マネジメントコンソールを使用して AWS アカウントで顧客にライセンスを付与できます。受取人は、ライセンスを使用する前に許可に同意する必要があります。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 AWS アカウントを持っていない場合は、License Manager API を使用して、顧客が[ライセンスを消費](#)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. 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 – ライセンス受信者の AWS 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 AWS アカウントに配布できる場合は、Distribution を選択します。
 - ID または認証情報を使用せずに、オンプレミストークン生成が共有ライセンスを認証することを許可するを選択します。 AWS
 - 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 – ライセンス AWS リージョン の。
6. [Create grant(権限の作成)]を選択します。

AWS アカウントを持たない ISV 顧客の一時的な認証情報を取得する

AWS アカウントを持たないお客様は、AWS アカウントを持つお客様と同じ方法で使用権限を使用できます。AWS アカウントを持たないお客様の一時的な AWS 認証情報を取得するには、次の手順に従います。APIコールは、ホームリージョンで行う必要があります。

License Manager APIコールに使用する一時的な認証情報を取得するには

1. [CreateToken](#) APIアクションを呼び出して、JWTトークンとしてエンコードされたリフレッシュトークンを取得します。
2. [GetAccessToken](#) APIアクションを呼び出し、CreateToken前のステップで受けとったリフレッシュトークンを指定して、一時的なアクセストークンを受けとります。
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 AWS 認証情報を取得します。

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

1. [License Manager コンソール](#)から、AWS アカウントなしで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。
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。[チェックアウトライセンス](#)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] - ライセンスを作成する際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。同じ商品SKUが複数のISVにわたって存在する場合があります。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 : 1a2b3c4d2f5e69f440bae30eaec9570bb1f7358824f9dfa1aa5a0daExample

- [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) の ISVs は、顧客識別子を含めることで、顧客に代わってライセンスをチェックアウトすることができます。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。

AWS マネジメントコンソール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。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. 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。

License Managerの設定

AWS License Manager コンソールの設定セクションには、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ように設定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
- ライセンスアセットグループのライセンスアセット検出とルールセット設定

ライセンスアセットグループを使用している組織では、複数のリージョンとアカウントでクロス AWS リージョン検出と組織全体のライセンス管理に追加設定を使用できます。

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。管理者は、AWS CLI または から委任管理者を登録できます AWS マネジメントコンソール。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。

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](#)
 - [ライセンスアセットの検出とルールセットの設定](#)
 - [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. 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 [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。

ライセンスアセットの検出とルールセットの設定

ライセンスアセットグループを使用する組織の場合、ライセンスアセット検出とルールセットの設定を設定して、AWS Organizations 内の複数の AWS リージョンとアカウントでクロスリージョン検出と組織全体のライセンス管理を有効にすることができます。

ライセンスアセット検出設定には以下が含まれます。

- ソフトウェア検出のソースリージョンを選択する AWS リージョン検出設定
- 組織所有者の組織全体の検出設定

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、のアカウント AWS Organizations がリンクされているかどうか、アカウントの License Manager S3 バケット ARN、AWS Resource Access Manager 共有 ARN などの情報を確認できます。このセクションでは、AWS Organizations アカウントをリンクすることもできます。

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、AWS Organizations アカウントのリンクを選択します。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、のすべての機能を有効にします AWS Organizations。詳細については、「AWS Organizations ユーザーガイド」の「[組織内のすべての機能の有効化](#)」を参照してください。

この選択により、管理アカウントに AWS Resource Access Manager リソース共有も作成されるため、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、「[AWS Resource Access Manager ユーザーガイド](#)」を参照してください。

このオプションを無効にするには、[UpdateServiceSettings](#)APIを呼び出してください。

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オンにすると、AWS Organizationsのすべてのアカウントのライセンス使用状況を管理できます。

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 は自動的にリンクされ、すべてのアカウントでリソース検出を実行します。

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、次のものがが必要です:

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

Note

商用 AWS パーティションリージョン (aws) では Amazon Athena、ソフトウェアの使用を検出 AWS Glue するために 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する必要はありません。ただし、Amazon Athena aws-us-gov、aws-cn、aws-iso リージョンなどの他のパーティションでも と AWS Glue が必要です。

Simple Notification Service (SNS)

License Manager から通知とアラートを受信するように Amazon SNS 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 ARN を次の形式で指定します。

```
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 Linux サブスクリプション AWS アカウント で検索します。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を設定するには、次のアクションを使用できます。

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 で検出もアクティブ化している場合、License Manager はまず RHSM 登録済み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 (RHSM) のアクセスシークレットには影響しません。不要になった関連シークレットの AWS 請求料金を回避するには、AWS Secrets Manager 「ユーザーガイド」の「[AWS Secrets Manager シークレットの削除](#)」を参照してください。

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

必要に応じて、のアカウント全体でサブスクリプションデータを集約します 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た場合は、License Manager のアクセスを設定して、Red Hat Subscription Manager (RHSM) を通じて管理される RHEL サブスクリプションの追加データを取得できます。

RHSM サブスクリプション検出を設定するには、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 登録済み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 (RHSM) のアクセスシークレットには影響しません。不要になった関連シークレットの AWS 請求額を回避するには、AWS Secrets Manager 「ユーザーガイド」の「[AWS Secrets Manager シークレットの削除](#)」を参照してください。

RHSM 検出用の License Manager コンソールには、次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

Red Hat オフライントークン AWS Secrets Manager を含む の RHSM アクセスシークレットへのリンク。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 (RHSM) からサブスクリプションデータをリクエストします。

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、「[AWS Secrets Manager ユーザーガイド](#)」の「[AWS Secrets Manager シークレットの変更](#)」を参照してください。シークレット値を更新するには、「[AWS Secrets Manager シークレットの値を更新する](#)」を参照してください。

で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ために、License Manager のサービスにリンクされたロールポリシーでは、シークレットと関連する AWS KMS key に次のタグを割り当てる必要があります。

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

登録プロセス中に License Manager が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 キーに割り当てます。タグを追加するには、「[AWS Secrets Manager ユーザーガイド](#)」の「[AWS Secrets Manager シークレットの変更](#)」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 は 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、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 AWS Managed Microsoft AD、に加えて VPC を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。

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 の委任された管理者が組織内に 1 人います。

AWS CLI または SDKs を使用すると、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、「[Inviting an AWS account to join your organization](#)」および「[Enable trusted access with AWS Organizations](#)」を参照してください。

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

所有および実行している商用 Linux サブスクリプションと AWS リージョン アカウントの表示や管理などの管理タスクを実行できます AWS Organizations。Linux サブスクリプション向けの 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 インスタンスを表示できます。

[AWS License Manager コンソール](#)、[AWS CLI](#)、または [AWS SDK](#) を使用して、委任された管理者の登録および登録解除を行うことができます。

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

委任管理者は、AWS CLI または を使用して登録できます AWS マネジメントコンソール。

Console

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

1. 管理アカウントの管理者 AWS として にサインインします。
2. 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、次の AWS CLI コマンドを実行します。

```
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、次の AWS CLI コマンドを実行します。

```
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を解除するには、AWS CLI または を使用します AWS マネジメントコンソール。

Console

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

1. 管理アカウントの管理者 AWS として にサインインします。
2. 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. [を削除] 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、次の AWS CLI コマンドを実行します。

```
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、次の AWS CLI コマンドを実行します。

```
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 のモニタリング

Amazon CloudWatch AWS License Manager を使用して、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。CloudWatch は、raw データを収集して、それを読み取り可能なほぼリアルタイムのメトリクスに変換します。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 CloudWatch による License Manager のモニタリング](#)」を参照してください。

を使用して、によって、またはに代わって行われた API コールおよび関連イベントを AWS アカウント キャプチャできます 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 AWS、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、「[を使用した AWS License Manager API コールのログ記録 AWS CloudTrail](#)」を参照してください。

目次

- [Amazon CloudWatch による License Manager のモニタリング](#)
 - [Secrets Manager のメトリクスを監視するアラームを作成する](#)
- [を使用した AWS License Manager API コールのログ記録 AWS CloudTrail](#)
 - [CloudTrailのLicense Manager情報](#)
 - [ライセンスLicense Managerのログ・ ファイルエントリーについて](#)

Amazon CloudWatch による License Manager のモニタリング

Amazon CloudWatch 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。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 CloudWatch ユーザーガイド](#)」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	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。 単位: カウント ディメンション: SubscriptionName : サブスクリプションの名前。
AggregateRunningInstancesCount	現在の AWS リージョン内の AWS Organizations の全アカウントにわたって集計された実行中のインスタンスの総数。 単位: カウント ディメンション: SubscriptionName : サブスクリプションの名前。
TotalLicenseConfigurationUsageCount	使用可能なライセンス設定の総数。 単位: カウント ディメンション: - 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	この設定の使用済みライセンスの総数。 単位: カウント ディメンション: - LicenseConfigurationArn : ライセンス設定の ARN。 - LicenseConfigurationType : ライセンス設定のタイプ。
LicenseConfigurationUsagePercentage	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。

メトリクス	説明
	単位: パーセント デイメンション: - LicenseConfigurationArn : ライセンス設定の ARN。 - LicenseConfigurationType : ライセンス設定のタイプ。
InstanceCount	ライセンスアセットグループ内のインスタンスの数。 単位: カウント デイメンション: - LicenseAssetGroupArn : ライセンスアセットグループ ARN。 - LicensingModel : ライセンスモデル (LicenseIncluded または AWSMarketplace)。AWS マネージドルールセットを持つライセンスアセットグループでのみ使用できます。
InstanceConsumedLicenseCount	ライセンスアセットグループ内のインスタンスの消費されたライセンスの数。 単位: カウント デイメンション: - LicenseAssetGroupArn : ライセンスアセットグループ ARN。 - LicenseCountingType : ライセンスカウントタイプ (インスタンス、vCPU、ソケット、またはコア)。 - LicensingModel : ライセンスモデル (LicenseIncluded または AWSMarketplace)。AWS マネージドルールセットを持つライセンスアセットグループでのみ使用できます。

Secrets Manager のメトリクスを監視するアラームを作成する

メトリクスが変化し、アラームの状態が変わったときに Amazon Simple Notification Service (Amazon SNS) メッセージを送信する CloudWatch のアラームを作成することができます。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、持続している状態変化に対してのみアクションを呼び出します。CloudWatch のアラームは、メトリクスが特定の状態にあるだけではアクションを呼び出しません。アクションを呼び出すには、指定した期間継続している必要があります。詳細については、「[Amazon CloudWatch アラームを使用する](#)」を参照してください。

を使用した AWS License Manager API コールのログ記録 AWS CloudTrail

AWS License Manager は AWS CloudTrail、License Manager のユーザー、ロール、または のサービスによって実行されたアクションを記録する AWS サービスであると統合されています。CloudTrailはLicense Managerのすべての API コールをイベントとしてキャプチャーします。キャプチャーされた呼び出しには、License Manager・ コンソールの呼び出しと、License ManagerAPIオペレーションへのコード呼び出しが含まれます。追跡を作成すると、License Managerのイベントを含むCloudTrail・ イベントのAmazon S3バケットへの継続的な配信が有効になります。追跡を設定しない場合でも、CloudTrail・ コンソールのEvent history (イベント履歴)で最新のイベントを表示できます。CloudTrailで収集された情報を使用して、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特定できます。

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

トピック

- [CloudTrailのLicense Manager情報](#)
- [ライセンスLicense Managerのログ・ ファイルエントリについて](#)

CloudTrailのLicense Manager情報

CloudTrail は、アカウントの作成 AWS アカウント 時に 有効になります。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イベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。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、「[CloudTrail イベント履歴でのイベントの表示](#)」を参照してください。

License Manager のイベントなど AWS アカウント、 のイベントの継続的な記録については、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きに、証跡がすべての AWS リージョンに適用されま

す。証跡は、AWS パーティション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、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、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。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 がサポートされているサービスと統合](#)
- 「[CloudTrail の Amazon SNS 通知の設定](#)」
- [複数のリージョンから CloudTrail ログファイルを受け取る](#) および [複数のアカウントから CloudTrail ログファイルを受け取る](#)

すべての License Manager アクションは CloudTrail によってログに記録され、[AWS License Manager API リファレンス](#)に記載されています。たとえば、、、DeleteLicenseConfigurationアクションへの呼び出しを呼び出すListResourceInventoryとCreateLicenseConfiguration、CloudTrail ログファイルにエントリが生成されます。

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。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- 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 AWS サービスによって行われたかどうか。

詳細については、「[CloudTrail userIdentity エlement](#)」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

追跡は、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するように設定できるものです。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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。

以下の例は、DeleteLicenseConfiguration アクションを示す CloudTrail ログエントリです。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAIIF2U5EXAMPLEH5AP6",
    "arn": "arn:aws:iam::123456789012:user/Administrator",
    "accountId": "012345678901",
    "accessKeyId": "AKIDEXAMPLE",
    "userName": "Administrator"
  },
  "eventTime": "2019-02-15T06:48:37Z",
  "eventSource": "license-manager.amazonaws.com",
  "eventName": "DeleteLicenseConfiguration",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.83",
  "userAgent": "aws-cli/2.4.6 Python/3.8.8 Linux",
  "requestParameters": {
    "licenseConfigurationArn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-9ab477f4bEXAMPLE55f3ec08a5423f77"
  },
  "responseElements": null,
  "requestID": "3366df5f-4166-415f-9437-c38EXAMPLE48",
  "eventID": "6c2c949b-1a81-406a-a0d7-52EXAMPLE5bd",
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

License Manager のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS、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を活用できます。

セキュリティは、お客様と AWS お客様の間の責任共有です。[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 クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。AWS また、では、安全に使用できるサービスも提供しています。サードパーティーの監査者は、[AWS コンプライアンスプログラム](#)コンプライアンスプログラムの一環として、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。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、「[コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム](#)」を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。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。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように License Manager を設定する方法について説明します。また、License Manager リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- [License Manager でのデータ保護](#)
- [License Manager の Identity and Access Management](#)
- [License Manager のサービスにリンクされたロールの使用](#)
- [AWS License Manager の 管理ポリシー](#)
- [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

責任 AWS [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。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「AWS のサービス」のセキュリティ設定と管理タスクもユーザーの責任となります。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に関するよくある質問](#)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、AWS セキュリティブログに投稿された「[AWS 責任共有モデルおよび GDPR](#)」のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント、AWS IAM アイデンティティセンターまたは AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。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 AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「AWS CloudTrail ユーザーガイド」の[CloudTrail 証跡の使用](#)を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理された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。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、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を、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含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して License Manager AWS CLI または他の AWS のサービスを使用する場合も同様です。AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そ

のサーバーへのリクエストを検証できるように、認証情報を URL 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 で管理された暗号化キー (SSE-S3) を使用して設定されています。

License Manager の Identity and Access Management

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 では、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。IAM は追加料金なしでご利用いただけます。

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。ユーザーが License Manager のリソース管理できるようにするには、許可を明示的に付与する 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出来ます。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、特定の許可があり、アカウントで作成できるもう 1 つの IAM アイデンティティです。IAM ロールは、AWS アイデンティティ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アイデンティティであるという点で、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。その代わりに、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 ポリシーの構造

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、ユーザーはリソースおよび API オペレーションを使用するアクセス権がないため、リクエストはすべて拒否されます。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す。
- [Action]: アクション は、許可または拒否する特定の API 操作のことです。
- [リソース]: リソースはアクションの影響を受けます。一部の License Manager API オペレーションでは、オペレーションによって作成/変更できるリソースをポリシー内に含めることができます。ステートメント内でリソースを指定するには、Amazon リソースネーム (ARN) を使用する必要があります。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、IAMをサポートするすべて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。License Manager は、API オペレーションの名前に次のようなプレフィックスを付けます。

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

例えば、次のようになります。

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

使用可能な License Manager API の詳細については、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。たとえば、名前がListで始まるすべての License Manager API操作を次のように指定することができます。

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

すべてのLicense Manager API操作を指定するには、次のように*ワイルドカードを使用します。

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

License Manager を使用する ISV のポリシーの例

License Managerを使用してライセンスを配布するISV には、次の許可が必要です。

JSON

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

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、ユーザー、グループ、ロールにこれらの許可を付与する必要があります。

アクセスを提供するには、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。

- 以下のユーザーとグループ AWS IAM アイデンティティセンター:

アクセス許可セットを作成します。「AWS IAM アイデンティティセンター ユーザーガイド」の「[アクセス許可セットを作成する](#)」の手順に従ってください。

- IAM 内で、ID プロバイダーによって管理されているユーザー:

ID フェデレーションの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 [サードパーティー ID プロバイダー \(フェデレーション\) 用のロールを作成する](#) を参照してください。

- IAM ユーザー:

- ユーザーが担当できるロールを作成します。手順については IAM ユーザーガイド の [IAM ユーザーのロールの作成](#) を参照してください。
- (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します。詳細については IAM ユーザーガイド の [ユーザー \(コンソール\) へのアクセス権限の追加](#) 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の使用

AWS License Manager は AWS Identity and Access Management (IAM) [サービスにリンクされたロール](#)を使用します。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ユニークなタイプの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、サービスがユーザーに代わって他の AWS サービス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。

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 Manager の設定が簡単になります。License Manager 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 Manager のみがそのロールを引き受けることができます。定義される許可には、信頼ポリシーと許可ポリシーが含まれており、その許可ポリシーを他のIAM エンティティに添付することはできません。

サービスにリンクされたロールを削除するには、まずその関連リソースを削除します。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 Manager 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 Manager 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 Manager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により、License Manager はユーザーに代わって AWS リソースにアクセスしてライセンスを管理できます。

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](#)。サービスリンクロールの権限の設定の詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの権限](#)」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 Managerコンソールに初めてアクセスしたときにLicense Manager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、または IAM API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。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、「[IAMアカウントに新しいロールが表示される](#)」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。

サービスにリンクされたロールを作成するには

1. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. License Manager の使用開始を選択します
3. IAM アクセス許可 (one-time-setup) フォーム AWS License Manager で、必要なアクセス許可を付与するを選択し、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リンク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 で、IAM を使用してサービス `license-manager.amazonaws.com` 名で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場合、この同じプロセスを使用して、もう一度ロールを作成できます。

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の作成後は、さまざまなエンティティがロールを参照す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を必要とする機能やサービスが不要になった場合は、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、サービスリンク役割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には、最初に、そのロールで使用されているリソースをすべて削除する必要があります。つまり、関連付けられているインスタンスや AMI からセルフマネージドライセンスとの関連付けを解除してから、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 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. 自分が所有しているセルフマネージドライセンスを選択し、[関連する AMI] と [リソース] タブ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。

サービスリンク役割の手動による削除

IAM コンソール、AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerRole` サービスにリンクされたロール

を削除します。 [AWSServiceRoleForAWSLicenseManagerMasterAccountRole](#) と

[AWSLicenseManagerMemberAccountRole](#) も使用している場合は、まずそ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「サービスリンクロールの削除」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` を使用すると、License Manager は AWS リソースにアクセスして、ユーザーに代わって一元管理アカウントのライセンス管理アクションを管理できます。

`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`](#)。サービスリンクロールの権限の設定の詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの権限](#)」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と AWS マネジメントコンソール、License Manager によってサービスにリンクされたロールが作成されます。

Note

License Manager でクロスアカウントサポートを使用するには、を使用する必要があります
AWS Organizations。

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、または IAM API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。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、「[IAM アカウントに新しいロールが表示される](#)」を参照してください。

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. License Manager コンソールを開きます <https://console.aws.amazon.com/license-manager/>。
2. [Settings]、[Edit] を選択します。
3. AWS Organizations アカウントをリンクを選択します。
4. [Apply] (適用) を選択します。

IAM コンソールを使用して、License Manager - メンバーアカウント 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 で、IAM を使用してサービス名で `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場合、この同じプロセスを使用して、もう一度ロールを作成できます。

License Manager のサービスにリンクされたロールの編集

License Manager は、`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の作成後は、さまざまなエンティティがロールを参照す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を必要とする機能やサービスが不要になった場合は、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、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割の手動による削除

IAM コンソール AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerMasterAccountRole` サービスにリンクされた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「サービスリンクロールの削除」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アクションの AWS リソースにアクセスできます。

`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](#)。サービスリンクロールの権限の設定の詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの権限](#)」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。設定ページの License Manager コンソールで、管理アカウント AWS Organizations からとの統合を有効にできます。これを行うには、AWS CLI (を実行 `update-service-settings`) または AWS API (を呼び出す) を使用します `UpdateServiceSettings`。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、または AWS API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。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 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、「[IAMアカウントに新しいロールが表示される](#)」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. AWS Organizations 管理アカウントにログインします。
2. 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. AWS Organizations アカウントのリンクを選択します。
5. [Apply] (適用) を選択します。これにより、すべての子アカウントに ロール [AWSServiceRoleForAWSLicenseManagerRole](#) と [AWSServiceRoleForAWSLicenseManagerMemberAccountRole](#) が作成されます。

License Manager - Member account ユースケースでサービスリンクロールを作成するには、IAM コンソールも使用できます。または、AWS CLI または AWS API で、サービス名を使用して `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場合、この同じプロセスを使用して、もう一度ロールを作成できます。

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の作成後は、さまざまなエンティティがロールを参照す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を必要とする機能やサービスが不要になった場合は、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、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割の手動による削除

IAM コンソール、AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` サービスにリンクされた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「サービスリンクロールの削除」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、ユーザーベースのサブスクリプションを提供する AWS リソース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。

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 リソースを利用、AWS Systems Manager および管理し、Directory Service リソースを記述できます。

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](#)。サービスリンクロールの権限の設定の詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの権限](#)」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、または IAM API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。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。

サービスにリンクされたロールを作成するには

1. License Manager コンソールを開きます<https://console.aws.amazon.com/license-manager/>。
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. [作成] を選択します。これにより、ロールが作成されます。

License Manager - User-based subscriptions ユースケースでサービスリンクロールを作成するには、IAM コンソールも使用できます。または、AWS CLI または AWS API で、サービス名を使用して `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場合、この同じプロセスを使用して、もう一度ロールを作成できます。

License Manager のサービスにリンクされたロールの編集

License Manager は、`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の作成後は、さまざまなエンティティがロールを参照す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を必要とする機能やサービスが不要になった場合は、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、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割の手動による削除

IAM コンソール、AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService` サービスにリンクされた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「サービスリンクロールの削除」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、Linux サブスクリプションを提供する AWS リソース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。

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

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 リソースについて説明します。
- 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 AWS Secrets Manager にアクセスしてサブスクリプション情報を取得するために、`"LicenseManagerLinuxSubscriptions": "enabled"` からタグ付けされたシークレットを取得します。
- 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 マネージドポリシー](#):

[AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。サービスリンクロールの権限の設定の詳細については、「IAM ユーザーガイド」の「[サービスリンクロールの権限](#)」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、または IAM API を使用して AWS CLI、サービスにリンクされたロールを手動で作成することもできます。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。

サービスにリンクされたロールを作成するには

1. License Manager コンソールを開きます<https://console.aws.amazon.com/license-manager/>。
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. [作成] を選択します。これにより、ロールが作成されます。

License Manager - Linux subscriptions ユースケースでサービスリンクロールを作成するには、IAM コンソールも使用できます。または、AWS CLI または AWS API で、サービス名を使用して `license-manager-linux-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場合、この同じプロセスを使用して、もう一度ロールを作成できます。

License Manager のサービスにリンクされたロールの編集

License Manager

は、`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の作成後は、さまざまなエンティティがロールを参照す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を必要とする機能やサービスが不要になった場合は、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、サービスリンク役割をクリーンアップする必要があります。

サービスリンク役割の手動による削除

IAM コンソール AWS CLI、または AWS API を使用し

て、`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` サービスにリンクされた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。

AWS License Manager の 管理ポリシー

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。チームに必要な権限のみを提供する [IAM カスタマー マネージド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ターゲット範囲に含めており、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損なわれ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ジョブ関数の 管理ポリシー AWS をサポートしています。例えば、`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の読み取り専用アクセス許可 AWS を追加します。ジョブ機能のポリシーの一覧および詳細については、「IAM ユーザーガイド」の「[AWS のジョブ機能のマネージドポリシー](#)」を参照してください。

AWS 管理ポリシー: AWSLicenseManagerServiceRolePolicy

このポリシーは、AWSServiceRoleForAWSLicenseManagerRole という名前のサービスリンクロールにアタッチされ、License Manager がユーザーの代わりに API アクションを呼び出してライセンスを管理できるようにします。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
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-management.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceLicenseManagement
iam:CreateServiceLinkedRole	arn:aws:iam::*:role/aws-service-role/license-manager.member-account.amazonaws.com/AWSServiceRoleForAWSLicenseManagerMemberAccountRole
s3:GetBucketLocation	arn:aws:s3:::aws-license-manager-service-*
s3:ListBucket	arn:aws:s3:::aws-license-manager-service-*
s3:ListAllMyBuckets	*
s3:PutObject	arn:aws:s3:::aws-license-manager-service-*

Action	リソースARN
sns:Publish	arn:aws::sns:*:*:aws-license-manager-service-*
sns:ListTopics	*
ec2:DescribeInstances	*
ec2:DescribeImages	*
ec2:DescribeHosts	*
ssm:ListInventoryEntries	*
ssm:GetInventory	*
ssm:CreateAssociation	*
ssm:GetCommandInvocation	*
ssm:SendCommand	arn:aws:ec2:*:*:instance/*
ssm:SendCommand	arn:aws:ssm:*:*:managed-instance/*
ssm:SendCommand	arn:aws:ssm:*:*:document/AWSLicenseManager-*
organizations:ListAWSServiceAccessForOrganization	*
organizations:DescribeOrganization	*
organizations:ListDelegatedAdministrators	*
license-manager:GetServiceSettings	*

Action	リソースARN
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 マネジメントコンソール、「」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>*</code>
<code>iam:GetRole</code>	<code>*</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 マネジメントコンソール、「」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、`AWSServiceRoleForAWSLicenseManagerMemberAccountRole` という名前のサービスリンクロールにアタッチされ、License Manager がユーザーの代わりに設定された管理アカウントからライセンス管理のための API アクションを呼び出せるようにします。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 マネジメントコンソール、「」を参照してください [AWSLicenseManagerMemberAccountRolePolicy](#)。

AWS 管理ポリシー: AWSLicenseManagerConsumptionPolicy

AWSLicenseManagerConsumptionPolicyポリシーは IAM アイデンティティにアタッチできます。このポリシーは、ライセンスを消費するために必要なLicense Manager APIアクションへのアクセスを許可する権限を付与します。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確認するには、「AWS マネジメントコンソール」の「[AWSLicenseManagerConsumptionPolicy](#)」を参照してください。

AWS 管理ポリシー:

AWSLicenseManagerUserSubscriptionsServiceRolePolicy

このポリシーは、AWSServiceRoleForAWSLicenseManagerUserSubscriptionsService という名前のサービスリンクロールにアタッチされ、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のリソースを管理できるようにします。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	*
DS: 承認済みアプリケーションの詳細を取得	*

Action	リソースARN
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` で値が `UserSubscriptions` のインスタンスでのみ、`AWS-RunPowerShellScript` ドキュメントを使用して SSM 実行コマンドを実行できます。

でこのポリシーのアクセス許可を表示するには AWS マネジメントコンソール、「」を参照してください [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

AWS マネージドポリシー:

AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy

このポリシーは、`AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService` という名前のサービスリンクロールに添付され、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のリソースを管理できるようにします。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 マネジメントコンソール、「」を参照してください [AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy](#)。

License Manager の AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始してからの License Manager の AWS マネージドポリシーの更新に関する詳細を表示します。

変更	説明	日付
AWSLicenseManagerServiceRolePolicy - 既存ポリシーへの更新	License Manager は、AWS が管理する SSM ドキュメントを実行してインスタンスのライセンスアセットを検出するアクセス許可を追加しました。	2025 年 11 月 19 日
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の次のアクセス許可を追加しました。 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。	2024 年 11 月 7 日
AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy - 既存ポリシーへの更新	License Manager に、Bring Your Own License (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が追加されました。	2024 年 5 月 22 日

変更	説明	日付
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。	2022 年 12 月 21 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy – 既存ポリシーへの更新	License Manager が ec2:DescribeVpcPeeringConnections 権限を追加しました。	2022 年 11 月 28 日
AWSLicenseManagerUserSubscriptionsServiceRolePolicy - 新しいポリシー	License Manager が、AWSLicenseManagerUserSubscriptionsServiceRolePolicy 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。	2022 年 7 月 18 日

変更	説明	日付
AWSLicenseManagerMasterAccountRolePolicy – 既存ポリシーへの更新	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。	2022 年 6 月 27 日
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 <code>AWSLicenseManagerMasterAccountRolePolicy</code> 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

変更	説明	日付
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
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 は、AWS 管理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 ISV AWS Marketplace に代わって を通じて発行されたライセンスに暗号で署名できます。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 ISV AWS KMS key に属する非対称 を使用し、AWS Key Management Service () で保護されますAWS KMS。この顧客管理 CMK 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ペアで構成されます。ユーザーがライセンスを要求する

と、License ManagerはライセンスエンタイトルメントをリストアップしたJSONオブジェクトを生成し、このオブジェクトに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が離れることはありません AWS KMS。での非対称暗号化の詳細については 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は、AWS KMS [Sign](#)ライセンスの署名と検証時に および [Verify](#) API オペレーションを呼び出します。CMKがこれらの操作で使用されるためには、CMKのキー使用値が[SIGN_VERIFY](#)である必要があります。この種類のCMKは、暗号化や復号化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. AWS KMS コンソール、API、または SDK で、ライセンス管理者は非対称カスタマー管理 CMK を作成します。CMK には、署名と検証のキー使用があり、RSASSA-PSS SHA-256 署名アルゴリズムをサポートする必要があります。詳細については、「[非対称CMKの作成](#)」「[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 AWS KMS ARN または ID を含む消費設定を作成します。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。エンタイトルメントをリストアップしたJSONオブジェクトリストとともに、レスポンスの一部としてデジタル署名を返します。プレーンテキストJSONは次のようなものです。

```
{
  "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":"ABCDEFGHI"  
  }  
}
```

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 プログラムによるスコープ](#)」の「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ます。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 Reports in AWS Artifact](#)」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。を使用する際のコンプライアンス責任の詳細については AWS のサービス、[AWS 「セキュリティドキュメント」](#)を参照してください。

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を中心に構築されています。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。

AWS リージョンとアベイラビリティゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#)を参照してください。

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である AWS License Manager は、AWS グローバルネットワークセキュリティで保護されています。AWS セキュリティサービスと [ガインフラストラクチャ AWS](#) を保護する方法については、[AWS 「クラウドセキュリティ」](#)を参照してください。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して環境を AWS 設計するには、「Security Pillar AWS Well-Architected Framework」の「[Infrastructure Protection](#)」を参照してください。

AWS 公開された API コールを使用して、ネットワーク経由で License Manager にアクセスします。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)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

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

インターフェイス VPC エンドポイントを作成することで、仮想プライベートクラウド(VPC) と AWS License Manager APIの間にプライベート接続を確立できます。インターフェイスエンドポイントは、インターネットゲートウェイ[AWS PrivateLink](#)、NAT デバイス、VPN 接続、または Direct Connect 接続なしで License Manager API にプライベートにアクセスするために使用できるテクノロジーである [AWS PrivateLink](#) を利用しています。VPCのインスタンスは、License Managerとの通信にパブリックIP アドレスを必要としません。VPCと License Managerとの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、または複数の [Elastic Network Interface](#) によって表されます。

詳細については、「Amazon VPC ユーザーガイド」の「[インターフェイス VPC エンドポイント \(AWS PrivateLink\)](#)」を参照してください。

License Manager用のインターフェイスVPCエンドポイントの作成

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`

エンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名 (など) を使用して、License Managerに API リクエストを実行できます。例えば、`{license-manager.region.amazonaws.com}`。

詳細については、Amazon VPC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。

License Manager 用のVPCエンドポイントポリシーを作成する

License Managerへのアクセスをコントロールするために VPC エンドポイントにポリシーをアタッチすることができます。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 VPC 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。

License Manager のトラブルシューティング

以下の情報は、AWS License Managerを使用する際のトラブルシューティングに役立ちます。始める前に、お使いのLicense Managerのセットアップが[the section called “設定”](#)に記載された要件を満たしていることを確認してください。

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。

このエラーは、Athenaサービスが、AWS Glue Data CatalogではなくAthenaマネージドデータカタログを使用している場合に発生することがあります。アップグレード手順については、[「AWS Glue データカタログへのStep-by-Stepのアップグレード」](#)を参照してください。

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

組織のいずれかのメンバーアカウントにおい

て、AWSServiceRoleForAWSLicenseManagerMemberAccountRole サービスリンクロール (SLR) が削除され、セルフマネージドライセンスに関連付けられているメンバー所有リソースが存在する場合、管理アカウントは、該当するメンバーアカウントのリソースからライセンスの関連付けを解除できません。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、SLRを復元します。

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AMIの見かけ上の存続

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に関連付けられた AMI が Amazon EC2 を介して登録解除された場合、その AMI が License Manager のリソースインベントリに一時的に表示された後、消去されることがありました。

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。管理アカウントの AWS Glue コンソールLicenseManagerResourceSyncDataProcessJobTriggerで を編集することで、更新スクリプトの実行頻度を変更できます。

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。

AWS Organizations アカウントのリンクが失敗する

[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
License Asset Group のサポートを追加	License Manager は、License アセットグループを通じてライセンスアセットとソフトウェアの使用を検出するためのサポートを追加しました。これには、 の更新が含まれます AWS 管理ポリシー: AWSLicenseManagerServiceRolePolicy 。	2025 年 11 月 19 日
Microsoft Remote Desktop Services サブスクライバークセスライセンス (RDS SAL) 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 は、RDS 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。これには、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が含まれます。	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の次のアクセス許可を追加しました。 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。詳細については、 AWS 管理ポリシー: AWSLicenseManagerU	2024 年 11 月 7 日

変更	説明	日付
	serSubscriptionsServiceRolePolicy を参照してください。	
Red Hat Subscription Manager (RHSM) から BYOL 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 BYOL ライセンスのサブスクリプション情報を RHSM から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 AWSLicenseManagerLinuxSubscriptionsServiceRolePolicy 。	2024 年 7 月 10 日
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 EC2 上の Microsoft Office LTSC Professional Plus の Amazon 提供ライセンスを持つ Amazon マシンイメージ (AMIs) で Amazon EC2 2019 のサポートを追加しました。	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

変更	説明	日付
Ubuntu LTS サブスクリプションのライセンスタイプ変換	License Manager で、Ubuntu LTS インスタンスが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できるようにするサポートが追加されました。	2023 年 4 月 20 日
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

変更	説明	日付
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
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利用します。	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 提供されたライセンスと 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 AWS 、提供されたライセンスと Bring Your Own License Model (BYOL) の間でライセンスタイプを変更します。	2021年9月22日

変更	説明	日付
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
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 IDs。	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アソシエーションスコープ	セルフマネージドライセンスと AWS アカウントで共有されている AMI を関連付けます。	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 上での Oracle デプロイの追跡	Amazon RDS 上の 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 初期リリース	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。